Миколайчук В.В., магістр,
Єфіменко А.А., к.т.н., завідувач кафедри,
Житомирський державний технологічний університет

АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ ТА СПОСОБИ ЇХ ВИРІШЕННЯ

В умовах стрімкого розвитку інформаційно-комп'ютерних технологій, ідея впровадження передових технологій для різних способів збору даних, стає реальністю та використовується довкола у різних сферах нашого життя. Такою технологією є так званий Інтернет речей (англ. Internet of Things, IoT) – концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку.

На сьогодні такі компанії-велетні як Cisco та IBM співпрацюють з університетами та керівними органами міст щоб організувати розвиток систем керування даними для транспорту, управління сортуванням відходів, правоохоронних органів, енергетикою та ін., щоб покращити життя людей. За прогнозами Gartner, до 2020 року кількість підключених до всесвітньої мережі пристроїв становитиме 26 мільярдів, а дохід від продажу устаткування, програмного забезпечення та послуг становитиме 1,9 трлн доларів. Найбільші світові IT-компанії, зокрема Intel, Google, Microsoft, Amazon та ін., вже ведуть масштабну роботу на цьому ринку.

Сучасна концепція Інтернету речей передбачає комунікацію об'єктів, які використовують технології для взаємодії між собою та з навколишнім середовищем. Частина мережних протоколів адаптовані для використання в IoT і їх можна описати як складову TCP/IP моделі. Тому вразливості цих протоколів можна використовувати і для зламу систем, які використовують Інтернет речей. Зловмисник може атакувати мережне обладнання, що використовується в системі. Серед компонентів розумного дому та охоронних систем значна частина має проблеми з безпекою, які характерні для цілого ряду пристроїв, а не просто для певної серії ненадійного виробника.

Розглянемо масові грубі порушення принципів розробки: використання незмінних (hardcoded) та прихованих сервісних облікових записів; застосування однакових або легко передбачуваних паролів та ПІН-кодів; відсутність перевірки прав доступу при зверненні до відомої сторінки налаштувань або прямого виклику зображень та відеопотоку IP-камер; некоректна обробка отримуваних даних, що викликає переповнення буферу. Як наслідок, можна отримати виконання довільного коду при отримані попередньо складеного TCP-пакету; примусове переключення серверу на використання старих версій протоколів за запитом клієнтського пристрою; та інші типові помилки, які спрощують конфігурування пристроїв неспеціалістами, що в свою чергу послаблює параметри безпеки в цілому (в тому числі – віддаленого та без належної авторизації). З прикладів використання вразливостей систем IoT можна навести DNS rebinding, DoS/DDoS-атаки, ботнети, концепція Man-in-The-Middle та інші.

Уже сьогодні спеціалісти працюють над усуненням вразливостей в розумних пристроях. Для підвищення якості написання програмного забезпечення для даних пристроїв необхідно підняти питання сертифікації. За умов мінімальної бюрократії та надання користувачам гарантії, що продукт достатньо захищений від хакерських атак, рівень довіри до виробника значно зросте. Питанням сертифікації займаються приватні компанії. Зокрема компанія Online Trust Alliance (OTA) випустила IoT Trust Framework – ряд критеріїв для розробників, постачальників послуг, який направлений на покращення безпеки, конфіденційності та життєвого циклу їх IoT-продуктів.

Компанія Verizon запустила програму тестування безпеки та сертифікації IoT-пристроїв. Як стверджують її розробники, вона являється однією з перших в своєму роді, і тестує такі складові як сповіщення/протоколювання, криптографія, аутентифікації, зв'язок, фізична безпека та безпека платформи. Пристрої, що пройшли сертифікацію, будуть відмічені знаком схвалення ICSA Labs та буде вказувати, що вони були протестовані, а знайдені вразливості були усунені. Також пристроїв, що пройшли сертифікацію будуть знаходитись під наглядом і періодично тестуватись протягом їх життєвого циклу для збереження безпеки. Інтернет речей стала однією з перших сфер, в якій використовується блокчейн-технологія. Наприклад, управління аутентифікацією, перевірка роботоспроможності різних сервісів та ін. Ряд компаній, як Cisco, BNY Mellon, Bosch, Foxconn та ряд інших організували консорціум, який буде знаходити рішення з використання блокчейну для збільшення безпеки і покращення взаємодії IoT-продуктів.

Отже, довіра користувачів до інтернету речей залежить від реалізації безпеки в ньому, тому саме питання її забезпечення має бути ключовим для виробників. Позитивним є об'єднання компаній заради створення стандартів та реалізації різних концепцій для підтримки цієї технології та її популяризації.