тистичні дані. Обмеження Wireshark: потребує найкращого розуміння форматів протоколів; знання мови у форматі байтів; не є автоматизованим інструментом та не підтримує моніторинг в тривалому часі [2].

Для порівняння наданих інструментів мережевого аналізу слідує використовувати таки параметри, як тип вихідного коду, кількість підтримуваних протоколів, підтримувана операційна система, вартість, форми декодування тощо.

Colasoft має функції аналізу більш візуального пояснення зі статистикою захоплених пакетів, відображенням більшої кількості інформації про протоколи та користувацькі програми з графіками та матричним поданням для всіх підключених кінцевих точок. Colasoft, у порівнянні з Wireshark, забезпечує більшу мережеву безпеку. Проте, він охоплює лише 300 протоколів, що дуже менше порівняно з Wireshark, який підтримує 1100 протоколів. TCPDump - це дуже портативний і економічний пакет.

Таким чином, аналіз інструментів моніторингу мережевого трафіку показав, що Wireshark, Colasoft є досить ефективними інструментами в протидії кіберзлочинності, а завдяки своїй доступності Wireshark надає для кіберполіції широкі можливості аналізу множини протоколів, що прискорить розслідування протиправних діянь в кіберпросторі.

Список використаних джерел

1. Горбовський А. І., Войтович О. П. Дослідження безпеки у інтернеті речей // Матеріали XLVI науково-технічної конференції підрозділів ВНТУ, Вінниця, 22-24 березня 2017 р. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17277/2805.pdf?sequence=3 (дата звернення: 23.04.2021).

2. Smarter Security For Your Everything, Atmel Has You Covered // Microchip : вебсайт. 2019. URL: https://www.microchip.com/design-centers/security-ics (дата звернення: 23.04.2021).

3. Асангханва Ю., Ий Р., Сыров А. Повышение уровня безопасности граничных узлов интернета вещей с помощью микросхем ATECC608A компании microchip. *Электроника НТБ*. 2019. № 7 (00188). С. 60-64.

Одержано 18.04.2022

УДК 343.1:65.012.8+004

КАЛАНЧА Андрій Андрійович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3381-3350

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЯК СПОСІБ ПРОТИДІЇ ЗЛОЧИННОСТІ

Дедалі більше люди використовують Інтернет та техніку в повсякденному житті: розумні холодильники аналізують термін придатності продуктів, нагадують, що потрібно придбати в магазині; розумні чайники самі вмикаються за вашої присутності поряд, а жалюзі зачиняються в темну пору доби. У кожного «розумного» пристрою є доступ до Всесвітньої мережі, а кожен такий девайс має власну IP-/MAC-адресу, що дозволяє власнику керувати ними дистанційно. Проте постає запитання, чи залишається ця інформація лише на цьому пристрої, та чи не протікає вона у чиїсь злі руки?

Великі корпорації типу Google чи Amazon вже вирішили за Вас, що б Ви хотіли придбати, яке місце Ви б хотіли відвідати для прогулянки чи затишної вечері зі своєю другою половинкою [1].

Боротьба за анонімність та приватність також не вічна, оскільки «Корпорації Зла» вигадують дедалі жорстокіші способи вашої деанонімізації. Як приклад – двохфакторна авторизація Google-аккаунтів, яка наполягає на використанні вашого мобільного телефону в якості підтвердження власника, чи реєстрація gmail-пошти, яка вимагає у користувача реєстрацію з номером телефону (яку не можна пропустити). Лякає те, що відмовитися від цих сервісів, які намагаються викрасти вашу інформацію стає складніше, тож уникати їх, чи лягти під каток доксингу – вибір особисто кожного.

У провайдера міститься вся інформація про ваші запити в пошуковій стрічці браузера, усі завантажені та передані файли та документи, а також кому ви і коли писали, а у великих українських компаніях спеціалісти з кібербезпеки постійно грають з балансом принципів конфіденційності, цілісності та доступності, щоб дані не потрапили у відкритий доступ.

Якщо упустити незаконну діяльність «Корпорацій зла» (шпигунство, продаж даних користувачів), то основну загрозу в мережі Інтернет становлять grey-/black-hat хакери, вішинг-/смішинг-/фішинг-шахраї та script-kiddy (хакери, що не мають, власне, досвіду в створенні власних скриптів, а лише використовують такі, що створені досвідченими хакерами).

Щоб детальніше розібратися з проблемою, звернемося до законодавства України. Кіберзлочин - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, де кіберпростір - середовище, яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом [2].

У кіберполіції для розслідування злочинів необхідні знання з форензики, мережевих концепцій, методів атак та криптографії. Проте левову частку від успішності цих розслідувань грає саме провайдер, оскільки у нього міститься вся інформація про дії злочинця у Всесвітній мережі.

Провайдери мають доступ до такої інформації:

1) усі відвідані сайти з протоколом http/https;

2) завантажені дані;

3) трафік і дані з месенджерів (за умови, що в них не використовується шифрування);

Ключовим моментом є, на теперішній час, відсутність безпосередньої комунікації між провайдерами та кіберполіцією. Тож досить часто доводиться власноруч перехоплювати трафік та слідкувати за мережевою активністю підозрюваного.

Наразі доступним інструментом для здійснення аналізу трафіку є рішення від Джеральда Комбса –Wireshark [3].

Wireshark у реальному часі перехоплює мережеві пакети та зберігає їх. Ці дані потім використовують з метою вивчення трафіку, відновлення інформації, аналізу роботи мережі, виявлення атак. Це альтернатива та доповнення до стандартної утиліти tcpdump, з графічним інтерфейсом, фільтрами та ширшими можливостями.

Він здатен розшифровувати SSL/TLS трафік, показувати вміст пакетів, пошук пакетів по вмісту, трафік з телефенів, телевізорів та інших побутових пристроїв, інспектувати потоки TCP і UDP [4].

Висновки. Отже, у час залежності пристроїв від Інтернету, на мою думку, аналіз мережевого трафіку за допомогою програмного забезпечення Wireshark є досить ефективним методом попередження та протидії кіберзлочинності, а завдяки своїй доступності та наявності зручного графічного інтерфейсу значно спрощує власну експлуатацію. Та є надія, що в майбутньому кіберполіції нададуть доступ до безпосереднього трафіку від провайдера, що прискорить розслідування протиправних діянь в рази.

Список використаних джерел

1. Як Google шпигує за користувачами. КДБ і не снилось // Економічна правда : вебсайт. URL: https://www.epravda.com.ua/rus/publications/2019/07/2/649257/ (дата звернення: 17.04.2022).

2. Про основні засади забезпечення кібербезпеки України: закон України від 15.12.2021 № 2163-VIII, // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.04.2022).

3. Офіційний сайт програмного забезпечення Wireshark // вебсайт. URL: https://www.wireshark.org/ (дата звернення: 17.04.2022).

4. Wireshark для всіх // вебсайт. URL: https://habr.com/ru/company/vdsina/blog/562110/ (дата звернення: 17.04.2022).

Одержано 17.04.2022

УДК 343.1:65.012.8+004

КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399;
СПАСІБОВ Дмитро Вікторович,
кандидат технічних наук,
начальник відділу технічного захисту інформації
Департаменту технічного супроводження Харківської міської ради

СИМЕТРИЧНА АВТЕНТИФІКАЦІЯ: ПОТЕНЦІЙНЕ ЗАСТОСУВАННЯ АПАРАТНО ЗАХИЩЕНИХ МІКРОСХЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (Internet of Things – IoT) – це мережа, що складається із взаємозв'язаних фізичних об'єктів (пристроїв), які мають вбудовані мікроконтролери, датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між ними за протоколами зв'язку.

Метою роботи є дослідження способів застосування криптографічних мікросхем для забезпечення безпечної автентентифікації вузлів інтернет речей з використанням процедур симетричної криптографії.

Автентифікація може бути виконана двома основними способами - симетричним і асиметричним. Основна відмінність між ними полягає в тому, яким чином використовуються таємні ключі. Якщо і на стороні хоста, і на стороні клієнта застосовується один і той же ключ, то автентифікація – симетрична. Якщо ж використовується математично пов'язана пара відкритого і таємного ключів, то автентифікація асиметрична.

До основних переваг апаратних засобів реалізації стандарту симетричного блочного шифрування (Advanced Encryption Standard – AES) для захисту IoT відносять [1]:

1) наявність апаратного вбудованого генератора випадкових чисел, який забезпечує генерацію більш надійних криптографічних ключів;

2) зберігання криптографічних ключів та виконання криптографічних процедур над даними здійснюються в захищеної криптографічної мікросхемі;

3) виконання функції спеціалізованого мікропроцесора для виконання криптографічних перетворень, що розвантажує центральний процесор комп'ютера;

4) гарантування цілісності реалізації алгоритмів криптографічних перетворень;

5) підвищення швидкості шифрування/дешифрування даних.