УДК 681. 281

Маліновський В.І.

АНАЛІЗ РИЗИКІВ КІБЕРЗАГРОЗ І ЗАХИСТ ДАНИХ В СУЧАСНИХ СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Аннотація. Розглянуто аспекти і проведено короткий аналіз проблем кібербезпеки і ризиків кіберзагроз, які виникають у сучасних системах Інтернету речей (IoT), які підключаються і керуються через мережу Інтернет. Розглядяються основні чинники впливу появи інформаційних загроз та наслідки їх прояву. Розглянуто перспективи розвитку і підходи до комплексних методів захисту даних і захищеного процессу оброблення у приладах і інформаційних системах Інтернету речей (IoT).

Ключові слова: Інтернет речей, Internet of things (IoT), канали зв'язку, процесорні тракти, кіберзагрози, *ПЗ, ШПЗ*.

Abstract. Aspects and analyses of cybersecurity problems and risks in modern devices of Internet of Thinks (IoT) are considered. The cyber security threats in IoT, which are connected and controlled via the Internet is one of the main problem on the way to it's wide implementation. The main factors influencing the appearance of information threats and the consequences of their successful manifestation are considered. Perspectives of development and approaches to complex methods of data secures and protection by cryptographic processing and complex methods in information devices of IoT are considered.

Keywords: Internet of Things (IoT), communication channels, CPUs, cyber threats, malware software.

Сучасні технології і прилади Інтернету речей досить широко охоплюють всі сфери сучасного життя від побутового персонального використання до промислових індустріальних систем професійного спеціалізованого спрямування. Інтернет речей являє собою сукупність пристроїв, як персональних пристроїв користувачів (смартфони, біо- фітне- стрекери, старт-годинники, різні персональні портативні пристрої) до промислових окремих вузлів і старт сенсорів комплексної обробки даних із використанням підключення і об'єднання у мережу із іншими інформаційними ресурсами із використанням каналів Інтернет. Більшість сучасних пристроїв IoT є високоінтелектуальними інформаційними системами, що містять мікропроцесорні і мікроконтролерні тракти із мікропрограмами і окремими мобільними операційними системами в своєму складі, що дозволяє майже повністю автоматизувати процеси оброблення і обміну даними через мережу і канали передачі Інтернет. Останні тенденції до впровадження технологій IoT і телемоніторингу та телеуправління дозволяють організовувати високоефективне, комфортне і автоматизоване керування,моніторинг і представлення даних інформаційних систем. Разом з тим, існує значна проблема із впровадженням технологій IoT – це комплексні інформаційні без пекові ризики для процесів і систем IoT, які використовують канали і інтерфейси широкодоступної мережі Інтернет. Це несе значні ризики від впровадження сучасних інформаційних технологій, пов'язані із кібербезпекою, інформаційною цілісності, стабільністю і конфіденційності таких даних і несе загрозу стабільності функціонування мереж і системи IoT, а також є одним із головних стримуючих факторів по їх впровадженню в критичних сферах і критичних системах.

Тренди сучасних років показують, що основними кіберзагрозами у сучасних IoT є:

- перехоплення і спотворення даних в каналах і інтерфейсах;
- влаштовування «ін'єкція» шкідливого коду та скриптів або перехопленого спотворенного коду керування в інформаційні потоки і програмні модулі (в т.ч. окремі програмні компоненти) і функціонал керування пристроїв IoT;
- кіберзагрози ядра операційних систем, програмних модулів і контролерів управління пристроїв IoT(як локальних так і централізованих);
- інформаційні загрози для пограничних пристроїв (пристроїв EDGE-рівня: комутатори. маршрутизатори, модеми, шлюзи і інтерфейси зв'язку);
- таргетовані/цілеспрямовані кібератаки і підключення до програмних модулів систем і пристроїв IoT і вивід їх із ладу – DoS (Denial of Service в т.ч. розподілений DDoS -Distributed Denial of Service);

- перехоплення керування та/або перехоплення та/або спотворення потоків даних моніторингу;
- шкідливе та підмінене(модифіковане) програмне забезпечення ШПЗ та МПЗ;\
- шкідливі посилання і фітинг;

Тому тренди останніх років і тенденції кіберзагроз свідчать, що у 2020-2022 велика частка до - 35-44% загроз у глобальній мережі припадає саме на галузь Інтернету речей, 25-44% із якої спрямовано саме на мобільні персональні пристрої (BYoD- Bring you owned Device) і системи із комунікаційними можливостями і влаштованими мережевими інтерфейсами або функціями підключення до мережі Інтернет. В часи інформаційного протистояння і в подальшому із розвитком програмних інструментів для здійснення кібератак прогнозується збільшення числа атак на індустріальні, персональні IoT-пристрої і на сферу пристроїв Інтернету взагалі, охоплюючи системи від портативних пристроїв користувачів і системи "розумний будинок" і "розумний кабінет лікаря» до систем індустріального старт-керування виробничими процесами на підприємствах, включаючи окремі компоненти автоматизації та телемоніторингу і телеуправління в них. З'явиться більше проблем безпеки, заснованих на штучному інтелекті, які допоможуть компаніям покращити захист, адже ступінь захисту і наслідків відповідальності вищий. Також значними є ризики для сервісів розподілених хмарних і туманних обчислень («Cloud computing», «Fog computing») та їх гнучкий функціонал. Однак, коли справа доходить до захисту хмарних сервісів і апаратної розподіленої інфраструктури, гнучкість, легкість і переваги від використання технологій IoT можуть мати протилежні наслідки в плані кібербезпеки. Найбільша вразливість для хмарних і туманних обчислень — порушення безпеки рівня ядра (Core) на рівні серверних програмних модулів і його невірні конфігурації. Також трендами 2020-2022рр. є атаки на комунікації та комунікаційні канали і інтерфейси зв'язку пристроїв із використанням методів порушення процедур захищеного обміну даними, а також модифікація ПЗ і ін'єкції шкідливого програмного забезпечення.

Підвищення безпеки мобільних платформ і пристроїв. Із зростанням популярності смарт-пристроїв і сервісів IoT зростає інтенсивність кіберзагроз. Способи і інструменти для атак постійно еволюціонують. По статистиці 4 із 10 атак і кіберзагроз спрямовані на персональні і IoT пристрої. Основними елементами і мішенями для атак в IoT системах є:

- канали передачі LTE/EDGE, GPS, Wi-Fi та Bluetooth та кабельні комунікації;

- ядро і компоненти вводу-виводу на суміжних мобільних операційних систем пристроїв керування/моніторингу біомедичної системи(Android і др.), а також неперевірені додатки;

- підміна програмних компонент і оновлень ПЗ або постачання ПЗ із додатковим функціоналом;

- порушення прав розмежування доступу/отримання перевищення адмін. прав;

- недосконаліть і вразливості мобільних операційних систем пристроїв IoT;

- відсутність інформаційного захисту IPS/IDS та захисту каналів VPN/Proxy із належним рівнем шифрування (IP Sec + RSA) та відсутність мережевого екрану;

- використання методів соціальної інженерії і фішингу із подальшим впровадженням і виконанням експлойтів і ін'єкцій шкідливого коду „пробиття" для порушення штатного функціоналу - ПЗ/ядра операційних систем пристроїв IoT, що призводить до порушення/додання/модифікування/зрізання системних програмних функцій ПЗ;

- порушення механізму захисту пам'яті ECC на рівні ядра пристроїв IoT (виконання методів несанкціонованого доступу до захищених областей пам'яті: переповнення буфера, вичитка буфера, доступ до пам'яті в захищ.областях);

- порушення безпеки пограничних пристроїв та інтерфейсів зв'язку у пристрої (маршрутизатори, комутатори, обладнання радіозв'язку та інше), у сукупності із - вразливостями проміжних протоколів зв'язку і передачі даних;

- порушення механізму встановлення захищеного з'єднання та атаки MITM(Man in the Midle);

- недосконаліть і кіберзагрози опорної архітектури і суміжних пристроїв IoT;

- Сучасне ШПЗ віруси, троянські коні і бекдори, які адаптовані спеціально під конкретну інфраструктуру мережі розподілених IoT і біомедичних пристроїв і архітектуру системи. Використання кіберзброї для мобільних пристроїв;

- недосконаліть мережевих і хмарних сервісів, програмних інтерфейсів API і недосконаліть налаштування безпеки мобільних пристроїв. Використння відомих вразливостей CVE XXn;

- використання і експлуатація інформаційних загроз і вразливостей «0-го» для;

Враховуючи таку велику кількість потенційно можливих кіберзагроз та інформаційних ризиків для IoT та мобільних персональних пристроїв, необхідним є використання комплексних підходів і механізмів захисту пристроїв і інфраструктури IoT на всіх рівнях із метою зменшення рівня ймовірностей ризиків кіберзагроз. Також актуальною є розробка нових прогресивних підходів і передових світових практик – таких як розмежування мережі і сегментів IoT на області нульової довіри (Zero Trust) із пограничними механізмами і елементами захисту і перевірки. Також актуальним є використання комплексного метода перевірки і нейтралізації кіберзагроз: із використанням декількох одночасно працюючих інформаційних систем захисту IDS/IPS (Intruder Preventition System / Intruder Defense System) у комплексі із моделями захисту даних для критичної інфраструктури IoT . Взагальному випадку структурний механізм захисту IoT і його компонент повинен включати комплексне використання механізмів інформаційного захисту, який можна зобразити у вигляді абстрактної ілюстративної формули захисту:

Max IoT Data Security → End Point IDS/IPS + End Point Component Firewall + VPN/VPS(with IPSec) + RSA Sessions + Zero Trust Zone Policies

де, *Max IoT Data Security* – умовне позначення функцій максимального інформаційного захисту із мінімальною кількістю загроз в системах IoT ; *End Point IDS/IPS* – умовне позначення функцій сучасних інструментів антивірусного захисту і аналізу даних в IoT; *End Point Component Firewall* – ум. позначення функцій сучасних мережевих екранів із аналізатором трафіку даних в трактах мережі IoT; *VPN/VPS(with IPSec)* – ум. позн.функцій використання компонент мережевого тунелю із шифруванням і захищеним протоколом передачі IPSec; *RSA Sessions* – ум. позн. функцій використання механізмів і алгоритмів криптографічного захисту при обміні даних із ключами шифрування ; *Zero Trust Zone Policies* – ум. позн. функцій використання політик розмежування прав доступу та інформаційних політик безпеки, заснованих на концепції нульової довіри в зонах для IoT.

Взагалом досягти максимального рівня захисту в IoT можливо тільки із використанням комплексного підходу використання компонент у вищенаведеній абстрактній формулі захисту.

Забезпечити повну безпеку функціоналу і захищену передачу даних та їх обробку для IoT персонального спрямування із мобільними персональними пристроями користувачів в його складі вкрай складно, враховуючи різні функціональне спрямування і використання окремих компонент такої IoT, а також використання каналів Інтернет – як одного із джерела проникнення інформаційних загроз. Забезпечення сталості і надійності функціоналу, концепції цілісності. Доступності та конфіденційності даних (CPA) в таких IoT – є однією із головних завдань. Нові моделі і методи повинні базуватись на комплексному поєднані функціоналу віртуалізації даних, перевірка їх компонентами *IDS/IPS* в окремих ізольованих програмних контейнерах для окремих потоків і процесів інформації із змішаним додатковим функціоналом. Також для підвищення рівня безпеки повинні бути створені додаткові умови перевірки і контролю сторонніх інформаційних потоків із надійним вдосконаленим шифруванням із зміщенням та у поєднанні із розпаралелюванням обчислювального процесу із розмежуванням прав доступу на різних рівнях обчислень і віртуальних обчислювальних середовищах(оболонок) для різних процесів.

Сьогодні, в століття цифрової епохи інформаційних технологій, в умовах інформаційних протистоянь і сучасних інформаційних викликів, для кожного користувача персонального пристрою і користувачів IoT вцілому дуже гостро стоїть проблема інформаційної безпеки і конфіденційності персональних даних, стабільності роботи їх систем. Для кожного персонального мобільного пристрою і пристрою IoT із інтелектуальними функціями, або функціями керування, для ПК/мобільного пристрою який входить до концепції IoT важливо розуміти необхідність безпечної експлуатації передавання, оброблення та зберігання даних, а також кібербезпеку і наслідки від її порушення в цілому.

Вирішення цієї проблеми можливе шляхом використанням комплексних підходів інформаційної безпеки на різних рівнях. Це дозволить подальший розвиток галузі IoT і їх безпечне впровадження у інші сфери життєдіяльності і в т.ч. використання в критичних системах господарства і життєдіяльності.

Маліновский Вадим Ігоревич – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Malinovskyi Vadym — PhD (Eng), Associated Professor of Data Protection Department in Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.