УДК 004.056.53

СИСТЕМИ ВИЯВЛЕННЯ DOS-АТАК В ІНТЕРНЕТІ РЕЧЕЙ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

О.І. Луньова, О.В. Кручінін
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Інтернет речей - це концепція комунікації об’єктів, які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини[1]. Ідея самостійної взаємодії фізичних об’єктів отримала стрімкий розвиток – вже сьогодні принципи Інтернету речей активно використовуються в медицині, промисловості, збройних силах. Разом із розвитком «розумних» систем значно погіршився стан інформаційної безпеки у сфері Інтернету речей.

Сьогодні крім небезпечних конфігурацій і стандартних налаштувань, гострою проблемою безпеки є DoS-атаки[2]. DoS-атака (Denial of Service) - вид зловмисної діяльності, що ставить собі за мету довести комп'ютерну систему до стану, коли обслуговування правомірних користувачів і коректне виконання функцій неможливе. Зловмисниками була продемонстрована можливість дистанційного керування кардіостимуляторами, дефібриляторами та інсуліновими помпами.

У результаті аналізу десяти популярних пристроїв Інтернету речей було виявлено вразливості, які спрощують реалізацію атак на відмову в обслуговуванні. Так, у 2016 році було здійснено масштабну атаку на інфраструктуру Dyn DNS, через що багато популярних сервісів, включаючи Amazon, CNN, Github, Netflix, Paypal, стали недоступними протягом декількох годин. У 2017 році вихідний код атаки було опубліковано, що дало змогу зловмисникам модифікувати його та вдосконалювати. Ця зростаюча загроза повинна мотивувати до розробки нових методів та систем виявлення та блокування трафіку атак.

У системах Інтернету речей, які побудовані за принципом «видавець - підписник», найбільшу критичність має брокер - компонент, що відповідає за прийом всіх повідомлень, їх фільтрацію, прийняття рішення про те, кому цікаві ці повідомлення, і, в кінцевому підсумку, за пересилку повідомлень всім підписаним клієнтам[3]. Саме на брокер здійснюються DoS-атаки задля неможливості обробки корисних запитів.

Аналіз досліджень. Дослідженням проблеми DoS-атак на Інтернет речей займалися такі компанії як Avast - «Avast Threat Landscape Report»[4], IBM - «The weaponization of IoT devices»[5], Google - «Security of IoT devices»[6]. Зазначені роботи створюють теоретичну базу результатів вивчення питання безпеки в Інтернеті речей, але не повністю розкривають всі аспекти даної проблеми. Більш детального аналізу потребують причини виникнення вразливості та можливостей для здійснення атак.

Постановка завдання. Актуальною задачею у сфері безпеки Інтернету речей є створення нових методів виявлення аномалій у мережі задля запобігання атак на відмову в обслуговуванні. Методи, що вже існують, схильні помилково класифікувати нормальний трафік, приймаючи його за аномальний, і не можуть адаптуватися до природи атак, що постійно розвивається. Варто також брати до уваги обмеженість ресурсів моделювання системи, наприклад: кількість робочих машин, з яких здійснюється атака; можливості операційної системи та швидкість роботи системи.

Для вирішення цієї задачі необхідно:

- проаналізувати наявні ресурси та елементну базу для оцінки можливостей системи;
- виконати аналіз методів виявлення мережевих аномалій, що існують;
- розробити систему виявлення DoS-атак з використанням принципів нечіткої логіки;
- створити базу здійснених атак для подальшого використання при моделюванні;
- виконати аналіз отриманих результатів та ефективності роботи даної моделі.

Матеріали дослідження. Одним із найбільш розповсюджених протоколів, за яким здійснюється взаємодія складових частин Інтернету речей, у тому числі і з брокером, є протокол MQTT. На сьогоднішній день саме особливості цього протоколу надають зловмисникам можливості для реалізації атак на відмову в обслуговуванні. У новій версії протоколу, MQTT 5.0, що була опублікована на початку 2019 року, наведено перелік змін, які також варто розглядати у контексті можливості реалізації атак. Наприклад, надання ширших прав користувачам і можливість контролювати параметри та налаштування окремих пакетів клієнтськими додатками. Ці характеристики не тільки спрощують використання системи правомірними користувачами, а і створюють більш сприятливе середовище для здійснення атак, і саме вони стали ключовим об’єктом дослідження даної роботи.

Висновки. В ході роботи було проаналізовано слабкі сторони одного із найбільш розповсюджених протоколів, що використовується у сфері Інтернету речей. Також будо запропоновано основні етапи роботи. Кінцевою метою дослідження є створення системи аналізу активності в мережі Інтернету речей, з врахуванням нових стандартів протоколу, яка буде здатна відрізняти звичайний мережевий трафік від атаки на відмову в обслуговуванні.

ПЕРЕЛІК ПОСИЛАНЬ:

1. https://techno.nv.ua/popscience/chto-takoe-internet-veshchej-1326653.html
2. https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9
3. https://h20195.www2.hpe.com/V2/getpdf.aspx/4AA6-3316ENW.pdf?

4. https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf
5. https://www.ibm.com/downloads/cas/6MLEALKV
6. https://cloud.google.com/iot/docs/concepts/device-security

УДК 651.3:518.6

ВИКОРИСТАННЯ ТРИФАКТОРНОЇ АБО ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ: ПЕРЕВАГИ І НЕДОЛІКИ, ВИБІР ОПТИМАЛЬНОГО ВАРІАНТУ

М.В. Маркіна
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. З розвитком технологій дедалі частіше виникають загрози, які використовують вразливості двофакторної аутентифікації для доступу до критичної інформації. Тому, необхідно зрозуміти, які нові рішення можуть бути використані для захисту від подібних загроз (у тому числі перехід до трифакторної аутентифікації) та у яких випадках яке рішення є найбільш оптимальним.

Двофакторна аутентифікація. Метод 2FA (Two-Factor authentication) був придуманий як додатковий спосіб підтвердження власника аккаунта. Він заснований на двох з трьох способах аутентифікації:

– користувач щось знає (наприклад, пароль);
– користувач володіє унікальними рисами, які можна оцифрувати і порівняти (біометрична аутентифікація, наприклад, відбиток пальця);
– користувач щось має (наприклад якийсь девайс з унікальним ідентифікатором, ключ-карту, флешку з ключовим файлом, тощо).

За думкою експертів у галузі інформаційної безпеки, двофакторна аутентифікація різко знижує можливість крадіжки особистих даних онлайн, так як знання пароля жертви недостатньо для здійснення шахрайства. Тим не менш, двофакторні підходи аутентифікації залишаються уразливими для атак типу «фішинг» та «людина посередині».

На сьогоднішній день, найпопулярнішим методом 2FA є пароль користувача (користувач щось знає) та SMS з перевірочними кодами, що генеруються за технологією OTP (one time password) та відправляється на смартфон (користувач щось має). Код приходить кожен раз різний, тому вгадати його практично неможливо.

Однак чим складніше подолати захист технічними методами, тим легше буває це зробити за допомогою соціальної інженерії. Всі настільки впевнені в надійності 2FA, що використовують її для найвідповідальніших операцій - від авторизації в Google (що дозволяє доступ до пошти, хмарного сховища, контактів і всієї інформації, що зберігається в історії) до систем клієнт-банк.

Національний Інститут стандартів і технологій США (The National Institute of Standards and Technology, NIST) оприлюднив влітку 2016 року попередню