ПЕРЕЛІК ПОСИЛАНЬ:

1. В.А. Втюрин, Основы АСУТП. Учебное пособие для студентов специальности 220301 “Автоматизация технологических процессов и производств” (по отраслям), Санк-Петербург, Санкт-Петербургская государственная лесотехническая академия имени С.М. Кирова, 2006, – с.154.

2. Дьяконов В.П., MATLAB 6.5 SP1/7 + Simulink 5/6. Обработка сигналов и проектирование фильтров. – М.: СОЛОН-Пресс, 2005. – 576 с.

3. Сергиенко А.Б., Цифровая обработка сигналов – СПб.: Питер, 2007. –751 с.

УДК 004.056.5: 004.414.22

ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ВЕКТОРІВ АТАК У ІНТЕРНЕТІ РЕЧЕЙ ТА ОСНОВНИХ МЕХАНІЗМІВ ЗАХИСТУ

Ж.В. Гула, Д.С. Тимофєєв
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Інтернет речей (англ. Internet of Things - IoT) швидко зростає через розповсюдження інформаційно-телекомунікаційних технологій, наявності пристроїв та обчислювальних систем. Безпека IoT викликає занепокоєння для захисту апаратних засобів та мереж системи IoT. Проте, оскільки ідея мережевих приладів все ще відносно нова, безпека при виробництві цих приладів майже не розглядається.

Прикладами існуючих систем IoT є транспортні засоби із самостійним керуванням (англ. self-driving vehicles - SDV) для автоматизованих автомобільних систем, мікросітки для розподілених систем енергоресурсів та Smart City Drones для систем спостереження. Кіберфізичною системою є мікросітка, що пов'язує всі розподілені енергетичні ресурси (англ. distributed energy resources - DER) разом, щоб забезпечити комплексне енергетичне рішення для місцевого географічного регіону. Система мікрорешітки IoT використовує систему диспетчерського управління та збору даних (англ. Supervisory Control and Data Acquisition - SCADA). Інтеграція фізичного та кібер-домену збільшує можливість реалізації атак: кібер-атаки можуть націлювати на контроль SCADA і паралізувати фізичний домен, або фізичні пристрої можуть бути підроблені або скомпрометовані, впливаючи на систему контролю. Наразі ринок безпілотників рухається до впровадження методик автоматизації і може бути інтегрований у боротьбу з пожежами, поліцію, розумне спостереження міста та реагування на надзвичайні ситуації. Оскільки муніципалітети та громадяни почнуть розраховувати на таку систему, стане критично важливим зберегти систему надійною та достовірною.

Останнім часом академічні дослідження з вирішення питань конфіденційності та безпеки систем IoT досягли позитивних зрушень. На сьогодні найпоширеніші методи безпеки, засновані на звичайних методах мережевої безпеки. Проте застосування механізмів захисту в системі IoT є більш складною задачею, ніж у традиційній мережі, через неоднорідність

пристроїв та протоколів, а також масштаб і кількість вузлів у системі. Проблеми поліпшення безпеки IoT, які пов'язані з фізичним зв'язком, неоднорідністю, обмеженням ресурсів, конфіденційністю, великим масштабом, управлінням довірою та непідготовленістю до безпеки, детально пояснюються в [4].

Дослідження [1], [5], [7], оцінюють можливі загрози системам IoT відповідно до рівнів стека протоколів TCP/IP та наявних контрзаходів. Ключовим фактором швидкого прогресу наукових досліджень безпеки IoT є наявність інструменту для моделювання мереж IoT. Вичерпний перелік симуляторів, використовуваних у сучасних дослідженнях, представлений Чернишевим у [5]. Саме завдяки застосуванню симуляції мереж IoT та механізмів безпеки є можливою адекватна оцінка безпеки в IoT та визначення та вивчення основних векторів атак.

Проблеми безпеки IoT актуальні на всіх основних рівнях стека протоколів TCP/IP. Наприклад, відсутність «транспортного» шифрування стосується незахищеного зв’язку між пристроєм та Хмарним сховищем, пристроєм та шлюзом, пристроєм та мобільними додатками, одним пристроєм та іншим пристроєм.

Популярний вектор для отримання доступу до пристроїв IoT виникає через неадекватні процедури автентифікації та авторизації. У нинішніх системах IoT протоколами, що підтримують автентифікацію, є MQTT, DDS, Zigbee та Zwave. Проте, навіть якщо розробник надав інструменти автентифікації, необхідні для спілкування в Інтернеті, можливості для викрадення зв'язку все одно існують. Небезпечні мережеві сервіси можуть спричинити загрозу розвідування мережі та поширюватись через неї.

Недостатня конфігурація безпеки пояснюється вбудованними повноваженнями, які часто використовуються на пристроях IoT. Завдяки цьому облікові дані легко піддаються компроментуванню через використання одного і того ж пароля на багатьох пристроях. Погана фізична безпека - ще один вектор атаки, викликаний вразливістю апаратних засобів. Основна перешкода в шифруванні пристроїв пояснюється простотою датчиків.

Небезпечні веб- та хмарні інтерфейси - це вразливості, які можуть бути вектором атаки в системі IoT на програмному рівні. Тому, хмарні шлюзи повинні бути обладнані механізмами безпеки, щоб обмежити можливість несанкціонованих користувачів (порушників) від зміни конфігурацій. Застосування біометрії та багаторівневої автентифікації для контролю доступу є одним з найкращих механізмів захисту на програмному рівні. Через зміни тенденцій загроз безпеці [7] запропонував розгляд поточних проблем безпеки відповідно до рівня та можливих контрзаходів. Деякі поточні проблеми та запропоновані контрзаходи розглянуті у [1].

Розробка діючих механізмів безпеки IoT на разі перебуває у постійному розвитку. Основними механізмами захисту є:

– Автентифікація - процес ідентифікації користувачів та пристроїв у мережі та надання доступу уповноваженим особам. Це один із способів пом’якшення атак на системи IoT (атака «Людина в середині», атака Sybil).

Автентифікація на даний час залишається найпопулярнішим методом надання доступу користувачеві на рівні додатків, а також надання доступу до пристрою в мережі IoT.

– Шифрування. Досягаючи цільової безпеки, вузли шифруються. Оскільки метою шифрування IoT є досягнення ефективної взаємодії з низьким споживанням енергії, симетричні та асиметричні алгоритми для IoT розроблені таким чином, щоб відповідати вимогам [6].

– Довірче управління. Мета управління довірою IoT - виявити та усунути шкідливі вузли та забезпечити безпечний контроль доступу. Автоматизовані та динамічні обчислення довіри для перевірки довірчих значень вузлів-учасників мережі IoT є найсучаснішими у дослідженні управління довірою. Проте, на сьогодні більшість досліджень зосереджена саме на виявленні шкідливих вузлів.

– Безпечна маршрутизація. Масштабованість, автономність та енергоефективність є важливими для будь-якого рішення маршрутизації. Завдяки великому масштабу мереж IoT, IP-адреси цих пристроїв базуються на IPv6 (англ. Internet Protocol version 6), що дозволяє забезпечити більш надійну та покращену модель маршрутизації пакетів.

– Нові технології. Існують два базових типи нових технологій. Програмно визначена мережа (англ. software defined network – SDN) та блокчейн (англ. blockchain) є одними з найпопулярніших нових технологій, що поєднуються з вирішеннями безпеки IoT. Основна ідея SDN - розділити мережевий контроль та управління даними (можливе як централізоване управління, так і динамічне управління мережею для вирішення проблем в середовищі IoT, таких як, наприклад, розподіл ресурсів в пристроях IoT). Блокчейн є основою криптовалюти. Програми на базі IoT користуються захищеними та приватними транзакціями, а також децентралізацією комунікацій та процесів. Застосування блокчейну досягло значних успіхів у фінансових додатках.

Результатом цієї роботи є огляд сучасних тенденцій дослідження безпеки IoT. Різні інформаційні джерела з питань захисту IoT було переглянуто з метою визначення основних векторів атак та проблем безпеки IoT. Було встановлено основні механізми захисту безпеки IoT, їх підґрунтя та особливості функціонування. Мета цієї роботи була досягнута шляхом надання адекватного огляду тенденцій дослідження в галузі безпеки IoT за період останніх років.

ПЕРЕЛІК ПОСИЛАНЬ:

1. А. Теварі, Б. Б. Гупта. Безпека, конфіденційність та довіра різних рівнів в рамках Інтернету речей (IoT) // Наступ. Генер. Обчислення. Сист. – 2018 1–13 с.

2. Дж. Камінья, А. Перкусич, М. Перкусич. Інтелектуальний метод управління довірою для виявлення атак, що підключаються в Інтернеті речей // Секур. Комун. Мереж. – 2018.

3. Ж.А. Гутьєррес, С. Кумар. SecTrust - RPL: безпечний протокол маршрутизації RPL для Інтернету речей, комп'ютерних систем майбутнього покоління.

4. К. Ша, У. Вей, Т. Ендрю Янг, З. Ванг, У. Ши. Про проблеми безпеки та відкриті проблеми в Інтернеті речей // Наступ. Генер. Обчислення. Сист. – 2018 – №83.

5. М. Чернишев, З. Байг, О. Белло, С. Зеадалі. Інтернет речей (IoT): Дослідження // IEEE Інтернет речей, журнал – 2018 – №5. 1637–1647.

6. С. Сінгх. Розширені легкі алгоритми шифрування пристроїв IoT: опитування, виклики та рішення // Інтел. Гуманіз. Обчислення – 2017.

7. Х.З. Ячень Ян, Лонгфей Ву, Гуйчен Інь, Ліє Лі. Огляд з питань безпеки та конфіденційності в Інтернеті речей // Інт. Конф. Інтернет Технол. Зах. – 2015. – 202–207 с.

УДК 004.056.53

КЛАСИФІКАЦІЯ ВИДІВ АВТЕНТИФІКАЦІЇ

К.О. Діденко, Ю.А. Мілінчук
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Атаки на системи автентифікації, на жаль, не рідкісне явище в наш час і багато статей присвячені різноманітним методам, видам та способам автентифікації. Для легшого розуміння кожного з видів, потрібно знати, які методи та способи можна використовувати і які типи протоколів при цьому застосовуються.

Саме автентифікація являє собою процедуру перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту. [1] Ця процедура може виконуватись за допомогою наступних методів:

- парольні, в яких може використовуватись одноразові або багаторазові паролі;
- Public Key Infrastructure (PKI), заснований на асиметричній криптографії, де закритий ключ користувача може бути на смарт карті, криптографічному токені або знімному накопичувачі;
- мобільна автентифікація, де, за допомогою спеціальної програми, на смартфоні генерується одноразовий пароль (one time password, OTP). Таким чином, смартфон виступає OTP токеном; [2]
- біометричні, де перевірка проходить за фізіологічними характеристиками користувача;
- інформація користувача, до якої відноситься номер телефону, дівоче прізвище матері, дата реєстрації та інше, що може використовуватись для відновлення логіна і пароля або для двофакторної автентифікації;
- користувацькі дані, де використовуються інформація про точки доступу бездротового зв'язку та геодані про місце знаходження користувача. [3]

Способи можна класифікувати наступним чином [4]:

- базова автентифікація, при застосуванні якої логін і пароль користувача входять до складу веб-запиту. Будь-який зловмисник, що перехоплює пакети інформації легко впізнає засекречені дані;