Створення глобальної мережі розумних пристроїв на основі концепції Internet of Everything

Персіков Михайло Анатолійович,
Жерноклеєв Віктор Сергійович,
Рибінський Валентин Максимович

Харківський національний університет радіоелектроніки,
пр. Науки,14, м. Харків, 61166, Україна,
mihapersikov@gmail.com

Анотація. *Проведено аналіз розгортання глобальної мережі розумних пристроїв на основі концепції Internet of Everything. Виявлено необхідність забезпечення інтероперабельності між множиною різнорідних пристроїв за умови забезпечення конфіденційності та безпеки кінцевих користувачів. Запропоновано проводити розробку відповідних аналітичних моделей, здатних виявляти як зовнішні, так і внутрішні загрози в умовах, де будь-який пристрій може бути скомпрометованим.*

Ключові слова: *глобальна мережа, розумні пристрої, IoT, IoE, мережна безпека.*

I. Вступ

Сучасний стан розвитку інформаційного суспільства характеризується появою еволюційних обчислювальних технологій, що використовують Інтернет як засіб комунікацій. Ця інфокомунікаційна технологія, названа Internet of Everything (IoE), встановлює вільний потік інформації між різними взаємопов'язаними пристроями [1-5]. Використання IoE є багаторівневим і знаходить своє застосування практично у всіх сферах життя, починаючи від з'єднання між собою пристроїв розумних будинків до їх комунікацій з віртуальними середовищами для організації зв'язку між ними [1, 2, 5]. Хоча IoE використовується як інфраструктура для обміну інформацією, в той же час проблеми конфіденційності та питання безпеки кінцевих користувачів є надзвичайно актуальними [4, 5]. IoE має широкі можливості щодо інформаційного обміну, але це вимагає вживання відповідних заходів для його ефективного та безпечного впровадження та розповсюдження в значній мірі.

II. Забезпечення конфіденційності та безпеки в IoE

IoE є складною мережею, що складається з мільярдів ідентифікованих пристроїв, які взаємодіють один з одним для досягнення спільних цілей при застосуванні різних технологій на рівнях програмного, підпрограмного та апаратного забезпечення. При цьому всі фізичні пристрої формують апаратний рівень мережі, наприклад, на основі безпроводових технологій: пристрої з радіочастотною ідентифікацією (Radio Frequency Identification, RFID), сенсори, смартфони, розумний одяг (wearable technology) тощо [5]. Далі використовувані пристрої на апаратному рівні поділяються на три робочі процеси: пристрої зв'язку, датчики та ідентифікація. Обробка, візуалізація або інтерпретація необхідних даних керується програмним рівнем за допомогою спеціалізованого програмного забезпечення. Слід відмітити, що рівень підпрограмного забезпечення є сполученням між програмним та апаратним рівнями. Підпрограмний рівень відіграє найважливішу роль серед усіх трьох при впровадженні нового програмного забезпечення, організуючи сумісність апаратного рівня. На сьогодні проводиться достатньо розробок щодо впровадження IoE з урахуванням питань конфіденційності та безпеки, але все ще вимагає досліджень і нових рішень щодо вдосконалення мережної безпеки в рамках технології IoE [4]. Досягнення високої інтероперабельності між множиною пристроїв є ключовим завданням, оскільки вони є неоднорідними, що призводить до значної складності щодо вирішення питань конфіденційності та безпеки.

III. Висновки

Дослідження процесів розгортання глобальної мережі розумних пристроїв на основі концепції IoE призводить до висновків щодо необхідності врахування як зовнішніх, так і внутрішніх атак. При цьому використання особистих пристроїв IoE може бути застосовано саме для проведення інсайдерських атак. Отже, актуальною представляється розробка нових аналітичних моделей, здатних виявляти загрози, а також будувати інфокомунікаційні системи та мережі, стійкі до середовищ IoE, де будь-який пристрій може бути скомпрометованим.

Список літератури

[1] S. Cirani, G. Ferrari, M. Picone and L. Veltri. *Internet of Things: Architectures, Protocols and Standards*. 1 edition. John Wiley & Sons, 2018.

[2] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton and J. Henry. *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*. 1 edition. Cisco Press, 2017.

[3] M. Rao. *Internet of Things with Raspberry Pi 3: Leverage the power of Raspberry Pi 3 and JavaScript to build exciting IoT projects*. Packt Publishing Ltd, 2018.

[4] A. Gupta. *IoT Hackers Handbook: An Ultimate Guide to Hacking the Internet of Things and Learning IoT Security*. 1.0 edition. CreateSpace Independent Publishing Platform, 2017.

[5] A. Majeed, A.U. Haq, A. Jamal, R. Bhana, F. Banigo and S. Baadel. "Internet of everything (IoE) exploiting organisational inside threats: Global network of smart devices (GNSD)," in Proc. *2016 IEEE International Symposium on Systems Engineering (ISSE)*, 3-5 October 2016, pp. 1-7.