Пулеко І. В., канд. техн. наук, кафедри КІтаКБ
Державний університет «Житомирська політехніка»,
Топольницький П. П., канд. техн. наук, доцент кафедри комп'ютерних технологій і моделювання систем
Поліський національний університет

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ З ПОГЛЯДУ ПРИВАТНОГО РОЗРОБНИКА

Незважаючи на те, що проблеми забезпечення безпеки в області інформаційних технологій самі по собі не є новими, багато прикладів роз-робки і впровадження систем Інтернету речей (англ. Internet of Things, IoT) ставлять перед розробниками нові унікальні проблеми безпеки.

Так у міру постійного збільшення числа пристроїв, підключених до Інтернету, виникають нові потенційно вразливі місця. Несправні чи дефектні пристрої можуть створювати вразливі точки. Недостатньо захищені пристрої можуть служити точками доступу для кібератак, що доз-волить зловмисникам перепрограмувати пристрій або викликати його несправність. Погано спроєктовані пристрої з конструктивними вадами наражають на небезпеку розкрадання дані користувачів за рахунок недостатнього захисту потоків даних.

Прагнення до створення недорогих IoT-пристроїв невеликого розміру роблять ці проблеми настільки ж гострими, або навіть ще гострішими, ніж для комп'ютерів, які традиційно використовувалися для підключення до Інтернету.

Крім потенційно вразливих місць, суттєве збільшення кількості і типів пристроїв IoT також може сприяти збільшенню ймовірності кібер-атак. З урахуванням наявної функції взаємного підключення пристроїв IoT, кожен з них, що не має достатнього захисту, надає потенційно негативний вплив на безпеку і стійкість як локальної системи так і в глобальному масштабі Інтернету в цілому.

З кожним днем ступінь нашої підключеності до Інтернету зростає і ми стаємо все більш залежними від пристроїв IoT для виконання своїх основних завдань. Цей зростаючий рівень залежності від пристроїв IoT та інтернет-послуг, з якими вони взаємодіють, також відкриває зловмис-никам можливості доступу до даних та пристроїв IoT. Тому проблема забезпечення безпеки систем Інтернету речей є дуже актуальною.

Аналіз наукових джерел інформації показує, що, незважаючи на деякі розходження думок, фахівці з кібербезпеки в основному виділяють три рівні забезпечення безпеки IoT систем, які пов'язані з архі-тектурою Інтернету речей: рівень сприйняття, мережевий рівень та прикладний рівень. Рівень сприйняття повинен забезпечувати надійну іден-тифікацію та зчитування інформації з сенсорів.

Мережевий рівень повинен забезпечувати повсюдний доступ, передачу і зберігання інформації. Як правило тут виділяють ще два рівні: рівень доступу (мережі зв'язку, що надають доступ до мереж вищого рівня ієрархії глобальності, наприклад до Інтернету) і рівень основного обміну (Інтернет, NGN, віртуальні приватні мережі).

Прикладний рівень повинен забезпечувати обробку і аналіз прийнятої інформації для прийняття оптимального управлінського рішення та контролю за управлінням, додатками і послугами.

Забезпечення і підтримання безпеки на усіх цих рівнях і покладається на розробників систем IoT. Для промислових розробників та великих фірм питання забезпечення безпеки є одним з пріоритетних. Однак, на сьогоднішній день широка доступність готових модулів сенсорів, актуаторів та засобів бездротового підключення до Інтернету надають можливість проєктування, підключення та налагодження систем IoT навіть у приватних (домашніх) умовах. Прикладом може бути широко розповсюджена ланка засобів Arduino. У цьому випадку саме професіоналізм приватного розробника і стає отою «слабкою ланкою» усієї системи. Адже в IoT система безпеки повинна бути повсюдною. Підхід до забезпечення безпеки повинен бути:

- автоматизованим і послідовним та досягати захищених меж інших організацій;
- динамічним для поліпшеного розпізнавання загроз безпеки за допомогою попереджувального аналізу в реальному часі;
- інтелектуальним для забезпечення повного контролю усіх підключень і елементів інфраструктури;
- масштабуємим для задоволення потреб зростаючої організації;
- адаптивним і здатним реагувати на загрози в реальному часі;
- комплексним і повноцінним рішенням.

Тому у рамках даного дослідження аналізуються два рівні забезпечення безпеки IoT: рівень сприйняття і рівень доступу до мережі, які і є найбільш вразливими при приватній розробці IoT систем.

Авторами наводиться ряд досить простих рекомендацій, слідування яким дозволить значно знизити ризики та ускладнити роботу зловмисника щодо зламу системи IoT чи несанкціонованого доступу до інформації.