УДК 004.7

І. П. Малініч
В. І. Месюра

Інструментарій вбудованих ОС для розмежування доступу VPN-користувачів до IoT-пристроїв

Вінницький Національний Технічний Університет

Анотація

Сучасні мережі IoT-пристроїв часто є об'єктами хакерських атак через обмеженість можливостей IoT-пристроїв у плані криптографічного захисту. Подібні пристрої не завжди мають достатньо обчислювальних ресурсів навіть для забезпечення SSL-захисту. Традиційні методи забезпечення зв'язку без SSL-захисту між IoT-пристроєм та хмарою, або IoT-пристроєм та мобільним додатком досить часто можуть бути перехоплені зловмисниками - це суттєво зменшує їх надійність. Крім безпекових ризиків у даному матеріалі також розглядається інструментарій вбудованих ОС за допомогою якого можливо виконати розмежування доступу VPN-користувачів до IoT-пристроїв. Розглядаються можливості інструментарію розмежування доступу на базі NetFilter для відслідковування спроб несанкціонованого доступу.

Ключові слова: операційні системи, розмежування доступу, VPN-мережі, мережевий стек операційних систем

Abstract

Modern networks of IoT devices are often acting as the target of hacking attacks due to the limited capabilities of IoT devices for full-fledged cryptographic protection. Such devices in most cases don't have enough computing resources to provide SSL security. Traditional methods of providing SSL-encrypted communication between an IoT device and a cloud, or an IoT device and a mobile application, can often be intercepted by attackers, significantly reducing their reliability. In addition to given security risks, this paper also discusses the embedded OS built in tools that are capable of delimiting the access of VPN users to IoT devices. The possibilities of NetFilter-based access restriction tools for tracking unauthorized access attempts are also considered.

Keywords: operating systems, access restrictions, VPN networks, operating system network stack

Вступ

Досить багато сучасних IoT-пристроїв створюються без слідування прийнятим у індустрії мережевого обладнання безпековим стандартам та рекомендаціям. Це у першу чергу пов'язано з швидким розвитком IoT-стартапів, які досить часно не готові йти на здорожчання своїх рішень, якщо це безпосередньо не створює конкурентну перевагу їхнім рішенням на ринку. Існує чимало прикладів коли безпекова складова, якщо взагалі є присутньою в програмній реалізації, не зазнає суттєвих змін із PoC-стадії розвитку проекту [1]. На території Європейського Союзу діє регламент про загальне положення про захист даних (GDPR), діючий на території всіх держав-членів ЄС, який вимагає щоб заходи з захисту даних були включені у процес розробки бізнес-процесів та послуг [2]. Оскільки норми GDPR обмежені територією, громадянами та резидентами держав-членів ЄС, необхідності слідувати їм на ринках інших держав, у тому числі і України, у виробників IoT-пристроїв немає. Ця причина спонукає виробників пристроїв зі складовою комп'ютерних мереж виготовляти окремі версії пристроїв для ЄС, в той час як для інших країн може існувати більш дешева та доступна у ціні версія. Саме тому необхідно розглянути яким чином можна покращити безпекову ситуацію з використанням менш захищених IoT-пристроїв з використанням мережевого інструментарію вбудованих операційних систем.

Основні проблеми менш захищених IoT-пристроїв та підходи для їх усунення

Деякі автори, які приділяють увагу захищеності IoT-пристроїв [1, 2] утримують фокус на проблемах таких основних напрямках: авторизація, аутентифікація, контроль доступу, шифрування, анонімність,

конфіденційність та деяких інших. У процесів авторизації та автентифікації існує чимало проблем, однак найбільшими серед них у сфері IoT є дві: дефолтні паролі [3] та прив'язка сесії до IP-адреси. Проблеми анонімності та конфіденційності зазвичай витікають в результаті таких чинників: відсутності або слабкості шифрування передаваємих даних, неналежному їх захисті у хмарі та неналежному розпорядженні ними оператором хмарної частини IoT-рішення.

Щоб краще зрозуміти, які підходи можна застосувати для усунення цих слабких сторін менш захищених пристроїв, необхідно зрозуміти яким чином відбувається управління ними. Серед найбільш розповсюджених методів управління IoT-пристроями можна виділити такі:

- налаштування пристрою із браузеру, можливість синхронізації параметрів з хмарою;
- налаштування пристрою із мобільного або десктопного додатку, можливість синхронізації параметрів з хмарою;
- пристрій отримує всю інформацію безпосередньо із хмари, керування пристроєм із додатку відбувається через хмару (без прямого безпосереднього зв'язку між додатком та пристроєм).

Якщо у перших двох випадках клієнт має принаймні обмежений самостійний контроль над пристроєм і це дає певну свободу маніпуляцій, то у останньому випадку клієнт не має прямого контролю над IoT-пристроєм. Питання доцільності використання пристроїв того чи іншого типу доступу не є предметом даного матеріалу.

Є такі основні підходи для забезпечення роботи менш захищених IoT-пристроїв: використання мережевих екранів (для фільтрування потенційно небажаного трафіку [4]), використання IDS (Intrusion detection system, виявлення потенційно небажаного трафіку) та використання VPN-мережі (шифрування трафіку, рис. 1).

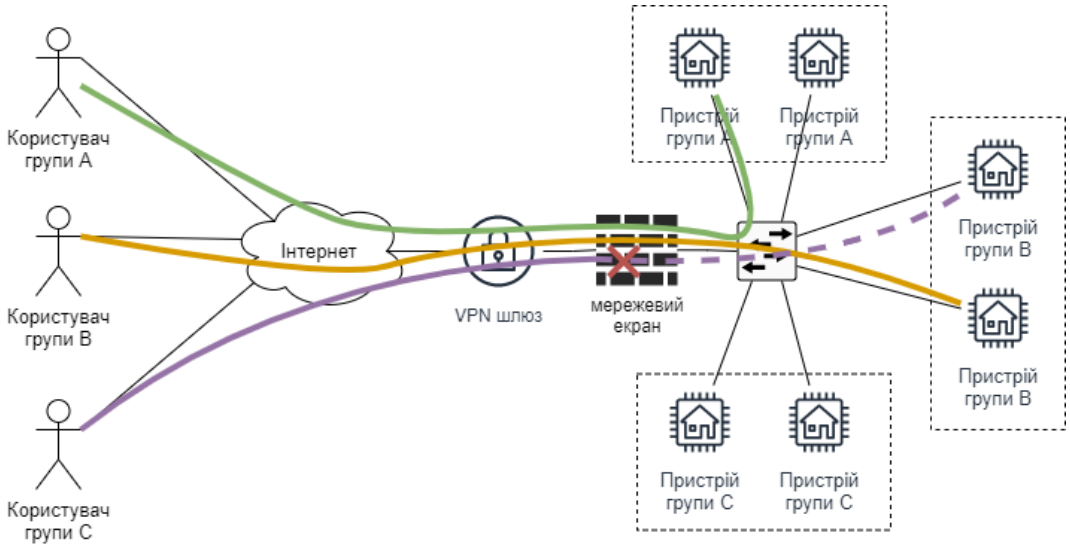

Рисунок 1 - Приклад групування доступу з використанням VPN-мереж із мережевим екраном

Налаштування VPN-доступу або інших видів тунелювання у внутрішню мережу IoT-пристроїв дозволяє відмовитись від недосконалих практик побудови IoT-мереж таких як налаштування Port Forwarding у внутрішню мережу з мережі Інтернет, або самостійна автоконфігурація доступу до таких портів IoT-пристроєм [5], що робить його видимим для всієї мережі Інтернет і може збільшити кількість потенційних безпекових ризиків.

Найбільш вдалим прикладом поєднання VPN-шлюзів та мережевих екранів з розподіленням доступу є хмарні застосунки такі як AWS Client VPN, Azure VPN та CloudFlare Access. Простота організації подібної схеми за допомогою груп IAM або Active Directory полягає у тому, що для кожної групи

користувачів можна задати певний набір правил [6], і як результат отримати як шифрування, так і розмежування по індивідуальній або груповій ознаці.

Однак використання хмарних VPN-рішень є не завжди фінансово доцільним рішенням при необхідності забезпечення доступу до невеликої IoT-мережі яка знаходиться лише в одній локації. Весь функціонал для дистанційного доступу можна також перемістити на один із IoT-пристроїв [7]. Серед найбільш відомих реалізацій операційних систем для IoT-пристроїв можна виділити Raspbian та OpenWRT. Найбільш повноцінним рішенням де б з коробки був би доступним увесь функціонал для налаштування VPN-шлюзів з шифруванням, розмежування доступу на основі груп або індивідуальних користувачів, а також відслідковування порушень заданих правил є OpenWRT. Крім того OpenWRT також має досить широку підтримку як різних моделей маршрутизаторів та точок доступу, а також дедалі зростаючу підтримку різних IoT-пристроїв [8].

Серед вимог до таких пристроїв має бути наявність ОС з можливістю налаштування VPN або тунелювання (напирклад SSH) [9], наявність мережевого екрану (наприклад NetFilter [10], pf чи ipfw), а також системи яка буде збирати (наприклад NFLOG) або обробляти [11] спроби несанкціонованого доступу. Як відомо у GNU/Linux та BSD-подібних ОС немає можливості фільтрувати трафік по групам VPN користувачів, навіть якщо їх база формується на базі системи доступу PAM, оскільки більшість реалізацій VPN-серверів всі процеси, які обслуговують підключення тримають запущеними під певним користувачем (наприклад nobody) і на рівні файрволу втрачається можливість розрізнити користувачів або їх належність до тих чи інших груп. В якості рішення можна розглядати такі інструменти як ipset (для GNU/Linux) чи ipfw tables (для BSD-подібних ОС). Для контролю належності користувача до групи розглядається можливість фіксувати у групових таблицях його внутрішньомережеву IP-алресу, отриману при підключенні до VPN.

Висновки

Розглянуто переваги використання VPN-доступу для доступу до мереж IoT-пристроїв, найбільш розповсюджені методи віддаленого управління IoT-пристроями, ризики використання IoT-пристроїв які створюють можливість безпосереднього віддаленого доступу. Також наведено можливості хмарних рішень для створення хмарних VPN мереж для отримання віддаленого доступу до IoT-пристроїв. Розглянуто основні інструменти вбудованих ОС для розмежування доступу VPN-користувачів до IoT-пристроїв. Очікується подальший розвиток вивчення можливостей виявлення IoT-пристроїв за NAT-шлюзами.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Meneghello, F., Calore, M., Zucchetto, D., Polese, M. and Zanella, A., 2019. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 6(5), pp.8182-8201.
2. Wachter, S., 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer law & security review, 34(3), pp.436-449.
3. Knieriem, B., Zhang, X., Levine, P., Breitinger, F. and Baggili, I., 2017, October. An overview of the usage of default passwords. In International conference on digital forensics and cyber crime (pp. 195-203). Springer, Cham.
4. Bellovin, S.M. and Cheswick, W.R., 1994. Network firewalls. IEEE communications magazine, 32(9), pp.50-57.
5. Schmitz, M., Warrier, U. and Iyer, P., 2001, November. WANIPConnection: 1 Service Template Version 1.01. In UPNP Forum Standard, XP002298367 (pp. 1-33).
6. Xu, G., Cao, Y., Ren, Y., Li, X. and Feng, Z., 2017. Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things. IEEE Access, 5, pp.21046-21056.
7. Zhang, J. and Liu, X., 2013. The wireless router based on the linux system. arXiv preprint arXiv:1307.6343.
8. Kim, C.G. and Kim, K.J., 2014. Implementation of a cost-effective home lighting control system on embedded Linux with OpenWrt. Personal and ubiquitous computing, 18(3), pp.535-542.
9. Малініч, І.П. and Месюра, В.І., 2020. Проблеми використання високоінтерактивних Honeypot-середовищ при дослідженні характеру мережевих вторгнень. In Proceedings of the XII International scientific-practical conference «INTERNET-EDUCATION-SCIENCE»(IES-2020), Ukraine, Vinnytsia, 26-29 May 2020: 71-73.. ВНТУ.
10. Marmorstein, R.M. and Kearns, P., 2005, April. A Tool for Automated iptables Firewall Analysis. In Usenix annual technical conference, Freenix Track (pp. 71-81).
11. І. П. Малініч, В. І. Месюра, і І. Р. Арсенюк, «АНАЛІЗ ВИКОРИСТАННЯ ТРАФІКУ ПРИ СКАНУВАННІ КОМП'ЮТЕРНИХ МЕРЕЖ РІЗНИМИ ВЕРСІЯМИ NMAP», Вісник ВПІ, вип. 2, с. 92–97, Квіт. 2021.

Маліні́ч Ілля Павлович – асистент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця, e-mail: malinich@vntu.edu.ua

Месюра Володимир Іванович **–** канд. техн. наук, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

Illia P . Malinich – assistant of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia, e-mail: malinich@vntu.edu.ua

Volodymyr I. Mesyura **–** Cand. Sc. (Eng.), Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.