PROCEEDINGS OF THE V INTERNATIONAL SCIENTIFIC AND THEORETICAL CONFERENCE

SCIENCE OF XXI CENTURY: DEVELOPMENT, MAIN THEORIES AND ACHIEVEMENTS

26.01.2024

HELSINKI
REPUBLIC OF FINLAND

SCIENTIA
COLLECTION OF SCIENTIFIC PAPERS

SCIENTIA
COLLECTION OF SCIENTIFIC PAPERS

with the proceedings of the

V International Scientific and Theoretical Conference

Science of XXI century: development, main theories and achievements

26.01.2024

Helsinki, Republic of Finland

Helsinki, 2024

UDC 082:001
S 40

https://doi.org/10.36074/scientia-26.01.2024

S 40 **Science of XXI century: development, main theories and achievements**: collection of scientific papers «SCIENTIA» with Proceedings of the V International Scientific and Theoretical Conference, January 26, 2024. Helsinki, Republic of Finland: International Center of Scientific Research.

ISBN 979-8-88955-774-6 (series)
DOI 10.36074/scientia-26.01.2024

Papers of participants of the V International Multidisciplinary Scientific and Theoretical Conference «Science of XXI century: development, main theories and achievements», held on January 26, 2024 in Helsinki are presented in the collection of scientific papers.

The conference is included in the Academic Research Index ReserchBib International catalog of scientific conferences and registered for holding on the territory of Ukraine in UKRISTEI (Certificate № 318 dated June 16th, 2023).

UDC 082:001

ISBN 979-8-88955-774-6

Ісмайлов К.Ю.
Поліський національний університет, Україна
Науковий керівник: Веретюк С. М.
канд.техн.наук, старший викладач кафедри комп'ютерних технологій і моделювання
Поліський національний університет, Україна

АНАЛІЗ СУЧАСНИХ ЗАГРОЗ ТА МЕХАНІЗМІВ БЕЗПЕКИ IOT

Наразі технологія Internet of Things (IoT) відіграє ключову роль у повсякденному житті. Ці пристрої, від розумних термостатів до охоронних систем, забезпечують зручність та ефективність. Однак, зі збільшенням їхньої популярності, зростає і ризик кібератак. Особливо це актуально для охоронних систем, таких як AJAX, що використовуються в контексті Smart Home

Система AJAX представляє собою комплексне рішення для охорони приміщень, використовуючи різні датчики та пристрої, що зв'язуються через бездротові технології. Вона включає в себе датчики руху, відкриття дверей/вікон, а також системи пожежної та протипожежної безпеки. Управління системою відбувається через спеціалізоване мобільний додаток, що дозволяє користувачам моніторити стан свого дому в реальному часі.

Типи Кібератак на IoT Системи:

Фішинг - це вид атаки, що використовує інженерні методи соціального маніпулювання для отримання конфіденційної інформації від користувачів. У контексті системи AJAX, це може включати шахрайські електронні листи або SMS, що імітують офіційні повідомлення з метою отримання паролів або доступу до облікового запису користувача. На важливість навчання користувачів правилам кібербезпеки та використання двофакторної аутентифікації не можна недооцінювати.

MitM атаки здійснюються шляхом перехоплення комунікації між двома сторонами, дозволяючи зловмисникам зчитувати або модифікувати передані дані[1]. В контексті AJAX, це може призвести до незаконного доступу до системи керування охороною, дозволяючи зловмисникам контролювати або вимкнути систему. Захист від таких атак включає в себе використання шифрування для всіх переданих даних та застосування безпечних протоколів зв'язку.

DoS атаки спрямовані на перевантаження системи з метою зробити її недоступною. Для системи AJAX, це може означати відключення від мережі або перешкоду в нормальному функціонуванні системи охорони. Заходи безпеки включають захист від DoS атак, використання резервних каналів зв'язку та стратегій балансування навантаження[2].

Цей тип атак включає в себе використання відомих вразливостей у програмному забезпеченні. Для AJAX це може означати використання вразливостей в мобільному додатку або в самій охоронній системі для отримання несанкціонованого доступу або крадіжки даних. Регулярне оновлення ПЗ та своєчасне використання патчів безпеки є ключовими для захисту від таких атак.

Встановлення шкідливого ПЗ може дати зловмисникам контроль над системою або дозволити їм красти конфіденційну інформацію. У випадку з AJAX, це може включати в себе встановлення шкідливого ПЗ на мобільний пристрій користувача. Захист від таких атак включає в себе використання антивірусного ПЗ та файрволів.

Ці атаки включають в себе спроби перебору або викрадення паролів. В контексті AJAX, це може призвести до несанкціонованого доступу до системи. Використання

складних паролів, обмеження спроб входу в систему та двофакторна аутентифікація є ефективними засобами захисту.

Для забезпечення безпеки системи AJAX важливо регулярно оновлювати програмне забезпечення, використовувати складні паролі та двофакторну аутентифікацію, а також забезпечувати шифрування даних. Крім того, навчання користувачів основам кібергігієни може значно знизити ризик соціальної інженерії та фішингових атак.

Системи Ajax використовують бездротові технології для комунікації між компонентами, що може створювати потенційні точки входу для кібератак.

Припустимо, в системі Ajax було виявлено вразливість у фірмовому ПЗ, яка дозволяє зловмисникам виконувати незаконний віддалений доступ до системи. Вразливість може бути пов'язана з недоліками у протоколі шифрування, що використовується для захисту комунікацій між центральним хабом і датчиками. Зловмисник використовує інструменти сканування мережі для ідентифікації пристроїв Ajax у місцевій мережі. Застосовуються методи реверс-інжинірингу для аналізу фірмового ПЗ пристроїв, виявлення слабких місць у протоколі шифрування.

На основі виявлених вразливостей розробляється експлойт, який може використовувати слабкі сторони протоколу для перехоплення або модифікації даних. Експлойт може включати в себе методи криптографічного аналізу для розшифровки або фальсифікації комунікаційних пакетів. Зловмисник розгортає експлойт в мережі, спрямовуючи його на центральний хаб або індивідуальні датчики. Використовуючи експлойт, зловмисник може відправляти фальшиві сигнали до центрального хабу, імітуючи відключення або активацію датчиків. Зловмисник може деактивувати систему безпеки або маніпулювати її поведінкою, створюючи умови для несанкціонованого доступу.

Щоб запобігти таким атакам, важливо використовувати сильне шифрування мережевих з'єднань. Регулярне оновлення програмного забезпечення системи безпеки для усунення вразливостей. Використання захищених і надійних Wi-Fi мереж з сильними паролями і WPA3 шифруванням.

Список використаних джерел:

1. P. Lopez, D. Fernandez, A. J. Jara, and A. F. Skarmeta, “Survey of Internet of Things technologies for clinical environments,” in Proc. 27th Int. Conf. WAINA, 2013, pp. 1349–1354.
2. Internet of Things Platforms. Postscapes. // [Електронний ресурс.] – Режим доступу: http://postscapes.com/internet-of-thingsplatforms?order=rhits/