Palchevska O., Malaniuk M., Ivanyshyn N.

TRANSLATION FOR SPECIFIC PURPOSES:

DIGITALIZATION AND CYBERSECURITY

TRANSLATION FOR SPECIFIC PURPOSES: DIGITALIZATION AND CYBERSECURITY

Навчальний посібник

Львів 2023

Укладачі: Пальчевська О. С., Маланюк М. С., Іванишин

Рецензенти:

Лотоцька Н.Я. – PhD, доцент кафедри прикладної інгвістики Національного університету «Львівська політехніка».

Ткачук Р.Л. – д. тех. наук, професор, начальник кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності.

Рекомендовано до друку Вченою радою Навчально-наукового інституту психології та соціального захисту

Протокол № 1 від 21 вересня 2023 року

Рекомендовано до друку Вченою радою ЛДУ БЖД

Протокол №3 від 15 листопада 2023 р.

Навчальний посібник адресовано студентам, які вивчають галузевий переклад у сфері ІТ та кібербезпеки з англійської мови як першої іноземної. Мета посібника – формування у студентів перекладацької компетенції, а саме спеціальної складової її прагматичної частини, що передбачає знання, вміння та навики, які необхідні перекладачу при перекладі текстів у сфері інформаційних технологій та кібербезпеки. Посібник містить необхідний практичний матеріал, що ґрунтується на теоретичних положеннях, які студенти опановують протягом вивчення курсів “Вступ до перекладознавства”, “Теорія та практика перекладу”.

Foreword

Today, the model of higher education in the field of philology and translation is being implemented with due regard for modern social realities and the need for highly qualified translators, recognising the leading role of language for successful intercultural communication and Ukraine's integration into the world. To ensure that students have a thorough knowledge of linguistics and translation, the dynamics and current trends in translation practices, it is intended to acquire both theoretical and practical skills in specialized translation.

The Translation for Specific Purposes: Digitalization and Cybersecurity textbook integrates various teaching materials that will help in the training of translators in the field of cybersecurity. The textbook contains 25 chapters. They cover the main principles of digitalization and cybersecurity at the international, regional and national levels. The textbook also discusses the problematic issues of digitalization and cybersecurity at each level and ways to solve them. Particular attention is paid to emerging cyber security threats and the system of cyber actions.

The textbook has been compiled in accordance with the new educational and professional programmes for translators. It is the basis for developing various aspects of translation competence. When translating a text in the digitalization and cybersecurity field, a whole range of different tasks has to be solved. The texts in this manual are selected with regard to lexical and grammatical features, richness of terms and special vocabulary. The purpose of the manual is to form and build skills in translation and interpretation from English into Ukrainian to create an active lexicon of minimum cybersecurity terminology.

Achievement of this goal ensures the formation of basic knowledge of the translator in the field of cybersecurity. After successfully mastering the material presented, students will gain knowledge of the peculiarities and specifics of the purpose of digitalization and cybersecurity texts; the basic conceptual apparatus of such texts; provisions on the semantic and structural features of digitalization and cybersecurity terminology; peculiarities of the stages of translation and editing of technical texts in the digitalization and cybersecurity fields. The materials for

translation included in the manual are selected from authentic legislative, educational, reference and informative materials (conventions, standards, regulations, guidelines, dictionaries, reference books, encyclopedias, textbooks, Internet sources) in the fields of digitalization and cybersecurity.

CONTENTS

UNIT 1. 7
UNIT 2. 14
UNIT 3. 19
UNIT 4 26
UNIT 5 32
UNIT 6. 37
UNIT 7 41
UNIT 8 46
UNIT 9 51
UNIT 10 56
UNIT 11 62
UNIT 12 68
UNIT 13 73
UNIT 14 79
UNIT 15 84
UNIT 16 91
UNIT 17 95
UNIT 18 104
UNIT 19 109
UNIT 20 116
UNIT 21 122
UNIT 22 128
UNIT 23 136
UNIT 24 143
UNIT 25 148

UNIT 1.
Task I.

Read the texts. Translate each instance into Ukrainian.

Text 1.

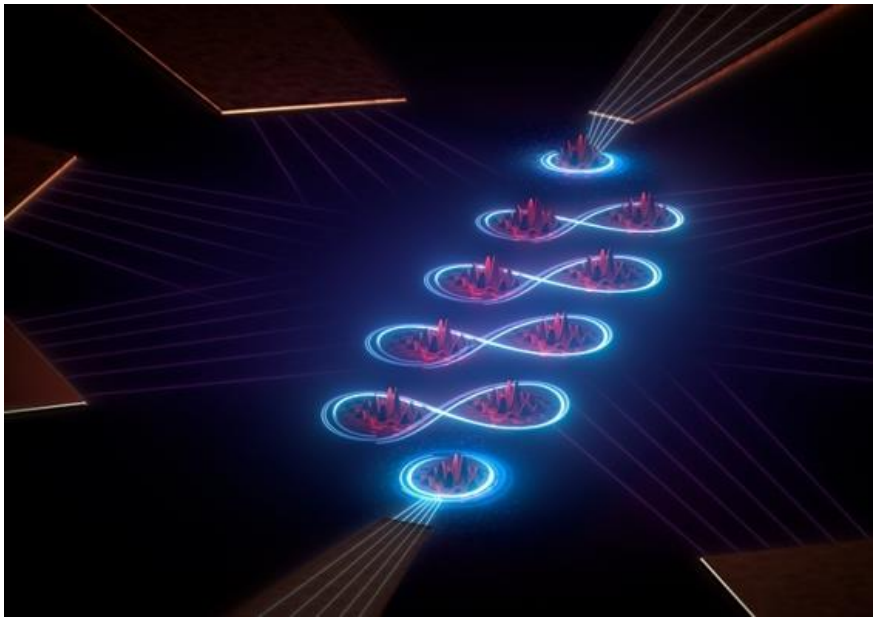
Modelling the carbon chain

Quantum computing hardware specialists at UNSW have built a quantum process. A team of quantum computer physicists at UNSW Sydney have engineered a quantum processor at the atomic scale to simulate the behaviour of a small organic molecule, solving a challenge set some 60 years ago by theoretical physicist Richard Feynman.

The achievement, which occurred two years ahead of schedule, represents a major milestone in the race to build the world's first quantum computer, and demonstrates the team's ability to control the quantum states of electrons and atoms in silicon at an exquisite level not achieved before.

In a paper published today in the journal *Nature*, the researchers described how they were able to mimic the structure and energy states of the organic compound polyacetylene – a repeating chain of carbon and hydrogen atoms distinguished by alternating single and double bonds of carbon.

Lead researcher and former Australian of the Year, Scientia Professor Michelle Simmons, said the team at Silicon Quantum Computing, one of UNSW's most exciting start-ups, built a quantum integrated circuit comprising a chain of 10 quantum dots to simulate the precise location of atoms in the polyacetylene chain.



An artist's impression of inside the quantum integrated circuit modeling the carbon chain. The simulated carbon atoms are in red, while the blue depicts electrons exchanged between them. Image: SQC

“If you go back to the 1950s, Richard Feynman said you can't understand how nature works unless you can build matter at the same length scale,” Prof. Simmons said.

“And so that’s what we're doing, we're literally building it from the bottom up, where we are mimicking the polyacetylene molecule by putting atoms in silicon with the exact distances that represent the single and double carbon-carbon bonds.”

Text 2.

Chain reaction

The research relied on measuring the electric current through a deliberately engineered 10-quantum dot replica of the polyacetylene molecule as each new electron passed from the source outlet of the device to the drain – the other end of the circuit.

To be doubly sure, they simulated two different strands of the polymer chains.

In the first device they cut a snippet of the chain to leave double bonds at the end giving 10 peaks in the current. In the second device they cut a different snippet of the chain to leave single bonds at the end only giving rise to two peaks in the current. The current that passes through each chain was therefore dramatically different due to the different bond lengths of the atoms at the end of the chain.

Not only did the measurements match the theoretical predictions, they matched perfectly.

'We should have some kind of commercial outcome from our technology five years from now.' - Michelle Simmons

“What it's showing is that you can literally mimic what actually happens in the real molecule. And that's why it's exciting because the signatures of the two chains are very different,” Prof. Simmons said.

“Most of the other quantum computing architectures out there haven't got the ability to engineer atoms with sub-nanometer precision or allow the atoms to sit that close.

“And so that means that now we can start to understand more and more complicated molecules based on putting the atoms in place as if they're mimicking the real physical system.”

Text 3.

Standing at the edge

According to Prof. Simmons, it was no accident that a carbon chain of 10 atoms was chosen because that sits within the size limit of what a classical computer is able to compute, with up to 1024 separate interactions of electrons in that system. Increasing it to a 20-dot chain would see the number of possible interactions rise exponentially, making it difficult for a classical computer to solve.

“We're near the limit of what classical computers can do, so it's like stepping off the edge into the unknown,” she says.

“And this is the thing that’s exciting, we can now make bigger devices that are beyond what a classical computer can model. So we can look at molecules that haven't been simulated before. We're going to be able to understand the world in a different way, addressing fundamental questions that we've never been able to solve before.”

One of the questions Prof. Simmons alluded to is about understanding and mimicking photosynthesis – how plants use light to create chemical energy for

growth. Or understanding how to optimise the design of catalysts used for fertilisers, currently a high-energy, high-cost process.

“So there’re huge implications for fundamentally understanding how nature works,” she said.

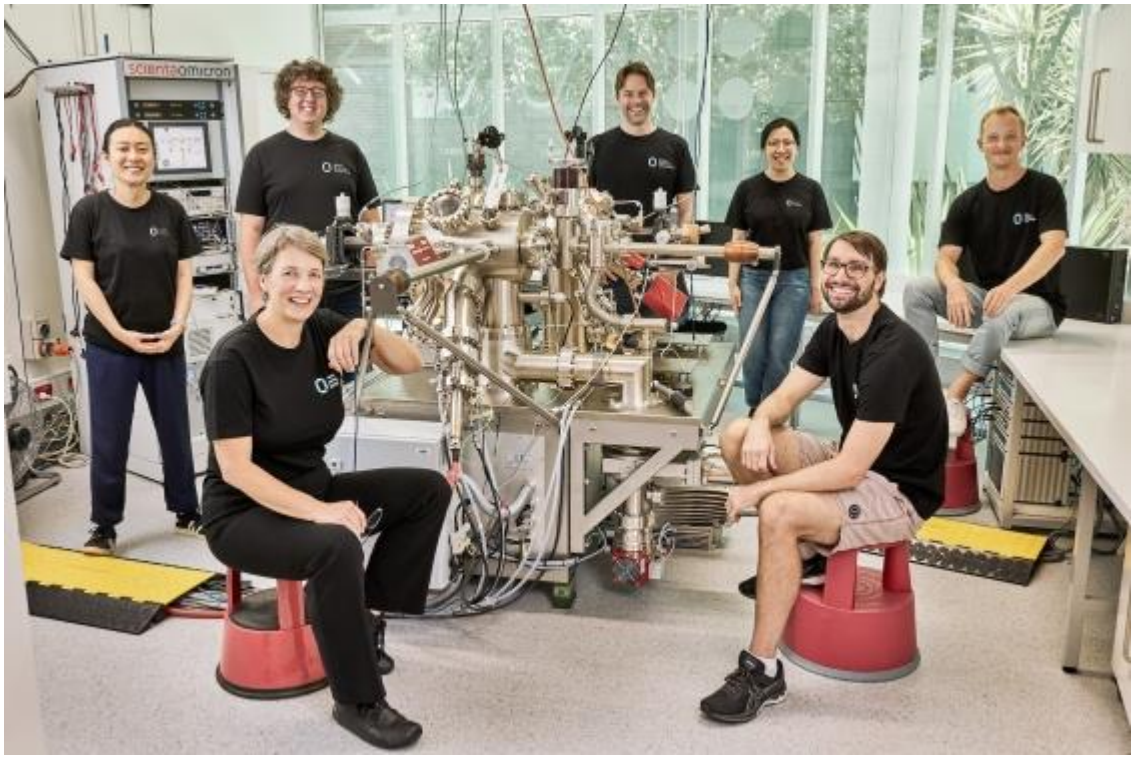
Text 4.

Future quantum computers

Much has been written about quantum computers in the last three decades with the billion-dollar question always being ‘but when can we see one?’.

Prof. Simmons says that the development of quantum computers is on a comparable trajectory to how classical computers evolved – from a transistor in 1947 to an integrated circuit in 1958, and then small computing chips that went into commercial products like calculators approximately five years after that.

“And so we're now replicating that roadmap for quantum computers,” Prof. Simmons says.



The authors of the *Nature* paper in the Silicon Quantum Computing laboratory.

“We started with a single atom transistor in 2012. And this latest result, realised in 2021 is the equivalent of the atom-scale quantum integrated circuit, two years ahead of time. If we map it to the evolution of classical computing, we're predicting we should have some kind of commercial outcome from our technology five years from now.”

One of the advantages that the UNSW/SQC team’s research brings is that the technology is scalable because it manages to use fewer components in the circuit to control the qubits – the basic bits of quantum information.

“In quantum systems, you need something that creates the qubits, some kind of structure in the device that allows you to form the quantum state,” Prof. Simmons says.

“In our system, the atoms themselves create the qubits, requiring fewer elements in the circuits. We only needed six metallic gates to control the electrons in our 10-dot system – in other words, we have fewer gates than there are active device components. Whereas most quantum computing architectures need almost double the number or more of the control systems to move the electrons in the qubit architecture.”

Needing fewer components packed in tightly together minimises the amount of any interference with the quantum states, allowing devices to be scaled up to make more complex and powerful quantum systems.

“So that very low physical gate density is also very exciting for us, because it shows that we've got this nice clean system that we can manipulate, keeping coherence across long distances with minimal overhead in the gates. That's why it's valuable for scalable quantum computing.”

Looking ahead, Prof. Simmons and her colleagues will explore larger compounds that may have been predicted theoretically, but have never been simulated and fully understood before, such as high temperature superconductors.

or in silicon to simulate an organic molecule with astounding precision.

(https://newsroom.unsw.edu.au/news/science-tech/scientists-emulate-nature-quantum-leap-towards-computers-future)

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text 3 into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. powerful quantum system
2. physical gate density
3. atom-scale quantum integrated circuit
4. commercial outcome
5. qubit architecture

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. One of the questions Prof. Simmons alluded to is about understanding and mimicking photosynthesis – how plants use light to create chemical energy for growth. Or understanding how to optimise the design of catalysts used for fertilisers, currently a high-energy, high-cost process. “So there’re huge implications for fundamentally understanding how nature works,” she said.
2. The research relied on measuring the electric current through a deliberately engineered 10-quantum dot replica of the polyacetylene molecule as each new electron passed from the source outlet of the device to the drain – the other end of the circuit. To be doubly sure, they simulated two different strands of the polymer chains. In the first device they cut a snippet of the chain to leave double bonds at the end giving 10 peaks in the current. In the second device they cut a different snippet of the chain to leave single bonds at the end only giving rise to two peaks in the current. The current that passes through each chain was therefore dramatically different due to the different bond lengths of the atoms at the end of the chain.
3. Much has been written about quantum computers in the last three decades with the billion-dollar question always being ‘but when can we see one?’ Prof. Simmons says that the development of quantum computers is on a comparable trajectory to how classical computers evolved – from a transistor in 1947 to an integrated circuit in 1958, and then small computing chips that went into commercial products like calculators approximately five years after that.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 2.

Task I.

Read the text. Translate each instance into Ukrainian.

Tech Companies Want More Eyes in the Sky for Wildfire Season

As US fires have become more frequent and devastating, a cottage industry in fire detection technology has emerged.

A camera in the hills overlooking Cloverdale, California – one of seven pilot stations Pano AI has installed in Sonoma, Napa and Lake counties.

"Can you see that?" he asks, pointing to some rolling, foggy hills in rural Oregon. The footage was captured seven minutes before Nuñez opened up his browser. Barely perceptible on the screen is a rising plume of smoke.

"I would not have caught that," Nuñez said after hitting replay. "But the AI does." The artificial intelligence Nuñez is referring to comes from Pano AI, a California startup that makes high-definition cameras to detect, track and manage flames. As the manager of wildfire planning and analytics at Portland General

Electric, Nuñez is responsible for doing everything possible, as early as possible, to find and put out fires.

A cottage industry in fire detection technology has taken root, especially in the western US, as fires have become more frequent, larger and financially ruinous.

PGE so far has installed five Pano cameras, with plans to add 17 more across Oregon this summer. The hardware offers minute-by-minute snapshots of the surroundings. According to Sonia Kastner, the startup's founder and chief executive officer, Pano's software can distinguish benign clouds from troubling smoke. The artificial intelligence that makes that possible has become the main selling point. For firefighters, government agencies and utilities, spotting wildfires early is critical to limiting the damage.

"Minutes matter here," said Mark Miller, chief commercial officer for AEM, an environmental technology company owned by Union Park Capital. AEM sells weather stations and panoramic cameras for weather detection, along with satellite data. Like Pano, AEM says it relies on advanced AI that has learned to identify what a wildfire looks like and when it arrives.

False alarms do occur, but less than some might expect. Pano operates a call center where staff analyze the video footage before alerting local customers or authorities. Kastner said Pano's 32 active camera systems have spotted actual wildfires with 90% accuracy.

Cameras aren't particularly novel solutions. Marin County, north of San Francisco, installed a fleet of remote security cameras to replace volunteer fire lookouts in 2014, after a record drought. The county had to swap them out within four years because they couldn't properly distinguish smoke from fog. Now Marin uses a statewide camera system that multiple utilities finance.

Nuñez believes additional use cases for the devices will emerge. "From a safety and environmental risk perspective, it's probably one of the most important projects in our portfolio," he said. PGE has spent $4.5 million on Pano's systems so far.

Certainly, utilities and state governments are spending more to combat the problem. PGE has budgeted $32 million for wildfire operations this year. In 2021, the agency reported incremental costs of $45 million from wildfire responses, up threefold from the year before.

The sums are miniscule compared with what Pano and other consumer or enterprise tech companies can earn in revenue. (Pano declined to disclose that figure.) Pano's Kastner used to work on smart-home devices for Google's Nest. She founded the company in 2019, then recruited other alums from Google, Apple and Tesla.

The startup estimated that California would only need 1,800 of its cameras to have fully equipped statewide detection, if the money arrives. "We're a team that's used to shipping millions of products a month," said Kastner.

Pano also markets its cameras to private businesses, including a timber company in Australia, where the startup will install six cameras this summer. It is working with two resorts in Big Sky, Montana. AEM, according to Miller, has more than 6,500 customers, primarily in government; there are some prospective deals AEM is exploring with insurance companies.

Chris Martinelli, the fire captain for Marin County, has seen waves of demos from companies pitching AI for fire detection. "Some of them are really expensive," he said. He's mostly interested in adding the software to the county's existing cameras. And he's yet to see any product that helps with detection at night. For that, the AI tech might not offer any advantage. "It's not as beneficial as just getting a visual," he said.

(https://www.bloomberg.com/news/articles/2022-06-24/tech-companies-want-more-eyes-in-the-sky-for-wildfire-season).

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

Translate the following English terms:

1.financially ruinous

2. take our brief survey

3. installed a fleet

4. high-definition cameras

5. distinguish benign clouds

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of fire detection. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. “Can you see that?” he asks, pointing to some rolling, foggy hills in rural Oregon. The footage was captured seven minutes before Nuñez opened up his browser. Barely perceptible on the screen is a rising plume of smoke.

2. “Minutes matter here,” said Mark Miller, chief commercial officer for AEM, an environmental technology company owned by Union Park Capital. AEM sells weather stations and panoramic cameras for weather detection, along with satellite data. Like Pano, AEM says it relies on advanced AI that has learned to identify what a wildfire looks like and when it arrives.

3. The sums are miniscule compared with what Pano and other consumer or enterprise tech companies can earn in revenue. (Pano declined to disclose that figure.) Pano’s Kastner used to work on smart-home devices for Google’s Nest. She founded the company in 2019, then recruited other alums from Google, Apple and Tesla.

The startup estimated that California would only need 1,800 of its cameras to have fully equipped statewide detection, if the money arrives. “We’re a team that’s used to shipping millions of products a month,” said Kastner.

Task VI

Divide the text into 6 passages. Write sort headings for them.

UNIT 3.

Task I.

Read the text. Translate each instance into Ukrainian.

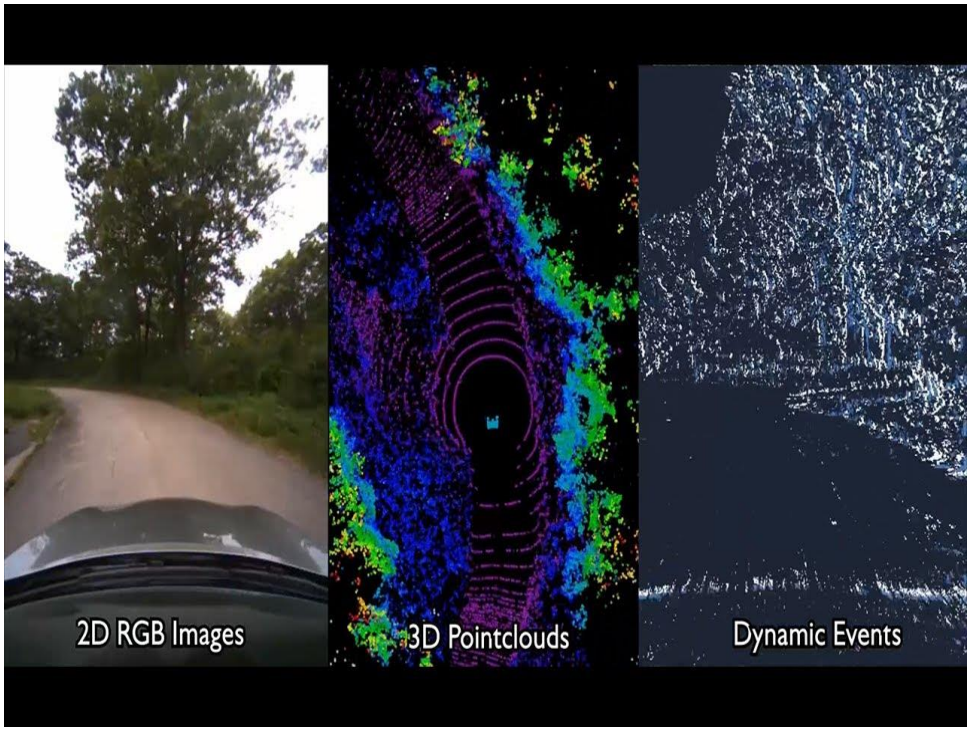
Researchers release open-source photorealistic simulator for autonomous driving

MIT scientists unveil the first open-source simulation engine capable of constructing realistic environments for deployable training and testing of autonomous vehicles.

Hyper-realistic virtual worlds have been heralded as the best driving schools for autonomous vehicles (AVs), since they've proven fruitful test beds for safely trying out dangerous driving scenarios. Tesla, Waymo, and other self-driving companies all rely heavily on data to enable expensive and proprietary photorealistic simulators, since testing and gathering nuanced I-almost-crashed data usually isn't the most easy or desirable to recreate.

To that end, scientists from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) created "VISTA 2.0," a data-driven simulation engine where vehicles can learn to drive in the real world and recover from near-crash scenarios. What's more, all of the code is being open-sourced to the public.

"Today, only companies have software like the type of simulation environments and capabilities of VISTA 2.0, and this software is proprietary. With this release, the research community will have access to a powerful new tool for accelerating the research and development of adaptive robust control for autonomous driving," says MIT Professor and CSAIL Director Daniela Rus, senior author on a paper about the research.



VISTA is a data-driven, photorealistic simulator for autonomous driving. It can simulate not just live video but LiDAR data and event cameras, and also incorporate other simulated vehicles to model complex driving situations. VISTA is open source and the code can be found below.

VISTA 2.0 builds off of the team's previous model, VISTA, and it's fundamentally different from existing AV simulators since it's data-driven — meaning it was built and photorealistically rendered from real-world data — thereby enabling direct transfer to reality. While the initial iteration supported only single car lane-following with one camera sensor, achieving high-fidelity data-driven simulation required rethinking the foundations of how different sensors and behavioral interactions can be synthesized.

Enter VISTA 2.0: a data-driven system that can simulate complex sensor types and massively interactive scenarios and intersections at scale. With much less data than previous models, the team was able to train autonomous vehicles that could be substantially more robust than those trained on large amounts of real-world data.

"This is a massive jump in capabilities of data-driven simulation for autonomous vehicles, as well as the increase of scale and ability to handle greater driving complexity," says Alexander Amini, CSAIL PhD student and co-lead author on two new papers, together with fellow PhD student Tsun-Hsuan Wang. "VISTA

2.0 demonstrates the ability to simulate sensor data far beyond 2D RGB cameras, but also extremely high dimensional 3D lidars with millions of points, irregularly timed event-based cameras, and even interactive and dynamic scenarios with other vehicles as well."

The team was able to scale the complexity of the interactive driving tasks for things like overtaking, following, and negotiating, including multiagent scenarios in highly photorealistic environments.

Training AI models for autonomous vehicles involves hard-to-secure fodder of different varieties of edge cases and strange, dangerous scenarios, because most of our data (thankfully) is just run-of-the-mill, day-to-day driving. Logically, we can't just crash into other cars just to teach a neural network how to not crash into other cars.

Recently, there's been a shift away from more classic, human-designed simulation environments to those built up from real-world data. The latter have immense photorealism, but the former can easily model virtual cameras and lidars. With this paradigm shift, a key question has emerged: Can the richness and complexity of all of the sensors that autonomous vehicles need, such as lidar and event-based cameras that are more sparse, accurately be synthesized?

Lidar sensor data is much harder to interpret in a data-driven world – you're effectively trying to generate brand-new 3D point clouds with millions of points, only from sparse views of the world. To synthesize 3D lidar point clouds, the team used the data that the car collected, projected it into a 3D space coming from the lidar data, and then let a new virtual vehicle drive around locally from where that original vehicle was. Finally, they projected all of that sensory information back into the frame of view of this new virtual vehicle, with the help of neural networks.

Together with the simulation of event-based cameras, which operate at speeds greater than thousands of events per second, the simulator was capable of not only simulating this multimodal information, but also doing so all in real time – making it possible to train neural nets offline, but also test online on the car in augmented reality setups for safe evaluations. "The question of if multisensor simulation at this

scale of complexity and photorealism was possible in the realm of data-driven simulation was very much an open question," says Amini.

With that, the driving school becomes a party. In the simulation, you can move around, have different types of controllers, simulate different types of events, create interactive scenarios, and just drop in brand new vehicles that weren't even in the original data. They tested for lane following, lane turning, car following, and more dicey scenarios like static and dynamic overtaking (seeing obstacles and moving around so you don't collide). With the multi-agency, both real and simulated agents interact, and new agents can be dropped into the scene and controlled any which way. Taking their full-scale car out into the "wild" – a.k.a. Devens, Massachusetts – the team saw immediate transferability of results, with both failures and successes. They were also able to demonstrate the bodacious, magic word of self-driving car models: "robust." They showed that AVs, trained entirely in VISTA 2.0, were so robust in the real world that they could handle that elusive tail of challenging failures.

Now, one guardrail humans rely on that can't yet be simulated is human emotion. It's the friendly wave, nod, or blinker switch of acknowledgement, which are the type of nuances the team wants to implement in future work.

"The central algorithm of this research is how we can take a dataset and build a completely synthetic world for learning and autonomy," says Amini. "It's a platform that I believe one day could extend in many different axes across robotics. Not just autonomous driving, but many areas that rely on vision and complex behaviors. We're excited to release VISTA 2.0 to help enable the community to collect their own datasets and convert them into virtual worlds where they can directly simulate their own virtual autonomous vehicles, drive around these virtual terrains, train autonomous vehicles in these worlds, and then can directly transfer them to full-sized, real self-driving cars."

Amini and Wang wrote the paper alongside Zhijian Liu, MIT CSAIL PhD student; Igor Gilitschenski, assistant professor in computer science at the University of Toronto; Wilko Schwarting, AI research scientist and MIT CSAIL PhD '20; Song Han, associate professor at MIT's Department of Electrical Engineering and

Computer Science; Sertac Karaman, associate professor of aeronautics and astronautics at MIT; and Daniela Rus, MIT professor and CSAIL director. The researchers presented the work at the IEEE International Conference on Robotics and Automation (ICRA) in Philadelphia.

This work was supported by the National Science Foundation and Toyota Research Institute. The team acknowledges the support of NVIDIA with the donation of the Drive AGX Pegasus.

(https://news.mit.edu/2022/researchers-release-open-source-photorealistic-simulator-autonomous-driving-0621).

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

Translate the following English terms:

1. vehicles
2. adaptive robust control
3. near-crash scenarios
4. behavioral interactions
5. dynamic overtaking

➤*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of autonomous driving. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. VISTA 2.0 builds off of the team's previous model, VISTA, and it's fundamentally different from existing AV simulators since it's data-driven — meaning it was built and photorealistically rendered from real-world data — thereby enabling direct transfer to reality. While the initial iteration supported only single car lane-following with one camera sensor, achieving high-fidelity data-driven simulation required rethinking the foundations of how different sensors and behavioral interactions can be synthesized.

2. "This is a massive jump in capabilities of data-driven simulation for autonomous vehicles, as well as the increase of scale and ability to handle greater driving complexity," says Alexander Amini, CSAIL PhD student and co-lead author on two new papers, together with fellow PhD student Tsun-Hsuan Wang. "VISTA 2.0 demonstrates the ability to simulate sensor data far beyond 2D RGB cameras, but also extremely high dimensional 3D lidars with millions of points, irregularly timed event-based cameras, and even interactive and dynamic scenarios with other vehicles as well."

3. “The central algorithm of this research is how we can take a dataset and build a completely synthetic world for learning and autonomy," says Amini. "It’s a platform that I believe one day could extend in many different axes across robotics. Not just autonomous driving, but many areas that rely on vision and complex behaviors. We're excited to release VISTA 2.0 to help enable the community to collect their own datasets and convert them into virtual worlds where they can directly simulate their own virtual autonomous vehicles, drive around these virtual terrains, train autonomous vehicles in these worlds, and then can directly transfer them to full-sized, real self-driving cars.”

Task VI

Divide the text into 6 passages. Write sort headings for them.

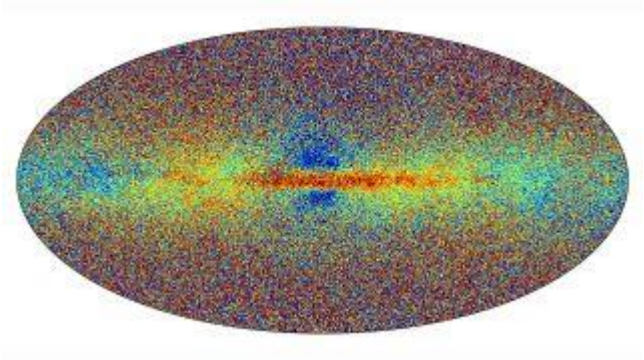
UNIT 4

Task I. *Read the texts. Translate each instance into Ukrainian.*

Text 1.

Untangling the Milky Way's evolution through big-data astronomy

The Gaia database currently contains 1 petabyte of data, which is equivalent to the data capacity of 200,000 DVDs.



A map revealing the distribution of metals in our galaxy, the Milky Way. Metal content varies across generations of stars. (Image credit: ESA/Gaia/DPAC)

Untangling the evolution of our home galaxy, the Milky Way, is a challenge similar to mapping the human genome, according to the European Space Agency (ESA). ESA's galaxy mapper, Gaia, takes trillions of measurements of 2 billion of the brightest stars in the sky. Here, we look at what it takes to unpick those measurements to reveal the galaxy's secrets.

On June 13, the Gaia Data Processing and Analysis Consortium (DPAC), a collaboration of 450 European astronomers and engineers supporting the galaxy-mapping endeavor, released what DPAC chair Anthony Brown described as "the richest set of astronomical data ever published."

To create the 10-terabyte catalog of compressed data, DPAC computers had to ingest 940 billion observations of 2 billion of the brightest light sources in the sky, Brown, an astronomer at Leiden University in the Netherlands, said at an ESA news conference on June 13.

The data, captured by Gaia between June 2014 and June 2017, contained information about 1.5 billion stars' precise positions and motions in the sky; details about the ages, temperatures and brightness levels of about half a billion of those stars; and detailed chemical compositions of several million of them.

It took five years for the data to pass through the sophisticated computational pipeline of validation, calibration and analysis procedures, which involve six supercomputing centers in six European countries. It would take a thousand years for a single (and rather powerful) personal computer to process the data set, Gonzalo Gracia, DPAC project coordinator for data processing, told Space.com.

As of 2022, the main Gaia database contains 1 petabyte of data, Gracia added, which is equivalent to the data capacity of 200,000 DVDs. To date, the telescope has made over 100 measurements of every single one of the 2 billion light sources it sees.

"Every day, Gaia sends us between 20 and 100 gigabytes of data," Gracia said. "That might not seem like that much if you compare it to the bandwidth you have at home, but we are talking about a satellite that is 1.5 million kilometers [930,000 miles] away from Earth."

The Gaia telescope observes 2 billion of the brightest stars in our home galaxy, the Milky Way. (Image credit: ESA/ATG medialab; background: ESO/S. Brunier, CC BY-NC)

Text 2.

The journey of the data

From Gaia's vantage point at Lagrange Point 2, a stable point in the sun-Earth system where the gravitational pulls of the two bodies are in balance, the spacecraft observes the cosmos while shielded from the sun's glare.

Three ESA deep-space antennas (one each near Madrid; Malargüe, Argentina; and New Norcia, Australia) receive the data collected by the space probe's two telescopes and other instruments. From those ground stations, the measurements

travel on conventional internet lines to the European Space Operations Centre in Darmstadt, Germany, for basic checks, before the data are sent to the agency's Science Operations Center in Madrid.

"This is when we do the first round of processing," Gracia said. "We do some initial calibrations and run the data through a piece of software to assess the health of the satellite. This happens in the first hours after the data is received."

Then, things start to get complicated. A data-processing center at CNES, the French space agency, in Toulouse scans the data set for fast-moving objects in the solar system: asteroids and comets that might be on a collision course with Earth.

"They have a pipeline, which detects those objects and checks whether they are already known," Gracia said. "If they are not known, they raise an alarm with the solar system objects community in the world, who can do the follow-up observation and find what the object is about and what is its trajectory."

Gaia is quite efficient in monitoring asteroids and might even be able to see some that are not visible from Earth. The mission's June 13 data release contained information about detailed trajectories of 60,000 solar system space rocks. On top of that, Gaia measured light spectra of these space rocks, revealing their chemical compositions. Previously, astronomers knew detailed chemical compositions of only 4,500 asteroids.

Separately, a team in Cambridge, England, compares new brightness measurements delivered by Gaia with data acquired earlier. Significant changes in brightness levels of stars are always a reason for excitement, as they might indicate supernovas, explosions that occur when massive stars die before collapsing into black holes or neutron stars.

Sometimes, dim distant stars and galaxies can temporarily lighten up through microlensing, an odd phenomenon that happens when an extremely massive object comes between the dim star and the observer, its powerful light-bending gravity acting as a magnifying glass. Gaia, which completes a scan of the entire sky every two months, sees all that.

In the meantime, the rest of the consortium conducts what Gracia calls "cyclic processing": endless rounds of redigesting, validating and analyzing the data to extract the most accurate information that astronomers can use to create precise maps of the Milky Way galaxy and model its life into the past and future. Several thousand servers running tens of thousands of core processors are involved in the operation.

"We have to process the data several times," Gracia said. "We process it, we give it to the scientists for checks, and then we have to tune our calibrations, our algorithms; we have to improve them every time."

The data sets are also dependent on each other. For example, without information about precise positions of the observed objects, the data on brightness changes or movements of asteroids would be worthless.

"We essentially have the information about the amount of photons hitting the Gaia telescopes, and from their position in the window, we derive the positions in the sky," Gracia said. "This is done in Barcelona, where we produce this astrometric information for all the sources in the sky. This is the input for basically all the other processing that we do. It takes a lot of time to do all that and to do it with a sufficient amount of data to ensure that the data is really of the best quality."

This amount of processing is the reason behind the delay between the acquisition of the data and its release. Gaia launched in December 2013, but the astronomical community didn't get their hands on the first batch of data until September 2016. The second data release followed in April 2018. The June 13 data dump was preceded by a partial early release in December 2020. Each new catalog increases the precision of the data as well as the amount of available information about each of the 2 billion light sources the telescope sees. Although the mission is already in its ninth year, there is no stopping for the 450 researchers and engineers at DPAC.

While the world's Milky Way researchers are unpacking the gifts of the June 13 data release, looking for evidence of the galaxy's dynamic life, Gracia and his colleagues are already busy working on the next data dump, which promises, among other things, to unleash Gaia's potential to spot planets around faraway stars.

Thousands of new finds are expected to enrich the existing exoplanet catalog as the DPAC researchers train their algorithms to spot the characteristic mild dimming of a star caused by a planet crossing in front of its disk.

"We started processing data for the fourth cycle two years ago and are already planning the fifth cycle," Gracia said. "It's really nonstop."

https://www.space.com/untangling-milky-way-evolution-through-big-data-astronomy

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text 2 into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III. *Translate the following English terms:*

1. Neutron stars
2. Milky Way
3. Solar system
4. To create precise maps
5. The human genome

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. The data, captured by Gaia between June 2014 and June 2017, contained information about 1.5 billion stars' precise positions and motions in the sky; details about the ages, temperatures and brightness levels of about half a billion of those stars; and detailed chemical compositions of several million of them.
2. Then, things start to get complicated. A data-processing center at CNES, the French space agency, in Toulouse scans the data set for fast-moving objects in the solar system: asteroids and comets that might be on a collision course with Earth.
3. While the world's Milky Way researchers are unpacking the gifts of the June 13 data release, looking for evidence of the galaxy's dynamic life, Gracia and his colleagues are already busy working on the next data dump, which promises, among other things, to unleash Gaia's potential to spot planets around faraway stars. Thousands of new finds are expected to enrich the existing exoplanet catalog as the DPAC researchers train their algorithms to spot the characteristic mild dimming of a star caused by a planet crossing in front of its disk.

Task VI.

Divide the text into 6 passages. Wright sort headings for them.

UNIT 5

Task I. *Read the text. Translate each instance into Ukrainian.*

Brain-Computer Interface Startup Implants First Device in US Patient

On July 6 a doctor at the Mount Sinai West medical center in New York threaded a 1.5-inch-long implant made up of wires and electrodes into a blood vessel in the brain of a patient with ALS, or amyotrophic lateral sclerosis. The hope is that the patient, who's lost the ability to move and speak, will be able to surf the web and communicate via email and text simply by thinking – the device will translate his thoughts into commands sent to a computer.

Synchron, the startup behind the technology, has already implanted its devices in four patients in Australia, who haven't experienced side effects and have been able to carry out such tasks as sending WhatsApp messages and making online purchases. The recent procedure was the first the company has done in the US, putting it ahead of competitors including Elon Musk's Neuralink Corp. "This surgery was special because of its implications and huge potential," says Dr. Shahram Majidi, the neurointerventional surgeon who performed it.

Founded in 2016, Synchron has caught the attention of the brain-computer interface (BCI) field because its device, known as the stentrode, can be inserted into the brain without cutting through a person's skull or damaging their tissue. A doctor makes an incision in the patient's neck and feeds the stentrode via a catheter through the jugular vein into a blood vessel nestled within the motor cortex. As the catheter is removed, the stentrode – a cylindrical, hollow wire mesh – opens up and begins to fuse with the outer edges of the vessel. According to Majidi, the process is very similar to implanting a coronary stent and takes just a few minutes.

A second procedure then connects the stentrode via a wire to a computing device implanted in the patient's chest. To do this, the surgeon must create a tunnel for the wire and a pocket for the device underneath the patient's skin, much like what's done to accommodate a pacemaker. The stentrode reads the signals when

neurons fire in the brain, and the computing device amplifies those signals and sends them out to a computer or smartphone via Bluetooth.

Although this may make some people squeamish, it's far less invasive than the current state-of-the-art technology, known as the Utah array, which requires doctors to cut the scalp and drill into the skull to place rigid needles in the brain. Those then attach to a lime-size device placed on top of a person's head.

The Utah array has allowed patients with severe disabilities to do remarkable things like command robotic arms to bring them a cup of water. But they generally use the devices only under supervision at a hospital, and the brain tends to form scar tissue around it, degrading the signals gathered by the electronics over time.

Neuralink has been working to develop a much smaller, more powerful implant that can be placed in the brain through a simplified surgical procedure aided by a robot. Still, it would also require the removal of a chunk of a patient's skull, and the company has yet to receive approval for human trials.

The US has more cautious policies around these types of procedures than Australia, and it took years of work for Synchron to receive a go-ahead from the Food and Drug Administration. The US patient is the first in a six-person, $10 million trial funded by the National Institutes of Health and led by Douglas Weber, a professor of mechanical engineering at Carnegie Mellon University, and David Putrino, the director of rehabilitation innovation at Mount Sinai.

The technology remains in its early stages of development, and the trial is meant to focus more on how the human body reacts to the implant and how clear the brain signals are than on the functions a person can perform with the device.

Tucked into the motor cortex, the stentrode uses 16 electrodes to monitor brain activity and record the firing of neurons when a person thinks. The signal strength improves over time, as the device fuses deeper into the blood vessel and gets closer to the neurons. Software is used to analyze the patterns of brain data and match them with the goal a person is trying to accomplish.

People in the BCI field have a long history of hyping technologies that end up with limitations preventing broad use. In light of that, the US patient requested

anonymity and declined to discuss the operation so as not to promote the Synchron device before experiencing its pros and cons.

The limited computing power of the stentrode means the device can't translate whole sentences. Rather, a patient with the implant picks letters one-by-one on a screen, and the technology converts those "yes or no" thoughts into commands.

Still, doctors and researchers think Synchron's technology could lead to major advances in the way people with severe disabilities go about their day-to-day lives. "One of the untold secrets of the brain-implant technologies trialed over the past two decades is that they have never, once, really translated into independent home use," says Putrino. Unlike people with Utah arrays, Synchron's Australian patients are using the devices in their own homes.

Dr. Tom Oxley, Synchron's co-founder and chief executive officer, hopes to implant as many as 16 stentrodes in the coming year, as his company looks to move beyond the NIH study and to advance trials for review by the FDA. Although many of the early implants will go to ALS patients, it's thought that the technology should also benefit people who have had strokes and spinal cord injuries, or have multiple sclerosis, among other conditions.

Oxley, a physician with a doctorate in neuroscience, grew up in Australia and developed the technology there before moving his company to Brooklyn. He's hoping this first US procedure will show that the operation is so similar to existing surgeries around stents and pacemakers that it can be performed on a regular basis by thousands of doctors. "I feel like we have broken through this barrier and that people get it," he says.

Synchron has raised more than $70 million and includes Khosla Ventures and Max Hodak, the former president of Neuralink, as investors. Thomas Reardon, a well-known BCI expert who developed related technology at a startup acquired by Meta Platforms Inc., is also an investor.

The company's noninvasive approach does have some drawbacks. Because the stentrode is placed in a blood vessel, its electrodes are not as close to the neurons as the implants being developed by Neuralink, making its signal less clear.

In the months and years ahead, Synchron aims to shrink the size of its devices while increasing their computing power. If it's successful, the company would be able to place numerous stentrodes in each patient in different parts of the brain, allowing them to perform more functions. Oxley expects that his technology will help generate a flood of new data and insights into how the brain works and could lead to breakthroughs with a number of disorders, including mental health issues. "I feel like we are at the beginning of a renaissance around brain decoding," he says.
https://www.bloomberg.com/news/articles/2022-07-18/brain-computer-interface-company-implants-new-type-of-device

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

Translate the following English terms:

1. blood vessel
2. To accomplish
3. Related technology
4. Spinal cord injuries
5. The process is very similar to implanting a coronary stent

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Founded in 2016, Synchron has caught the attention of the brain-computer interface (BCI) field because its device, known as the stentrode, can be inserted into the brain without cutting through a person's skull or damaging their tissue. A doctor makes an incision in the patient's neck and feeds the stentrode via a catheter through the jugular vein into a blood vessel nestled within the motor cortex. As the catheter is removed, the stentrode—a cylindrical, hollow wire mesh—opens up and begins to fuse with the outer edges of the vessel. According to Majidi, the process is very similar to implanting a coronary stent and takes just a few minutes.
2. The Utah array has allowed patients with severe disabilities to do remarkable things like command robotic arms to bring them a cup of water. But they generally use the devices only under supervision at a hospital, and the brain tends to form scar tissue around it, degrading the signals gathered by the electronics over time.
3. The company's noninvasive approach does have some drawbacks. Because the stentrode is placed in a blood vessel, its electrodes are not as close to the neurons as the implants being developed by Neuralink, making its signal less clear.

Task VI

Divide the text into 6 passages. Write sort headings for them.

UNIT 6.

Task I.

Read the text. Translate each instance into Ukrainian.

Twitter breach exposed anonymous account owners

A vulnerability in Twitter's software that exposed an undetermined number of owners of anonymous accounts to potential identity compromise last year was apparently exploited by a malicious actor, the social media company said Friday.

It did not confirm a report that data on 5.4 million users was offered for sale online as a result but said users worldwide were affected.

The breach is especially worrisome because many Twitter account owners, including human rights activists, do not disclose their identities in their profiles for security reasons that include fear of persecution by repressive authorities.

"This is very bad for many who use pseudonymous Twitter accounts," U.S. Naval Academy data security expert Jeff Kosseff tweeted.

The vulnerability allowed someone to determine during log-in whether a particular phone number or email address was tied to an existing Twitter account, thereby revealing account owners, the company said.

Twitter said it did not know how many users may have been affected, and stressed that no passwords were exposed.

"We can confirm the impact was global," a Twitter spokesperson said via email. "We cannot determine exactly how many accounts were impacted or the location of the account holders."

Twitter's acknowledgment in a blog post Friday followed a report last month by the digital privacy advocacy group Restore Privacy detailing how data presumably obtained from the vulnerability was being sold on a popular hacking forum for $30,000.

A security researcher discovered the flaw in January, informed Twitter and was paid a reported $5,000 bounty. Twitter said the bug, introduced in a June 2021 software update, was immediately fixed.

Twitter said it learned about the data sale on the hacking forum from media reports and "confirmed that a bad actor had taken advantage of the issue before it was addressed."

It said it was directly notifying all account owners that it can confirm were affected.

"We are publishing this update because we aren't able to confirm every account that was potentially impacted, and are particularly mindful of people with pseudonymous accounts who can be targeted by state or other actors," the company said.

It recommended users seeking to keep their identities veiled not add a publicly known phone number or email address to their Twitter account.

"If you operate a pseudonymous Twitter account, we understand the risks an incident like this can introduce and deeply regret that this happened," it said.

The revelation of the breach comes while Twitter is in a legal battle with Tesla CEO Elon Musk over his attempt to back out from his previous offer to buy San Francisco-based Twitter for $44 billion.

(https://apnews.com/article/twitter-inc-technology-social-media-27382aa1537c97e6266f8a7d9ad977d6)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

Translate the following English terms:

1. repressive authorities
2. data presumably obtained
3. pseudonymous accounts
4. to keep their identities veiled
5. the revelation of the breach

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translation in your language would you suggest for these words?*

Task IV

Underline the words related to the topic of Twitter breach exposed anonymous account owners in the passage. Translate them. Do not use the dictionary.

Task V

Skim- read the passage below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. The breach is especially worrisome because many Twitter account owners, including human rights activists, do not disclose their identities in their profiles for security reasons that include fear of persecution by repressive authorities.

2. The revelation of the breach comes while Twitter is in a legal battle with Tesla CEO Elon Musk over his attempt to back out from his previous offer to buy San Francisco-based Twitter for $44 billion.

3. Twitter's acknowledgment in a blog post Friday followed a report last month by the digital privacy advocacy group Restore Privacy detailing how data presumably obtained from the vulnerability was being sold on a popular hacking forum for $30,000.

Task VI

Devide the text into 6 passage. Wright sort headlines for them.

UNIT 7

Task I.

Read the text. Translate each instance into Ukrainian.

NEW YORK (AP) — Amazon on Friday announced it has agreed to acquire the vacuum cleaner maker iRobot for approximately $1.7 billion, scooping up another company to add to its collection of smart home appliances amid broader concerns from anti-monopoly and privacy advocates about Amazon's market power and ability to gain deeper insights into consumers' lives.

iRobot sells its products worldwide and is most famous for the circular-shaped Roomba vacuum, which would join voice assistant Alexa, the Astro robot and Ring security cameras and others in the list of smart home features offered by the Seattle-based e-commerce and tech giant.

The move is part of Amazon's bid to own part of the home space through services and accelerate its growth beyond retail, said Neil Saunders, managing director at GlobalData Retail. A slew of home-cleaning robots adds to the company's tech arsenal, making it more involved in consumers' lives beyond static things like voice control. The latest line of Roombas use sensors to map -- and remember -- a home's floor plan, offering a trove of data that Amazon could potentially integrate with its other products.

Amazon's Astro robot, which helps with tasks like setting an alarm, was unveiled last year at an introductory price of $1,000. But its rollout has been limited and has received a lackluster response.

Amazon hasn't had much success with household robots, but the iRobot acquisition and the company's strong market reputation provide a "massive foothold in the consumer robot market" that could help Amazon replicate the success of its Echo line of smart speakers, said Lian Jye Su, a robotics industry analyst for ABI Research.

Su said it also illustrates the shortcomings of consumer robotics vendors like iRobot, which struggled to expand beyond a niche product and was in a "race-to-the-bottom" competition with Korean and Chinese manufacturers offering cheaper versions of a robotic vacuum.

On Friday, iRobot reported its quarterly results. Revenue plunged 30% primarily on order reductions and delays, and the company announced it was laying off 10% of its workforce.

Amazon said it will acquire iRobot for $61 per share in an all-cash transaction that will include iRobot's net debt. The company has total current debt of approximately $332.1 million as of July 2. The deal is subject to approval by shareholders and regulators. Upon completion, iRobot's CEO, Colin Angle, will remain in his position.

Noting that iRobot has been running its robotics platform on Amazon's cloud service unit AWS for many years, Su said the acquisition could lead to more integration of Amazon speech recognition and other capabilities into vacuums.

In afternoon trading, iRobot shares rose 19%. Amazon's were down 1.7%.

The deal comes as anti-monopoly advocates continue to raise concerns about Amazon's increasing dominance. The purchase of iRobot is Amazon's fourth-largest acquisition, led by its $13.7 billion deal to buy Whole Foods in 2017. Last month, the company said it would buy the primary care provider One Medical in a deal valued roughly at $3.9 billion, a move that expanded its reach further into health care.

On Friday, groups advocating for stricter antitrust regulations called on regulators to block the iRobot merger, arguing it gives Amazon more access into consumers' lives and furthers its dominance in the smart home market.

"The last thing American and the world needs is Amazon vacuuming up even more of our personal information," said Robert Weissman, president of the progressive consumer rights advocacy group Public Citizen.

"This is not just about Amazon selling another device in its marketplace," Weissman said. "It's about the company gaining still more intimate details of our lives to gain unfair market advantage and sell us more stuff."

Landmark antitrust legislation targeting Amazon and other Big Tech companies has languished for months in Congress as prospects for votes by the full Senate or House have dimmed.

Last month, Sen. Amy Klobuchar, D-Minn., who heads the Senate Judiciary antitrust panel, urged the the Federal Trade Commission to investigate the One Medical acquisition, in the mold of other critics who've called on regulators to block the purchase over concerns about Amazon's past conduct and potential implications for consumers' health data. Regulators also have discretion to challenge Amazon's $8.5 billion buyout of Hollywood studio MGM, which was completed earlier this year.

Founded in 1990 by a trio of Massachusetts Institute of Technology roboticists, including Angle, iRobot's early ventures led to rovers that could perform military and disaster-relief tasks in the aftermath of the Sept. 11 attacks.

The profits from defense contracts allowed iRobot to experiment with a variety of other robots, producing some duds and one huge commercial success: the first Roomba, introduced in 2002, which pioneered the market for automated vacuum cleaners.

The company spun off its defense robotics division in 2016 to become almost exclusively a seller of vacuums and some other home robots, such as the Braava robotic mop. It planned to launch a robotic lawn mower in 2020 but backed off, citing problems tied to the pandemic.

(https://apnews.com/article/colin-angle-d4de06cdcf36beeec71166ff44abdf68)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

1. a slew of home-cleaning robots
2. companies has languished pseudonymous accounts
3. a robotic lawn mower
4. ventures led to rovers
5. a trove of data

➤*Analyse the meaning of the different expressions.*

➤*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translation in your language would you suggest for these words?*

Task IV

Underline the words related to the topic of Amazon to buy vacuum maker iRobot for roughly $1.7B in the passage. Translate them. Do not use the dictionary.

Task V

Skim- read the passage below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Last month, Sen. Amy Klobuchar, D-Minn., who heads the Senate Judiciary antitrust panel, urged the the Federal Trade Commission to investigate the One Medical acquisition, in the mold of other critics who've called on regulators to block the purchase over concerns about Amazon's past conduct and potential implications for consumers' health data. Regulators also have discretion to challenge Amazon's $8.5 billion buyout of Hollywood studio MGM, which was completed earlier this year.
2. Amazon said it will acquire iRobot for $61 per share in an all-cash transaction that will include iRobot's net debt. The company has total current debt of approximately $332.1 million as of July 2. The deal is subject to approval by shareholders and regulators. Upon completion, iRobot's CEO, Colin Angle, will remain in his position. Noting that iRobot has been running its robotics platform on Amazon's cloud service unit AWS for many years, Su said the acquisition could lead to more integration of Amazon speech recognition and other capabilities into vacuums.
3. The move is part of Amazon's bid to own part of the home space through services and accelerate its growth beyond retail, said Neil Saunders, managing director at GlobalData Retail. A slew of home-cleaning robots adds to the company's tech arsenal, making it more involved in consumers' lives beyond static things like voice control. The latest line of Roombas use sensors to map -- and remember -- a home's floor plan, offering a trove of data that Amazon could potentially integrate with its other products.

Task VI

Devide the text into 6 passage. Wright sort headlines for them.

UNIT 8

Text 1.

Task I. *Read the text. Translate each instance into Ukrainian.*

US agency probes Tesla crashes that killed 2 motorcyclists

DETROIT (AP) — Two crashes involving Teslas apparently running on Autopilot are drawing scrutiny from federal regulators and point to a potential new hazard on U.S. freeways: The partially automated vehicles may not stop for motorcycles.

The National Highway Traffic Safety Administration sent investigation teams to two crashes last month in which Teslas collided with motorcycles on freeways in the darkness. Both were fatal.

The agency suspects that Tesla's partially automated driver-assist system was in use in each. The agency says that once it gathers more information, it may include the crashes in an broader probe of Teslas striking emergency vehicles parked along freeways. NHTSA also is investigating over 750 complaints that Teslas can brake for no reason.

The first crash involving a motorcyclist happened at 4:47 a.m. July 7 on State Route 91, a freeway in Riverside, California. A white Tesla Model Y SUV was traveling east in the high occupancy vehicle lane. Ahead of it was a rider on a green Yamaha V-Star motorcycle, the California Highway Patrol said in a statement.

At some point, the vehicles collided, and the unidentified motorcyclist was ejected from the Yamaha. He was pronounced dead at the scene by the Fire Department.

Whether or not the Tesla was operating on Autopilot remains under investigation, a CHP spokesman said.

The second crash happened about 1:09 a.m. July 24 on Interstate 15 near Draper, Utah. A Tesla Model 3 sedan was behind a Harley-Davidson motorcycle,

also in an HOV lane. “The driver of the Tesla did not see the motorcyclist and collided with the back of the motorcycle, which threw the rider from the bike,” the Utah Department of Public Safety said in a prepared statement.

The rider, identified as Landon Embry, 34, of Orem, Utah, died at the scene. The Tesla driver told authorities that he had the vehicle’s Autopilot setting on, the statement said.

Michael Brooks, acting executive director of the nonprofit Center for Auto Safety, called on NHTSA to recall Tesla’s Autopilot because it is not recognizing motorcyclists, emergency vehicles or pedestrians.

“It’s pretty clear to me, and it should be to a lot of Tesla owners by now, this stuff isn’t working properly and it’s not going to live up to the expectations, and it is putting innocent people in danger on the roads,” Brooks said.

Since 2016, NHTSA has sent teams to 39 crashes in which automated driving systems are suspected of being in use, according to agency documents. Of those, 30 involved Teslas, including crashes that caused 19 deaths.

Brooks criticized the agency for continuing to investigate but not taking action. “What the Hell are they doing while these crashes continue to occur?” he asked. “Drivers are being lured into thinking this protects them and others on the roads, and it’s just not working.”

Tesla CEO Elon Musk has eliminated use of radar from his systems and relies solely on cameras and computer memory. Brooks and other safety advocates say the lack of radar hurts vision in the darkness.

Messages were left seeking comment from Tesla, which has disbanded its media relations department.

Tesla has said that Autopilot and “Full Self-Driving” cannot drive themselves, and that drivers should be ready to intervene at all times.

The Los Angeles Times, meanwhile, on Friday reported that California’s Department of Motor Vehicles has accused Tesla of false advertising in its promotion of Autopilot and Full Self-Driving. The accusations came in complaints filed with the state’s Office of Administrative Hearings on July 28, the Times reported.

In a June interview, new NHTSA Administrator Steven Cliff said the agency is intensifying efforts to understand risks posed by automated vehicles so it can decide what regulations may be necessary to protect drivers, passengers and pedestrians. There are no federal regulations that directly cover either self-driving vehicles or those with partially automated driver-assist systems such as Autopilot.

The agency also says the technology holds great promise of reducing traffic crashes.

NHTSA also has ordered all automakers and tech companies with automated driving systems to report all crashes. The agency released the first batch of data in June showing that nearly 400 crashes were reported over a 10-month period, including 273 with Teslas. But it cautioned against making comparisons, saying that Tesla's telematics allow it to gather data in real time, much faster than other companies.

Tesla's Autopilot keeps cars in their lane and a distance behind other vehicles. The company also is using selected owners to test "Full Self-Driving" software, which is designed to complete a route on its own with human supervision. Eventually, Musk says the cars will drive themselves, enabling a fleet of autonomous robotaxis that will boost Tesla's earnings. In 2019, Musk had pledged to have the robotaxis running in 2020.

He said at the company's annual shareholders' meeting Thursday that "Full Self-Driving" is greatly improved, and he expects to make the software available by the end of the year to all owners who request it.

(https://apnews.com/article/technology-12ba38bd863e2b128a8e2914179049e0)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

1. autopilot are drawing scrutiny
2. a fleet of autonomous robotaxis
3. which has disbanded
4. to intervene

➤*Analyse the meaning of the different expressions.*

➤*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translation in your language would you suggest for these words?*

Task IV

Underline the words related to the topic of US agency probes Tesla crashes that killed 2 motorcyclists in the passage. Translate them. Do not use the dictionary.

Task V

Skim- read the passage below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Tesla's Autopilot keeps cars in their lane and a distance behind other vehicles. The company also is using selected owners to test "Full Self-Driving" software, which is designed to complete a route on its own with human supervision. Eventually, Musk says the cars will drive themselves, enabling a fleet of autonomous robotaxis that will boost Tesla's earnings. In 2019, Musk had pledged to have the robotaxis running in 2020.

2. Since 2016, NHTSA has sent teams to 39 crashes in which automated driving systems are suspected of being in use, according to agency documents. Of those, 30 involved Teslas, including crashes that caused 19 deaths.

3. The agency suspects that Tesla's partially automated driver-assist system was in use in each. The agency says that once it gathers more information, it may include the crashes in an broader probe of Teslas striking emergency vehicles parked along freeways. NHTSA also is investigating over 750 complaints that Teslas can brake for no reason.

Task VI

Devide the text into 6 passage. Wright sort headlines for them.

UNIT 9

Task I.

Read the texts. Translate each instance into Ukrainian.

Earable' uses sonar to reconstruct facial expressions

Cornell researchers have developed a wearable earphone device – or "earable" – that bounces sound off the cheeks and transforms the echoes into an avatar of a person's entire moving face.

A team led by Cheng Zhang, assistant professor of information science, and François Guimbretière, professor of information science, both in the Cornell Ann 87S. Bowers College of Computing and Information Science, designed the system, named EarIO. It transmits facial movements to a smartphone in real time and is compatible with commercially available headsets for hands-free, cordless video conferencing.

Devices that track facial movements using a camera are "large, heavy and energy-hungry, which is a big issue for wearables," said Zhang, principal investigator of the Smart Computer Interfaces for Future Interactions (SciFi) Lab. "Also importantly, they capture a lot of private information."

Facial tracking through acoustic technology can offer better privacy, affordability, comfort and battery life, he said.

The team described their earable in "EarIO: A Low-power Acoustic Sensing Earable for Continuously Tracking Detailed Facial Movements," published this month in the Proceedings of the Association for Computing Machinery on Interactive, Mobile, Wearable and Ubiquitous Technologies.

The EarIO works like a ship sending out pulses of sonar. A speaker on each side of the earphone sends acoustic signals to the sides of the face and a microphone

picks up the echoes. As wearers talk, smile or raise their eyebrows, the skin moves and stretches, changing the echo profiles. A deep learning algorithm developed by the researchers uses artificial intelligence to continually process the data and translate the shifting echoes into complete facial expressions.

"Through the power of AI, the algorithm finds complex connections between muscle movement and facial expressions that human eyes cannot identify," said co-author Ke Li, a doctoral student in the field of information science. "We can use that to infer complex information that is harder to capture – the whole front of the face."

Previous efforts by the Zhang lab to track facial movements using earphones with a camera recreated the entire face based on cheek movements as seen from the ear.

By collecting sound instead of data-heavy images, the earable can communicate with a smartphone through a wireless Bluetooth connection, keeping the user's information private. With images, the device would need to connect to a Wi-Fi network and send data back and forth to the cloud, potentially making it vulnerable to hackers.

"People may not realize how smart wearables are – what that information says about you, and what companies can do with that information," Guimbretière said. With images of the face, someone could also infer emotions and actions. "The goal of this project is to be sure that all the information, which is very valuable to your privacy, is always under your control and computed locally."

Using acoustic signals also takes less energy than recording images, and the EarIO uses 1/25 of the energy of another camera-based system the Zhang lab developed previously. Currently, the earable lasts about three hours on a wireless earphone battery, but future research will focus on extending the use time.

The researchers tested the device on 16 participants and used a smartphone camera to verify the accuracy of its face-mimicking performance. Initial experiments show that it works while users are sitting and walking around, and that wind, road noise and background discussions don't interfere with its acoustic signaling.

In future versions, the researchers hope to improve the earable's ability to tune out nearby noises and other disruptions.

"The acoustic sensing method that we use is very sensitive," said co-author Ruidong Zhang, a doctoral student in the field of information science. "It's good, because it's able to track very subtle movements, but it's also bad because when something changes in the environment, or when your head moves slightly, we also capture that."

One limitation of the technology is that before the first use, the EarIO must collect 32 minutes of facial data to train the algorithm. "Eventually we hope to make this device plug and play," Zhang said.

Cornell Bowers CIS provided funding for the research.

(https://news.cornell.edu/stories/2022/07/earable-uses-sonar-reconstruct-facial-expressions)

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. pulses of sonar

2. cordless video conferencing
3. facial movements
4. a Low-power Acoustic Sensing Earable
5. ubiquitous Technologies.

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of 'Earable' uses sonar to reconstruct facial expressions in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Devices that track facial movements using a camera are "large, heavy and energy-hungry, which is a big issue for wearables," said Zhang, principal investigator of the Smart Computer Interfaces for Future Interactions (SciFi) Lab. "Also importantly, they capture a lot of private information."
Facial tracking through acoustic technology can offer better privacy, affordability, comfort and battery life, he said.
2. The EarIO works like a ship sending out pulses of sonar. A speaker on each side of the earphone sends acoustic signals to the sides of the face and a microphone picks up the echoes. As wearers talk, smile or raise their eyebrows, the skin moves and

stretches, changing the echo profiles. A deep learning algorithm developed by the researchers uses artificial intelligence to continually process the data and translate the shifting echoes into complete facial expressions.

3. “People may not realize how smart wearables are – what that information says about you, and what companies can do with that information,” Guimbretière said. With images of the face, someone could also infer emotions and actions. “The goal of this project is to be sure that all the information, which is very valuable to your privacy, is always under your control and computed locally.”

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 10

Task I. *Read the texts. Translate each instance into Ukrainian.*

Microsoft launches simulator to train drone AI systems

Microsoft has launched a platform to train the artificial intelligence (AI) systems of autonomous aircraft. Project AirSim is, in effect, a flight simulator for drones, which companies can use to train and develop software controlling them. It makes it possible for test flights in places that would be too risky in reality, such as near power lines. And it means, Microsoft says, that millions of flights can be simulated in seconds.

For example, companies can virtually see how the vehicle flies in rain, or how strong winds might affect its battery life.

In a statement announcing the launch, Microsoft's Gurdeep Pall said that it showed "the power of the industrial metaverse - the virtual worlds where businesses will build, test and hone solutions, and then bring them into the real world". The firm envisages the tech being used to train the AI systems which fly autonomous air vehicles from air taxis to delivery drones.

Turning 40

The Seattle software giant has a long history in virtual flight - this November its Flight Simulator game will celebrate its 40th anniversary.

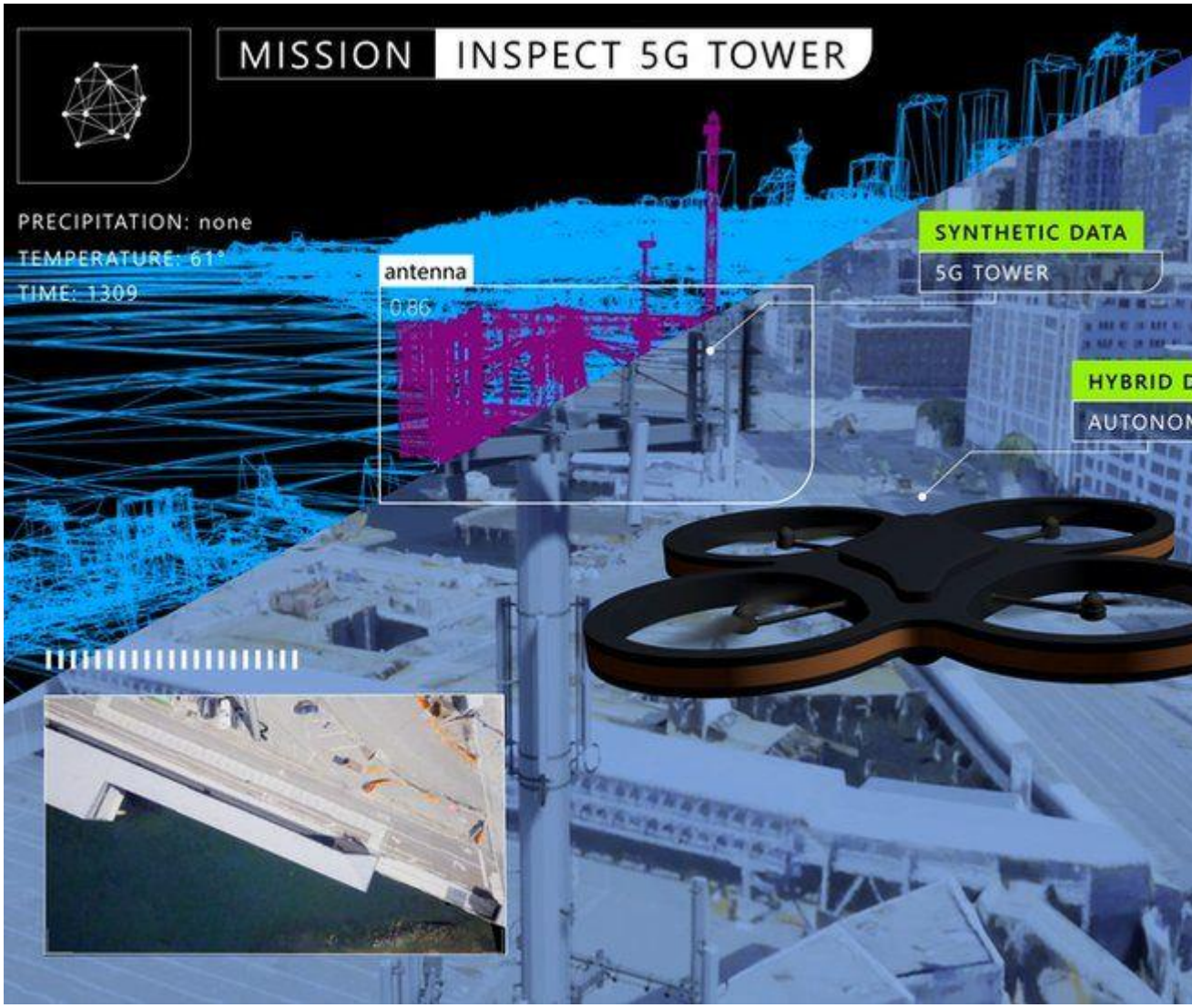


IMAGE SOURCE, MICROSOFT

The simulated flight of a drone near a phone mast above Seattle. Microsoft has announced that it will retire that project. Users will still have access to the original open-source project's code, the company told the BBC, but it will be archived, and instead the firm will focus its efforts on the new product. The new proprietary platform, the company says, contains more out-of-the box features, and requires less technical knowledge to use.

However, Microsoft says its goal is to offer a free option, and says it will provide more information as the general release date approaches. The project runs on Microsoft's cloud computing platform Azure. US firm Airtonomy was given early access to the platform.

Airtonomy uses drones to inspect infrastructure, such as wind turbines and power lines. Chief executive Josh Riedy told the BBC that previously a "crew of

three individuals rappelled down those blades - the towers are at a height of 80m (262 ft), so not only was it a nearly a day-long job for three individuals, safety is certainly a consideration". Now the drones fly autonomously and can be controlled by only one person on the ground. "They simply need to know how to put batteries in a drone, and push a button," he said.

The flight routines that enable this are developed in the virtual environment of Project AirSim, and Mr Riedy says a big advantage is the "simulated environment allows us to make mistakes" when working with critical infrastructure. It also allows developers to imagine "what if" scenarios that would be unsafe to test in real life - such as what happens if a drone's vision is obscured. Microsoft hopes that it could also be used by civil aviation regulators to test systems - seeing how the drone performs in extremely heavy rain, or copes with a loss of positioning data.

IMAGE SOURCE,MICROSOFT

Four simulated drones fly through forest settings in AirSim. As well as libraries of digital environments, developers will also have to access already trained AI "building blocks" which the firm hopes will reduce the expertise needed to develop systems. Ashish Kapoor, creator of the original open-source AirSim, said in a statement that he hoped data gathered on the new platform would help put "many more vehicles in the sky, helping to monitor farms, inspect critical infrastructure and transport goods and people to the remotest of places".

(https://www.bbc.com/news/technology-62202118)

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. battery life
2. industrial metaverse
3. proprietary platform
4. a loss of positioning data
5. out-of-the box features

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Microsoft launches simulator to train drone AI systems in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Project AirSim is, in effect, a flight simulator for drones, which companies can use to train and develop software controlling them.

It makes it possible for test flights in places that would be too risky in reality, such as near power lines.

And it means, Microsoft says, that millions of flights can be simulated in seconds.

2. Microsoft has announced that it will retire that project.

Users will still have access to the original open-source project's code, the company told the BBC, but it will be archived, and instead the firm will focus its efforts on the new product. The new proprietary platform, the company says, contains more out-of-the box features, and requires less technical knowledge to use.

3. Ashish Kapoor, creator of the original open-source AirSim, said in a statement that he hoped data gathered on the new platform would help put "many more vehicles in the sky, helping to monitor farms, inspect critical infrastructure and transport goods and people to the remotest of places".

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 11

Task I. *Read the texts. Translate each instance into Ukrainian.*

Online platform designed to improve reproducibility, scientific collaborations

For centuries, scientists relied on a pen or pencil and trusty lab notebook to make sure their experiments could be understood and replicated by colleagues. Now, as experiments may involve dozens of steps and hundreds of materials, produce gigabytes of data that require supercomputers to process and are shared with collaborators around the globe, the lab notebook may no longer suffice.

In a recent study, the researchers report on the development of an online platform that can help genomic researchers track experiments from conception to publication, keeping exacting records for quality control purposes and easing potential reproducibility efforts.

The system, named Platform for Epi-Genomic Research, or PEGR, is designed as a tool to help experimental life sciences laboratories – or wet-labs – keep track of highly complex operations and turn raw data into scientific insights. For example, rather than relying on painstaking hand-written notes, PEGR incorporates two dimensional barcodes – called quick response, or QR codes – to electronically collect and track detailed information on samples as they advance along the experimental process.

The efficiency of PEGR can improve reproducibility, a key reason for the development of the tool, according to William Lai, an assistant research professor, Cornell University, and formerly an assistant research professor in biochemistry and molecular biology, Penn State. Reproducibility, a critical step in the scientific process, requires scientists to check their work to make sure it is accurate, safe and functional in real world applications.

“It’s already well recognized that reproducibility is an issue not only in the life sciences, but across all STEM (science, technology, engineering and medical) fields,” said Lai. “There has been story after story of research teams that claimed to discover

something and then, a few years later, we find that no one has reproduced those results outside of the lab that generated the findings. PEGR is an approach to getting a handle on tracking experimental processes – what a user is using and when are they using it – so that we can improve reproducibility."

Because it is an online platform, PEGR can connect scientists across the world to facilitate reproducibility efforts. The platform also addresses the rapid development of equipment for genomic research – including robotic sampling and high throughput sequencers that can run many experiments simultaneously – that create vast amounts of data, according to Danying Shao, research and development engineer for the Institute for Computational and Data Science's (ICDS) Research Innovations with Scientists and Engineers, or RISE, team.

"There is no doubt a data explosion is happening in bioinformatics," said Shao, who helped design the platform. "Big data sets are being generated at an unprecedented pace. For example, a single sample can generate gigabytes of data. And, when we are sequencing hundreds of samples, you can see that we can get to the level where we are creating terabytes of data."

According to the researchers, who published details about the system in Genome Biology, PEGR is integrated with the Galaxy platform, an open-source scientific workflow system. PEGR is designed to track the sample and sequencing experiment, manage the processing of the data and then produce reports and visualizations of the experimental results.

In the first few runs with the platform, the researchers are already experiencing early benefits. "Just as an example, recently a technician was experiencing a string of failed experiments, so we went into PEGR and by examining the experimental metadata, we realized that they were using a bad batch of a certain chemical," said Lai. "Now, historically, the process to find the cause of the failing experiments could have dragged on for months – if not, a year or two – instead of finding the source right away."

RISE-powered research

According to Chuck Pavloski, RISE team lead, the PEGR project is just one example of how members of RISE are helping Penn State researchers, as well as the research community at large. Pavloski likens the team a bond between researchers with computational tools and expertise that can expand the power of science to tackle important scientific and societal challenges.

"The RISE engineers are effectively the glue between science and today's computational needs," said Pavloski. "In other words, they allow the scientists to be what they're good at. We act much the same way as a staff scientist works at a national lab, paving the way so that our scientists can explore their fields and pursue their research ideas."

This RISE-powered partnership can help scientists with traditional computational research questions, such as providing guidance on best practices for using Penn State's Roar supercomputer to offering ways to optimize and improve code, but the team can also apply their own deep understanding of academic research to collaborate with scientists on cutting-edge, interdisciplinary projects.

"The RISE team is made up of master's and Ph.D.-level scientists who have a deep understanding of how science works, but work outside of their fields all the time," said Pavloski. "For example, we might have a trained meteorologist who also work on biochemistry or genomic projects, or we have engineers on our team who may be help scientists in astronomy or biochemistry."

This interdisciplinarity offers another advantage. RISE team members can leverage best computational science practices in one field to investigations in other fields or disciplines.

"We also provide a strong link to new technologies, such as using artificial intelligence techniques, or exploring the use of graphic processing unit – or GPU – computation in a research project," Pavloski said.

RISE engineers are also working with data visualization specialists to help scientists create compelling visualizations for their work, as well as take advantage of new immersive technologies, such as virtual reality and augmented reality, to explore data in deeply engaging ways.

Future uses

The researchers hope that PEGR, which is open source, could produce benefits across the scientific enterprise, saving time, money and headaches, and lead to everything from richer understanding of the genome to better medical treatments reaching patients faster.

In the future, the researchers may explore whether the online platform can be expanded outside of use in wet-labs and for use in translational science, which would help scientists bring treatments and solutions to the real world.

"This platform was originally designed around basic research, but we're actively working to move it into the translational biomedical field in the future," said Lai.

https://newsroom.unsw.edu.au/news/science-tech/scientists-emulate-nature-quantum-leap-towards-computers-future)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

1. gigabytes of data
2. dimensional barcodes

3. STEM
4. robotic sampling
5. interdisciplinary projects

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Online platform designed to improve reproducibility, scientific collaborations. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. UNIVERSITY PARK, Pa. – For centuries, scientists relied on a pen or pencil and trusty lab notebook to make sure their experiments could be understood and replicated by colleagues.

2. The system, named Platform for Epi-Genomic Research, or PEGR, is designed as a tool to help experimental life sciences laboratories – or wet-labs – keep track of highly complex operations and turn raw data into scientific insights.

3. PEGR is integrated with the Galaxy platform, an open-source scientific workflow system. PEGR is designed to track the sample and sequencing experiment, manage the processing of the data and then produce reports and visualizations of the experimental results.

4. “The RISE engineers are effectively the glue between science and today’s computational needs,” said Pavloski. “In other words, they allow the scientists to be what they’re good at. We act much the same way as a staff scientist works at a national lab, paving the way so that our scientists can explore their fields and pursue their research ideas.”
5. PEGR could produce benefits across the scientific enterprise, saving time, money and headaches, and lead to everything from richer understanding of the genome to better medical treatments reaching patients faster.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 12

Task I. *Read the texts. Translate each instance into Ukrainian.*

SMART IMPLANTS TO MONITOR HEALING

Researchers at the University of Pittsburgh Swanson School of Engineering are creating patient-specific 3D-printed smart metamaterial implants that double as sensors to monitor spinal healing. A paper detailing their work was recently published in the journal Advanced Functional Materials.

Spinal fusion – fusing two vertebrae together – can treat a wide variety of spinal disorders. Often, surgeons will use a cage to provide support where the disk once was between the vertebrae. But what if those cages could support the spine's healing in more ways than one?

Researchers at the University of Pittsburgh Swanson School of Engineering are creating patient-specific 3D-printed smart metamaterial implants that double as sensors to monitor spinal healing. A paper detailing their work was recently published in the journal Advanced Functional Materials. "Smart implants can provide real-time biofeedback and offer many therapeutic and diagnostic benefits," said Amir Alavi, assistant professor of civil and environmental engineering, whose iSMaRT Lab led the research. "But it is very challenging to integrate bulky circuits or power sources into the small area of implants. The solution is to use the implant matrix as an active sensing and energy harvesting medium. That's what we've been focused on."

The Intelligent Structural Monitoring and Response Testing (iSMaRT) Lab has developed a new class of multifunctional mechanical metamaterials, which act as their own sensors, recording and relaying important information about the pressure and stresses on its structure. The so-called "meta-tribomaterials" a.k.a. self-aware metamaterials, generate their own power and can be used for a wide array of sensing and monitoring applications.

The material is designed such that under pressure, contact-electrification occurs between its conductive and dielectric microlayers, creating an electric charge that relays information about the condition of the material matrix. In addition, it naturally inherits the outstanding mechanical tunability of standard metamaterials. The power generated using its built-in triboelectric nanogenerator mechanism eliminates the need for a separate power source, and a tiny chip records data about the pressure on the cage, which is an important indicator of healing. The data can then be read noninvasively using a portable ultrasound scanner.

Not only is the proposed cage unique in its sensing capabilities, but it's also made of a highly tunable material that can be customized to the patient's needs.
"Spinal fusion cages are being widely used in spinal fusion surgeries, but they're usually made of titanium or PEEK polymer materials (a semi-crystalline, high-performance engineering thermoplastic) with certain mechanical properties," explained Alavi. "The stiffness of our metamaterial interbody cages can be readily tuned. The implant can be 3D-printed based on the patient's specific anatomy before surgery, making it a much more natural fit."

The team has successfully tested the device in human cadavers and are looking to move on to animal models next. Because the material itself is incredibly tunable and scalable, the smart sensor design could be adapted to many other medical applications in the future, like cardiovascular stents or components for knee or hip replacements.

"This is a first-of-its-kind implant that leverages advances in nanogenerators and metamaterial to build multifunctionality into the fabric of medical implants," said Alavi. "This technological advancement is going to play a major part in the future of implantable devices."

The paper, "Patient-Specific Self-Powered Metamaterial Implants for Detecting Bone Healing Progress," (DOI: 10.1002/adfm.202203533) was published in Advanced Functional Materials. It was coauthored by researchers and surgeons at the University of Pittsburgh, Georgia Institute of Technology, the Beijing Institute of

Nanoenergy and Nanosystems, and the Allegheny Health Network Department of Neurosurgery.

https://news.engineering.pitt.edu/smart-implants-to-monitor-healing/

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. spinal healing
2. Spinal fusion
3. metamaterial implants
4. dielectric microlayers
5. to integrate bulky circuits
6. mechanical tunability
7. cardiovascular stents

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of SMART IMPLANTS TO MONITOR HEALING. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Researchers at the University of Pittsburgh Swanson School of Engineering are creating patient-specific 3D-printed smart metamaterial implants that double as sensors to monitor spinal healing.
2. Spinal fusion—fusing two vertebrae together—can treat a wide variety of spinal disorders.
3. The Intelligent Structural Monitoring and Response Testing (iSMaRT) Lab has developed a new class of multifunctional mechanical metamaterials, which act as their own sensors, recording and relaying important information about the pressure and stresses on its structure.
4. The material is designed such that under pressure, contact-electrification occurs between its conductive and dielectric microlayers, creating an electric charge that relays information about the condition of the material matrix.
5. Spinal fusion cages are being widely used in spinal fusion surgeries, but they're usually made of titanium or PEEK polymer materials (a semi-crystalline, high-performance engineering thermoplastic) with certain mechanical properties
6. The team has successfully tested the device in human cadavers and are looking to move on to animal models next.
7. This is a first-of-its-kind implant that leverages advances in nanogenerators and metamaterial to build multifunctionality into the fabric of medical implants.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 13

Task I. *Read the texts. Translate each instance into Ukrainian.*

Amazon Unveils First Fully Autonomous Mobile Robot Called Proteus

Meet Proteus, Amazon's first fully autonomous mobile robot.

Proteus, which looks a lot like a robot vacuum, was designed to automatically perform tasks and safely move around employees using proprietary safety, perception, and navigation technology.

"Historically, it's been difficult to safely incorporate robotics in the same physical space as people," Amazon explained in a company announcement(Opens in a new window). "We believe Proteus will change that while remaining smart, safe, and collaborative."

Proteus is capable of lifting and transporting GoCarts, Amazon's wheeled trolleys used to move packages through facilities. The video below shows the robot in action, including what happens when a human steps into its path. Proteus stops, waits, and resumes its journey once the person moves out of range.

The autonomous robot will initially be deployed in the outbound GoCart handling areas of Amazon's fulfillment and sort centers. "Our vision is to automate GoCart handling throughout the network, which will help reduce the need for people to manually move heavy objects through our facility and instead let them focus on more rewarding work," the company said.

Celebrating 10 years of robotic evolution, Amazon unveiled several more automated systems. Cardinal(Opens in a new window) is an AI-based robot arm that can select one package out of a pile of boxes, lift it, read the label, and place it on the appropriate GoCart (for Proteus to collect). Amazon is currently trialing a Cardinal prototype for handling packages up to 50 pounds and expects to deploy the technology in fulfillment centers next year.

Other tech includes an AI-powered product scanner called AR ID(Opens in a new window) that replaces employees' handheld barcode readers, and a new

Containerized Storage System(Opens in a new window) that relies on an assortment of machines to deliver products to workers and put staff in "a safer and more ergonomic position through a highly choreographed dance of robotics and software." "What started as an interesting acquisition [of robotics firm Kiva in 2012] has grown into a dedicated team" of experts, Amazon said, adding that its facilities are "safer and more collaborative than ever."

https://www.pcmag.com/news/amazon-unveils-first-fully-autonomous-mobile-robot-called-proteus

Text 2.

Instagram rolls out age verification, but not to keep children off app

Instagram might ask you to prove your age – but only in certain circumstances.

Thursday it will start testing new tools for age verification if accounts listed as younger than 18 try to change their age to over 18.

But users could still misrepresent their birth dates when setting up an account. The change comes as Instagram's parent company, Meta, faces increased scrutiny over the presence of children younger than 13 on its apps. A federal privacy law prohibits collecting data on people under 13 without parental permission, but only if the platforms know it's happening, which lets companies look the other way, privacy advocates claim. State and federal legislators have proposed a variety of bills – including the Kids Online Safety Act in the Senate, the Children and Teens' Online Privacy Protection Act in the Senate and the Age-Appropriate Design Code Act in California – which would significantly increase tech companies' legal responsibility to protect children online.

Thursday's change focuses not on keeping young children off Instagram, said Meta's director of data governance and public policy, Erica Finkle, but on making sure teen accounts reflect true ages and receive the right safeguards. Teen accounts can't receive direct messages from adults they're not connected with, for example, and they're protected from certain types of ad targeting. Instagram also recently

started nudging teen accounts to turn on the “take a break” feature, which reminds them to stop scrolling the platform’s infinite-scroll feeds.

“I’ve been working with policymakers, with regulators, and we all share the same goals,” Finkle said. “What’s really driving all of this, regardless of the specific piece of legislation, is ensuring that teens have appropriate experiences online and are safe and protected.”

Adult accounts who attempt to change their age to under 18 already had to provide a form of ID for verification. Now, the company is experimenting with new ways to verify age. People can still send an accepted form of ID, which Meta says it will store securely and delete within 30 days. They can ask three Instagram friends to vouch for their age — those friends must be adults, must respond within three days and can’t be vouching for anyone else. Or, they can submit a “video selfie” and Meta will use AI from digital-identity company Yoti to guess their age, the company says. Yoti says its AI is trained on images of faces from people around the world who gave their “explicit, revocable” consent.

For parents and others concerned about young people on Instagram, the move feels incomplete, says Irene Ly, policy counsel for Common Sense Media, an organization that advocates for child-friendly media policies. In 2021, leaked documents suggested Meta had buried internal research on Instagram’s harmful effects on young women, according to whistleblower and former Meta employee Frances Haugen.

“While it is good Instagram is trying to experiment with verifying users’ ages with technology that would not compromise users’ privacy, Instagram must still make design changes to the platform so it is safer for young users,” Ly said. “This will not address the fact that their algorithm is amplifying harmful content promoting disordered eating, self-harm, or substance abuse.”

Meta spokeswoman Faith Eischen pointed to the app’s existing guidelines for algorithmically recommended content and its sensitive content control, which lets people reduce or increase the amount of guns, drugs, bare bodies and violence they see on Instagram.

Even the idea that Instagram's age-guessing AI protects privacy is up for debate, says Mutale Nkonde, founder of algorithmic justice organization AI for the People and member of TikTok's content moderation advisory board. Meta is notorious for sharing data internally to build detailed profiles on its users, she said – how can people be sure Meta and Yoti aren't using their video selfies for any purpose besides age verification? Furthermore, Nkonde said one reason Instagram can run its age-verification test in the United States is because, unlike in the European Union, companies can collect data from people younger than 16. She asked: Why are teenagers the guinea pigs for Meta's face-scanning partnership?

"Children are a protected class, so every precaution should be taken to protect them rather than use them to test a new technology," she said. "This is an inappropriate use case."

Eischen said Yoti is a respected company with internal research that supports the accuracy and fairness of its AI. The system never recognizes faces, only estimates their ages, she noted. And Meta will never use data it collects for age verification for any other purpose, she said.

https://www.washingtonpost.com/technology/2022/06/23/instagram-age-verification/

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text 2 into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. robot vacuum
2. data governance
3. scrutiny over
4. ergonomic position

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Amazon Unveils in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Adult accounts who attempt to change their age to under 18 already had to provide a form of ID for verification. Now, the company is experimenting with new ways to verify age. People can still send an accepted form of ID, which Meta says it will store securely and delete within 30 days. They can ask three Instagram friends to vouch for their age – those friends must be adults, must respond within three days and can't be vouching for anyone else. Or, they can submit a "video selfie" and Meta will use AI from digital-identity company Yoti to guess their age, the company says.

2. Thursday's change focuses not on keeping young children off Instagram, said Meta's director of data governance and public policy, Erica Finkle, but on making sure teen accounts reflect true ages and receive the right safeguards. Teen accounts can't receive direct messages from adults they're not connected with, for example, and they're protected from certain types of ad targeting. Instagram also recently started nudging teen accounts to turn on the "take a break" feature, which reminds them to stop scrolling the platform's infinite-scroll feeds.
3. A federal privacy law prohibits collecting data on people under 13 without parental permission, but only if the platforms know it's happening, which lets companies look the other way, privacy advocates claim. State and federal legislators have proposed a variety of bills – including the Kids Online Safety Act in the Senate, the Children and Teens' Online Privacy Protection Act in the Senate and the Age-Appropriate Design Code Act in California – which would significantly increase tech companies' legal responsibility to protect children online.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 14

Task I. *Read the texts. Translate each instance into Ukrainian.*

Computer Simulations of Proteins Help Unravel Why Chemotherapy Resistance Occurs

Understanding why and how chemotherapy resistance occurs is a major step toward optimizing treatments for cancer.

A team of scientists including Markus Seeliger, from the Stony Brook Cancer Center and Renaissance School of Medicine at Stony Brook University, believe they have found a new process through which drug resistance happens. They are using a computer simulation model that is helping them understand exactly how molecules interact with the cancer drug Imatinib (known as Gleevec) in the chemotherapy resistant process. Imatinib treats chronic myeloid leukemia (CML) highly effectively, yet many late-stage patients experience drug resistance, which renders the drug minimally effective at that stage.

The research is highlighted in a paper published in Angewandte Chemie, a top chemistry journal, and builds upon previous research detailed in 2021 in PNAS.

Imatinib inhibits the BCR-Abl protein kinase, an overly active cellular signaling machinery in CML. In the PNAS study, researchers showed that variations in the building plan of the kinase can make it harder for Imatinib to bind to the kinase and also speed up drug release from the kinase. In the Angewandte Chemie paper, the research team took the computational methodology – developed by co-author Pratyush Tiwary from the University of Maryland – that enabled them to study the very slow release of Imatinib from the kinase.

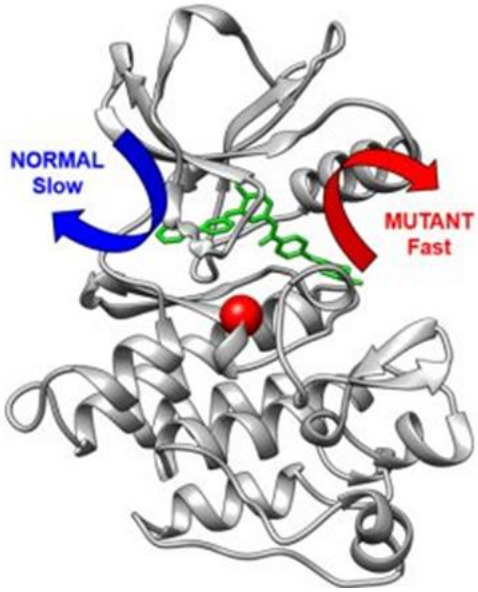
“This method in itself is a major technical achievement that extends computational abilities for drug resistance research, and importantly led to us being able to predict how rapidly healthy and mutant proteins would release this drug,” said Seeliger, associate professor in the Department of Pharmacological Sciences. “For the first time, we could see the release of a drug from a protein in such detail and

accuracy. Moreover, we could show that the mutation changes fundamentally within the exit route of the drug from the protein.

Three-dimensional structure of the cancer drug target Abl kinase (grey) bound to the anti-cancer drug Imatinib. Normally, the drug exits slowing via the blue arrow. A modification in the kinase (red sphere) causes the drug to exit via a fast route (red arrow).

"This is important since the speed of the drug release may be just as important for the therapeutic effect of a drug as how tightly a drug binds to the protein."
Seeliger further explains that the method could provide a foundation for understanding the molecular mechanisms behind chemotherapy resistance.

More broadly, the implications of what they discovered are that if scientists can understand how drugs are released from their proteins, they may be able to design drugs with a slower release and higher therapeutic impact.



Additionally, if rapid drug release could cause drug resistance, and clinicians can show this is happening, they may be able to re-activate the drug effectiveness by asking the patient to take the drug more frequently.

The groundwork for the mutation testing via the computational method was outlined in the PNAS paper. Seeliger and colleagues tested how Imatinib binds to mutations in patients with imatinib-resistant CML. They found that the majority of mutations readily bind to Imatinib, so that posed the question just how do these

mutations cause resistance in patients? The researchers then identified several mutants that bound Imatinib readily but they release the drug much faster.

After identifying these mutants with a faster drug release, the team used nuclear magnetic resonance (NMR) and molecular dynamics to link the protein to drug disassociation – underlying the importance of drug disassociation kinetics for drug efficacy. This enabled them to identity a novel mechanism of Imatinib resistance.

The work resulting in the paper published in PNAS involved the collaborative efforts of Seeliger and his colleagues at Stony Brook, and researchers at Memorial Sloan Kettering Cancer Center and at Goethe University of Frankfurt, Germany.

Research that resulted in the more recent paper was led by Tiwary and colleagues at the University of Maryland, in collaboration with Seeliger and scientists at the Broad Institute at MIT and Harvard University.

https://news.stonybrook.edu/university/computer-simulations-of-proteins-help-unravel-why-chemotherapy-resistance-occurs-2/

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. chemotherapy resistant process
2. rapid drug
3. nuclear magnetic resonance (NMR)
4. drug efficacy

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Computer Simulations in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. After identifying these mutants with a faster drug release, the team used nuclear magnetic resonance (NMR) and molecular dynamics to link the protein to drug disassociation – underlying the importance of drug disassociation kinetics for drug efficacy.
2. Three-dimensional structure of the cancer drug target Abl kinase (grey) bound to the anti-cancer drug Imatinib. Normally, the drug exits slowing via the blue arrow. A modification in the kinase (red sphere) causes the drug to exit via a fast route (red arrow).

3. In the PNAS study, researchers showed that variations in the building plan of the kinase can make it harder for Imatinib to bind to the kinase and also speed up drug release from the kinase. In the Angewandte Chemie paper, the research team took the computational methodology – developed by co-author Pratyush Tiwary from the University of Maryland – that enabled them to study the very slow release of Imatinib from the kinase.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 15

Task I. Read the texts. Translate each instance into Ukrainian.

Text 1.

Sweden's Einride to Test Autonomous Trucks on U.S. Roads

The company will put its chunky, self-driving vehicles on short runs between warehouses in Tennessee under an agreement with GE Appliances

An autonomous, electric freight truck at a logistics facility operated by GE Appliances in Louisville, Ky.

Swedish autonomous-truck startup Einride AB will test its self-driving freight vehicles on public roads in the U.S. in an operation with GE Appliances after getting approval from federal regulators.

Einride plans to put one of its chunky electric vehicles, which have no cabs for drivers, on a one-mile stretch of road between two warehouses in Tennessee for GE Appliances, a subsidiary of home appliances company Haier. The National Highway Traffic Safety Administration recently greenlighted the company's test run.

"This is a step-by-step approach, and this is a major step forward, in that it's actually now on public roads," said Robert Falck, chief executive of the six-year-old Stockholm-based company.

Einride is joining a growing field of autonomous-truck startups in the race to get their technology on the road and bringing in revenue. Companies including San Diego-based TuSimple Holdings Inc., Pittsburgh-based Aurora Innovation Inc., and Waymo LLC, a division of Google parent Alphabet Inc., have announced tests of their driverless-truck technology in commercial operations carrying freight.

Steve Viscelli, a University of Pennsylvania fellow and lecturer and trucking-industry expert who is on an advisory council for Aurora, said the freight sector is moving more rapidly toward autonomous transport than the passenger-car business, in part because the technology can reduce costs and simplify operations for commercial trucking companies.

"Trucks will be first, without a doubt, in the true driverless system, partly for the economics of it," Mr. Viscelli said. "Right now, we have huge limitations on how long a truck can move because it's piloted by a human being, who needs to sleep and use the bathroom and take 10-hour mandatory breaks and other things."

Einride calls its stubby, snub-nosed vehicles Pods. They have room for about 10 pallets of freight, or about 57,000 pounds. There is no onboard driver and they are managed by remote operators, who may monitor several vehicles at a time, according to Einride. Those remote operators take actions drivers would typically make, such as calling someone when a vehicle gets stuck at a gate, Mr. Falck said.

Einride's pilot program, which will run for two weeks in the third quarter of 2022, will put the Pod on public roads that carry trucks and cars.

As driverless vehicle companies Aurora and Embark are making their stock-market debut this month, WSJ's George Downs spoke with the CEOs about why they're focusing on autonomous trucks and whether that could spell a solution for the U.S. truck-driver shortage.

Einride last year signed an agreement to deliver 300 electric trucks to shipping giant A.P. Moller-Maersk A/S.

Many of the autonomous trucks other companies are developing aren't electric. That is partly because the return on investment isn't there right now for the distance they would drive versus how much time they would have to spend charging, Mr. Viscelli said.

One challenge facing electric vehicle companies in the U.S. is the lack of charging infrastructure. That shouldn't be a concern on the short stretch Einride will use in Tennessee, but Mr. Falck said his company is prepared to build out the infrastructure it needs to operate its vehicles.

https://www.wsj.com/articles/swedens-einride-to-test-autonomous-trucks-on-u-s-roads-11655985601

Text 2

Quantum network nodes with warm atoms

Communication networks need nodes at which information is processed or rerouted. Physicists at the University of Basel have now developed a network node for quantum communication networks that can store single photons in a vapor cell and pass them on later.

In quantum communication networks, information is transmitted by single particles of light (photons). At the nodes of such a network buffer elements are needed which can temporarily store, and later re-emit, the quantum information contained in the photons.

Researchers at the University of Basel in the group of Prof. Philipp Treutlein have now developed a quantum memory that is based on an atomic gas inside a glass cell. The atoms do not have to be specially cooled, which makes the memory easy to produce and versatile, even for satellite applications. Moreover, the researchers have realized a single photon source which allowed them to test the quality and storage time of the quantum memory. Their results were recently published in the scientific journal PRX Quantum.

Warm atoms in vapor cells

“The suitability of warm atoms in vapor cells for quantum memories has been investigated for the past twenty years”, says Gianni Buser, who worked on the experiment as a PhD student. “Usually, however, attenuated laser beams - and hence classical light - were used”. In classical light, the number of photons hitting the vapor cell in a certain period follows a statistical distribution; on average it is one photon, but sometimes it can be two, three or none.

Further information

To test the quantum memory with “quantum light” – that is, always precisely one photon – Treutlein and his co-workers developed a dedicated single photon source that emits exactly one photon at a time. The instant when that happens is heralded by a second photon, which is always sent out simultaneously with the first one. This allows the quantum memory to be activated at the right moment.

The single photon is then directed into the quantum memory where, with the help of a control laser beam, the photon causes more than a billion rubidium atoms to take on a so-called superposition state of two possible energy levels of the atoms. The photon itself vanishes in the process, but the information contained in it is transformed into the superposition state of the atoms. A brief pulse of the control

laser can then read out that information after a certain storage time and transform it back into a photon.

Reducing read-out noise

"Up to now, a critical point has been noise – additional light that is produced during the read-out and that can compromise the quality of the photon", explains Roberto Mottola, another PhD student in Treutlein's lab. Using a few tricks, the physicists were able to reduce that noise sufficiently so that after storage times of several hundred nanoseconds the single photon quality was still high.

"Those storage times are not very long, and we didn't actually optimize them for this study", Treutlein says, "but already now they are more than a hundred times longer than the duration of the stored single photon pulse". This means that the quantum memory developed by the Basel researchers can already be employed for interesting applications. For instance, it can synchronize randomly produced single photons, which can then be used in various quantum information applications.

https://www.unibas.ch/en/News-Events/News/Uni-Research/Quantum-network-nodes-with-warm-atoms.html

Task II.

➤ *Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text 2 into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

1. quantum light
2. vapor cell
3. photon pulse
4. laser beam
5. statistical distribution

➤*Analyse the meaning of the different expressions.*

➤*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. Many of the autonomous trucks other companies are developing aren't electric. That is partly because the return on investment isn't there right now for the distance they would drive versus how much time they would have to spend charging, Mr. Viscelli said.

2. Researchers at the University of Basel in the group of Prof. Philipp Treutlein have now developed a quantum memory that is based on an atomic gas inside a glass cell. The atoms do not have to be specially cooled, which makes the memory easy to produce and versatile, even for satellite applications. Moreover, the researchers have

realized a single photon source which allowed them to test the quality and storage time of the quantum memory. Their results were recently published in the scientific journal PRX Quantum.

3. The single photon is then directed into the quantum memory where, with the help of a control laser beam, the photon causes more than a billion rubidium atoms to take on a so-called superposition state of two possible energy levels of the atoms. The photon itself vanishes in the process, but the information contained in it is transformed into the superposition state of the atoms. A brief pulse of the control laser can then read out that information after a certain storage time and transform it back into a photon.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 16

Task I. *Read the texts. Translate each instance into Ukrainian.*

Strava app flaw revealed runs of Israeli officials at secret bases

A security vulnerability in the fitness app Strava allowed suspicious figures to identify and track security personnel working at secretive bases in Israel, a disinformation watchdog says.

FakeReporter found that by uploading fake running "segments" a user could learn the identities and past routes of others active in the area, even if they had the strongest privacy settings.

Information about 100 individuals who exercised at six bases was viewable.

Strava said it had addressed the issue.

The Israeli military said it was "aware of the evolving threats in cyberspace".

"In order to handle these threats, and in light of previous events such as the one mentioned, the rules and regulations are regularly reiterated and reinforced among those serving in sensitive positions," it added.

This is not the first time that Strava's tracking features have sparked such security concerns.

In 2018, the company published a global "heatmap" that revealed the exercise routes of people at military bases around the world, including US facilities in Syria and Afghanistan.

San Francisco-based Strava is used by more than 95 million people in 195 countries.

Its app takes data, including GPS co-ordinates, from a person's mobile phone or wearable fitness device to track their exercise activity.

People are able to upload their running and cycling times and compare their performances with others who followed the same routes.

FakeReporter, an Israeli group that combats malicious online activity, reported that a suspicious user named "Ez Shehl" had exploited these functions to upload fake

GPS data to create route segments inside secret facilities associated with Israel's military, the Mossad intelligence agency and the Shin Bet internal security service.

The segments featured straight GPS lines, no times, and unrealistic pacing, such as covering 500m in 0 seconds.

The timings and personal details – including photos, home addresses and the identities of family members – of other users who ran the same segments were subsequently revealed on the Strava scoreboard, even if they had their accounts set to "private".

A senior defence official identified as "N" was one of at least 100 Israeli individuals affected by the vulnerability, according to FakeReporter. It posted screenshots showing runs from their home and inside various air force bases in Israel, as well as runs in Ukraine.

FakeReporter said it had told Israeli authorities about the security breach as soon as it became aware and that it had contacted Strava after receiving their approval.

"Despite past revelations, it does not appear that Israeli security agencies have caught up," Achiya Schatz, the watchdog's director, said in a statement. "Although Strava made significant updates to its privacy settings, confused users might still be exposed publicly, even if their profiles were set to 'private'."

"By exploiting the capability to upload engineered files, revealing the details of users anywhere in the world, hostile elements have taken one alarming step closer to exploiting a popular app in order to harm the security of citizens and countries alike."

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. security vulnerability
2. evolving threats in cyberspace
3. malicious online activity
4. security breach
5. hostile elements

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Strava app flaw revealed runs of Israeli officials at secret bases in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1. FakeReporter, an Israeli group that combats malicious online activity, reported that a suspicious user named "Ez Shehl" had exploited these functions to upload fake GPS data to create route segments inside secret facilities associated with Israel's military, the Mossad intelligence agency and the Shin Bet internal security service.

2. The timings and personal details - including photos, home addresses and the identities of family members - of other users who ran the same segments were subsequently revealed on the Strava scoreboard, even if they had their accounts set to "private".
3. "Despite past revelations, it does not appear that Israeli security agencies have caught up," Achiya Schatz, the watchdog's director, said in a statement. "Although Strava made significant updates to its privacy settings, confused users might still be exposed publicly, even if their profiles were set to 'private'."

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 17

Task I. *Read the texts. Translate each instance into Ukrainian.*

Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands

After a Florida man was accused of vehicular homicide, his lawyer used Clearview AI's facial recognition software to prove his innocence. But other defense lawyers say Clearview's offer rings hollow.

The police believed Andrew Grantt Conlyn had been driving during a car crash that killed his friend. Facial recognition software helped find the witness who knew Mr. Conlyn had been in the passenger’s seat.

The police believed Andrew Grantt Conlyn had been driving during a car crash that killed his friend. Facial recognition software helped find the witness who knew Mr. Conlyn had been in the passenger's seat.

It was the scariest night of Andrew Grantt Conlyn's life. He sat in the passenger seat of a two-door 1997 Ford Mustang, clutching his seatbelt, as his friend drove approximately 100 miles per hour down a palm-tree-lined avenue in Fort Myers, Fla. His friend, inebriated and distraught, occasionally swerved onto the wrong side of the road to pass cars that were complying with the 35-m.p.h. speed limit. "Someone is going to die tonight," Mr. Conlyn thought. And then his friend hit a curb and lost control of the car. The Mustang began spinning wildly, hitting a light pole and three palm trees before coming to a stop, the passenger's side against a tree.

At some point, Mr. Conlyn blacked out. When he came to, his friend was gone, the car was on fire and his seatbelt buckle was jammed. Luckily, a good Samaritan intervened, prying open the driver's door and pulling Mr. Conlyn out of the burning vehicle.

Mr. Conlyn didn't learn his savior's name that Wednesday night in March 2017, nor did the police, who came to the scene and found the body of his friend, Colton Hassut, in the bushes near the crash; he had been ejected from the car and had died. In the years that followed, the inability to track down that good Samaritan derailed Mr. Conlyn's life. If Clearview AI, which is based in New York, hadn't granted his lawyer special access to a facial recognition database of 20 billion faces, Mr. Conlyn might have spent up to 15 years in prison because the police believed he had been the one driving the car.

Before crashing on a main road in Fort Myers, Fla., the vehicle Mr. Conlyn was traveling in was going about 100 m.p.h.

Before crashing on a main road in Fort Myers, Fla., the vehicle Mr. Conlyn was traveling in was going about 100 m.p.h.Credit...Scott McIntyre for The New York Times

For the last few years, Clearview AI's tool has been largely restricted to law enforcement, but the company now plans to offer access to public defenders. Hoan Ton-That, the chief executive, said this would help "balance the scales of justice," but critics of the company are skeptical given the legal and ethical concerns that swirl around Clearview AI's groundbreaking technology. The company scraped billions of faces from social media sites, such as Facebook, LinkedIn and Instagram, and other parts of the web in order to build an app that seeks to unearth every public photo of a person that exists online.

"I think it's a rare situation in which most defense attorneys would want to use it," said Jerome Greco, who oversees a forensics technology lab at the Legal Aid Society, in New York City. "This is mostly being done as a P.R. stunt to try to push back against the negative publicity that Clearview has about its tool and how it's being used by law enforcement."

Civil liberty advocates believe Clearview's expansive database of photos violates privacy, because the images, though public on the web, were collected without people's consent. The tool can unearth photos that people did not post themselves and may not even realize are online. Critics say it puts millions of law-

abiding people in a perpetual lineup for law enforcement, which is particularly troubling given broader concerns about the accuracy of automated facial recognition.

Clearview AI has been the target of multiple lawsuits, and its database has been declared illegal in Canada, Australia, Britain, France, Italy and Greece. It faces multiple multimillion-dollar fines in Europe.

The controversy around Clearview AI aside, some public defenders see potential benefits in having access to the company's technology — and, in the case of Mr. Conlyn, it played an indispensable role.

"There is nothing worse than being held responsible for a crime you did not commit," said Mr. Ton-That of Clearview. "I was honored to assist."

Lawyers used an image from the body-camera footage taken at the scene of the accident to search Clearview AI’s database of 20 billion faces.

In November 2019, almost three years after the car accident, Mr. Conlyn was charged with vehicular homicide. Prosecutors said that Mr. Conlyn had been the one recklessly driving Mr. Hassut's Mustang that night and that he was responsible for his friend's death.

Public Defenders: Clearview AI's facial recognition software has been largely restricted to law enforcement. Now, the company plans to offer access to defense lawyers.

Creating Art: Artwork made with artificial intelligence won a prize at the Colorado State Fair's art competition — and set off fierce backlash about how art is generated.

Making Strides: We're in a golden age of progress in artificial intelligence. It's time to start taking its potential and risks seriously, our technology columnist writes.

Are These People Real?: We created our own artificial-technology system to understand how easy it is for a computer to generate fake faces.

Mr. Conlyn vehemently denied this, but his version of events was hard to corroborate without the man who had pulled him from the passenger seat of the burning car. The police had talked to the good Samaritan that night, and recorded the conversation on their body cameras.

“The driver got ejected out of one of the windows. He’s in the bushes,” said the man, who had tattoos on his left arm and wore an orange tank top with “Event Security” emblazoned on it. “I just pulled out the passenger. He’s over there. His name is Andrew.”

The police did not ask for the man’s name or contact information. The good Samaritan and his girlfriend, who was with him that night, drove off in a black pickup truck.

The body-camera footage did not seem to hold much weight with the prosecution.

“There was contradicting evidence,” said Samantha Syoen, the communications director for the state attorney’s office.

Witnesses who had arrived late to the scene saw Mr. Conlyn pulled out of the driver’s side of the car. Mr. Conlyn said, and police body camera footage appeared to confirm, that the passenger’s side door had been against a tree, which was why he’d had to be rescued from the other side. The police found his blood on the passenger’s side of the car but also on the driver’s side airbag.

An accident reconstruction expert hired by the prosecution said the injuries to the right side of Mr. Conlyn’s body could have come from the center console, not the passenger door. After Mr. Hassut’s father sued Mr. Conlyn in civil court in 2019, for the wrongful death of his son, Mr. Conlyn’s insurance agency settled the suit, unable to prove that Mr. Conlyn had not been driving the car.

Mr. Conlyn, who is now 32, was a carpenter without much income. His lawyers, whose fees were paid by his family, filed an application with the court to declare him indigent so that the state would cover any other expenses he incurred to defend himself. The experts his lawyers hired struggled to gather evidence. It had been years since the accident; the Mustang had been flattened into a pancake and left out in the elements. His legal team became obsessed with finding the man in the orange tank top.

Mr. Conlyn, center, with his lawyers, Christopher O'Brien, left, and Patrick Bailey. After learning that facial recognition technology might help his client, Mr. Bailey wrote an imploring letter to Clearview AI.

Mr. Conlyn, center, with his lawyers, Christopher O'Brien, left, and Patrick Bailey. After learning that facial recognition technology might help his client, Mr. Bailey wrote an imploring letter to Clearview AI.

They asked for help from the public, providing an image of the man from the body camera to local news outlets and putting it on social media. They made fliers. One of Mr. Conlyn's lawyers, Patrick Bailey, looked at the websites of local tattoo parlors. He searched nearby streets for a black pickup truck like the one at the scene that night and got access to county vehicle ownership records for black Ford Rangers, the model of truck he thought the man had been driving. He searched the names of over 1,000 Ranger owners on social media to see if any of them looked like the good Samaritan or his girlfriend. He did not know that the truck in question was actually a Nissan Frontier.

"We spent hundreds of hours looking for him," Mr. Bailey said.

Mr. Bailey heard about facial recognition technology in late 2021 and began to research options for using it in Mr. Conlyn's case. He tried a free facial recognition site called PimEyes, but the dark screenshot from the body camera footage didn't get any good hits. In June, Mr. Bailey wrote an imploring letter to Mr. Ton-That, the chief executive of Clearview AI. He knew that the company was popular with local police and federal agencies, and that it claimed to have superior technology.

"I am aware that your company only provides facial recognition software to law enforcement agencies," Mr. Bailey wrote. "What happens if those same agencies refuse to use Clearview AI's important and powerful software to identify an otherwise unidentified eyewitness that could clear an innocent person?"

According to internal Clearview documents obtained by BuzzFeed, the Fort Myers Police Department had trial access to Clearview's technology at some point before February 2020, running more than a dozen searches, but the department had

not signed up for a paid account. A spokeswoman for the department declined to comment on the case.

Creative Thinking

Hoan Ton-That, the chief executive of Clearview AI, said allowing public defenders to use facial recognition software would help “balance the scales of justice.”

Hoan Ton-That, the chief executive of Clearview AI, said allowing public defenders to use facial recognition software would help “balance the scales of justice.”Credit...Andres Kudacki for The New York Times

Mr. Ton-That was accustomed to people asking to use his company’s tool.

“We have had a decent number of random requests,” he said. “Just random people saying, ‘Can you help find my long-lost daughter?’”

Typically, Clearview tells those people to contact local law enforcement. But Mr. Ton-That decided to grant Mr. Bailey’s request, and asked that he talk to the news media about it if the search worked.

This required some creative thinking. Clearview had recently settled a class-action lawsuit over privacy violations in Illinois by agreeing not to provide its tool to private individuals and companies, with the exception of financial institutions. Mr. Bailey was a private lawyer, but, because of Mr. Conlyn’s indigent status, he was also a subcontractor to the Justice Administrative Commission, a Florida state agency. In consultation with Clearview’s lawyers, Mr. Ton-That decided that this meant Clearview could allow Mr. Bailey to use the tool without violating the legal agreement.

“Within two seconds, I found a picture of him at some club in Tampa,” Mr. Bailey said.

The Clearview match looked identical to the man on the body camera, down to tattoos on his left arm. The website on which the photo appeared didn’t give the man’s name, but it did include the name of a man who had been with him at the club that night. Mr. Bailey contacted that person via Facebook and soon had the name of the man who had rescued Mr. Conlyn from the burning car five years earlier: Vince

Ramirez, a construction worker who had lived in Fort Myers for only a few months before moving to St. Augustine, in northern Florida.

When Mr. Bailey reached Mr. Ramirez by phone, the man remembered the night vividly. He and his girlfriend were driving home when a car sped past them. A few minutes later, they came upon the same car on fire. Mr. Ramirez pulled over and got out.

“I was afraid the car was going to blow up,” Mr. Ramirez, 31, said in a phone interview. “I pulled open the door, jumped in and pulled him out of the passenger’s seat. It was a real adrenaline rush.”

When the police arrived, Mr. Ramirez answered their questions. But no one told him to stay, so he and his girlfriend went home. For years afterward, he told the story to family and friends, but he never realized that people were trying to find him until he heard from Mr. Bailey.

“The way I was found, it kind of shocked me,” Mr. Ramirez said. He had heard of facial recognition technology but had thought it was used only to find criminals.

For years, Vince Ramirez told of pulling a man from a burning vehicle after a car accident. He had no idea that the man’s lawyers were searching for him.

For years, Vince Ramirez told of pulling a man from a burning vehicle after a car accident. He had no idea that the man’s lawyers were searching for him.Credit...Todd Anderson for The New York Times

“I’m grateful they did find me,” he added. “I didn’t want some innocent person to be sent to prison for 15 years for something he didn’t do.”

The prosecutor in the case deposed Mr. Ramirez on a Thursday afternoon in July, and dropped the vehicular homicide case against Mr. Conlyn that evening.

“That just goes to show you how important he was in this case,” Mr. Bailey said.

Facial recognition software like Clearview’s should “be available to the defense bar without, you know, too many hoops to jump through,” Mr. Bailey added. “Why is it so difficult for us to use this to exonerate somebody?”

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text 3 into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

Recognition
Public defenders
Innocent
Flattened into

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic Clearview AI, Used by Police to Find Criminals, Is Now in Public Defenders' Hands. *Translate them. Do not use the dictionary.*

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

4. “I am aware that your company only provides facial recognition software to law enforcement agencies,” Mr. Bailey wrote. “What happens if those same agencies refuse to use Clearview AI’s important and powerful software to identify an otherwise unidentified eyewitness that could clear an innocent person?”
5. This required some creative thinking. Clearview had recently settled a class-action lawsuit over privacy violations in Illinois by agreeing not to provide its tool to private individuals and companies, with the exception of financial institutions. Mr. Bailey was a private lawyer, but, because of Mr. Conlyn’s indigent status, he was also a subcontractor to the Justice Administrative Commission, a Florida state agency. In consultation with Clearview’s lawyers, Mr. Ton-That decided that this meant Clearview could allow Mr. Bailey to use the tool without violating the legal agreement.
6. For years, Vince Ramirez told of pulling a man from a burning vehicle after a car accident. He had no idea that the man’s lawyers were searching for him.

   For years, Vince Ramirez told of pulling a man from a burning vehicle after a car accident. He had no idea that the man’s lawyers were searching for him.Credit...Todd Anderson for The New York Times

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 18

Task I.

Read the text. Translate each instance into Ukrainian.

New Customers?

The case inspired Mr. Ton-That to start offering Clearview's tool to public defenders and lawyers contracted by the government to represent indigent clients.

"It would be free slash very inexpensive," Mr. Ton-That said.

The company now offers them 30-day free trials, as it does its law enforcement customers. It has charged police departments as little as $2,000 for a year's access to its service, though Clearview says it has raised its prices.

"This really levels the playing field," Mr. Ton-That said. "People would think of the technology a lot differently if public defenders had access to it as well."

He said that access would "build more trust in the system."

But public defenders, and experts in criminal defense, are skeptical. It might help them in some cases but at what cost?

Jumana Musa is the director of the Fourth Amendment Center at the National Association of Criminal Defense Lawyers, where she works to keep defense lawyers informed about the newest surveillance tools used by law enforcement.

"They can offer it to everybody," Ms. Musa said. "It is not going to wipe away the ethical concerns about the way in which they went about building this tool. The second thing it's not going to do is make us feel comfortable with the secrecy around how this tool works."

The problem with facial recognition, beyond bias concerns around how accurate it is across race, age and gender, Ms. Musa said, is a lack of transparency from law enforcement about how often it is used. Because any match the technology returns is

considered only a lead, and not probable cause for an arrest, the software's use is often not disclosed to defendants or their counsel, Ms. Musa said, which makes it harder to defend against.

"You don't address issues in a broken criminal legal system by layering technology on them," she said.

Mr. Greco, with the Legal Aid Society, said his organization was unlikely to use Clearview. He believes the company is offering its facial recognition tool to defense lawyers "in order to gain some form of legitimacy in its use in the criminal legal system."

"I'm hesitant to begrudge any defense attorney from doing what they think is best on an individual case for an individual client, because I do believe that is our obligation," Mr. Greco said. "At the same time, I don't think I can endorse the use of Clearview."

But Jonathan Lyon, who is the investigator resource coordinator at the National Association for Public Defense and who runs a website called Internet Sleuth, predicted "huge interest" in the technology. He said the facial recognition that Clearview offered would be a helpful tool, particularly for lawyers who were trying to track down people who had witnessed a fight or attended a party where criminal activity had occurred.

"From an investigator's standpoint, any tool I can get my hands on, I want," Mr. Lyon said. "Particularly if the other side has it. That, to me, is a win."

(https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results by other students or by studying other translators.*

Task III

➤*Translate the following English terms:*

- public defenders
- law enforcement customers
- facial recognition
- lack of transparency
- disclose to defendants

➤*Analyse the meaning of the different expressions.*

➤*If any of of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translations in your languages would you suggest for these words?*

Task IV

Underline the words to the topic of new customers in the passage. Translate them. Do not use the dictionary.

Task V

Skim-read the passages below. Then write one sentence saying what they are about. Do not look back at the text use your own words.

1. The company now offers them 30-day free trials, as it does its law enforcement customers. It has charged police departments as little as $2,000 for a year's access to its service, though Clearview says it has raised its prices.

"This really levels the playing field," Mr. Ton-That said. "People would think of the technology a lot differently if public defenders had access to it as well."

2. He said that access would "build more trust in the system."

"They can offer it to everybody," Ms. Musa said. "It is not going to wipe away the ethical concerns about the way in which they went about building this tool. The second thing it's not going to do is make us feel comfortable with the secrecy around how this tool works."

The problem with facial recognition, beyond bias concerns around how accurate it is across race, age and gender, Ms. Musa said, is a lack of transparency from law enforcement about how often it is used. Because any match the technology returns is considered only a lead, and not probable cause for an arrest, the software's use is often not disclosed to defendants or their counsel, Ms. Musa said, which makes it harder to defend against.

"You don't address issues in a broken criminal legal system by layering technology on them," she said.

3. But Jonathan Lyon, who is the investigator resource coordinator at the National Association for Public Defense and who runs a website called Internet Sleuth, predicted "huge interest" in the technology. He said the facial recognition that Clearview offered would be a helpful tool, particularly for lawyers who were trying to track down people who had witnessed a fight or attended a party where criminal activity had occurred.

"From an investigator's standpoint, any tool I can get my hands on, I want," Mr. Lyon said. "Particularly if the other side has it. That, to me, is a win."

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 19

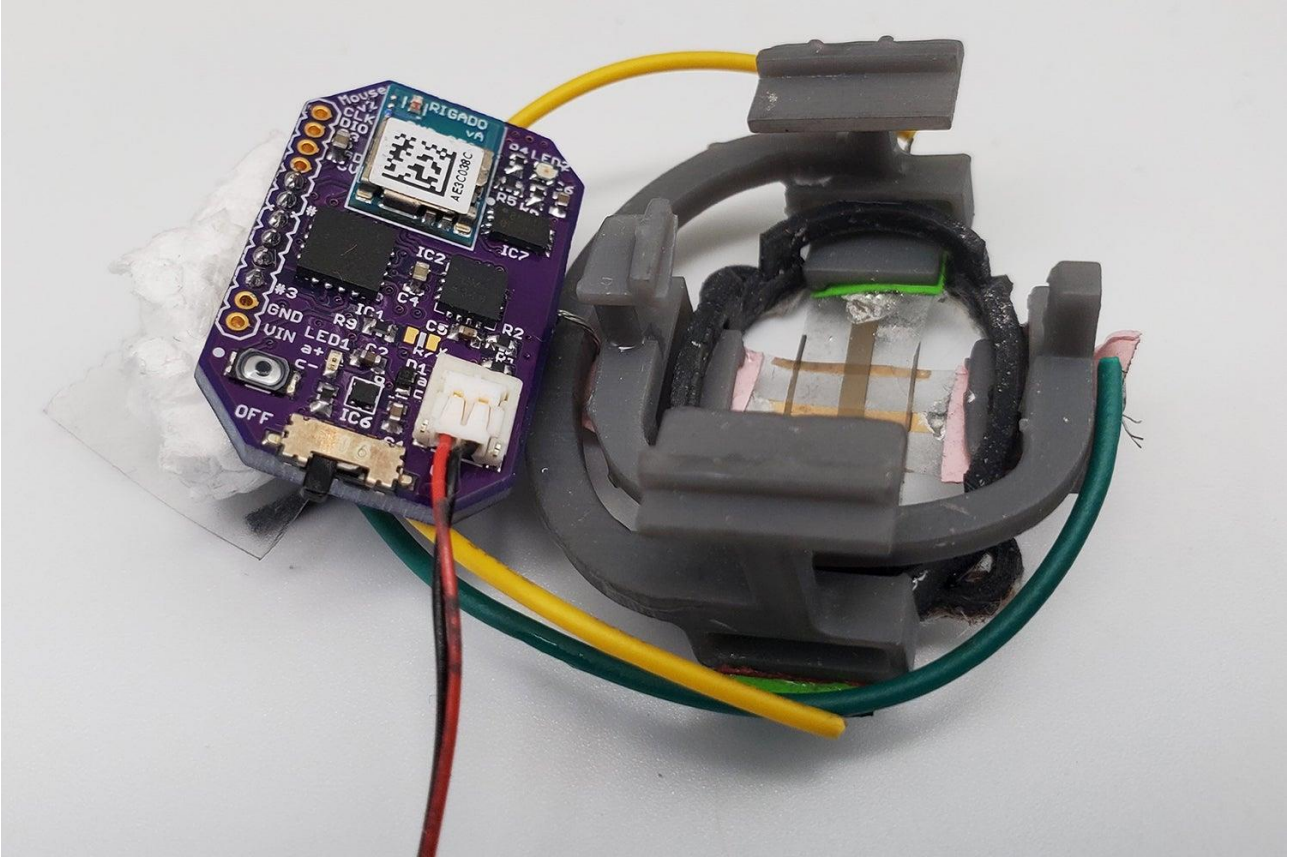
Task I.

Read the texts. Translate each instance into Ukrainian.

Stanford engineers develop new wearable device to monitor tumor size

Electronically sensitive, skin-like membrane can measure changes in tumor size to the hundredth of a millimeter. It represents a new, faster, and more accurate approach to screen cancer drugs.

Engineers at Stanford University have created a small, autonomous device with a stretchable and flexible sensor that can be adhered to the skin to measure the changing size of tumors below. The non-invasive, battery-operated device is sensitive to one-hundredth of a millimeter (10 micrometers) and can beam results to a smartphone app wirelessly in real time with the press of a button.



The FAST system measures tumor size regression and is a new way to test the efficacy of cancer drugs. (Image credit: Alex Abramson, Bao Group, Stanford University)

In practical terms, the researchers say, their device – dubbed FAST for "Flexible Autonomous Sensor measuring Tumors" – represents a wholly new, fast, inexpensive, hands-free, and accurate way to test the efficacy of cancer drugs. On a grander scale, it could lead to promising new directions in cancer treatment. FAST is detailed in a paper published Sept. 16 in Science Advances.

Each year researchers test thousands of potential cancer drugs on mice with subcutaneous tumors. Few make it to human patients, and the process for finding new therapies is slow because technologies for measuring tumor regression from drug treatment take weeks to read out a response. The inherent biological variation of tumors, the shortcomings of existing measuring approaches, and the relatively small sample sizes make drug screenings difficult and labor-intensive.

"In some cases, the tumors under observation must be measured by hand with calipers," says Alex Abramson, first author of the study and a recent postdoc in the lab of Zhenan Bao, the K.K. Lee Professor in Chemical Engineering in the Stanford School of Engineering.

The use of metal pincer-like calipers to measure soft tissues is not ideal, and radiological approaches cannot deliver the sort of continuous data needed for real-time assessment. FAST can detect changes in tumor volume on the minute-timescale, while caliper and bioluminescence measurements often require weeks-long observation periods to read out changes in tumor size.

The power of gold

FAST's sensor is composed of a flexible and stretchable skin-like polymer that includes an embedded layer of gold circuitry. This sensor is connected to a small electronic backpack designed by former postdocs and co-authors Yasser Khan and Naoji Matsuhisa. The device measures the strain on the membrane – how much it stretches or shrinks – and transmits that data to a smartphone. Using the FAST

backpack, potential therapies that are linked to tumor size regression can quickly and confidently be excluded as ineffective or fast-tracked for further study.

Based on studies with mice, the researchers say that the new device offers at least three significant advances. First, it provides continuous monitoring, as the sensor is physically connected to the mouse and remains in place over the entire experimental period. Second, the flexible sensor enshrouds the tumor and is therefore able to measure shape changes that are difficult to discern with other methods. Third, FAST is both autonomous and non-invasive. It is connected to the skin – not unlike an adhesive bandage – battery operated, and connected wirelessly. The mouse is free to move unencumbered by the device or wires, and scientists do not need to actively handle the mice following sensor placement. FAST packs are also reusable, cost just $60 or so to assemble, and can be attached to the mouse in minutes.

The breakthrough is in FAST's flexible electronic material. Coated on top of the skinlike polymer is a layer of gold, which, when stretched, develops small cracks that change the electrical conductivity of the material. Stretch the material and number of cracks increases, causing the electronic resistance in the sensor to increase as well. When the material contracts, the cracks come back into contact and conductivity improves.

Both Abramson and co-author Matsuhisa, an associate professor at the University of Tokyo, characterized how these crack propagation and exponential changes in conductivity can be mathematically equated with changes in dimension and volume.

One hurdle the researchers had to overcome was the concern that the sensor itself might compromise measurements by applying undue pressure to the tumor, effectively squeezing it. To circumvent that risk, they carefully matched the mechanical properties of the flexible material to skin itself to make the sensor as pliant and as supple as real skin.

"It is a deceptively simple design," Abramson says, "but these inherent advantages should be very interesting to the pharmaceutical and oncological

communities. FAST could significantly expedite, automate, and lower the cost of the process of screening cancer therapies."

Alex Abramson is now assistant professor of chemical and biomolecular engineering at Georgia Institute of Technology; Yasser Khan is assistant professor at the Ming Hsieh Department of Electrical and Computer Engineering at the University of Southern California; and Naoji Matsuhisa is associate professor in the Institute of Industrial Science Department of Informatics and Electronics at the University of Tokyo. Additional Stanford co-authors are Carmel T. Chan, former senior scientific manager; undergraduate Alana Mermin-Bunnell; Robyn Fong, life science research professor in the Department of Cardiothoracic Surgery; Rohan Shad, former postdoctoral fellow at the School of Medicine; William Hiesinger, assistant professor of cardiothoracic surgery; and Parag Mallick, associate professor of radiology. Zhenan Bao is also a member of Stanford Bio-X, the Stanford Cardiovascular Institute, and the Wu Tsai Human Performance Alliance. Hiesinger and Mallick are also members of Stanford Bio-X and the Cardiovascular Institute.

The research was supported in part by the National Institutes of Health and the Stanford Wearable Electronics Initiative (eWEAR).

The eWEAR-TCCI awards for science writing is a project commissioned by the Wearable Electronics Initiative (eWEAR) at Stanford University and made possible by funding through eWEAR industrial affiliates program member Shanda Group and the Tianqiao and Chrissy Chen Institute (TCCI®).

(https://news.stanford.edu/press/view/45207)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results by other students or by studying other translators.*

Task III

➤*Translate the following English terms:*

- subcutaneous tumors
- metal pincer-like calipers
- enshrouds the tumor
- crack propagation
- project commissione
- industrial affiliates

➤*Analyse the meaning of the different expressions.*

➤*If any of of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translations in your languages would you suggest for these words?*

Task IV

Underline the words to the topic of Stanford engineers develop new wearable device to monitor tumor size in the passage. Translate them. Do not use the dictionary.

Task V

Skim-read the passages below. Then write one sentence saying what they are about. Do not look back at the text use your own words.

1.In practical terms, the researchers say, their device – dubbed FAST for "Flexible Autonomous Sensor measuring Tumors" – represents a wholly new, fast, inexpensive, hands-free, and accurate way to test the efficacy of cancer drugs. On a grander scale, it could lead to promising new directions in cancer treatment. FAST is detailed in a paper published Sept. 16 in Science Advances.

Each year researchers test thousands of potential cancer drugs on mice with subcutaneous tumors. Few make it to human patients, and the process for finding new therapies is slow because technologies for measuring tumor regression from drug treatment take weeks to read out a response. The inherent biological variation of tumors, the shortcomings of existing measuring approaches, and the relatively small sample sizes make drug screenings difficult and labor-intensive.

"In some cases, the tumors under observation must be measured by hand with calipers," says Alex Abramson, first author of the study and a recent postdoc in the lab of Zhenan Bao, the K.K. Lee Professor in Chemical Engineering in the Stanford School of Engineering.

2. Based on studies with mice, the researchers say that the new device offers at least three significant advances. First, it provides continuous monitoring, as the sensor is physically connected to the mouse and remains in place over the entire experimental period. Second, the flexible sensor enshrouds the tumor and is therefore able to measure shape changes that are difficult to discern with other methods. Third, FAST is both autonomous and non-invasive. It is connected to the skin – not unlike an adhesive bandage – battery operated, and connected wirelessly. The mouse is free to move unencumbered by the device or wires, and scientists do not need to actively handle the mice following sensor placement. FAST packs are also reusable, cost just $60 or so to assemble, and can be attached to the mouse in minutes.

3 Alex Abramson is now assistant professor of chemical and biomolecular engineering at Georgia Institute of Technology; Yasser Khan is assistant professor at the Ming Hsieh Department of Electrical and Computer Engineering at the University

of Southern California; and Naoji Matsuhisa is associate professor in the Institute of Industrial Science Department of Informatics and Electronics at the University of Tokyo. Additional Stanford co-authors are Carmel T. Chan, former senior scientific manager; undergraduate Alana Mermin-Bunnell; Robyn Fong, life science research professor in the Department of Cardiothoracic Surgery; Rohan Shad, former postdoctoral fellow at the School of Medicine; William Hiesinger, assistant professor of cardiothoracic surgery; and Parag Mallick, associate professor of radiology. Zhenan Bao is also a member of Stanford Bio-X, the Stanford Cardiovascular Institute, and the Wu Tsai Human Performance Alliance. Hiesinger and Mallick are also members of Stanford Bio-X and the Cardiovascular Institute.

Task VI

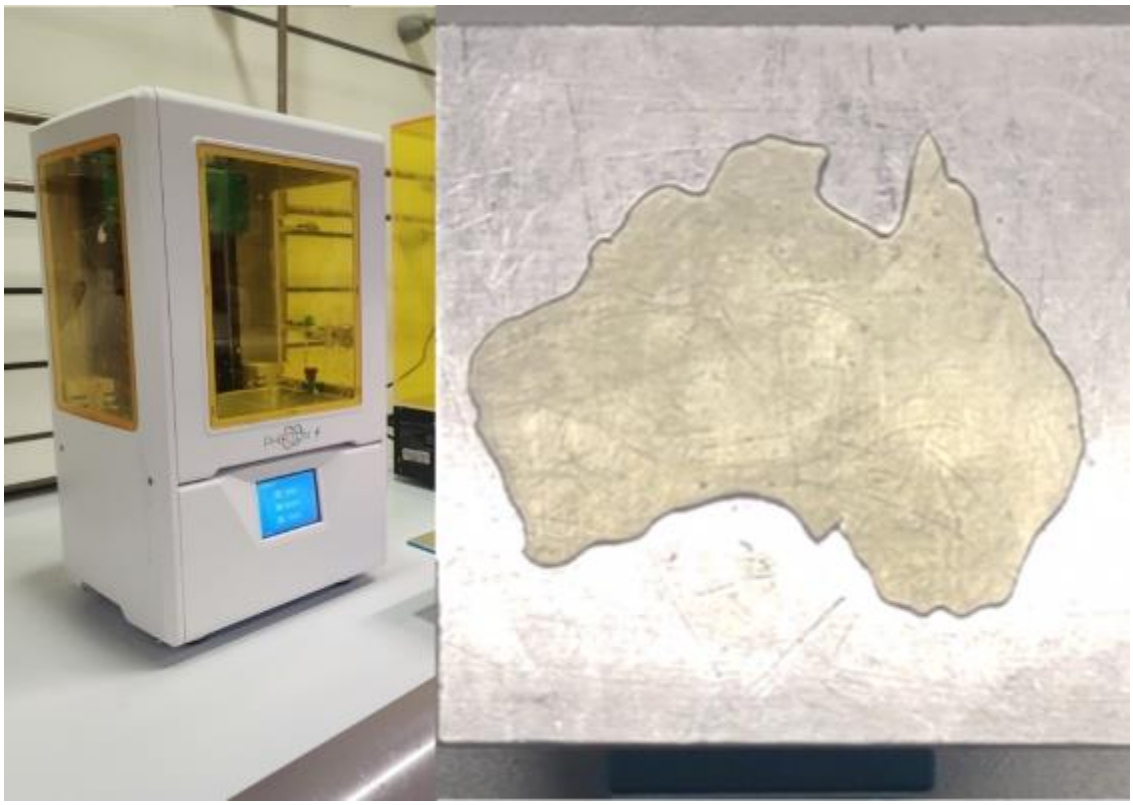
Divide the text into 6 passages. Wright sort headings for them.

UNIT 20

Task I. *Read the text. Translate each instance into Ukrainian.*

New 3D printing process offers novel energy storage design options

A team from UNSW Sydney has developed a way to 3D print strong, high-conducting solid polymer electrolytes into custom shapes.



Researchers at UNSW Sydney used a standard 3D printer to produce an intricate map of Australia made of solid polymer electrolyte which was then tested as an energy storage device. Photos from Dr Nathaniel Corrigan

UNSW engineers have developed a process to print solid-state polymer electrolytes into any shape desired for use in energy storage.

The research team from the School of Chemical Engineering led by Professor Cyrille Boyer, including Dr Nathaniel Corrigan and Kenny Lee – say the 3D printing process of such material could be particularly useful in future medical devices where small, intricately designed energy storage offers a number of benefits.

Solid-state electrolytes are a key component in solid-state batteries, although traditionally they have suffered from poor performance due to low ionic conductivities or poor mechanical properties.

However, in a paper published in Advanced Materials, the team from UNSW reports their 3D printed solid polymer electrolyte (SPE) offers high conductivity, as well as robust strength.

This means the solid-state electrolytes can potentially be used as the actual structure of a device, creating a range of conceivable design opportunities, particularly for future medical products.

“Nobody has 3D printed solid polymer electrolytes before. Traditionally they have been made using a mould, but previous processes did not offer the ability to control the strength of the material, or to form it into complex shapes,” says Kenny Lee.

“With existing solid-state electrolytes when you increase the mechanical strength of the material, you sacrifice a lot of the conductivity. If you want higher conductivity the material is much less robust. What we have achieved is a simultaneous combination of both, which can be 3D printed into sophisticated geometries.

“This polymer electrolyte has the potential to be a load-bearing energy storage material. Because of its strength, it could be used as the actual structure of small electronics, or in aerospace applications, or in small personal medical devices given our 3D printing process can be very intricate and precise.

“We can create really tiny structures with the kind of systems we're using. So it has fantastic application in nanotechnology and anywhere you need to design energy storage on a micro-scale level.”

Although the solid polymer electrolyte developed by the UNSW team is regarded as a high-performance material, the researchers say it can be manufactured using inexpensive and commercially available 3D printers, rather than sophisticated engineering equipment.

The SPE described in the paper is composed of nano-scale ion-conducting channels embedded in a rigid crosslinked polymer matrix. It is produced via a process known as polymerization-induced microphase separation (PIMS).

To showcase the versatility of the material, the researchers 3D printed an intricate map of Australia which was then tested as an energy storage device.

UNSW researcher Dr Nathaniel Corrigan working with a 3D printer in the laboratory. Photo from Dr Corrigan

"One of the other benefits of this SPE in energy storage devices is the fact it increases the cycling stability – that is the number of charging and discharging cycles until its capacity is reduced to a certain amount," says Dr Corrigan.

"In our paper, we show that this material is very stable and has the ability to charge and discharge over thousands of cycles. After 3000 cycles there was only roughly a 10 per cent drop."

The researchers say 3D printing also reduces wastage compared to other traditional forms of manufacturing and reduces costs since the same machine can be used to produce a variety of differently shaped materials.

In future, they say product designers could utilise their SPE to create items with a much higher energy storage density.

"Imagine an earpod predominantly made out of this material, which is also acting as the battery. The storage density will be much higher and the power would therefore last longer," says Professor Boyer.

"We really hope to be able to push forward in terms of commercialisation because we've created some really incredible materials and processes."

https://newsroom.unsw.edu.au/news/science-tech/new-3d-printing-process-offers-novel-energy-storage-design-options

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

1. Solid polymer electrolytes –
2. 3D printing
3. Cycling stability
4. Energy storage density
5. Wastage
6. Versatility

➤*Analyse the meaning of the different expressions.*

➤*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translation in your language would you suggest for these words?*

Task IV

Underline the words related to the topic of in the passage . Translate them. Do not use the dictionary.

Task V

Skim- read the passage below. Then write one sentence saying what they are about. Do not look back at the text use your own words.

1. This remarkable achievement suggests that solid-state electrolytes could potentially serve as structural elements within devices themselves, presenting a wide range of design possibilities, particularly in the realm of future medical products. By leveraging the intricate and precise nature of 3D printing, the team envisions the utilization of SPE in micro-scale energy storage applications and various nanotechnology-related fields.
2. In addition to its superior performance, 3D printing offers significant benefits in terms of reduced wastage and manufacturing costs. By employing inexpensive and readily available 3D printers, the UNSW team emphasizes the potential for mass production of their high-performance SPE, making it a more accessible and cost-effective energy storage solution.
3. Looking ahead, the researchers envision the application of their SPE technology in creating energy-dense products. They envision a future where everyday items, such as earpods, can incorporate this advanced material, effectively integrating energy storage capabilities and significantly extending their power endurance.

Task VI

Divide the text into 6 passages. Write sort headings for them.

UNIT 21

Task I. *Read the text. Translate each instance into Ukrainian.*

Pervasive ‘Dark Patterns’ Are Fooling People Into Signing Up for Services They Don’t Want

In a new report, the FTC laid out the multitude of “dark pattern” techniques used by apps and websites to confuse and trick users into spending more money online.Photo: Ivan Kruk (Shutterstock)

As much as you think you have full control of you and your wallet, it’s getting increasingly difficult for anybody using an app or a website to avoid getting suckered into surrendering your money or personal information to misleading or tricky UI design.

In a report released Thursday by the Federal Trade Commission, regulators said that there were more and more companies employing tactics to get users to relinquish their user information, buy products they don’t want, or sign up for services they might not otherwise.

The report is based on a public workshop the agency hosted last year, taking into account testimony by consumer advocates, researchers, and other industry experts. Much of what the FTC describes is already well-documented online and those keeping track have been aware of these deceptive tactics for years. Still, putting all the most prominent tactics in one place does offer a sobering reminder of just how entrenched anti-consumer practices are on both scammy and more legitimate websites and services.

Regulators said sites are disguising ads and promotional messaging to lure users into purchasing services. Tech companies and online retailers also lure users into signing up for subscription services while obscuring costs or charges, then making it difficult to actually cancel. Some dark patterns include confusing users in

dense terms of service to obscure key limitations of products or junk fees attached to their use.

The report lays out example after example of design elements that are specifically designed to sap money from users' wallets. There are examples of sites forcing users to click through several pages of promotions and links that direct users away from canceling a service subscription.

The FTC noted companies like Credit Karma, saying the company conducted tests to see if users were more likely to click on links if it showed they had been "pre-approved" for credit cards, even though that's untrue for the vast majority of people who would click. In a recent complaint, the FTC alleged the company went ahead with the misleading ads anyway.

Although the term "Dark Patterns," first coined in 2010 by UI designer Harry Brignull, might seem broad, its all based around giving users the illusion of choice and awareness, all while hiding their intent of getting users to pay for unneeded or unwanted services or harvest their user data in order to maximize profits.

The report cited how products often include user interfaces that don't allow users to definitively reject data collection and make it difficult to choose what data the company decides to collect. It could be as simple as graying-out the choices the

company doesn't want users to select, or making data collection the default option when loading an app or site.

One panelist cited by the FTC mentioned how when setting up Android phones, users are encouraged to enable location data collection simply by the way Google asks them to set up their phones, without explaining how that data can be used to determine where you live, work, further details about your political or religious affiliations, or potentially even whether you might be seeking an abortion in the age post *Roe v. Wade*.

The FTC, led by noted big tech antagonist Lina Kahn, recently made overtures about cracking down on big tech data gathering. Still, that's a tall order considering just how much data is already out there.

The FTC has rung the bell about dark patterns before, especially among major companies. Back in March, the agency said they were investigating Amazon for its manipulative user interface they argued was tricking users into signing up for Prime memberships. They also attacked Amazon alongside Apple and Google for allowing kids games on their app stores that advertised themselves as "free" while allowing children to rack up multiple charges just by playing the game and tapping on certain buttons.

Other consumer advocate groups have tried to call out corporations for their use of dark patterns. Consumer Reports' Dark Patterns Tip Line has posted dozens upon dozens of examples of misleading UI or confusing consumer contracts meant to deceive users on everything from Microsoft Edge browser to Pottery Barn marketing emails.

Though as much as the FTC promises more enforcement and promotes all they've already done, it would be near-impossible for any one agency to address every single instance of misleading UI. The American Data Privacy and Protection Act has promised to legislate against these pesky and misleading UI practices, but it seems the ambitious bill remains stuck in Congress.

https://gizmodo.com/dark-patterns-ui-cancel-subscription-1849542166

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

Dark patterns –
Scammy websites –
Subscription services -
Junk fees –
Deceptive tactics-

➤*Analyse the meaning of the different expressions.*

➤*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translation in your language would you suggest for these words?*

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then write one sentence saying what they are about. Do not look back at the text use your own words.

1. In a report released Thursday by the Federal Trade Commission, regulators said that there were more and more companies employing tactics to get users to relinquish their user information, buy products they don't want, or sign up for services they might not otherwise. The report is based on a public workshop the agency hosted last year, taking into account testimony by consumer advocates, researchers, and other industry experts. Much of what the FTC describes is already well-documented online and those keeping track have been aware of these deceptive tactics for years.
2. The report lays out example after example of design elements that are specifically designed to sap money from users' wallets. There are examples of sites forcing users to click through several pages of promotions and links that direct users away from canceling a service subscription. The FTC noted companies like Credit Karma, saying the company conducted tests to see if users were more likely to click on links if it showed they had been "pre-approved" for credit cards, even though that's untrue for the vast majority of people who would click. In a recent complaint, the FTC alleged the company went ahead with the misleading ads anyway.
3. The FTC, led by noted big tech antagonist Lina Kahn, recently made overtures about cracking down on big tech data gathering. Still, that's a tall order considering just how much data is already out there. The FTC has rung the bell about dark patterns before, especially among major companies. Back in March, the agency said they were investigating Amazon for its manipulative user interface they argued was tricking users into signing up for Prime memberships. They also attacked Amazon alongside Apple and Google for allowing kids games on their app stores that advertised

themselves as “free” while allowing children to rack up multiple charges just by playing the game and tapping on certain buttons.

Task VI

Divide the text into 6 passages. Write sort headings for them.

UNIT 22

Task 1.

Read the text. Translate each instance into Ukrainian

NASA's Webb Space Telescope Is So Good, We Might Need Improved Planetary Models

•

Six of the 18 gold-plated James Webb Space Telescope mirrors, as they were readied for shipment during construction.

NASA/MSFC/David Higginbotham/Emmett Given

It has become exceedingly clear, over the past few months, that NASA's James Webb Space Telescope does exactly what it set out to do. Just as its creators had hoped, the multibillion-dollar machine is flawlessly "unfolding the universe" by revealing cosmic light we cannot see with our own eyes -- and its excellent results make even the most unlikely of stargazers feel alive.

Because of this gold-plated telescope, Twitter went wild one day over a bleary red dot. For 48 hours, people worldwide were gawking at a galaxy born shortly after

the birth of time itself. It would appear that, thanks to the technological prowess of the JWST, humanity stands united over stardust.

But here's the thing.

Amid personal awe, scientists from the Massachusetts Institute of Technology warn that we ought to consider one crucial *scientific* consequence of having a superhero telescope.

If the JWST is like a zero-to-100 'scope upgrade, they wonder, is it possible our science models need a zero-to-100 reboot, too? Are the datasets scientists have been using for decades unable to match the device's power and therefore falling short in revealing what it's trying to tell us?

"The data we will be getting from the JWST will be incredible, but ... our insights will be limited if our models don't match it in quality," Clara Sousa-Silva, a quantum astrochemist at the Center for Astrophysics, Harvard & Smithsonian, told CNET.

And, according to a new study of which she's a co-author, published Thursday in the journal Nature Astronomy, the answer is yes.

More specifically, this paper suggests some of the light-parsing tools scientists normally use to understand exoplanet atmospheres aren't totally equipped to deal with the JWST's exceptional light data. In the long run, such a hindrance may impact the most *massive* JWST quest of all: the hunt for extraterrestrial life.

"Currently, the model we use to decrypt spectral information is not up to par with the precision and quality of data we have from the James Webb telescope," Prajwal Niraula, graduate student at MIT's department of Earth, atmospheric and planetary sciences and co-author of the study, said in a statement. "We need to up our game."

The Carina Nebula, as imaged by NASA's James Webb Space Telescope.

Here's one way to think about the conundrum.

Imagine pairing the newest, most powerful Xbox console with the very first iteration of a TV. (Yes, I know the extreme hypothetical nature of my scenario). The Xbox would be trying to give the TV awesome high-resolution, colorful, beautiful graphics to show us -- but the TV wouldn't have the capacity to compute any of it.
I wouldn't be surprised if the TV straight up exploded. But the point is you wouldn't *know* what the Xbox is trying to provide for you, unless you get an equally high-res TV.

Similarly, in the vein of exoplanet discoveries, scientists feed a bunch of deep-space light, or photon, data into models that test for "opacity." Opacity measures how easily photons pass through a material and differs depending on things like light wavelength, material temperature and pressure.

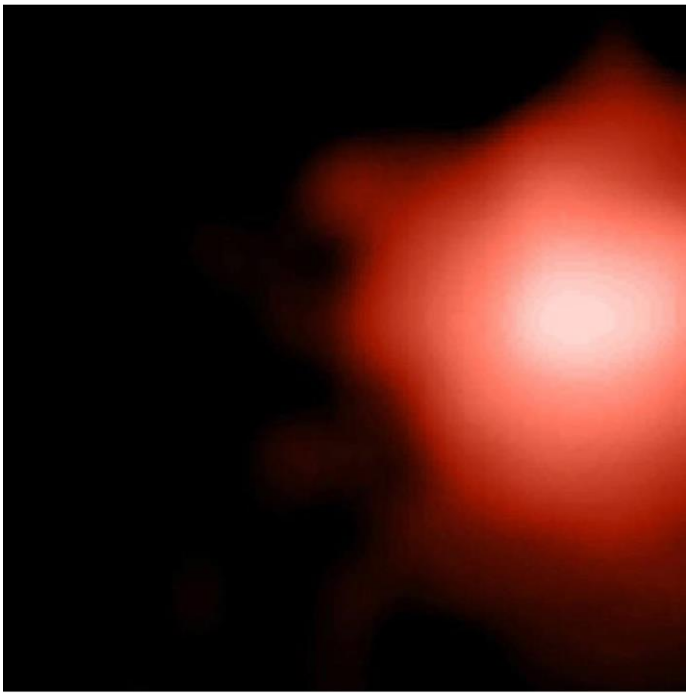
This means every such interaction leaves behind a telltale signature of what the photon's properties are, and therefore, when it comes to exoplanets, what kind of chemical atmosphere those photons passed through to get to the light detector. That's how scientists sort of reverse-calculate, from light data, what an exoplanet's atmosphere is composed of.

In this case, the detector liaison lies on the James Webb Space Telescope -- but in the team's new study, after putting the most commonly used opacity model to the test, the researchers saw JWST light data hitting what they call an "accuracy wall."

The model wasn't sensitive enough to parse stuff like whether a planet has an atmospheric temperature of 300 or 600 Kelvin, the researchers say, or whether a certain gas takes up 5% or 25% of the atmosphere. Such a difference is not only statistically significant, but per Niraula, also "matters in order for us to constrain planetary formation mechanisms and reliably identify biosignatures."

That is, evidence of alien life.

"We need to work on our interpretive tools," Sousa-Silva said, "so that we don't find ourselves seeing something amazing through JWST but not knowing how to interpret it."



Are we looking at the oldest galaxy ever found?

T. Treu/GLASS-JWST/NASA/CSA/ESA/STScI

Further, the team also found its models kind of disguising its uncertain readings. A few adjustments can easily paper over uncertainty, deeming results a good fit when they're incorrect.

"We found that there are enough parameters to tweak, even with a wrong model, to still get a good fit, meaning you wouldn't know that your model is wrong

and what it's telling you is wrong," Julien de Wit, assistant professor at MIT's EAPS and study co-author, said in a statement.

Going forward, the team urges opacity models be improved to accommodate our spectacular JWST revelations – especially calling for crossover studies between astronomy and spectroscopy.

"There is so much that could be done if we knew perfectly how light and matter interact," Niraula says. "We know that well enough around the Earth's conditions, but as soon as we move to different types of atmospheres, things change, and that's a lot of data, with increasing quality, that we risk misinterpreting."

De Wit compares the current opacity model to the ancient language translation tool the Rosetta Stone, explaining that so far, this Rosetta Stone has been doing OK, such as with the Hubble Space Telescope.

"But now that we're going to the next level with Webb's precision," the researcher said, "our translation process will prevent us from catching important subtleties, such as those making the difference between a planet being habitable or not."

As Sousa-Silva puts it, "it's a call to improve our models, so that we will not miss the subtleties of data."

(https://www.cnet.com/science/space/nasas-webb-space-telescope-is-so-good-we-might-need-improved-planetary-models/)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results by other students or by studying other translators.*

Task III

➤*Translate the following English terms:*

unfolding the universe
risk misinterpreting
reliably identify biosignatures
detector liaison lies
the vein of exoplanet discoveries

➤*Analyse the meaning of the different expressions.*

➤*If any of of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translations in your languages would you suggest for these words?*

Task IV

Underline the words to the topic of new customers in the passage. Translate them. Do not use the dictionary.

Task V

Skim-read the passages below. Then write one sentence saying what they are about. Do not look back at the text use your own words.

1. Because of this gold-plated telescope, Twitter went wild one day over a bleary red dot. For 48 hours, people worldwide were gawking at a galaxy born shortly after the

birth of time itself. It would appear that, thanks to the technological prowess of the JWST, humanity stands united over stardust. But here's the thing. Amid personal awe, scientists from the Massachusetts Institute of Technology warn that we ought to consider one crucial *scientific* consequence of having a superhero telescope.

2. Similarly, in the vein of exoplanet discoveries, scientists feed a bunch of deep-space light, or photon, data into models that test for "opacity." Opacity measures how easily photons pass through a material and differs depending on things like light wavelength, material temperature and pressure. This means every such interaction leaves behind a telltale signature of what the photon's properties are, and therefore, when it comes to exoplanets, what kind of chemical atmosphere those photons passed through to get to the light detector. That's how scientists sort of reverse-calculate, from light data, what an exoplanet's atmosphere is composed of. In this case, the detector liaison lies on the James Webb Space Telescope -- but in the team's new study, after putting the most commonly used opacity model to the test, the researchers saw JWST light data hitting what they call an "accuracy wall."

3. "There is so much that could be done if we knew perfectly how light and matter interact," Niraula says. "We know that well enough around the Earth's conditions, but as soon as we move to different types of atmospheres, things change, and that's a lot of data, with increasing quality, that we risk misinterpreting." De Wit compares the current opacity model to the ancient language translation tool the Rosetta Stone, explaining that so far, this Rosetta Stone has been doing OK, such as with the Hubble Space Telescope. "But now that we're going to the next level with Webb's precision," the researcher said, "our translation process will prevent us from catching important subtleties, such as those making the difference between a planet being habitable or not." As Sousa-Silva puts it, "it's a call to improve our models, so that we will not miss the subtleties of data."

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 23

Task I.

Read the texts. Translate each instance into Ukrainian.

First-of-its-kind 3D-printed home blends concrete, wood

Pouring layers of concrete like rows of toothpaste, an industrial-sized 3D printer this week continued adding a second floor to a Houston home that will be the first multistory printed structure in the United States.

In addition to that achievement, designers Leslie Lok and Sasa Zivkovic, assistant professors of architecture in the College of Architecture, Art and Planning (AAP) and co-principals of the HANNAH Design Office, say the two-story, single-family home is demonstrating innovative construction processes that can be scaled up to multifamily and mixed-use developments, helping to address housing shortages.

Credit:Leslie Lok and Sasa Zivkovic/Provided

A COBOD BOD2 3D construction printer builds structural elements of a Houston home that will be the first multistory 3D-printed structure in the United States.

Their first-of-its-kind hybrid design connects structural elements composed of 3D-printed concrete with conventional wood framing representative of most U.S. residential construction. The combination shows how each material can be used where it works best, with minimal waste, to create buildings that are efficient, resilient against increasingly intense weather events and potentially more affordable.

"Our hybrid construction approach creates a building system that is structurally efficient, easily replicable and materially responsive," Lok said. "The project also highlights the exciting design potential of mass-customized architectural components to meet homeowners' needs and to simplify building system integration."

Added Zivkovic: "These design efforts aim to increase the impact, applicability, sustainability and cost-efficiency of 3D printing for future residential and multifamily buildings in the U.S."

On Sept. 12, members of the media were invited to observe progress printing the three-bedroom, three-bathroom home that will also feature a two-car garage and a 40-foot chimney – making the home one of the tallest printed structures to date.

The home is being built in partnership with PERI 3D Construction, which has completed six 3D-printed structures in the U.S. and Europe; Houston-based engineering and design-build contractor CIVE; and other building industry partners. Of new concrete printing methods and robotically fabricated timber components. The project team continues to seek industry collaborators and sponsors.

For Lok, who leads the Rural-Urban Building Innovation Lab at AAP, and Zivkovic, who leads the Robotic Construction Lab, the project is the latest to emerge from years of research into 3D printing's potential to enable "mass customization" without increasing costs. They previously experimented with a hybrid design utilizing 3D-printed concrete and upcycled wood for the Ashen Cabin project in upstate New York. Lok's HoloWall installation on the Arts Quad explored customization using nonuniform building materials and digital modeling tools. Zivkovic's prior research involves the development.

The 4,000-square foot Houston project advances that work to a larger scale, one that will require another U.S. "first" – a relocation of the large gantry supporting

the printer, measuring roughly 60 feet long, 30 feet wide and 30 feet tall, to complete the structure.

"Apart from printing technology, the integration of printing with building design and building materials, and Rendering of the two-story Houston home designed by Leslie Lok and Sasa Zivkovic, which features a first-of-its-kind hybrid design utilizing 3D-printed concrete and Credit:Leslie Lok and Sasa Zivkovic/Provided wood framing.

Across various systems – from spray-foam insulation to a heating, ventilating, and air conditioning system more common to commercial buildings – the designers say the home integrates design and construction processes well-suited to multifamily developments that will be needed to expand housing capacity in fast-growing cities like Houston.

The designers said their approach could also accelerate construction timelines and reduce costs, since concrete printers may be operated by as few as three or four people. It also minimizes waste, as material can be mixed on demand and printed only for structurally important sections, and can more efficiently integrate wood framing in a modular design.

The streamlining of construction process are important aspects in the realization of such a project," Zivkovic said. "We are using this project to

demonstrate how 3D printing is not only market-ready, but also capable of building well-designed and high-performance architecture."

For the Houston home, the printed material is locally sourced and uses cement with a reduced carbon footprint, a mix that may include fly ash, slag and other industrial byproducts. The designers are collaborating with colleagues in the College of Engineering on research relating to ecofriendly building materials, including the potential for concrete to store methane, a potent greenhouse gas. Wood framing, meanwhile, is a renewable resource but is often a product of forest monocultures and may be transported over long distances.

Lok and Zivkovic said the Houston home optimizes use of both materials while taking better advantage of their design potential than many structures limited to only one of them.

"There isn't a design out there," Lok said, "that thinks about multifamily housing using these two systems together."

(https://news.cornell.edu/stories/2022/09/first-its-kind-3d-printed-home-blends-concrete-wood)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more «inclusive of the reader»*

➤*Examine your translation and compare your results with results by other students or by studying other translators.*

Task III

➤*Translate the following English terms:*

mixed-use developments

mass-customized architectural components

forest monocultures

a renewable resource

integrate wood framing

➤*Analyse the meaning of the different expressions.*

➤*If any of of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translations in your languages would you suggest for these words?*

Task IV

Underline the words to the topic of new customers in the passage. Translate them. Do not use the dictionary.

Task V

Skim-read the passages below. Then write one sentence saying what they are about. Do not look back at the text use your own words.

1. "Our hybrid construction approach creates a building system that is structurally efficient, easily replicable and materially responsive," Lok said. "The project also highlights the exciting design potential of mass-customized architectural components to meet homeowners' needs and to simplify building system integration."

Added Zivkovic: "These design efforts aim to increase the impact, applicability, sustainability and cost-efficiency of 3D printing for future residential and multifamily buildings in the U.S."

2. The project team continues to seek industry collaborators and sponsors.

For Lok, who leads the Rural-Urban Building Innovation Lab at AAP, and Zivkovic, who leads the Robotic Construction Lab, the project is the latest to emerge from years of research into 3D printing's potential to enable "mass customization" without increasing costs. They previously experimented with a hybrid design utilizing 3D-printed concrete and upcycled wood for the Ashen Cabin project in upstate New York. Lok's HoloWall installation on the Arts Quad explored customization using nonuniform building materials and digital modeling tools. Zivkovic's prior research involves the development.

The 4,000-square foot Houston project advances that work to a larger scale, one that will require another U.S. "first" – a relocation of the large gantry supporting the printer, measuring roughly 60 feet long, 30 feet wide and 30 feet tall, to complete the structure.

3. For the Houston home, the printed material is locally sourced and uses cement with a reduced carbon footprint, a mix that may include fly ash, slag and other industrial byproducts. The designers are collaborating with colleagues in the College of Engineering on research relating to ecofriendly building materials, including the potential for concrete to store methane, a potent greenhouse gas. Wood framing, meanwhile, is a renewable resource but is often a product of forest monocultures and may be transported over long distances.

Lok and Zivkovic said the Houston home optimizes use of both materials while taking better advantage of their design potential than many structures limited to only one of them.

"There isn't a design out there," Lok said, "that thinks about multifamily housing using these two systems together."

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 24

Task I.

Read the text. Translate each instance into Ukrainian.

Scientists try to teach robot to laugh at the right time

Research team hopes system could improve natural conversations between humans and AI systems

Laughter comes in many forms, from a polite chuckle to a contagious howl of mirth. Scientists are now developing an AI system that aims to recreate these nuances of humour by laughing in the right way at the right time.

The team behind the laughing robot, which is called Erica, say that the system could improve natural conversations between people and AI systems.

“We think that one of the important functions of conversational AI is empathy,” said Dr Koji Inoue, of Kyoto University, the lead author of the research, published in Frontiers in Robotics and AI. “So we decided that one way a robot can empathise with users is to share their laughter.”

Inoue and his colleagues have set out to teach their AI system the art of conversational laughter. They gathered training data from more than 80 speed-dating

dialogues between male university students and the robot, who was initially teleoperated by four female amateur actors.

The dialogue data was annotated for solo laughs, social laughs (where humour isn't involved, such as in polite or embarrassed laughter) and laughter of mirth. This data was then used to train a machine learning system to decide whether to laugh, and to choose the appropriate type.

It might feel socially awkward to mimic a small chuckle, but empathetic to join in with a hearty laugh. Based on the audio files, the algorithm learned the basic characteristics of social laughs, which tend to be more subdued, and mirthful laughs, with the aim of mirroring these in appropriate situations.

"Our biggest challenge in this work was identifying the actual cases of shared laughter, which isn't easy because as you know, most laughter is actually not shared at all," said Inoue. "We had to carefully categorise exactly which laughs we could use for our analysis and not just assume that any laugh can be responded to."

The team tested out Erica's "sense of humour" by creating four short dialogues for it to share with a person, integrating the new shared-laughter algorithm into existing conversation software. These were compared to scenarios where Erica didn't laugh at all or emitted a social laugh every time she detected laughter.

The clips were played to 130 volunteers who rated the shared-laughter algorithm most favourably for empathy, naturalness, human-likeness and understanding.

The team said laughter could help create robots with their own distinct character. "We think that they can show this through their conversational behaviours, such as laughing, eye gaze, gestures and speaking style," said Inoue, although he added that it could take more than 20 years before it would be possible to have a "casual chat with a robot like we would with a friend."

Prof Sandra Wachter, of the Oxford Internet Institute at the University of Oxford, said: "One of the things I'd keep in mind is that a robot or algorithm will never be able to understand you. It doesn't know you, it doesn't understand you and doesn't understand the meaning of laughter.

“They’re not sentient, but they might get very good at making you believe they understand what’s going on,” she added.

We have a small favour to ask. Millions are turning to the Guardian for open, independent, quality news every day, and readers in 180 countries around the world now support us financially.

We believe everyone deserves access to information that’s grounded in science and truth, and analysis rooted in authority and integrity. That’s why we made a different choice: to keep our reporting open for all readers, regardless of where they live or what they can afford to pay. This means more people can be better informed, united, and inspired to take meaningful action.

In these perilous times, a truth-seeking global news organisation like the Guardian is essential. We have no shareholders or billionaire owner, meaning our journalism is free from commercial and political influence – this makes us different. When it’s never been more important, our independence allows us to fearlessly investigate, challenge and expose those in power.

(https://www.theguardian.com/technology/2022/sep/15/scientists-teach-robot-laugh-right-time-research)

Task II.

➢*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➢*Translate the text into your own language, aiming for a use of language that is more ‘inclusive of the reader’.*

➢*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➢*Translate the following English terms:*

1. contagious howl of mirth
2. mirthful laughs
3. perilous times
4. truth-seeking
5. a polite chuckle

➢*Analyse the meaning of the different expressions.*

➢*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➢*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1.… we have a small favour to ask. Millions are turning to the Guardian for open, independent, quality news every day, and readers in 180 countries around the world now support us financially.

2. The team said laughter could help create robots with their own distinct character. “We think that they can show this through their conversational behaviours, such as

laughing, eye gaze, gestures and speaking style," said Inoue, although he added that it could take more than 20 years before it would be possible to have a "casual chat with a robot like we would with a friend."

3. The dialogue data was annotated for solo laughs, social laughs (where humour isn't involved, such as in polite or embarrassed laughter) and laughter of mirth. This data was then used to train a machine learning system to decide whether to laugh, and to choose the appropriate type.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

UNIT 25

Task I.

Read the text. Translate each instance into Ukrainian.

Unlocking human-like perception in self-driving vehicles

Freiburg computer scientists make an important step towards advancing perception in complex urban environments

How can mobile robots perceive and understand the environment correctly, even if parts of the environment are occluded by other objects? This is a key question that must be solved for self-driving vehicles to safely navigate in large crowded cities. While humans can imagine complete physical structures of objects even when they are partially occluded, existing artificial intelligence (AI) algorithms that enable robots and self-driving vehicles to perceive their environment do not have this capability. Robots with AI can already find their way around and navigate on their own once they have learned what their environment looks like. However, perceiving the entire structure of objects when they are partially hidden, such as people in crowds or vehicles in traffic jams, has been a significant challenge. A major step towards solving this problem has now been taken by Freiburg robotics researchers Prof. Dr. Abhinav Valada and PhD student Rohit Mohan from the Robot Learning Lab at the University of Freiburg, which they have presented in two joint publications.

A task whose solution promises more safety.

The two Freiburg scientists have developed the amodal panoptic segmentation task and demonstrated its feasibility using novel AI approaches. Until now, self-driving vehicles have used panoptic segmentation to understand their surroundings. This means that they can so far only predict which pixels of an image belong to which “visible” regions of an object such as a person or car, and identify instances of those objects. What they lack so far is being able to also predict the entire shape of

objects even when they are partially occluded by other objects next to them. The new task of perception with amodal panoptic segmentation makes this holistic understanding of the environment possible.

Amodal refers to the case that any partial occlusion of objects must be abstracted and instead of viewing them as fragments, there should be a general understanding of viewing them as a whole. Thus, this improved ability of visual recognition will lead to enormous progress in improving the safety of self-driving vehicles.

Potential to revolutionize urban visual scene understanding

In a new paper published at the IEEE/CVF Computer Vision and Pattern Recognition Conference (CVPR), the researchers have added the new task to established benchmark datasets and made them publicly available. They are now calling on scientists to participate in the benchmarking with their own AI algorithms. The goal of this task is the pixel-wise semantic segmentation of the visible regions of amorphous background classes such as roads, vegetation, sky, and the instance segmentation of both the visible and occluded object regions of countable classes such as cars, trucks, and pedestrians.

The benchmark and datasets are publicly available on the website, including two proposed novel learning algorithms. “We are confident that novel AI algorithms for this task will enable robots to emulate the visual experience that humans have by perceiving complete physical structures of objects,” Valada explains. “Amodal panoptic segmentation will significantly help downstream automated driving tasks where occlusion is a major challenge such as depth estimation, optical flow, object tracking, pose estimation, motion prediction, etc. With more advanced AI algorithms for this task, visual recognition ability for self-driving cars can be revolutionized. For example, if the entire structure of road users is perceived at all times, regardless of partial occlusions, the risk of accidents can be significantly minimized.”

In addition, by inferring the relative depth ordering of objects in a scene, automated vehicles can make complex decisions such as in which direction to move toward the object to get a clearer view. In order to make these visions a reality, the

task and its benefits were presented to leading automotive industry professionals at AutoSens, which was held at the Autoworld Museum in Brussels.

Overview of facts:

- Abhinav Valada is an assistant professor and head of the Robot Learning Lab at the Department of Computer Science at the University of Freiburg as well as a member of the BrainLinks-BrainTools centre.
- He primarily conducts research on topics at the intersection of robotics, machine learning, and computer vision, such as fundamental problems in robot perception, state estimation, and planning using machine learning approaches to enable robots to reliably operate in more complex domains and diverse environments. His goal is to develop scalable, lifelong learning robotic systems.
- Robot Learning Lab: Valada's team focuses on developing scalable robot learning algorithms for mobility and manipulation. They combine modern machine learning techniques such as deep learning and reinforcement learning, with robotics to expand the abilities of robots to operate in diverse real-world environments.

(Illustrations: Berkeley DeepDrive; Abhinav Valada; Abhinav Valada)

In contrast to panoptic segmentation (middle), amodal panoptic segmentation (bottom) predicts entire object instances including their occluded regions, e.g. cars and people, of the input image (top). (Illustrations: Berkeley DeepDrive; Abhinav Valada; Abhinav Valada)

(https://kommunikation.uni-freiburg.de/pm-en/press-releases-2022/unlocking-human-like-perception-in-self-driving-vehicles)

Task II.

➤*Whilst reading the following text, make a list of infinitives what the author uses and add these to your translation glossary with a short definition you find useful.*

➤*Translate the text into your own language, aiming for a use of language that is more 'inclusive of the reader'.*

➤*Examine your translation and compare your results with results obtained by other students or by studying other translators.*

Task III.

➤*Translate the following English terms:*

1. existing artificial intelligence
2. panoptic segmentation
3. the benchmarking
4. amodal panoptic segmentation
5. pixel-wise semantic

➤*Analyse the meaning of the different expressions.*

➤*If any of these are unfamiliar to you, decide how you will first of all discover their meaning.*

➤*What translations in your languages would you suggest for these words?*

Task IV.

Underline the words related to the topic of Future quantum computers in the passage. Translate them. Do not use the dictionary.

Task V.

Skim-read the passages below. Then wright one sentence saying what they are about. Do not look back at the text use your own words.

1.He primarily conducts research on topics at the intersection of robotics, machine learning, and computer vision, such as fundamental problems in robot perception, state estimation, and planning using machine learning approaches to enable robots to reliably operate in more complex domains and diverse environments. His goal is to develop scalable, lifelong learning robotic systems.

2. The benchmark and datasets are publicly available on the website, including two proposed novel learning algorithms. “We are confident that novel AI algorithms for this task will enable robots to emulate the visual experience that humans have by perceiving complete physical structures of objects,” Valada explains. “Amodal panoptic segmentation will significantly help downstream automated driving tasks where occlusion is a major challenge such as depth estimation, optical flow, object tracking, pose estimation, motion prediction, etc. With more advanced AI algorithms for this task, visual recognition ability for self-driving cars can be revolutionized. For example, if the entire structure of road users is perceived at all times, regardless of partial occlusions, the risk of accidents can be significantly minimized.”

3. Amodal refers to the case that any partial occlusion of objects must be abstracted and instead of viewing them as fragments, there should be a general understanding of viewing them as a whole. Thus, this improved ability of visual recognition will lead to enormous progress in improving the safety of self-driving vehicles.

Task VI

Divide the text into 6 passages. Wright sort headings for them.

Glossary of digitalization and cybersecurity terms

Access Control

Access Control ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL)

A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control Service

A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

Access Management Access

Management is the maintenance of access information which consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Matrix

An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.

Account Harvesting

Account Harvesting is the process of collecting all the legitimate account names on a system.

ACK Piggybacking

ACK piggybacking is the practice of sending an ACK inside another packet going to the same destination.

Active Content

Program code embedded in the contents of a web page. When the page is accessed by a web browser, the embedded code is automatically downloaded and executed on the user's workstation. Ex. Java, ActiveX (MS)

Activity Monitors

Activity monitors aim to prevent virus infection by monitoring for malicious activity on a system, and blocking that activity when possible.

Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Advanced Encryption Standard (AES)

An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.

Algorithm

A finite set of step-by-step instructions for a problem-solving or computation procedure, especially one that can be implemented by a computer.

Applet

Java programs; an application program that uses the client's web browser to provide a user interface.

ARPANET

Advanced Research Projects Agency Network, a pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Asymmetric Cryptography

Public-key cryptography; A modern branch of cryptography in which the algorithms employ a pair of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.

Asymmetric Warfare

Asymmetric warfare is the fact that a small investment, properly leveraged, can yield incredible results.

Auditing

Auditing is the information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

Authentication

Authentication is the process of confirming the correctness of the claimed identity.

Authenticity

Authenticity is the validity and conformance of the original information.

Authorization

Authorization is the approval, permission, or empowerment for someone or something to do something.

Autonomous System

One network or series of networks that are all under one administrative control. An autonomous system is also sometimes referred to as a routing domain. An autonomous system is assigned a globally unique number, sometimes called an Autonomous System Number (ASN).

Availability

Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

Backdoor

A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.

Bandwidth

Commonly used to mean the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

Banner

A banner is the information that is displayed to a remote user trying to connect to a service. This may include version information, system information, or a warning about authorized use.

Basic Authentication

Basic Authentication is the simplest web-based authentication scheme that works by sending the username and password with each request.

Bastion Host

A bastion host has been hardened in anticipation of vulnerabilities that have not been discovered yet.

BIND

BIND stands for Berkeley Internet Name Domain and is an implementation of DNS. DNS is used for domain name to IP address resolution.

Biometrics

Biometrics use physical characteristics of the users to determine access.

Bit

The smallest unit of information storage; a contraction of the term "binary digit;" one of two symbolsN"0" (zero) and "1" (one) - that are used to represent binary numbers.

Block Cipher

A block cipher encrypts one block of data at a time.

Blue Team

The people who perform defensive cybersecurity tasks, including placing and configuring firewalls, implementing patching programs, enforcing strong authentication, ensuring physical security measures are adequate and a long list of similar undertakings.

Boot Record Infector

A boot record infector is a piece of malware that inserts malicious code into the boot sector of a disk.

Border Gateway Protocol (BGP)

An inter-autonomous system routing protocol. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

Botnet

A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack.

Bridge

A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

British Standard 7799

A standard code of practice and provides guidance on how to secure an information system. It includes the management framework, objectives, and control requirements for information security management systems.

Broadcast

To simultaneously send the same message to multiple recipients. One host to all hosts on network.

Broadcast Address

An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

Browser

A client computer program that can retrieve and display information from servers on the World Wide Web.

Brute Force

A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

Buffer Overflow

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Business Continuity Plan (BCP)

A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Business Impact Analysis (BIA)

A Business Impact Analysis determines what levels of impact to a system are tolerable.

Byte

A fundamental unit of computer storage; the smallest addressable unit in a computer's architecture. Usually holds one character of information and usually means eight bits.

Cache

Pronounced cash, a special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

Cache Cramming

Cache Cramming is the technique of tricking a browser to run cached Java code from the local disk, instead of the internet zone, so it runs with less restrictive permissions.

Cache Poisoning

Malicious or misleading data from a remote name server is saved [cached] by another name server. Typically used with DNS cache poisoning attacks.

Call Admission Control (CAC)

The inspection and control all inbound and outbound voice network activity by a voice firewall based on user-defined policies.

Cell

A cell is a unit of data transmitted over an ATM network.

Certificate-Based Authentication

Certificate-Based Authentication is the use of SSL and certificates to authenticate and encrypt HTTP traffic.

CGI

Common Gateway Interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

Chain of Custody

Chain of Custody is the important application of the Federal rules of evidence and its handling.

Challenge-Handshake Authentication Protocol (CHAP)

The Challenge-Handshake Authentication Protocol uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

Checksum

A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

Cipher

A cryptographic algorithm for encryption and decryption.

Ciphertext

Ciphertext is the encrypted form of the message being sent.

Circuit Switched Network

A circuit switched network is where a single continuous physical circuit connected two endpoints where the route was immutable once set up.

Client

A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

Cloud Computing

Utilization of remote servers in the data-center of a cloud provider to store, manage, and process your data instead of using local computer systems.

Cold/Warm/Hot Disaster Recovery Site

* Hot site. It contains fully redundant hardware and software, with telecommunications, telephone and utility connectivity to continue all primary site operations. Failover occurs within minutes or hours, following a disaster. Daily data synchronization usually occurs between the primary and hot site, resulting in minimum or no data loss. Offsite data backup tapes might be obtained and delivered to the hot site to help restore operations. Backup tapes should be regularly tested to detect data corruption, malicious code and environmental damage. A hot site is the most expensive option. * Warm site. It contains partially redundant hardware and software, with telecommunications, telephone and utility connectivity to continue some, but not all primary site operations. Failover occurs within hours or days, following a disaster. Daily or weekly data synchronization usually occurs between the primary and warm site, resulting in minimum data loss. Offsite data backup tapes must be obtained and delivered to the warm site to restore operations. A warm site is the second most expensive option. * Cold site. Hardware is ordered, shipped and installed, and software is loaded. Basic telecommunications, telephone and utility connectivity might need turning on to continue some, but not all primary site operations. Relocation occurs within weeks or longer, depending on hardware arrival time, following a disaster. No data synchronization occurs between the primary and cold site, and could result in significant data loss. Offsite data backup tapes must be obtained and delivered to the cold site to restore operations. A cold site is the least expensive option.

Collision

A collision occurs when multiple systems transmit simultaneously on the same wire.

Competitive Intelligence

Competitive Intelligence is espionage using legal, or at least not obviously illegal, means.

Computer Emergency Response Team (CERT)

An organization that studies computer and network INFOSEC in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and offer other information to help improve computer and network security.

Computer Network

A collection of host computers together with the sub-network or inter-network through which they can exchange data.

Confidentiality

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Configuration Management

Establish a known baseline condition and manage it.

Cookie

Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.

Corruption

A threat action that undesirably alters system operation by adversely modifying system functions or data.

Cost Benefit Analysis

A cost benefit analysis compares the cost of implementing countermeasures with the value of the reduced risk.

Countermeasure

Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders form gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.

Covert Channels

Covert Channels are the means by which information can be communicated between two parties in a covert fashion using normal system operations. For example by changing the amount of hard drive space that is available on a file server can be used to communicate information.

Crimeware

A type of malware used by cyber criminals. The malware is designed to enable the cyber criminal to make money off of the infected system (such as harvesting key strokes, using the infected systems to launch Denial of Service Attacks, etc.).

Cron

Cron is a Unix application that runs jobs for users and administrators at scheduled times of the day.

Crossover Cable

A crossover cable reverses the pairs of cables at the other end and can be used to connect devices directly together.

Cryptanalysis

The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.

Cryptographic Algorithm or Hash

An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

Cut-Through

Cut-Through is a method of switching where only the header of a packet is read before it is forwarded to its destination.

Cyclic Redundancy Check (CRC)

Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

Daemon

A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

Data Aggregation

Data Aggregation is the ability to get a more complete picture of the information by analyzing several different types of records at once.

Data Custodian

A Data Custodian is the entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

Data Encryption Standard (DES)

A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Data Mining

Data Mining is a technique used to analyze existing information, usually with the intention of pursuing new avenues to pursue business.

Data Owner

A Data Owner is the entity having responsibility and authority for the data.

Data Warehousing

Data Warehousing is the consolidation of several previously independent databases into one location.

Datagram

Request for Comment 1594 says, "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

Day Zero

The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero day" exploit is referred to an exploit for which no patch is available yet. ("day one"-> day at which the patch is made available).

Decapsulation

Decapsulation is the process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

Decryption

Decryption is the process of transforming an encrypted message into its original plaintext.

Defacement

Defacement is the method of modifying the content of a website in such a way that it becomes "vandalized" or embarrassing to the website owner.

Defense In-Depth

Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

Demilitarized Zone (DMZ)

In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination. In some cases, a screened subnet which is used for servers accessible from the outside is referred to as a DMZ.

Denial of Service

The prevention of authorized access to a system resource or the delaying of system operations and functions.

Dictionary Attack

An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Diffie-Hellman

A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication

Digest Authentication allows a web client to compute MD5 hashes of the password to prove it has the password.

Digital Certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Envelope

A digital envelope is an encrypted message with the encrypted session key.

Digital Signature

A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Digital Signature Algorithm (DSA)

An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Digital Signature Standard (DSS)

The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

Disassembly

The process of taking a binary program and deriving the source code from it.

Disaster Recovery Plan (DRP)

A Disaster Recovery Plan is the process of recovery of IT systems in the event of a disruption or disaster.

Discretionary Access Control (DAC)

Discretionary Access Control consists of something the user can manage, such as a document password.

Disruption

A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Distance Vector

Distance vectors measure the cost of routes to determine the best route to all known networks.

Distributed Scans

Distributed Scans are scans that use multiple source addresses to gather information.

Domain

A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

Domain Hijacking

Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name

A domain name locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.

Domain Name System (DNS)

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Due Care

Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.

Due Diligence

Due diligence is the requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

DumpSec

DumpSec is a security tool that dumps a variety of information about a system's users, file system, registry, permissions, password policy, and services.

Dumpster Diving

Dumpster Diving is obtaining passwords and corporate directories by searching through discarded media.

Dynamic Link Library

A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

Dynamic Routing Protocol

Allows network devices to learn routes. Ex. RIP, EIGRP Dynamic routing occurs when routers talk to adjacent routers, informing each other of what networks each router is currently connected to. The routers must communicate using a routing

protocol, of which there are many to choose from. The process on the router that is running the routing protocol, communicating with its neighbor routers, is usually called a routing daemon. The routing daemon updates the kernel's routing table with information it receives from neighbor routers.

Eavesdropping

Eavesdropping is simply listening to a private conversation which may reveal information which can provide access to a facility or network.

Echo Reply

An echo reply is the response a machine that has received an echo request sends over ICMP.

Echo Request

An echo request is an ICMP message sent to a machine to determine if it is online and how long traffic takes to get to it.

Egress Filtering

Filtering outbound traffic.

Emanations Analysis

Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Encapsulation

The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

Encryption

Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

Ephemeral Port

Also called a transient port or a temporary port. Usually is on the client side. It is set up when a client application wants to connect to a server and is destroyed when the client application terminates. It has a number chosen at random that is greater than 1023.

Escrow Passwords

Escrow Passwords are passwords that are written down and stored in a secure location (like a safe) that are used by emergency personnel when privileged personnel are unavailable.

Ethernet

The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

Event

An event is an observable occurrence in a system or network.

Exponential Backoff Algorithm

An exponential backoff algorithm is used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

Exposure

A threat action whereby sensitive data is directly released to an unauthorized entity.

Extended ACLs (Cisco)

Extended ACLs are a more powerful form of Standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

Extensible Authentication Protocol (EAP)

A framework that supports multiple, optional authentication mechanisms for PPP, including clear-text passwords, challenge-response, and arbitrary dialog sequences.

Exterior Gateway Protocol (EGP)

A protocol which distributes routing information to the routers which connect autonomous systems.

False Rejects

False Rejects are when an authentication system fails to recognize a valid user.

Fast File System

The first major revision to the Unix file system, providing faster read access and faster (delayed, asynchronous) write access through a disk cache and better file system layout on disk. It uses inodes (pointers) and data blocks.

Fast Flux

Protection method used by botnets consisting of a continuous and fast change of the DNS records for a domain name through different IP addresses.

Fault Line Attacks

Fault Line Attacks use weaknesses between interfaces of systems to exploit gaps in coverage.

File Transfer Protocol (FTP)

A TCP/IP protocol specifying the transfer of text or binary files across the network.

Filter

A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

Filtering Router

An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

Finger

A protocol to lookup user information on a given host. A Unix program that takes an e-mail address as input and returns information about the user who owns that e-mail address. On some systems, finger only reports whether the user is currently logged on. Other systems return additional information, such as the user's full name, address, and telephone number. Of course, the user must first enter this information into the system. Many e-mail programs now have a finger utility built into them.

Fingerprinting

Sending strange packets to a system in order to gauge how it responds to determine the operating system.

Firewall

A logical or physical discontinuity in a network to prevent unauthorized access to data or resources.

Flooding

An attack that attempts to cause a failure in (especially, in the security of) a computer system or other data processing entity by providing more input than the entity can process properly.

Forest

A forest is a set of Active Directory domains that replicate their databases with each other.

Fork Bomb

A Fork Bomb works by using the fork() call to create a new process which is a copy of the original. By doing this repeatedly, all available processes on the machine can be taken up.

Form-Based Authentication

Form-Based Authentication uses forms on a webpage to ask a user to input username and password information.

Forward Lookup

Forward lookup uses an Internet domain name to find an IP address

Forward Proxy

Forward Proxies are designed to be the server through which all requests are made.

Fragment Offset

The fragment offset field tells the sender where a particular fragment falls in relation to other fragments in the original larger packet.

Fragment Overlap Attack

A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

Fragmentation

The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

Frames

Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit

by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)

Full Duplex

A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

Fully-Qualified Domain Name

A Fully-Qualified Domain Name is a server name with a hostname followed by the full domain name.

Fuzzing

The use of special regression testing tools to generate out-of-spec input for an application in order to find security vulnerabilities. Also see "regression testing".

Gateway

A network point that acts as an entrance to another network.

gethostbyaddr

The gethostbyaddr DNS query is when the address of a machine is known and the name is needed.

gethostbyname

The gethostbyname DNS quest is when the name of a machine is known and the address is needed.

GNU

GNU is a Unix-like operating system that comes with source code that can be copied, modified, and redistributed. The GNU project was started in 1983 by Richard Stallman and others, who formed the Free Software Foundation.

Gnutella

An Internet file sharing utility. Gnutella acts as a server for sharing files while simultaneously acting as a client that searches for and downloads files from other users.

Hardening

Hardening is the process of identifying and fixing vulnerabilities on a system.

Hash Function

An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

Hash Functions

(cryptographic) hash functions are used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

Header

A header is the extra information in a packet that is needed for the protocol stack to process the packet.

Hijack Attack

A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Honey Client

see Honeymonkey.

Honey pot

Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you're running vulnerable services that can be

used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Honeymonkey

Automated system simulating a user browsing websites. The system is typically configured to detect web sites which exploit vulnerabilities in the browser. Also known as Honey Client.

Hops

A hop is each exchange with a gateway a packet takes on its way to the destination.

Host

Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Host-Based ID

Host-based intrusion detection systems use information from the operating system audit records to watch all operations occurring on the host that the intrusion detection software has been installed upon. These operations are then compared with a pre-defined security policy. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilized by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

HTTP Proxy

An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

HTTPS

When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.

Hub

A hub is a network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub.

Hybrid Attack

A Hybrid Attack builds on the dictionary attack method by adding numerals and symbols to dictionary words.

Hybrid Encryption

An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

Hyperlink

In hypertext or hypermedia, an information object (such as a word, a phrase, or an image; usually highlighted by color or underscoring) that points (indicates how to connect) to related information that is located elsewhere and can be retrieved by activating the link.

Hypertext Markup Language (HTML)

The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

Hypertext Transfer Protocol (HTTP)

The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

Identity

Identity is whom someone or what something is, for example, the name by which something is known.

Incident

An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

Incident Handling

Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Incremental Backups

Incremental backups only backup the files that have been modified since the last backup. If dump levels are used, incremental backups only backup files changed since last backup of a lower dump level.

Inetd (xinetd)

Inetd (or Internet Daemon) is an application that controls smaller internet services like telnet, ftp, and POP.

Inference Attack

Inference Attacks rely on the user to make logical connections between seemingly unrelated pieces of information.

Information Warfare

Information Warfare is the competition between offensive and defensive players over information resources.

Ingress Filtering

Ingress Filtering is filtering inbound traffic.

Input Validation Attacks

Input Validations Attacks are where an attacker intentionally sends unusual input in the hopes of confusing an application.

Integrity

Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Integrity Star Property

In Integrity Star Property a user cannot read data of a lower integrity level then their own.

Internet

A term to describe connecting multiple separate networks together.

Internet Control Message Protocol (ICMP)

An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.

Internet Engineering Task Force (IETF)

The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

Internet Message Access Protocol (IMAP)

A protocol that defines how a client should fetch mail from and return mail to a mail server. IMAP is intended as a replacement for or extension to the Post Office Protocol (POP). It is defined in RFC 1203 (v3) and RFC 2060 (v4).

Internet Protocol (IP)

The method or protocol by which data is sent from one computer to another on the Internet.

Internet Protocol Security (IPsec)

A developing standard for security at the network or packet processing layer of network communication.

Internet Standard

A specification, approved by the IESG and published as an RFC, that is stable and well-understood, is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet.

Interrupt

An Interrupt is a signal that informs the OS that something has occurred.

Intranet

A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

Intrusion Detection

A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Address

A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Flood

A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP Forwarding

IP forwarding is an Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP Spoofing

The technique of supplying a false IP address.

ISO

International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

Issue-Specific Policy

An Issue-Specific Policy is intended to address specific needs within an organization, such as a password policy.

ITU-T

International Telecommunications Union, Telecommunication Standardization Sector (formerly "CCITT"), a United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations."

Jitter

Jitter or Noise is the modification of fields in a database while preserving the aggregate characteristics of that make the database useful in the first place.

Jump Bag

A Jump Bag is a container that has all the items necessary to respond to an incident inside to help mitigate the effects of delayed reactions.

Kerberos

A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

Kernel

The essential center of a computer operating system, the core that provides basic services for all other parts of the operating system. A synonym is nucleus. A kernel can be contrasted with a shell, the outermost part of an operating system that interacts with user commands. Kernel and shell are terms used more frequently in Unix and some other operating systems than in IBM mainframe systems.

Lattice Techniques

Lattice Techniques use security designations to determine access to information.

Layer 2 Forwarding Protocol (L2F)

An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP)

An extension of the Point-to-Point Tunneling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

Least Privilege

Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

Legion

Software to detect unprotected shares.

Lightweight Directory Access Protocol (LDAP)

A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

Link State

With link state, routes maintain information about all routers and router-to-router links within a geographic area, and creates a table of best routes with that information.

List Based Access Control

List Based Access Control associates a list of users and their privileges with each object.

Loadable Kernel Modules (LKM)

Loadable Kernel Modules allow for the adding of additional functionality directly into the kernel while the system is running.

Log Clipping

Log clipping is the selective removal of log entries from a system log to hide a compromise.

Logic bombs

Logic bombs are programs or snippets of code that execute when a certain predefined event occurs. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs.

Logic Gate

A logic gate is an elementary building block of a digital circuit. Most logic gates have two inputs and one output. As digital circuits can only understand binary, inputs and outputs can assume only one of two states, 0 or 1.

Loopback Address

The loopback address (127.0.0.1) is a pseudo IP address that always refer back to the local host and are never sent out onto a network.

MAC Address

A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

Malicious Code

Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware

A generic term for a number of different types of malicious code.

Mandatory Access Control (MAC)

Mandatory Access Control controls is where the system controls access to resources based on classification levels assigned to both the objects and the users. These controls cannot be changed by anyone.

Man-in-the-Middle Attack (MitM)

A man-in-the-middle attack is a type of cyber attack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

Masquerade Attack

A type of attack in which one system entity illegitimately poses as (assumes the identity of) another entity.

md5

A one way cryptographic hash function. Also see "hash functions" and "sha1"

Measures of Effectiveness (MOE)

Measures of Effectiveness is a probability model based on engineering concepts that allows one to approximate the impact a give action will have on an environment. In Information warfare it is the ability to attack or defend within an Internet environment.

Monoculture

Monoculture is the case where a large number of users run the same software, and are vulnerable to the same attacks.

Morris Worm

A worm program written by Robert T. Morris, Jr. that flooded the ARPANET in November, 1988, causing problems for thousands of hosts.

Multi-Cast

Broadcasting from one host to a given set of hosts.

Multi-Homed

You are "multi-homed" if your network is directly connected to two or more ISP's.

Multiplexing

To combine multiple signals from possibly disparate sources, in order to transmit them over a single path.

NAT

Network Address Translation. It is used to share one or a small number of publicly routable IP addresses among a larger number of hosts. The hosts are assigned private IP addresses, which are then "translated" into one of the publicly routed IP addresses. Typically home or small business networks use NAT to share a single DLS or Cable modem IP address. However, in some cases NAT is used for servers as an additional layer of protection.

National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Natural Disaster

Any "act of God" (e.g., fire, flood, earthquake, lightning, or wind) that disables a system component.

Netmask

32-bit number indicating the range of IP addresses residing on a single IP network/subnet/supernet. This specification displays network masks as hexadecimal numbers. For example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed elsewhere in the literature as 255.255.255.0.

Network Address Translation

The translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

Network Mapping

To compile an electronic inventory of the systems and the services on your network.

Network Taps

Network taps are hardware devices that hook directly onto the network cable and send a copy of the traffic that passes through it to one or more other networked devices.

Network-Based IDS

A network-based IDS system monitors the traffic on its network segment as a data source. This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment.

Network traffic on other segments, and traffic on other means of communication (like phone lines) can't be monitored. Network-based IDS involves looking at the packets on the network as they pass by some sensor. The sensor can only see the packets that happen to be carried on the network segment it's attached to. Packets are considered to be of interest if they match a signature.Network-based intrusion detection passively monitors network activity for indications of attacks. Network monitoring offers several advantages over traditional host-based intrusion detection systems. Because many intrusions occur over networks at some point, and because networks are increasingly becoming the targets of attack, these techniques are an excellent method of detecting many attacks which may be missed by host-based intrusion detection mechanisms.

Non-Printable Character

A character that doesn't have a corresponding character letter to its corresponding ASCII code. Examples would be the Linefeed, which is ASCII character code 10 decimal, the Carriage Return, which is 13 decimal, or the bell sound, which is decimal 7. On a PC, you can often add non-printable characters by holding down the Alt key, and typing in the decimal value (i.e., Alt-007 gets you a bell). There are other character encoding schemes, but ASCII is the most prevalent.

Non-Repudiation

Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

Null Session

Known as Anonymous Logon, it is a way of letting an anonymous user retrieve information such as user names and shares over the network or connect without authentication. It is used by applications such as explorer.exe to enumerate shares on remote servers.

Octet

A sequence of eight bits. An octet is an eight-bit byte.

One-Way Encryption

Irreversible transformation of plaintext to cipher text, such that the plaintext cannot be recovered from the cipher text by other than exhaustive procedures even if the cryptographic key is known.

One-Way Function

A (mathematical) function, f, which is easy to compute the output based on a given input. However given only the output value it is impossible (except for a brute force attack) to figure out what the input value is.

Open Shortest Path First (OSPF)

Open Shortest Path First is a link state routing algorithm used in interior gateway routing. Routers maintain a database of all routers in the autonomous system with links between the routers, link costs, and link states (up and down).

OSI

OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

OSI layers

The main idea in OSI is that the process of communication between two end points in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions. Each communicating user or program is at a computer equipped with these seven layers of function. So, in a given message between users, there will be a flow of data through each layer at one end down through the layers in that computer and, at the other end, when the message arrives, another flow of data up through the layers in the receiving computer and ultimately to the end user or program. The actual programming and hardware that furnishes these seven layers of function is usually a combination of the computer operating system, applications (such as your Web browser), TCP/IP or alternative transport and

network protocols, and the software and hardware that enable you to put a signal on one of the lines attached to your computer. OSI divides telecommunication into seven layers. The layers are in two groups. The upper four layers are used whenever a message passes from or to a user. The lower three layers (up to the network layer) are used when any message passes through the host computer or router. Messages intended for this computer pass to the upper layers. Messages destined for some other host are not passed up to the upper layers but are forwarded to another host. The seven layers are: Layer 7: The application layer...This is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. (This layer is not the application itself, although some applications may perform application layer functions.) Layer 6: The presentation layer...This is a layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). Sometimes called the syntax layer. Layer 5: The session layer...This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It deals with session and connection coordination. Layer 4: The transport layer...This layer manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer. Layer 3: The network layer...This layer handles the routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). The network layer does routing and forwarding. Layer 2: The data-link layer...This layer provides synchronization for the physical level and does bit-stuffing for strings of 1's in excess of 5. It furnishes transmission protocol knowledge and management. Layer 1: The physical layer...This layer conveys the bit stream through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier.

Overload

Hindrance of system operation by placing excess burden on the performance capabilities of a system component.

Packet

A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Packet Switched Network

A packet switched network is where individual packets each follow their own paths through the network from one endpoint to another.

Partitions

Major divisions of the total physical hard disk space.

Password Authentication Protocol (PAP)

Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear.

Password Cracking

Password cracking is the process of attempting to guess passwords, given the password file information.

Password Sniffing

Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch

A patch is a small update released by a software manufacturer to fix bugs in existing programs.

Patching

Patching is the process of updating software to a different version.

Payload

Payload is the actual application data a packet contains.

Penetration

Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Penetration Testing

Penetration testing is used to test the external perimeter security of a network or facility.

Permutation

Permutation keeps the same letters but changes the position within a text to scramble the message.

Personal Firewalls

Personal firewalls are those firewalls that are installed and run on individual PCs.

Pharming

This is a more sophisticated form of MITM attack. A user's session is redirected to a masquerading website. This can be achieved by corrupting a DNS server on the Internet and pointing a URL to the masquerading website's IP. Almost all users use a URL like www.worldbank.com instead of the real IP (192.86.99.140) of the website. Changing the pointers on a DNS server, the URL can be redirected to send traffic to the IP of the pseudo website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.

Phishing

The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site looks like they are part of a bank the user is doing business with.

Ping of Death

An attack that sends an improperly large ICMP echo request packet (a "ping") with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Ping Scan

A ping scan looks for machines that are responding to ICMP Echo Requests.

Ping Sweep

An attack that sends ICMP echo requests ("pings") to a range of IP addresses, with the goal of finding hosts that can be probed for vulnerabilities.

Plaintext

Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Point-to-Point Protocol (PPP)

A protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. It packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

Point-to-Point Tunneling Protocol (PPTP)

A protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet.

Poison Reverse

Split horizon with poisoned reverse (more simply, poison reverse) does include such routes in updates, but sets their metrics to infinity. In effect, advertising the fact that there routes are not reachable.

Polyinstantiation

Polyinstantiation is the ability of a database to maintain multiple records with the same key. It is used to prevent inference attacks.

Polymorphism

Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

Port

A port is nothing more than an integer that uniquely identifies an endpoint of a communication stream. Only one process per machine can listen on the same port number.

Port Scan

A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.

Possession

Possession is the holding, control, and ability to use information.

Post Office Protocol, Version 3 (POP3)

An Internet Standard protocol by which a client workstation can dynamically access a mailbox on a server host to retrieve mail messages that the server has received and is holding for the client.

Practical Extraction and Reporting Language (Perl)

A script programming language that is similar in syntax to the C language and that includes a number of popular Unix facilities such as sed, awk, and tr.

Preamble

A preamble is a signal used in network communications to synchronize the transmission timing between two or more systems. Proper timing ensures that all systems are interpreting the start of the information transfer correctly. A preamble defines a specific series of transmission pulses that is understood by communicating systems to mean "someone is about to transmit data". This ensures that systems receiving the information correctly interpret when the data transmission starts. The

actual pulses used as a preamble vary depending on the network communication technology in use.

Pretty Good Privacy (PGP)TM

Trademark of Network Associates, Inc., referring to a computer program (and related protocols) that uses cryptography to provide data security for electronic mail and other applications on the Internet.

Private Addressing

IANA has set aside three address ranges for use by private or non-Internet connected networks. This is referred to as Private Address Space and is defined in RFC 1918. The reserved address blocks are: 10.0.0.0 to 10.255.255.255 (10/8 prefix) 172.16.0.0 to 172.31.255.255 (172.16/12 prefix) 192.168.0.0 to 192.168.255.255 (192.168/16 prefix)

Program Infector

A program infector is a piece of malware that attaches itself to existing program files.

Program Policy

A program policy is a high-level policy that sets the overall tone of an organization's security approach.

Promiscuous Mode

When a machine reads all packets off the network, regardless of who they are addressed to. This is used by network administrators to diagnose network problems, but also by unsavory characters who are trying to eavesdrop on network traffic (which might contain passwords or other information).

Proprietary Information

Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

Protocol

A formal specification for communicating; an IP address the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection.

Protocol Stacks (OSI)

A set of network protocol layers that work together.

Proxy Server

A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Key

The publicly-disclosed component of a pair of cryptographic keys used for asymmetric cryptography.

Public Key Encryption

The popular synonym for "asymmetric cryptography".

Public Key Infrastructure (PKI)

A PKI (public key infrastructure) enables users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

Public-Key Forward Secrecy (PFS)

For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future.

QAZ

A network worm.

Race Condition

A race condition exploits the small window of time between a security control being applied and when the service is used.

Radiation Monitoring

Radiation monitoring is the process of receiving images, data, or audio from an unprotected source by listening to radiation signals.

Ransomware

A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

Reconnaissance

Reconnaissance is the phase of an attack where an attackers finds new systems, maps out networks, and probes for specific, exploitable vulnerabilities.

Reflexive ACLs (Cisco)

Reflexive ACLs for Cisco routers are a step towards making the router act like a stateful firewall. The router will make filtering decisions based on whether connections are a part of established traffic or not.

Registry

The Registry in Windows operating systems in the central set of settings and information required to run the Windows computer.

regression analysis

The use of scripted tests which are used to test software for all possible input is should expect. Typically developers will create a set of regression tests that are executed before a new version of a software is released. Also see "fuzzing".

Request for Comment (RFC)

A series of notes about the Internet, started in 1969 (when the Internet was the ARPANET). An Internet Document can be submitted to the IETF by anyone, but the IETF decides if the document becomes an RFC. Eventually, if it gains enough interest, it may evolve into an Internet standard.

Resource Exhaustion

Resource exhaustion attacks involve tying up finite resources on a system, making them unavailable to others.

Response

A response is information sent that is responding to some stimulus.

Reverse Address Resolution Protocol (RARP)

RARP (Reverse Address Resolution Protocol) is a protocol by which a physical machine in a local area network can request to learn its IP address from a gateway server's Address Resolution Protocol table or cache. A network administrator creates a table in a local area network's gateway router that maps the physical machine (or Media Access Control - MAC address) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine which can store it for future use.

Reverse Engineering

Acquiring sensitive data by disassembling and analyzing the design of a system component.

Reverse Lookup

Find out the hostname that corresponds to a particular IP address. Reverse lookup uses an IP (Internet Protocol) address to find a domain name.

Reverse Proxy

Reverse proxies take public HTTP requests and pass them to back-end webservers to send the content to it, so the proxy can then send the content to the end-user.

Risk

Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Assessment

A Risk Assessment is the process by which risks are identified and the impact of those risks determined.

Risk Averse

Avoiding risk even if this leads to the loss of opportunity. For example, using a (more expensive) phone call vs. sending an e-mail in order to avoid risks associated with e-mail may be considered "Risk Averse"

Rivest-Shamir-Adleman (RSA)

An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

Role Based Access Control

Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

Root

Root is the name of the administrator account in Unix systems.

Rootkit

A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

Router

Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.

Routing Information Protocol (RIP)

Routing Information Protocol is a distance vector protocol used for interior gateway routing which uses hop count as the sole metric of a path's cost.

Routing Loop

A routing loop is where two or more poorly configured routers repeatedly exchange the same packet over and over.

RPC Scans

RPC scans determine which RPC services are running on a machine.

Rule Set Based Access Control (RSBAC)

Rule Set Based Access Control targets actions based on rules for entities operating on objects.

S/Key

A security mechanism that uses a cryptographic hash function to generate a sequence of 64-bit, one-time passwords for remote user login. The client generates a one-time password by applying the MD4 cryptographic hash function multiple times to the user's secret key. For each successive authentication of the user, the number of hash applications is reduced by one.

Safety

Safety is the need to ensure that the people involved with the company, including employees, customers, and visitors, are protected from harm.

Scavenging

Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

Secure Electronic Transactions (SET)

Secure Electronic Transactions is a protocol developed for credit card transactions in which all parties (customers, merchant, and bank) are authenticated using digital signatures, encryption protects the message and provides integrity, and provides end-to-end security for credit card transactions online.

Secure Shell (SSH)

A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer (SSL)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Segment

Segment is another name for TCP packets.

Sensitive Information

Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Separation of Duties

Separation of duties is the principle of splitting privileges among multiple individuals or systems.

Server

A system entity that provides a service in response to requests from other system entities called clients.

Session

A session is a virtual connection between two hosts by which network traffic is passed.

Session Hijacking

Take over a session that someone else has established.

Session Key

In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

SHA1

A one way cryptographic hash function. Also see "MD5"

Shadow Password Files

A system file in which encryption user password are stored so that they aren't available to people who try to break into the system.

Share

A share is a resource made public on a machine, such as a directory (file share) or printer (printer share).

Shell

A Unix term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter. A shell usually implies an interface with a command syntax (think of the DOS operating system and its "C:>" prompts and user commands such as "dir" and "edit").

Signals Analysis

Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data.

Signature

A Signature is a distinct pattern in network traffic that can be identified to a specific tool or exploit.

Simple Integrity Property

In Simple Integrity Property a user cannot write data to a higher integrity level than their own.

Simple Network Management Protocol (SNMP)

The protocol governing network management and the monitoring of network devices and their functions. A set of protocols for managing complex networks.

Simple Security Property

In Simple Security Property a user cannot read data of a higher classification than their own.

Smartcard

A smartcard is an electronic badge that includes a magnetic strip or chip that can record and replay a set key.

Smishing

Smishing is a combination of the terms "SMS" and "phishing." It is similar to phishing, but refers to fraudulent messages sent over SMS (text messaging) rather than email.

Smurf

The Smurf attack works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer

A sniffer is a tool that monitors network traffic as it received in a network interface.

Sniffing

A synonym for "passive wiretapping."

Social Engineering

A euphemism for non-technical or low-technology means - such as lies, impersonation, tricks, bribes, blackmail, and threats - used to attack information systems.

Socket

The socket tells a host's IP stack where to plug in a data stream so that it connects to the right application.

Socket Pair

A way to uniquely specify a connection, i.e., source IP address, source port, destination IP address, destination port.

SOCKS

A protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. SOCKS uses

sockets to represent and keep track of individual connections. The client side of SOCKS is built into certain Web browsers and the server side can be added to a proxy server.

Software

Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Source Port

The port that a host uses to connect to a server. It is usually a number greater than or equal to 1024. It is randomly generated and is different each time a connection is made.

Spam

Electronic junk mail or junk newsgroup postings.

Spanning Port

Configures the switch to behave like a hub for a specific port.

Split Horizon

Split horizon is a algorithm for avoiding problems caused by including routes in updates sent to the gateway from which they were learned.

Split Key

A cryptographic key that is divided into two or more separate data items that individually convey no knowledge of the whole key that results from combining the items.

Spoof

Attempt by an unauthorized entity to gain access to a system by posing as an authorized user.

SQL Injection

SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

Stack Mashing

Stack mashing is the technique of using a buffer overflow to trick a computer into executing arbitrary code.

Standard ACLs (Cisco)

Standard ACLs on Cisco routers make packet filtering decisions based on Source IP address only.

Star Property

In Star Property, a user cannot write data to a lower classification level without logging in at that lower classification level.

State Machine

A system that moves through a series of progressive conditions.

Stateful Inspection

Also referred to as dynamic packet filtering. Stateful inspection is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection examines not just the header information but also the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination.

Static Host Tables

Static host tables are text files that contain hostname and address mapping.

Static Routing

Static routing means that routing table entries contain information that does not change.

Stealthing

Stealthing is a term that refers to approaches used by malicious code to conceal its presence on the infected system.

Steganalysis

Steganalysis is the process of detecting and defeating the use of steganography.

Steganography

Methods of hiding the existence of a message or other data. This is different than cryptography, which hides the meaning of a message but does not hide the message itself. An example of a steganographic method is "invisible" ink.

Stimulus

Stimulus is network traffic that initiates a connection or solicits a response.

Store-and-Forward

Store-and-Forward is a method of switching where the entire packet is read by a switch to determine if it is intact before forwarding it.

Straight-Through Cable

A straight-through cable is where the pins on one side of the connector are wired to the same pins on the other end. It is used for interconnecting nodes on the network.

Stream Cipher

A stream cipher works by encryption a message a single bit, byte, or computer word at a time.

Strong Star Property

In Strong Star Property, a user cannot write data to higher or lower classifications levels than their own.

Sub Network

A separately identifiable part of a larger network that typically represents a certain limited number of host computers, the hosts in a building or geographic area, or the hosts on an individual local area network.

Subnet Mask

A subnet mask (or number) is used to determine the number of bits used for the subnet and host portions of the address. The mask is a 32-bit value that uses one-bits for the network and subnet portions and zero-bits for the host portion.

Switch

A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.

Switched Network

A communications network, such as the public switched telephone network, in which any user may be connected to any other user through the use of message, circuit, or packet switching and control devices. Any network providing switched communications service.

Symbolic Links

Special files which point at another file.

Symmetric Cryptography

A branch of cryptography involving algorithms that use the same key for two different steps of the algorithm (such as encryption and decryption, or signature creation and signature verification). Symmetric cryptography is sometimes called "secret-key cryptography" (versus public-key cryptography) because the entities that share the key.

Symmetric Key

A cryptographic key that is used in a symmetric cryptographic algorithm.

SYN Flood

A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

Synchronization

Synchronization is the signal made up of a distinctive pattern of bits that network hardware looks for to signal that start of a frame.

Syslog

Syslog is the system logging facility for Unix systems.

System Security Officer (SSO)

A person responsible for enforcement or administration of the security policy that applies to the system.

System-Specific Policy

A System-specific policy is a policy written for a specific system or device.

T-U

T1, T3

A digital circuit using TDM (Time-Division Multiplexing).

Tamper

To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

TCP Fingerprinting

TCP fingerprinting is the user of odd packet header combinations to determine a remote operating system.

TCP Full Open Scan

TCP Full Open scans check each port by performing a full three-way handshake on each port to determine if it was open.

TCP Half Open Scan

TCP Half Open scans work by performing the first half of a three-way handshake to determine if a port is open.

TCP Wrapper

A software package which can be used to restrict access to certain network services based on the source of the connection; a simple tool to monitor and control incoming network traffic.

TCP/IP

A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

TCPDump

TCPDump is a freeware protocol analyzer for Unix that can monitor network traffic on a wire.

TELNET

A TCP-based, application-layer, Internet Standard protocol for remote login from one host to another.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment

A threat assessment is the identification of types of threats that an organization might be exposed to.

Threat Model

A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector

The method a threat uses to get to the target.

Time to Live

A value in an Internet Protocol packet that tells a network router whether or not the packet has been in the network too long and should be discarded.

Tiny Fragment Attack

With many IP implementations it is possible to impose an unusually small fragment size on outgoing packets. If the fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it didn't hit a match in the filter. STD 5, RFC 791 states: Every Internet module must be able to forward a datagram of 68 octets without further fragmentation. This is because an Internet header may be up to 60 octets, and the minimum fragment is 8 octets.

Token Ring

A token ring network is a local area network in which all computers are connected in a ring or star topology and a binary digit or token-passing scheme is used in order to prevent the collision of data between two computers that want to send messages at the same time.

Token-Based Access Control

Token based access control associates a list of objects and their privileges with each user. (The opposite of list based.)

Token-Based Devices

A token-based device is triggered by the time of day, so every minute the password changes, requiring the user to have the token with them when they log in.

Topology

The geometric arrangement of a computer system. Common topologies include a bus, star, and ring. The specific physical, i.e., real, or logical, i.e., virtual, arrangement of the elements of a network. Note 1: Two networks have the same topology if the connection configuration is the same, although the networks may differ in physical interconnections, distances between nodes, transmission rates, and/or signal types. Note 2: The common types of network topology are illustrated

Traceroute (tracert.exe)

Traceroute is a tool the maps the route a packet takes from the local machine to a remote destination.

Transmission Control Protocol (TCP)

A set of rules (protocol) used along with the Internet Protocol to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Transport Layer Security (TLS)

A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third

party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.

Triple DES

A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.

Triple-Wrapped

S/MIME usage: data that has been signed with a digital signature, and then encrypted, and then signed again.

Trojan Horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Trunking

Trunking is connecting switched together so that they can share VLAN information between them.

Trust

Trust determine which permissions and what actions other systems or users can perform on remote machines.

Trusted Ports

Trusted ports are ports below number 1024 usually allowed to be opened by the root user.

Tunnel

A communication channel created in a computer network by encapsulating a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one. Most often, a tunnel is a

logical point-to-point link - i.e., an OSI layer 2 connection - created by encapsulating the layer 2 protocol in a transport protocol (such as TCP), in a network or inter-network layer protocol (such as IP), or in another link layer protocol. Tunneling can move data between computers that use a protocol not supported by the network connecting them.

UDP Scan

UDP scans perform scans to determine which UDP ports are open.

Unicast

Broadcasting from host to host.

Uniform Resource Identifier (URI)

The generic term for all types of names and addresses that refer to objects on the World Wide Web.

Uniform Resource Locator (URL)

The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, http://www.pcwebopedia.com/ind... .

Unix

A popular multi-user, multitasking operating system developed at Bell Labs in the early 1970s. Created by just a handful of programmers, Unix was designed to be a small, flexible system used exclusively by programmers.

Unprotected Share

In Windows terminology, a "share" is a mechanism that allows a user to connect to file systems and printers on other systems. An "unprotected share" is one that allows anyone to connect to it.

User

A person, organization entity, or automated process that accesses a system, whether authorized to do so or not.

User Contingency Plan

User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

User Datagram Protocol (UDP)

A communications protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network. UDP uses the Internet Protocol to get a datagram from one computer to another but does not divide a message into packets (datagrams) and reassemble it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in.

Virtual Private Network (VPN)

A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corporation has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

Virus

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Vishing (voice or VoIP phishing)

Vishing refers to phishing attacks that involve the use of voice calls, using either conventional phone systems or Voice over Internet Procotol (VoIP) systems.

Voice Firewall

A physical discontinuity in a voice network that monitors, alerts and controls inbound and outbound voice network activity based on user-defined call admission control (CAC) policies, voice application layer security threats or unauthorized service use violations.

Voice Intrusion Prevention System (IPS)

Voice IPS is a security management system for voice networks which monitors voice traffic for multiple calling patterns or attack/abuse signatures to proactively detect and prevent toll fraud, Denial of Service, telecom attacks, service abuse, and other anomalous activity.

War Chalking

War chalking is marking areas, usually on sidewalks with chalk, that receive wireless signals that can be accessed.

War Dialer

A computer program that automatically dials a series of telephone numbers to find lines connected to computer systems, and catalogs those numbers so that a cracker can try to break into the systems.

War Dialing

War dialing is a simple means of trying to identify modems in a telephone exchange that may be susceptible to compromise in an attempt to circumvent perimeter security.

War Driving

War driving is the process of traveling around looking for wireless access point signals that can be used to get network access.

Web of Trust

A web of trust is the trust that naturally evolves as a user starts to trust other's signatures, and the signatures that they trust.

Web Server

A software process that runs on a host computer connected to the Internet to respond to HTTP requests for documents from client web browsers.

WHOIS

An IP for finding information about resources on networks.

Windowing

A windowing system is a system for sharing a computer's graphical display presentation resources among multiple applications at the same time. In a computer that has a graphical user interface (GUI), you may want to use a number of applications at the same time (this is called task). Using a separate window for each application, you can interact with each application and go from one application to another without having to reinitiate it. Having different information or activities in multiple windows may also make it easier for you to do your work. A windowing system uses a window manager to keep track of where each window is located on the display screen and its size and status. A windowing system doesn't just manage the windows but also other forms of graphical user interface entities.

Windump

Windump is a freeware tool for Windows that is a protocol analyzer that can monitor network traffic on a wire.

Wired Equivalent Privacy (WEP)

A security protocol for wireless local area networks defined in the standard IEEE 802.11b.

Wireless Application Protocol

A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for

Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat.

Wiretapping

Monitoring and recording data that is flowing between two points in a communication system.

World Wide Web ("the Web", WWW, W3)

The global, hypermedia-based collection of information and services that is available on Internet servers and is accessed by browsers using Hypertext Transfer Protocol and other information retrieval mechanisms.

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Zero Day

The "Day Zero" or "Zero Day" is the day a new vulnerability is made known. In some cases, a "zero day" exploit is referred to an exploit for which no patch is available yet. ("day one" - day at which the patch is made available).

Zero-day attack

A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

Zombies

A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most

owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.