УДК 004.056.5:004.421.2:004.415.2

МІКРОПРОЦЕСОРНА КРИМІНАЛІСТИКА: АНАЛІЗ АТАК ЧЕРЕЗ ПАРАЗИТНІ ЕНЕРГЕТИЧНІ КОЛИВАННЯ

Полотай О.І.
Львівський державний університет безпеки життєдіяльності

Анотація. *У роботі розглядається сучасний напрям кібербезпеки — мікропроцесорна криміналістика, що базується на аналізі паразитних енергетичних коливань мікропроцесорів для виявлення кіберзагроз. Показано, що навіть незначні зміни у споживанні енергії, коливання тактової частоти чи теплові аномалії можуть сигналізувати про присутність шкідливого програмного забезпечення, апаратних бекдорів або атак через side-channel. Проаналізовано основні методи криміналістики на мікропроцесорному рівні, включаючи аналіз енергоспоживання, електромагнітного випромінювання, кеш-патернів та тимчасових характеристик, а також їх застосування для розслідування і прогнозування кіберінцидентів. Результати підкреслюють ефективність апаратного моніторингу як додаткового інструменту кіберзахисту і цифрової криміналістики.*

Ключові слова: *мікропроцесорна криміналістика; паразитні енергетичні коливання; side-channel атаки; апаратна безпека; аналіз кеш-пам'яті; електромагнітний аналіз; тимчасові аномалії; цифрова криміналістика; кіберзагрози; апаратні бекдори..*

Вступ. Зростання складності сучасних комп'ютерних систем та процесорних архітектур створює нові виклики для кібербезпеки. Одним із перспективних і водночас маловивчених напрямів є мікропроцесорна криміналістика, яка дозволяє виявляти атаки та аномальні дії через аналіз паразитних енергетичних коливань, що виникають під час роботи електронних компонентів. Навіть незначні зміни у споживанні електроенергії або напрузі можуть сигналізувати про стороннє втручання, спроби експлуатації вразливостей або приховану діяльність шкідливого програмного забезпечення. Тема стає особливо актуальною в умовах росту кількості апаратних атак, коли класичні засоби виявлення шкідливого ПЗ або вторгнень можуть бути неефективними.

Основна частина. Мікропроцесорна криміналістика ґрунтується на тому, що будь-який електронний пристрій під час роботи генерує специфічні енергетичні сигнали, що залежать від виконуваних інструкцій, навантаження на ядра та взаємодії з периферією. Паразитні коливання, тобто мікроскопічні відхилення напруги або струму, можуть виникати через апаратні збої, а також бути наслідком впровадження шкідливого коду або сторонніх процесів, що намагаються використовувати уразливості мікропроцесора. Аналіз цих коливань дозволяє відстежувати навіть приховані дії, що не залишають слідів у традиційних журналах подій або операційних системах.

За допомогою спеціалізованих датчиків та високочастотного моніторингу енергетичних характеристик можна виявити аномалії, які корелюють з потенційними атаками. Наприклад, спроби здійснення side-channel

атак, таких як атаки на кеш або через коливання тактової частоти, створюють закономірні, хоч і мінімальні, відхилення у споживанні енергії. Виявлення цих відхилень дозволяє проводити ретроспективний аналіз дій на мікропроцесорному рівні, відтворювати сценарії атаки та ідентифікувати вектор вторгнення. Це відкриває нові можливості для цифрової криміналістики, особливо в умовах складних гібридних систем, де традиційні методи безпеки виявляються недостатньо чутливими.

В таблиці 1 наведено опис методів мікропроцесорної криміналістики, які є популярними на даний час.

Таблиця 1 – перелік методів мікропроцесорної криміналістики

Метод	Суть методу	Що дозволяє виявити	Типові сценарії застосування
Аналіз паразитних енергетичних коливань (Power Analysis)	Вимірювання коливань напруги та струму під час роботи мікропроцесора.	Приховані процеси, шкідливий код, side-channel атаки, аномальні інструкції.	Виявлення атак на криптографічні модулі, зчитування активності під час експлуатації вразливостей.
Електромагнітний аналіз (EM Analysis)	Реєстрація електромагнітного випромінювання, яке генерується процесором під час виконання інструкцій.	Стороннє втручання, шпигунські закладки, витік даних через ЕМ-канали.	Дослідження апаратних бекдорів, аналіз шкідливого ПЗ, що працює на низькому рівні.
Темпоральний аналіз (Timing Analysis)	Вимірювання часу виконання інструкцій і затримок.	Атаки на кеш, експлуатація вразливостей спекулятивного виконання, приховані інструкції.	Розслідування атак Spectre/Meltdown-типу, аналіз аномальних часових патернів.
Аналіз коливань тактової частоти (Clock Skew Analysis)	Відстеження змін стабільності та частоти тактового генератора.	Спроби зламати систему через зміну clock skew, приховане навантаження, несправності.	Виявлення прихованих обчислювальних процесів або шкідливих модифікацій мікропрограми.
Аналіз теплового профілю (Thermal Forensics)	Вимір температурних змін на корпусі або всередині чипа.	Перегрів через шкідливий код, нехарактерне навантаження, виконання прихованих інструкцій.	Діагностика майнерів, rootkit-ів, мікрофірмового шкідливого ПЗ.
Аналіз кеш-патернів (Cache Behaviour Analysis)	Відстеження поведінки кеш-пам'яті та її заповнення.	Side-channel атаки, атаки на кеш-лінії, приховані обчислення.	Розслідування атак типу Flush+Reload, Prime+Probe, Evict+Time.
Аналіз роботи шин (Bus Traffic Forensics)	Моніторинг даних, що передаються внутрішніми шинами процесора та пам'яті.	Несанкціоновані звернення, приховані DMA-операції, доступ до заборонених областей пам'яті.	Розслідування атак на периферію, firmware-бекдорів, апаратних троянів.

Інтеграція методів мікропроцесорної криміналістики у системи кіберзахисту підприємств або критичних об'єктів дозволяє підвищити точність моніторингу та скоротити час реагування на атаки. Аналіз паразитних енергетичних коливань може стати частиною багаторівневої стратегії безпеки, поєднуючи апаратний контроль із поведінковим моніторингом програмного забезпечення. Це забезпечує можливість виявлення атак, які приховані від традиційних засобів логування та мережевого аналізу, і сприяє формуванню більш ефективних методів захисту високотехнологічних систем.

Висновки. Мікропроцесорна криміналістика відкриває новий підхід до аналізу кіберзагроз, концентруючись на паразитних енергетичних коливаннях, що супроводжують роботу апаратних компонентів. Виявлення таких сигналів дозволяє ідентифікувати приховані атаки, які не фіксуються традиційними засобами безпеки, та формувати більш точні моделі кіберзахисту. Метод демонструє потенціал для інтеграції у сучасні багаторівневі системи моніторингу, що поєднують апаратний контроль, аналіз поведінки програмного забезпечення та прогнозування ризиків. Впровадження цього підходу здатне значно підвищити стійкість критичних об'єктів та корпоративних мереж до нових видів атак на апаратному рівні

Література

1. Гора І.В., Колесник В.А, Попович І.І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. Науковий вісник Ужгородського Національного Університету, 2024. С. 63-70.

2. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. – Харків : Право, 2024. – 208 с.

3. Полотай О.І. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. Вісник ЛДУБЖД : зб. наук. праць. Львів : ЛДУБЖД, 2023. № 28. С. 73–80.