ПІДХОДИ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ ПЕРЕДАЧІ ДАНИХ В ІНТЕРФЕЙС-КАНАЛАХ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

Маліновський Вадім Ігорович
кандидат технічних наук, доцент кафедри захисту інформації,
Вінницький національний технічний університет, Вінниця

Куперштейн Леонід Михайлович
кандидат технічних наук, доцент кафедри захисту інформації,
Вінницький національний технічний університет, Вінниця

Лукічов Віталій Володимирович
кандидат технічних наук, доцент кафедри захисту інформації,
Вінницький національний технічний університет, Вінниця

Інтернет-адреса публікації на сайті:
http://www.economy-confer.com.ua/full-article/4678/

Вступ. У зв'язку із значним збільшенням інформаційних атак і впливів в сфері інформаційних систем та пристроїв Інтернету речей (IoT), останнім часом в умовах значних інформаційних протистоянь, постала гостра проблема і необхідність забезпечення надійного інформаційного захисту даних в інтерфейсах IoT. Значне збільшення інтенсивності інформаційних загроз в секторі IoT, спричиняє значні ризики і реальні втрати та витоки інформації в системах IoT. Аналіз показав, що більша кількість інформаційних атак і загроз в IoT припадає саме на MITM-атаки із організацією підмінених (Rogu-AP) точок доступу. Таким чином дані IoT можуть бути втрачені чи передані стороннім особам. Тому постає проблема захисту цих даних по даному вектору втрат інформації.

Метою роботи є аналіз загроз і розробка дієвих підходів захисту інформації в каналах і інтерфейсах IoT, підвищення рівня захисту покращеними методами IoT.

Результати досліджень. Рівень захисту каналів IoT, які використовують радіоінтерфейси по вектору атак – MITM-атаки із Rogu-AP – точками доступу значно підвищується при використанні захищених протоколів шифрування. Але цей рівень все ще є не достатнім і потребує використання додаткових нових методів і заходів захисту даних в IoT. Проблема реалізації росту чинників інформаційних загроз через здійснення MITM-атаки із організацією «Rogu»-точок доступу (Атаки типу: AP Spoofing із підміненими точками доступу) із несанкціонованого зчитування і модифікацією даних в каналах є однією із основних проблем і загроз безпеки в каналах IoT. Перехоплення інформації із цих каналів, може призвести до втручання та / або втрати конфіденційної інформації, якщо вона не захищена надійно у інформаційній системі IoT. Також може бути здійснене втручання в структуру пакетів даних в IoT.

Організовувати високоефективне і захищене передавання даних в IoT можна із використанням надійних протоколів шифрування на базі криптографічних алгоритмів: RSA, DES, AES (LKEY>128bit), що відповідає концепції захищених ІКС IoT. Для сучасних систем бітова довжина ключа шифрування не може бути менша за 128 біт, в більшій мірі є достатньою для більшості каналів IoT, що підтримується білшістью існуючими протоколами захисту IoT і їх механізмами. Це протоколи IoT: CoAP; ZigBee; WiFi Bluethooth; MQTT; DDS. Основними сучасними загрозами в каналах і інтересах IoT із підтримкою цих протоколів є:

– *погана авторизація і несанкціоноване перехоплення: MITM-атак із Rogu-AP точками доступу та відсутність шифрування в кагалах та інтерфейсах IoT;*

– *впровадження підмінених сертифікатів шифрування RSA/DES/AES;*

– *«ін'єкція» шкідливих пакетів та/або сертифікату в дата-потоки IoT;*

– *перехоплення дата трафіку із супутніх вузлів IoT EDGE і дешифрація;*

– *таргетовані і цілеспрямовані сторонні підключення до EDGE IoT і API;*

– *втручання в захищені механізми формування VPN/ Proxy шифрування;*

– *використання мережевих експлойтів інтерфейсів і протоколів IoT;*

– *некоректні системні налаштування і порушення безпеки пограничних пристроїв EDGE IoT і кіберзагрози опорної архітектури і суміжних пристроїв;*

Проведений аналіз свідчить, що порушення механізму захищеного з'єднання і атаки MITM-атаки із Rogu-AP на пристрої IoT EDGE, а також атаки на програмні інтерфейси API є домінуючими в каналах і інтерфейсах IoT. Як показують дослідження, виконання на практиці високорівневого шифрування IoT та інших заходів захисту в IM IoT дозволяє підвищити рівні інформаційної захищеності IoT із 15-20% до 70-88% (і навіть в окремих випадках до 92-94%) що значно підсилює безпеку пристроїв і середовище інформаційного обміну IoT.

Інформаційна модель безпеки IoT і захищеної передачі даних виглядає:

$$ІБ_{КАНАЛІВ}\ (IoT) = f\ [(ІБ\ (IPS)+ІБ\ (VPN\ ZTA)+ІБ\ (ProtocolSec|DES|AES|RSA)+ІБ\ (Firewall)+ІБ\ (Network\ EDGE)]$$

Висновки. Забезпечити максимальну, повну безпеку функціоналу і особливо каналів і даних у них систем і пристроїв Інтернету речей вкрай важко і це є складною задачею. Велике число MITM- атак із використанням підмінених точок доступу Rogu є прихованими і можуть бути компенсовані тільки надійним шифруванням і додатковим захистом із використання сучасних *IDS/IPS*.