УДК 621.391.3
Сушин І.О. (НТУУ «КПІ ім. Ігоря Сікорського»)
к.т.н., с.н.с. **Міночкін Д.А.** (НТУУ «КПІ ім. Ігоря Сікорського»)

DOI: https://doi.org/10.17721/2519-481X/2020/68-08

ПРИМАНКА IOT З ВИКОРИСТАННЯМ БЕЗПЕЧНОЇ АУТЕНТИФІКАЦІЇ

У статті було розглянуто метод підвищення безпеки технологій Інтернету-речей. Користувачі побоюються наслідків порушень безпеки Інтернету-речей. Тому цифрова безпека повинна бути спроектована з нуля і у всіх точках системи для того щоб вразливості в певній частині не ставили під загрозу усю систему в цілому. Ризик повинен бути зменшений протягом всього життєвого циклу, особливо з урахуванням його масштабування і географічного розширення. Мережа Інтернету-речей складається з великої кількості недорогих пристроїв. Пристрої Інтернету-речей зазвичай мають обмежену пам'ять і живляться. від батареї, що дає дуже обмежені можливості в плані обчислень і зв'язку. Використання алгоритмів шифрування/дешифрування не повинно вимагати великих ресурсів, а діапазон частот, що використовується обмежений. Також це великомасштабна мережа, що підтримує масові з'єднання. Щоб задовольнити цей попит, протоколи мережевої передачі повинні включати в себе безліч нових функцій, таких як багатоперехідна маршрутизація, спільна ретрансляція, динамічний доступ та інше. При такому налаштуванні мережі вкрай складно керувати секретними ключами і поширювати їх. Різноманітність сценаріїв використання вимагають різних QoS та рівнів безпеки. На сьогоднішній день Інтернет-речей відіграє важливу роль у багатьох сценаріях і має великі перспективи для подальшого розповсюдження. Існує потреба в збільшенні ефективності роботи того чи іншого підприємства, процесів, тому збільшується кількість інтерактивних речей, що створюють розумні осередки (будинки, офіси, склади, міста). Реалізація даного напрямку досягається різноманітними технологіями, які з часом страждають від знайдених вразливостей, що призводить до значних втрат, як даних так і часу. Можна зустріти багато пропозицій, які направленні на вирішення тої чи іншої проблеми після знаходження певної вразливості, але це може бути недостатньо дієвим. Тому було запропоновано створити метод, який може вирішити комплекс проблем одночасно шляхом поєднання безпечної аутентифікації PKI та приманок. Він дозволить не лише виявляти нові вразливості та атаки швидше, але і марнувати ресурси атакуючих (всі захоплені атаки будуть ідентифікуватися і створюватись профілі атакуючих).

Ключові слова: PKI, Інтернет-речей, приманки, атаки, вразливості.

Вступ. Розповсюдженість технологій в нашому повсякденному житті означає, що світ навколо нас також стає «розумнішим». Цифрові пристрої знаходяться не тільки в наших кишенях або офісах, але все частіше в наших будинках, різноманітних будівлях, а також в багатьох місцях і містах. Граючи ключову роль в зборі, аналізі та моніторингу даних і інформації про навколишнє середовище, ці пристрої можуть зв'язуватися один з одним через величезну переплетену мережу, відому як «Інтернет-речей» (IoT). Вона дозволяє пристроям підключатися і «спілкуватися» один з одним, а також з нами, надаючи безліч даних і поглиблений аналіз, який покращить та розширить світ навколо нас. IoT все ще в стадії розробки, але налаштований на революцію в тому, як ми живемо і зробить найбільший технологічний вплив з часу хмарних обчислень.

Переваги IoT неможливо заперечувати, але успіх залежить від цілісності та конфіденційності рішень і даних разом із зниженням ризиків кібербезпеки. Кінцеві користувачі побоюються наслідків порушень безпеки IoT. Дослідження 2019-го року [1] показують що у багатьох аспектах 50 і більше відсотків опитаних не впевнені у безпеці пристроїв IoT. Мережа IoT складається з великої кількості недорогих пристроїв. Пристрої IoT, зазвичай, мають обмежену пам'ять і живляться від батареї, що дає дуже обмежені можливості в плані обчислень і зв'язку. Використання алгоритмів шифрування/дешифрування, зазвичай, заборонено, а діапазон частот, що використовується обмежений. Також це великомасштабна

мережа, що підтримує масові з'єднання. Щоб задовольнити цей попит, протоколи мережевої передачі повинні включати в себе безліч нових функцій, таких як багато перехідна маршрутизація, спільна ретрансляція, динамічний доступ та інше. При такому налаштуванні мережі вкрай складно керувати секретними ключами і поширювати їх. Різноманітність сценаріїв використання вимагають різних QoS та рівнів безпеки. Але попри усі вдосконалення описані вище проблеми лишаються через те, що з часом в будь-якому рішенні знаходять недоліки та пробіли завдяки яким можна відтворити ті чи інші атаки.

Аналіз останніх досліджень та публікацій. В літературі та дослідженнях пояснюються різні уразливості і можливі атаки на IoT [2-7]. Проте присвячені вони в більшості цих документів тільки певним типам загроз, заснованим на конкретних цілях безпеки. Актуальним лишається створення методу, який би протистояв декільком загрозам одночасно зважаючи на обмеження пристроїв та архітектури Інтернету-речей. Пропонується використовувати існуючий спосіб раннього виявлення атак на основі приманок [8-9] разом із безпечною аутентифікацією PKI, яка пристосована для пристроїв Інтернету-речей [10-11].

Мета статті. Метою статті є наведення методу підвищення безпеки технологій Інтернету-речей.

Виклад основного матеріалу. Приманка (honeypot) – це інструмент з окремою і відокремленою мережею, що імітує реальну цінну мережу або реальний пристрій, що буде корисним для зловмисників. Його можна розглядати як підроблену систему, яка виглядає як справжня, з метою привернути зловмисників, щоб вони могли потрапити в неї і, таким чином, відстежувати взаємодію між зловмисниками і зараженим пристроєм. Згодом приманка стала одним з важливих предметів для дослідників в області інформаційної безпеки для виявлення атак і інструментарію обману. В даний час розглядаються можливість впровадження приманки в IoT, оскільки пристрої IoT стали на меті зловмисників, до того ж це одна з популярних платформ в цьому столітті. З швидким розвитком комп'ютерів та Інтернету, приманка може надати нам інформацію про атаки зловмисних програм або навіть про шаблони атак.

Приманку можна розділити на два типи [12]: комерційну приманку і дослідницьку приманку. Зазвичай, комерційна приманка часто використовується для допомоги організації в захисті внутрішньої IT-інфраструктури. Оскільки у такої приманки менше функцій, її часто легко реалізувати. Можна сказати, що комерційна приманка вимагає компромісу між простотою експлуатації і кількістю інформації, що збирається. Антагоністом виробничої приманки є дослідницька приманка. Ця приманка дуже складна, оскільки призначена для максимального збору вичерпної інформації про зловмисника, тому її складніше розгорнути. Зібрана інформація допоможе експертам-криміналістам мережі краще зрозуміти шаблони атакуючих.

Згідно іншої класифікації [13] приманки поділені на рівні взаємодії: приманка з низьким рівнем взаємодії (LIH), приманка із середнім взаємодією (MIH) та приманка з високим рівнем взаємодії (HIH). *Приманка LIH* має невеликий набір служб, таких як SSH, Telnet і FTP, і, як правило, не надає зловмисникові доступу до операційної системи, так як на цій приманці не встановлена операційна система. Тому взаємодія зловмисника обмежується спробою входу в систему, наприклад вгадування пароля. LIH дає мінімальну відповідь, яка в основному використовується для статистичної оцінки. По суті, ця приманка є комерційною приманкою, оскільки її легко встановити і з великою ймовірністю зламати. *Приманка MIH* також не має операційної системи, але забезпечує більш високий рівень змодельованих послуг, щоб заінтригувати зловмисника. В результаті ця приманка видає розумну відповідь як каталізатор для запуску наступної атаки. Ризик компрометації відповідний рівню можливостей взаємодії. З іншого боку, *приманка HIH* являє собою складну і витончену приманку. Її складніше реалізувати і підтримувати, ніж попередні, оскільки він надає зловмисникові необмежену середу операційної системи з встановленим величезним набором сервісів. Іншими словами, HIH не просто емулює службу в операційній системі, а запускає саму операційну систему. Це

дозволяє збирати і вивчати поведінку зловмисника в повному обсязі. Ця приманка, зазвичай, використовується в якості приманки для досліджень.

Ґрунтуючись на цих спостереженнях, можна запропонувати гібридну платформу-приманку (рис. 1) для Інтернету-речей, яка дозволяє збирати більш повні зразки зловмисних програм, націлених на пристрої Інтернету-речей. Ключове нововведення складається з двох частин: використання HIH та LIH, що працюють у віртуальному середовищі. На відміну від певних LIH [14], які аналізують тільки сімейства зловмисних зразків, відбуватиметься аналіз подібності зловмисних зразків. І обидва вони використовуються для збору зловмисних зразків на пристроях Інтернету речей. Компонент з низьким рівнем інтерактивності імітує процедуру входу в систему служби Telnet/SSH на пристроях IoT. Після входу в систему зловмисники отримають конкретну банерну інформацію, яку зібрано від виробників пристроїв Інтернету-речей, таких як Huawei, Dahua, D-Link і тощо. Високоінтерактівний компонент відображає реальні вразливі служби на пристроях IoT в загальнодоступну мережу з допомогою методу, що має назву переадресація трафіку, і хакери можуть безпосередньо звертатися до цих служб в загальнодоступній мережі. Можна відстежувати трафік процесу зв'язку, щоб виявляти зловмисну поведінку, таку як завантаження двійкових файлів зловмисних програм.

Для полегшення розробки та розгортання даної приманки, конкретний код реалізації безпосередньо розгортається в Docker. Docker – це cgroup, простір імен та подібна до AUFS технологія UnionFS на основі Linux, яка інкапсулює та ізолює процеси. Це технологія віртуалізації на рівні операційної системи, яка значно підвищує ефективність розробки для розробників [15].

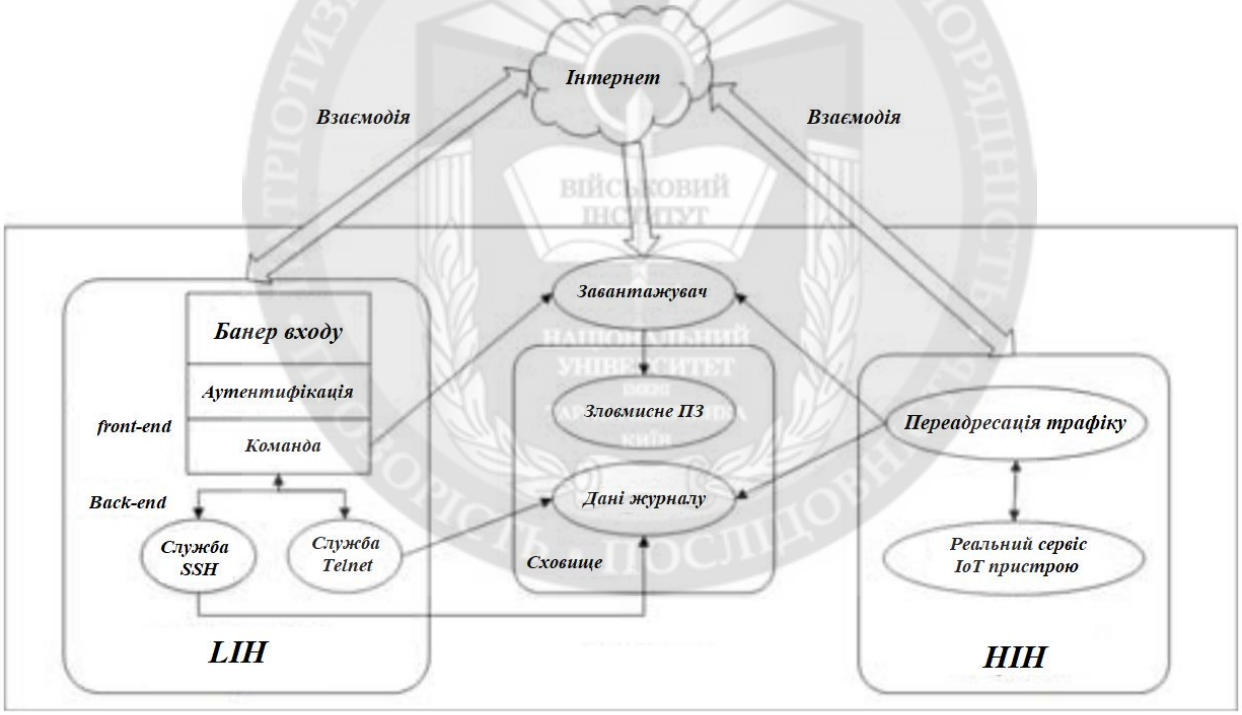

Рисунок 1 – Гібридна платформа-приманка

PKI (Public Key Infrastructure) – це ефективний підхід до розподіленого управління аутентифікацією для підтримки шифрування даних, тим самим підтримуючи засіб для безпечного і конфіденційного обміну даними через потенційно небезпечну інфраструктуру, яка, зазвичай, використовується IoT. PKI широко відомий і використовує пару ключів, відомих як відкритий ключ і закритий ключ. Ці ключі пов'язані і є похідними. Відкритий ключ надається безкоштовно для шифрування, а закритий ключ, як випливає з назви, зберігається в секреті і використовується для дешифрування. Знання відкритого ключа не дозволяє отримати закритий ключ з використанням сучасних обчислювальних методів [10]. Крім того, закритий

ключ можна використовувати для підпису повідомлень, відправлених користувачам, які можуть використовувати відкритий ключ для перевірки справжності повідомлення. Деякі криптографічні схеми, такі як RSA, дозволяють використовувати ключову пару як для шифрування, так і для підпису.

Як правило, цифрова сертифікація PKI використовує довірений сторонній об'єкт, який видає сертифікат після законної аутентифікації. Ці органи відомі як CA (Центр сертифікації), які генерують, видають і підписують цифровий сертифікат. RA (центр реєстрації) перевіряє ідентичність органів, які запитують цифрові сертифікати для видачі з CA, а механізм централізованого управління використовується для зберігання і індексації ключів сертифікатів для управління доступом до збережених цифрових сертифікатів [68]. RA вводиться для поліпшення масштабованості PKI, а також забезпечує високий ступінь захисту первинних ключів CA.

Розглянемо безпечну структуру аутентифікації IoT з використанням механізму цифрового сертифікату PKI. Ця структура заснована на тристоронньому зв'язку між користувачем, пристроєм IoT і хмарою. У цій структурі хмара аутентифікує як користувача, так і пристрій IoT, використовуючи їх цифровий сертифікат. Передбачається, що користувач не спілкується регулярно безпосередньо з пристроєм IoT, за винятком початкового завантаження. Таким чином, користувач повинен пройти через шлюз і хмарну систему, щоб обмінюватися даними з пристроєм IoT. Тобто, якщо пристрій IoT довіряє CA і користувач довіряє CA, то вони довіряють один одному. Це звичайна архітектура Інтернету речей в домашніх умовах, але не єдина модель. Передбачається, що інфраструктура хмарних обчислень забезпечує зручний спосіб надання обчислювальних ресурсів для спільної групи, наприклад мереж, служб, серверів і застосунків зберігання. Хмарні сервіси можуть надавати основні компоненти для шифрування, дешифрування і управління ключами PKI [11]. На рисунку 2 наведена безпечна структура, яка може надати можливість для реєстрації пристрою IoT з використанням цифрового сертифіката, а також користувача на хмарному сервері. Після завершення процесу реєстрації тільки справжній зареєстрований користувач може мати доступ для використання IoT пристрою, доступного в мережі.

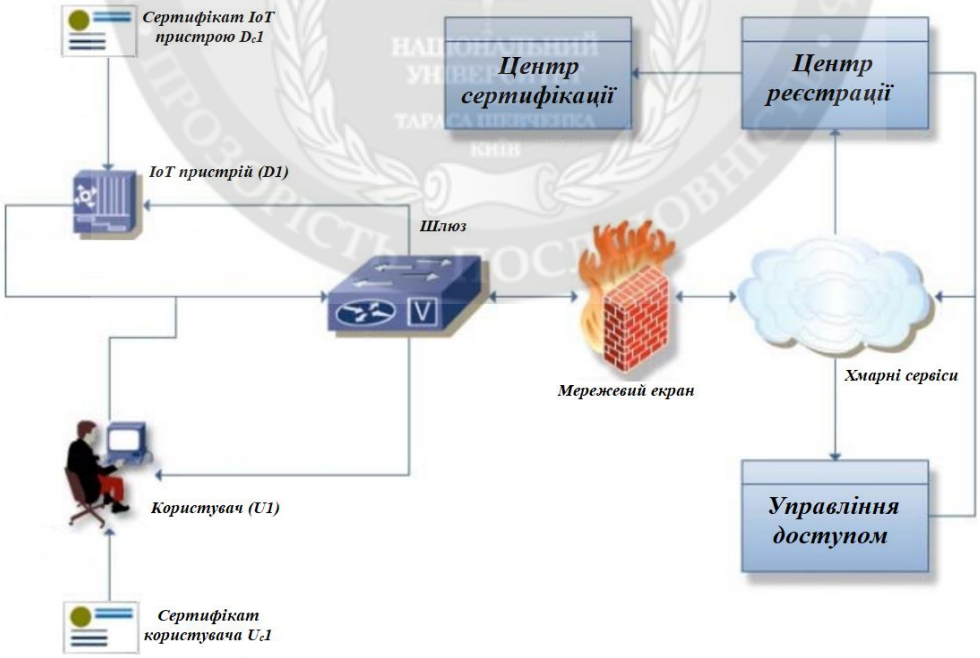

Рисунок 2 – Структура системи аутентифікації PKI для IoT

Виходячи з того що технології, що розглядалися вище ефективно допомагають підвищити безпеку та зрозуміти напрямки розвитку атак на технології Інтернету-речей, можливо поєднати їх для підвищення безпеки. Пропонується використовувати

аутентифікацію PKI замість протоколів telnet та SSH. При цьому приманка допоможе записати та зібрати логи зловмисників, які змогли обійти аутентифікацію чи використовують вразливості (нульового дня) сервісів Інтернету-речей, які ще не встигли закрити. Алгоритм роботи вдосконаленої гібридної приманки зображений на рис. 3.

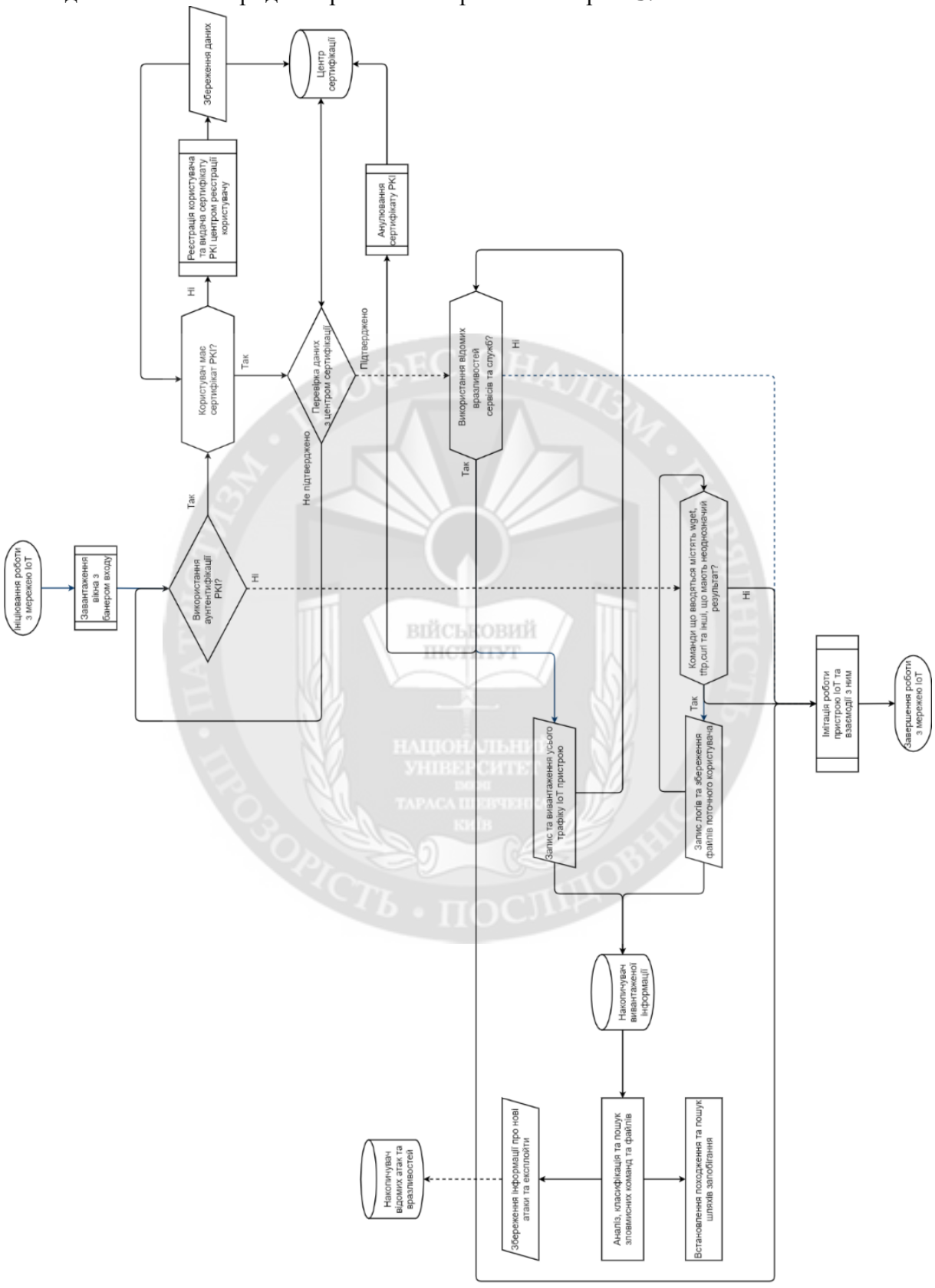

Рисунок 3 – Алгоритм роботи вдосконаленої гібридної приманки

Використовуючи дане рішення можливо зменшити кількість атак, але при цьому вони стануть більш якісними. Тобто, успішна атака на приманку дасть можливість та розуміння того як необхідно покращувати аутентифікацію PKI або цільові сервіси IoT.

Основними перевагами PKI є:

- Технологія у основі якої лежить стандарт X.509. Його підтримують більшість відомих сервісів, тому використання PKI можливого легко реалізувати змінивши стандартну конфігурацію за необхідності для використання під той чи інший сервіс;
- Масштабованість. Користувачі підтримують свої власні сертифікати, а перевірка справжності сертифіката включає обмін даними тільки між клієнтом і сервером. Це означає, що сторонній сервер аутентифікації не повинен бути в мережі. Таким чином, немає обмежень на кількість користувачів, яких можна підтримувати за допомогою PKI;
- Уповноважена довіра. Тобто користувач, який отримав сертифікат від визнаного і довіреного центру сертифікації, може аутентифікувати себе на сервері в найперший раз, коли він підключається до цього сервера, без попередньої реєстрації в системі.

Основними перевагами приманок є:

- Спостереження за хакерами у дії та вивчення їх поведінки;
- Збереження інформацію про вектори атак, зловмисне програмне забезпечення та експлойти;
- Створення профілів хакерів, які намагаються отримати доступ до цільових систем;
- Марнування часових та інших ресурсів хакерів.

Отже, виходячи з даних переваг, можна побачити загальні переваги вдосконаленої приманки (див. табл. 1)

Таблиця 1

Переваги вдосконаленої приманки

Перевага	*PKI*	*Honeypot*	*PKI + Honeypot*
Стандарт X.509	+		+
Масштабованість	+		+
Уповноважена довіра	+		+
Спостереження за атакуючими		+	+
Збереження логів та встановлення закономірностей		+	+
Марнування ресурсів атакуючих		+	+
Створення профілів атакуючих		+	+

Висновки і перспективи подальших досліджень. Було запропоновано використовувати безпечну аутентифікацію PKI у приманках, наведений алгоритм роботи вдосконаленої приманки. Це дозволило виявити дуже цінні нові атаки, які націлені безпосередньо на даний тип аутентифікації. Також існують вразливості у сервісах Інтернету-речей, які не встигають швидко виправити і проходить певний час. Якщо за цей час приманка буде реєструвати збіг використовуваної вразливості з тою що знаходиться в базі даних, то буде можливість анулювати сертифікат виданий поточному користувачу та замінити скомпрометовані, а також отримати інформацію про те, що на даний тип атаки необхідно звернути більше уваги. Вдосконалена приманка з використанням безпечної аутентифікації дозволить зменшити час на виправлення вразливостей, кількість атак, але, при цьому, вони стануть більш якісними. Тобто, успішна атака на приманку дасть можливість та розуміння того, як необхідно покращувати аутентифікацію PKI або сервіси IoT, які використовуються у діючих елементах мережі.

ЛІТЕРАТУРА:

1. Internet Society (2019), “The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things”. Available at: https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-

consumer-attitudes-to-iot/.

2. Fan K., Gong Y., Liang C., Li H., Yang Y. (2015) “Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G”. Security and Communication Networks 9(16), pp. 3095–3104.

3. I. Andrea, C. Chrysostomou and G. Hadjichristofi (2015), “Internet of Things: Security vulnerabilities and challenges”, IEEE Symposium on Computers and Communication (ISCC), pp.180-187.

4. Wahid, Abdul, P. Kumar (2015), “A Survey on attacks, Challenges and Security Mechanism in Wireless Sensor Network”, JIRST- International Journal for Research in Science & Technology, Volume 1, Issue 8, pp. 189-196.

5. S.N Uke, A.R Mahajan, R.C Thool (2013), “UML Modeling of Physical and Data Link Layer Security Attacks in WSN”, International Journal of Computer Applications, Volume 70– No.11.

6. Li, Hong, Y. Chen, and Z. He (2012), "The Survey of RFID Attacks and Defenses." 8th International Conference on IEEE Wireless Communications, Networking and Mobile Computing (WiCOM).

7. Kandah, Farah, Y. Singh, and C. Wang (2011), “Colluding injected attack in mobile ad-hoc networks”, IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPS).

8. M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder (2016), “A Survey on Honeypot Software and Data Analysis”.

9. C. H. Malin et al. (2017), “Sweet Deception: Honeypots,” Decept. Digit. Age, pp. 227–239.

10. Z. A. Alizai, N. F. Tareen, and I. Jadoon (2018), “Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures,” in 2018 International Conference on Applied and Engineering Mathematics (ICAEM), pp. 1–5.

11. J. Xu, W.-T. Zhu, and D.-G. Feng (2009), “An improved smart card-based password authentication scheme with provable security,” Comput. Stand. Interfaces, vol. 31, no. 4, pp. 723–728.

12. C. Seifert, I. Welch, and P. Komisarczuk (2006), “HoneyC-The LowInteraction Client Honeypot”

13. I. Mokube and M. Adams (2007), “Honeypots: Concepts, Approaches, and Challenges,” Proc. 45th Annu. southeast Reg. Conf. - ACM-SE 45, pp. 321–326.

14. Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow (2016), “Iotpot: A novel honeypot for revealing current iot threats,” Journal of Information Processing, vol. 24, no. 3, pp. 522–533.

15. C. Anderson (2015), “Docker [software engineering],” IEEE Software, vol. 32, no. 3, pp. 102–c3.

Sushyn I.O., Ph.D. Minochkin D.A.

IOT HONEYPOT WITH USING SECURE AUTHENTICATION

The article considers the method of increasing the security of Internet of Things technologies. Users fear the consequences of Internet security violations. Therefore, digital security must be designed from zero and at all points of the system so vulnerabilities do not jeopardize the whole system in a certain part. The risk must be reduced throughout the life cycle, especially in view of its scaling and geographical expansion. The Internet of Things consists of a large number of inexpensive devices. IoT devices usually have limited memory and battery power, which gives very limited computing and communication capabilities. The use of encryption/decryption algorithms should not require large resources, and the frequency range is limited. It is also a large-scale network that supports mass connections. Network transmission protocols must include many new features, such as multi-transient routing, shared relay, dynamic access, and other to meet this demand. It is extremely difficult to manage and distribute private keys with this network setup. A variety of usage scenarios require different QoS and security levels. Nowadays IoT plays an important role in many scenarios and has great potential for further dissemination. There is a need to increase the efficiency of a particular enterprise, processes, so the number of interactive things that create smart areas (houses, offices, warehouses, cities) is growing. The implementation of this areas reaches a variety of technologies, which vulnerable from the found attacks over time, leading to significant losses, as data and time. There are many suggestions that address target issue after finding a vulnerability, but this may not be effective enough. Therefore, it was proposed to create a method that can solve a set of problems simultaneously by combining PKI secure authentication and honeypots. It will not only detect new vulnerabilities and attacks faster, but also waste attackers' resources (all captured attacks will be identified and attacker profiles created).

Keywords: PKI, IoT, Honeypot, attacks, vulnerabilities.