Олійник, Ю.А., Вацлавик О.М.
Львівський державний університет безпеки життєдіяльності,
м. Львів

АТАКА НА ДРОНИ ТА ЗАХИСТ ПЕРЕДАЧІ ДАНИХ

Дрони зарекомендували себе у різних сферах життєдіяльності люди, вони широко застосовуються у кіноіндустрії, картографії, сільському господарстві, у розважальних цілях, як мобільні камери відео нагляду так і у наукови цілях, з метою добратися до важкодоступних місць. Їхнє використання може бути зумовленеодним із наступних чинників:необхідність забезпечення мобільності, неможливість використання дротової мережі, відсутність інших без провідникових технологій у робочій зоні.

Потрібно розуміти, що піднятися в повітря – не проблема. Після підйому в повітряний простір починається основний етап – збереження і передання отриманої інформації. Якщо говорити про сам етап використання безпілотних технологій у контексті якоїсь промислової експлуатації, то сам підйом у повітряний простір – це 20% успіху, решта – робота з інформацією. І саме це дає певну цінність при впровадженні цієї технології.

Всідрони сконструйовані на базізвичайних модулів, основним з яких є блок управління – чіп і набір сенсорів. Проаналізувавши конфігурацію і контролери декількох дронів в пошуках різних прогалин у системі безпеки і потенційних векторів атак, були виявлені слабкі місця.

Як з'ясувалося, електронний мозок дрона можнаобійти масою способів – від встановлення програмних закладок доінжекції сфальсифікованих пакетів даних радіоканалу телеметрії. Головна проблема полягає в тому, що для керування використовуються небезпечні методи. Використовуються протоколи загального призначення, відсутні засоби надійної аутентифікації, сигнал GPS легко глушиться, а завантажувач навіть не перевіряє цифровий підпис прошивки. В результаті програмне забезпечення базової станції дозволяє втрутитися в політ чужих дронів і викрасти їх.

Одним із перших на це звернув увагу Самі Камкар (Samy Kamkar). Пару років тому для демонстрації уразливості він навіть перетворив іграшковий дрон в радіоперехоплювач. Літаючи серед інших безпілотників, він сканував діапазон за допомогою модуля Wi-Fi. Розміщений на борту одноплатний комп'ютер обробляв

зібраніпакети програмою SkyJack. Виявивши керуючі команди для інших дронів, він підміняв їх і примушував слідувати ошукані дрони за собою, заглушаючи сигнали цих контролерів.

Spoofing атака на GPS - атака, яка намагається обдурити GPS-приймач, широкомовно передаючи трохи більш потужний сигнал, ніж отриманий від супутників GPS, такий, щоб бути схожим на ряд нормальних сигналів GPS. Ціімітуючі сигнали, змінені таким способом, щоб змусити одержувача не визначити своє місце розташування, вважаючи його таким, яке відправить атакуючий. Оскільки системи GPS працюють вимірюючи час, який потрібен для сигналу, щоб дійти від супутника доодержувача, успішний spoofing вимагає, щоб атакуючий точно знав, де його мета - так, щоб імітуючий сигнал міг бути структурований з належними затримками сигналу.

Більш складні дрони замість wi-fi мають вмонтованіінші технології бездротового зв'язку, але під час польоту вони також інтенсивнообмінюються даними з наземною станцією і запрошують коригування маршруту. Пакети телеметрії завжди можна розшифрувати, модифікувати і використовувати для перехоплення управління. При атаці надрона, йомупосилаються помилкові коригування маршруту, а від диспетчераскривається справжнє місцеположення дрона. Однак проблемапостає не стільки в конкретних помилках, скільки в нестачі загального підходу до проектування.

Отже, захист прошивки дрона, безпечного використання завантажувача, впровадження механізмів аутентифікації і шифрування – все це необхідні заходи, але кожну з них зловмисник можеобійти. Тому реальне завдання полягає не в тому, щоб створити «незламні» дрони, а максимально ускладнити сам процес перехоплення управління дроном і зробити йогоекономічно невиправданим.

Література

1. ARP Spoofing — подмена ARP-информации- [Електронний ресурс]. - Режим доступу: http://subnets.ru/blog/?p=26

2. GPS-спуфинг на беспилотный летательный апарат- [Електронний ресурс]. - Режим доступу:https://xakep.ru/2012/07/02/58927/

3. Дрон- [Електронний ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/%D0%94%D1%80%D0%BE%D0%BD