Використання трансферних вузлів рухомих мереж для атаки на комп'ютерні системи наземних абонентів мережі

Ірина Журавська
кафедра комп'ютерної інженерії,
Чорноморський національний університет імені Петра Могили
Миколаїв, Україна
irina.zhuravska@chmnu.edu.ua

Use of movable networks' transfer nodes to attack on computer systems of land subscribers of the network

Iryna Zhuravska
Department of Computer Engineering
Petro Mohyla Black Sea National University
Mykolaiv, Ukraine
irina.zhuravska@chmnu.edu.ua

***Анотація* – Розглянуто проблему використання трансферних вузлів рухомого мережі на основы безпілотних апаратів (БПЛА) для організації атаки на комп'ютерні системи наземних абонентів такої мережі. Досліджена техніка ARP-спуфінгу при залученні відкритих WiFi мереж. Намічено шляхи вирішення описаної проблеми.**

***Abstract* – The problem of using transfer nodes of a movable network based on unmanned vehicles (UAVs) for organizing attacks on computer systems of land subscribers of such a network is considered. The technique of ARP-spoofing was investigated with the use of open WiFi networks. The ways of solving the described problem are shown.**

Ключові слова* – *рухомі мережі БПЛА, атака «людина посередині», перехоплення трафіку, ARP-спуфінг, VPN-сервер.

Keywords* – *movable UAV's flock, MitM-атака, ARP-spoofing, VPN-server.

I.Вступ

Уразливість каналу передачі даних з безпілотного літального апарата (БПЛА) до наземного командного центру (КЦ) або до наземного рухомого абонента (НА) є об'єктом пильної уваги фахівців з інформаційної безпеки з 2009 р., коли «іранські хакери» здійснили перехоплення відео з військового дрона США за допомогою програмного забезпечення (ПЗ) SkyGrabber від російської компанії-виробника SkySoftware [1]. При цьому іранські повстанці використовували для відеоперехоплення незахищені канали зв'язку з БПЛА.

Останнім часом відомі приклади злому/перехоплення і аналізу трафіку дронів Parrot AR.Drone і DJI Phantom за допомогою програмного продукту WiFi Pineapple від американської компанії Hak5 LLC. ПЗ WiFi Pineapple на теперішній час вільно розповсюджуються через магазин додатків Google Play [2]. У випадку запуску цього ПЗ виконується примусове з'єднання бездротового клієнта-«жертви» з роутером «агресора», прошитим спеціальним ПЗ на базі OpenWRT, або ж з Android-пристроєм версії 4.0 або більш пізньої. Для аудиту бездротових мереж і перехоплення трафіку в цьому випадку використовуються утиліти Karma та PineAP [3].

Всі бездротові пристрої, не підключені в даний момент до мережі Wi-Fi, активно намагаються це зробити, розсилаючи запити в пошуках точок доступу (ТД), до яких раніше здійснювалося підключення. Karma відповідає на ці запити, представляючись тією ТД, яку шукає клієнт. Це поширюється тільки на запити відкритих мереж (в публічних кафе або ін. громадських місцях), не захищених шифруванням WEP/WPA/WPA2. На даний момент ефективність роботи Karma знизилася, так як нові пристрої і версії операційних систем (ОС) прагнуть убезпечити користувачів від цієї уразливості. Але, у такій ситуації не меншу небезпеку становить утиліта PineAP, яка діє за протилежним Karma принципом: не чекає запиту, а замість цього бомбардує клієнта запитами на підключення за списком ідентифікаторів бездротових мереж (англ. Service Set Identification або SSID), який можна вести як вручну, так і збирати утилітою Autoharvest.

Поєднання двох зазначених методів дає дуже високу ймовірність примусового підключення бездротового клієнта на ТД агресора.

II. Теоретичний базис
MitM-атаки у рухомих мережах

Метою атаки у рухомих мережах є отримання конфіденційних даних абонентів з метою перехоплення трафіку даних БПЛА-НА, БПЛА-КЦ, НА-КЦ та зворотного, тобто керуючого трафіку.

Припустимо, що НА не має доступ до КЦ безпосередньо через надмірне віддалення. Деякі з дронів (БПЛА) рухомої мережі також не мають безпосереднього зв'язку с КЦ. У такому разі трафік транслюється через трансферні вузли рухомої мережі, якими виступають БПЛА, що знаходяться на такій відстані один від одного, на якій забезпечується стабільний радіозв'язок між усіма парами абонентів мережі [4]. При такій топології мережі для трансферу даних з БПЛА можуть бути задіяні публічні мережі (кафе, пошти, аеропорту, вишів, тощо), підключення до яких здійснюється через ТД. Це означає, що користувач, відправляючи свої дані на певний сервер КЦ, направляє їх через ТД, а вона, в свою чергу, може направити їх на проксі-сервер, де зловмисник зможе їх обробити.

Такий тип атак називається MitM (Man-in-the-Middle) і схематично зображується, як показано на рис. 1.

A. SSL-strip техніка для перехоплення https-з'єднань

Зазвичай за такою схемою тип з'єднання – https. Це означає, що дані шифруються протоколом SSL і приймають зовсім «нечитабельним» вид для атакуючого. В такому випадку, для обходу такого захисту можна застосувати цілий ряд методів. Наприклад, SSL-strip.

SSL-strip – «тиха» техніка для перехоплення https-з'єднань. «Тихою» її називають саме тому, що користувачеві мережі її дуже важко помітити. Більш того, при наявності у мережі БПЛА за появою додаткових сторонніх підключень до безпілотних апаратів слідкувати не тільки неможливо, але й нікому. Тому в такій мережі суть цієї техніки гранично проста: атакуючим (на рис. 1 це дрон-агресор), що знаходяться «посередині», аналізується http-трафік, виявляються всі посилання виду https:// і проводиться їх заміна на http://. Отже, при цьому клієнт авторизується в нав'язаному сеансі дрона-агресора, і його облікові дані тут же потрапляють в журнал агресора. Після цього перехоплення даних проводиться практично як у легітимному сеансі зв'язку.

Управління MitM-комплексом здійснюється або через веб-інтерфейс, або віддалено по протоколу SSH (для віддаленого доступу до встановленої в цільової точці атаки в MitM-системі передбачається автоматично піднятий при включенні зворотний SSH-тунель).

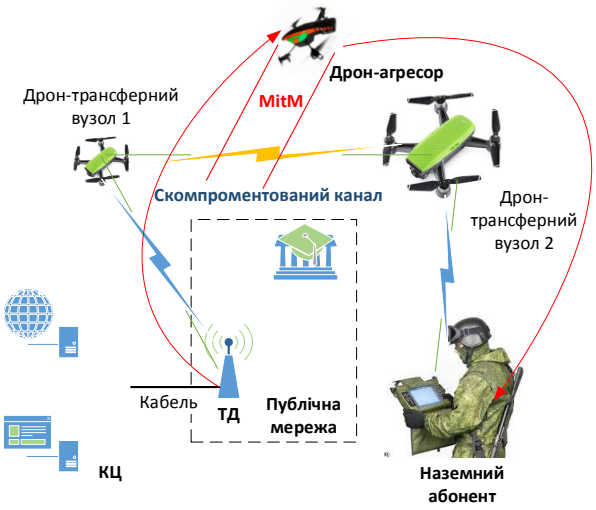

Рис. 1. Загальна схема MitM-атаки на наземного абонента рухомої мережі через трансферний вузол

B. Атака з імітацією техніки handshake`a

Існують також і інші способи, наприклад, імітація handshake`a («хендшейка») під час активного з'єднання. Суть такого методу полягає в тому, що зловмисник прикидається кінцевою точкою сеансу, і, отримавши дані користувача, розшифровує їх своїм ключем, аналізує їх в «читабельному» вигляді і передає далі на сервер КЦ та НА, зашифрованими іншим – власним – ключем (рис. 2).

Рис. 2. Схема MitM-атаки на наземного абонента рухомої мережі з імітацією handshake`a

C. Атака з використанням ARP-Spoofing'у

Якщо у зловмисника немає доступу до ТД, йому доводиться користуватися більш серйозними методиками атаки, наприклад, такими як ARP-Spoofing.

У цьому випадку контроль над ТД не потрібен. При реалізації даної атаки зловмисник отримує доступ до трафіку жертви за допомогою зміни її ARP-таблиці. Це досягається шляхом постійного

відправлення ARP-відповідей пристрою жертви (НА), і, якщо необхідний зворотний трафік, та й до ТД. При цьому ARP-відповіді відправляються без запиту від НА і ТД. Суть ARP-спуфінгу полягає в тому, що зловмисник змінює MAC-адресу ТД на свій, в результаті чого трафік починає проходити через пристрій агресора.

III. Дослідження процесу організації MitM-атаки у рухомій мережі

Припустимо, в одній мережі є 3 пристрої з наступними IP- та MAC-адресами (табл. 1).

TABLE IV. Таблиця 1. IP- та MAC-адреси об'єктів рухомої мережі

IP адреса	MAC-адреса	Тип об'єкту мережі
192.168.1.1	E8-94-F6-CA-8E-7C	ТД
192.168.1.170	30-85-A9-9F-3C-FA	Дрон-агресор
192.168.1.173	00-0C-29-43-8A-5D	НА

Так виглядає ARP-таблиця жертви – НА – до спуфінгу (рис. 3):

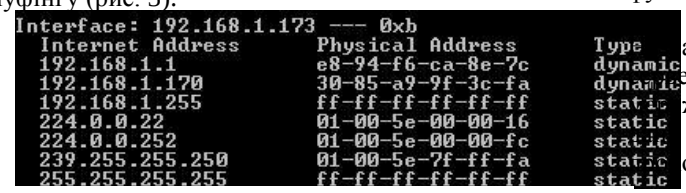

Рис. 3. ARP-таблиця НА до атаки

Для організації атаки використовувався інструмент аналізу безпеки Intercepter-NG [5]. Для початку була обрана і додана в список атакованих жертва – НА (рис. 4).

Рис. 4. Вибір жертви – НА – для ARP-спуфінгу

Був запущений сніфер й почата атака (рис. 5).

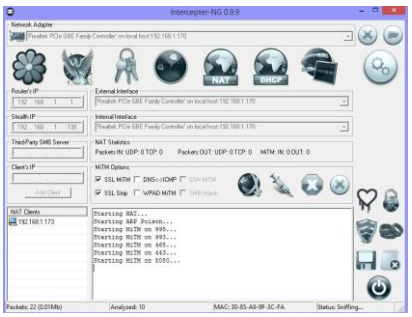

Рис. 5. Старт атаки

Почавши атаку, зловмисник посилає пристрою жертви свою MAC-адресу в якості MAC-адреси ТД, в результаті чого ARP-таблиця жертви набуває такого вигляду (рис. 6).

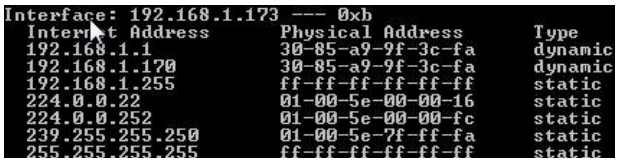

Рис. 6. ARP-таблиця НА в процесі атаки

Як можна побачити з рис. 6, MAC-адреса напроти IP-адреси 192.168.1.1 (IP-адреси ТД) змінився на MAC-адресу зловмисника. Таким чином, дроном-агресором був перехоплений доступ до трафіку жертви – НА, який фактично тепер буде надсилати дані не до КЦ через ТД, а на дрон-агресор.

Після отримання доступу до трафіку, зловмисник буде вирішувати питання криптоанализа даних, які пройшли через SSL-шифрування.

IV. Висновки

З цього дослідження можна зробити висновок, що при організації взаємодії об'єктів рухомої мережі дані, які накопичуються та передаються з НА до КЦ та навпаки через БПЛА, котрі виконують функцію трансферних вузлів, є дуже вразливими використанні відкритих публічних мереж. ажаючи на всілякі технології захисту з боку ерів КЦ, який здійснює керування рухомою жею, призначені для об'єктів рухомої мережі можуть бути скомпрометовані при одженні через публічну мережу.

Дієвим виходом з такої ситуації може бути мплементація VPN-серверів – власної розробки, сторонніх або вбудованих в системи антивірусного захисту. До того ж, доцільно розглянути ефективність для захисту трафіку заходів, що вживаються до підвищення завадостійкості канала зв'язку.

Література References

[1] S. Gorman, Yo. J. Dreazen, and A. Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal*, Upd. Dec. 17, 2009, URL : https://www.wsj.com/articles/SB126102247889095011 (Last accessed : 16.10.2017).

[2] WiFi Pineapple Connector, *Google Play* : Play Market, URL : https://play.google.com/store/apps/details?id=org.hak5.pineappleconnector&hl=ru (Last accessed 16.10.2017).

[3] С. Карасиков, "WiFi Pineapple Mark V: черный ящик для беспроводного перехвата," *Хабрахабр : Информационная безопасность*, Опубл. 12 декабря 2014 г., URL : https://habrahabr.ru/post/245717/ (дата обращения 16.10.2017).

[4] I. Burlachenko, I. Zhuravska, and M. Musiyenko, "Devising a method for the active coordination of video cameras in optical navigation based on multi-agent approach," *Eastern-European Journal of Enterprise Technologies*, vol. 1, issue 9 (85), pp. 17–25, 2017. doi: 10.15587/1729-4061.2017.90863.

[5] Обзор новых функций Intercepter-NG, *Хабрахабр : Информационная безопасность*, Опубл. 29 июля 2014 г., URL : http://habrahabr.ru/post/231369/ (дата обращения 16.10.2017).