

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В ІОТ-МЕРЕЖАХ

Виконала:
ст. гр. СКС-19-1
Ліхота О.І.

Дипломний керівник:
проф. Немченко В.П.

Мета роботи

2

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІОТ СИСТЕМІ.

Об'єкт дослідження

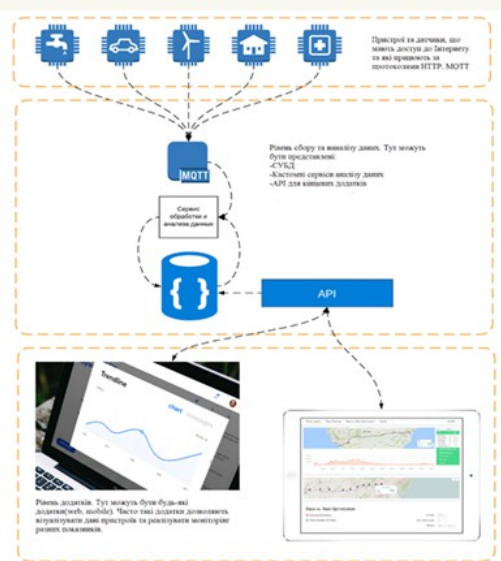
СИСТЕМИ, ЩО ПОБУДОВАНІ ПО ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ.

Предмет дослідження

МЕТОД ПОБУДОВИ ТА ВДОСКОНАЛЕННЯ БЕЗПЕКИ БЕЗДРОТОВОЇ ІОТ СИСТЕМИ.

Методи досліджень

АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ФОРМУЛЮВАННЯ ПРОБЛЕМ ТА ЗАГРО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, РАНЖУВАННЯ ВРАЗЛИВОСТЕЙ, МЕТОДИ ПОБУДОВИ ІОТ СИСТЕМ.



3

Що таке IoT

Інтернет речей (IoT - Interne of Things) – єдина мережа, що об'єднує техніку, якою ми користуємося щодня, та віртуальний світ. Технологія не лише дозволяє віддалено керувати різними приладами, а й пов'язує їх між собою. Обмінюючись даними, речі починають «спілкуватися» один з одним.

Основною концепцією IoT є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки.

Проблеми інформаційної безпеки систем, побудованих по технології Інтернету речей

КІБЕРАТАКИ НА СИСТЕМИ, ПОБУДОВАНІ ПО ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ ПРИЗВОДИТЬ ДО:

- несанкціонованого управління зловмисником системами охолодження (кондиціонування), системами управління водою, газом, освітленням, відкриття / закриття дверей розумних будинків;
- несанкціонованого керування зловмисником транспортною інфраструктурою (розумні автомобілі, залізничний / морський транспорт тощо);
- несанкціонованого управління зловмисником енергетичною сферою;
- несанкціонованого втручання в діяльність розумних медичних пристроїв (наприклад електрокардіостимулятора та інше).



Статистика атак на IoT:

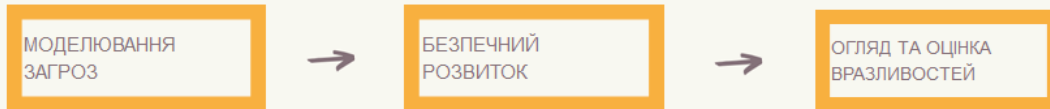
ДОСЛІДЖЕННЯ КОМПАНІЇ CISCO, ЖОВТЕНЬ 2018 РОКУ, ОПИТУВАННЯ 1816 РЕСПОНДЕНТІВ З 26 КРАЇН

- більше 53% невеликих підприємств піддавалися кібератакам, а 20% з них заявили про збитки в розмірі від 1 до 2,5 млн. дол.;
- 53% респондентів заявили, що їх компанії піддавалися вторгненням, яке спричинило суттєві фінансові витрати;
- у 40% респондентів (підприємства з чисельністю 250-499 співробітників) в результаті кібератак траплялися 8-годинні простої;
- у 39% респондентів половина систем постраждала в результаті кібератаки.



ЗАСТОСУВАННЯ ПІДХОДУ БЕЗПЕЧНОЇ СИСТЕМНОЇ ІНЖЕНЕРІЇ ДО АРХІТЕКТУРИ ТА РОЗГОРТАННЯ НОВОЇ СИСТЕМИ ІоТ

6



Оцінка вразливостей систем, побудованих по технології Інтернет речей. Методика CVSS

7

Загальна система оцінювання вразливостей (CVSS) – це вільний і відкритий галузевий стандарт для оцінки рівня вразливостей системної безпеки комп'ютера. CVSS намагається визначити оцінку ступеня вразливостей, що дозволяє респондентам визначити пріоритети захисту відповідно до загроз. Оцінки розраховуються на основі формули, яка залежить від кількох показників, що абліжають простоту використання та вплив експлуатації.

Кібератаки
з використанням
вразливостей, що
були проаналізовані:

ОТРИМАННЯ АВТЕНТИФІКАЦІЙНИХ
ДАНИХ КОРИСТУВАЧА

ENTERTAINMEПІДВИЩЕННЯ ПРИВІЛЕЇВ

ПІДВИЩЕННЯ ПРИВІЛЕЇВ В СЕРЕДЕНІ
СИСТЕМИ

ВІКОНАННЯ ДОВІЛЬНОГО КОДУ

Аналіз вразливості
для атаки
«Отримання
автентифікаційних
даних користувача»

CVSSv2:
Вектор доступу – Network;
Складність – Low;
Метрика «автентифікація» - Single;
Метрика «вплив на конфіденційність» - Complete;
Метрика «вплив на цілісність» - None;

CVSSv3:
Метрика «вплив на доступність» - None;
Необхідний рівень привілеїв – None;
Необхідність взаємодії з користувачем – None;
Межі експлуатації – Unchanged.

Аналіз вразливості
для атаки
«Отримання
автентифікаційних
даних користувача»

CVSSv2:
CVSS Base Score: 6.8
Impact Subscore: 6.9
Exploitability Subscore: 8.2.
Overall CVSS Score: 6.8

Вектор атаки:
[AV:N/ AC:L/ AU:S/ C:C/ I:N/ A:N]

CVSSv3:
CVSS Base Score: 7.5
Impact Subscore: 3.6
Exploitability Subscore: 3.9
Overall CVSS Score: 7.5

Вектор атаки:
[AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:
N/A:N].

СИСТЕМА БАГАТОРІВНЕВОГО ЗАХИСТУ БЕЗПЕКИ ДЛЯ АКТИВІВ ІoT



Мережевий
рівень



Прикладний
рівень



Рівень
пристроїв



Рівень
користувача

СИСТЕМА ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ



Ідентифікація
даних



Класифікація даних



Безпека даних

ВИЗНАЧЕННЯ ЗАСОБІВ КОНТРОЛЮ ЖИТТЕВОГО ЦИКЛУ ДЛЯ ПРИСТРОЇВ ІоТ



СИСТЕМА АФТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ДЛЯ РОЗГОРТАННЯ ІОТ СИСТЕМИ

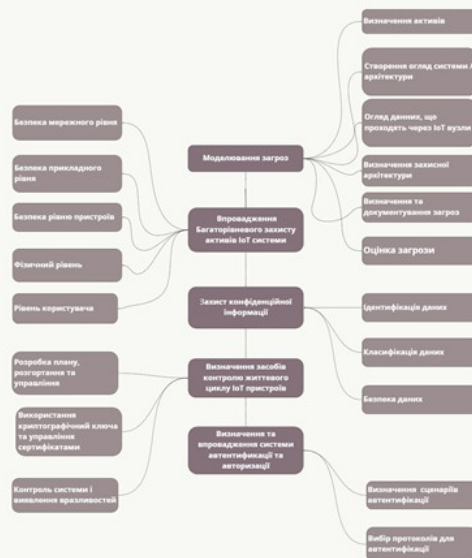
ВИЗНАЧЕННЯ СЦЕНАРІЇВ АВТЕНТИФІКАЦІЇ

Сценаріїв автентифікації ІоТ безліч. Компоненти ІоТ можуть взаємодіяти між собою, вимагаючи автентифікації машинно—машинного (м2м). Компоненти ІоТ можуть взаємодіяти з хмарними програмами, мобільними додатками, Інтернетом додатки або навіть безпосередньо з людьми.

Одним із складних аспектів автентифікації та авторизації в Інтернеті речей є те, що багато пристроїв працюватимуть у обмежених умовах, що означає, що використовувані протоколи можуть обмежувати параметри автентифікації або що пристрої не зможуть використовувати певні можливості автентифікації

ВИБІР ПРОТОКОЛІВ ДЛЯ АФТЕНТИФІКАЦІЇ

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В ІОТ–МЕРЕЖАХ



Висновки

В атестаційній роботі було проведено аналіз технології побудови системи Інтернет речей з точки зору інформаційної безпеки. Було розглянуто усі аспекти побудови таких систем, включаючи у себе як фізичну безпеку, так і безпеку пристор. у мережі.

Практична значимість полягає у тому, щоб запропонувати новий комплекс дій для побудови, розширення та підтримки системи за технологією IoT



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ
XXIV МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ
У XXI СТОЛІТТІ»

7 – 9 квітня 2020 р.

Том 5

КОНФЕРЕНЦІЯ
«ВІРТУАЛЬНИЙ ТА ФІЗИЧНИЙ КОМП'ЮТІНГ»

Харків 2020

ОЦІНКА ВРАЗЛИВОСТЕЙ СИСТЕМ, ПОБУДОВАНИХ ПО ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ ЗА МЕТОДИКОЮ CVSS

Ліхота О.І.

Науковий керівник – Немченко В.П.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, Кафедра автоматизації проектування
обчислювальної техніки, тел. (057) 702-13-06,

e-mail: oryna.likhota@nure.ua

The purpose of my work was to analyze the vulnerabilities that can occur in any device using Internet technology. An analysis of the threats that were detected in the device, such as the ThingsPro Suite the IIoT gateway and device manager from the company Moxa, was carried out. After analysis, the risk of information security was calculated using the CVSS methodology.

Загальна система оцінювання вразливостей (CVSS) – це вільний і відкритий галузевий стандарт для оцінки рівня вразливостей системної безпеки комп'ютера. CVSS намагається визначити оцінку ступеня вразливостей, що дозволяє респондентам визначити пріоритети захисту відповідно до загроз. Оцінки розраховуються на основі формули, яка залежить від кількох показників, що наближають простоту використання та вплив експлуатації.

Кібератаки з використанням вразливостей, що були проаналізовані:

- отримання автентифікаційних даних користувача;
- підвищення привілеїв;
- виконання довільного коду;
- підвищення привілеїв всередині системи;

Особливість вразливості «Отримання автентифікаційних даних користувача» полягає у тому, що У зловмисника є можливість спробувати отримати підтвердження того, що користувач існує в системі. Вона полягає в тому, що з відповідей від сервера на отримані ним дані автентифікації можна визначити, існує користувач в системі чи ні.

А вектор атаки: [AV:N/ AC:L/ AU:S/ C:C/ I:N/ A:N]. А загальна оцінка загрози: 6.8

Щодо вразливості «Підвищення привілеїв», то тут проблема полягає у тому, що Автентифікований користувач ThingsPro Suite в веб-панелі може змінювати дані свого облікового запису. Серед цих даних - логін, пароль, адресу електронної пошти та назву компанії. Для зміни цих даних веб-сервісу відправляється HTTP-запит. Після зміни значення role з user на root і повторної відправки повідомлення, у відповіді сервера було зазначено, що роль поточного користувача змінена з user на root.

Вектор атаки: [AV:N/ AC:L/ AU:S/ C:C/ I:C/ A:C]. Загальна оцінка: 9.0.

Атака «Виконання довільного коду». Для користувача з високим рівнем привілеїв в ThingsPro Suite доступна функціональність, яка змінює

системні настройки або поведінку ThingsPro Suite в цілому. Для обробки такого рівня запитів веб-додаток змушений звертатися до можливостей командного рядка операційної системи Linux.

Вектор атаки: [AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N]. Загальна оцінка: 9.0.

І остання атака «Підвищення привілеїв всередині системи». Як правило, для розвитку атаки на веб-сервер після отримання доступу до командної оболонки Linux потрібне підвищення привілеїв, тому що зазвичай веб-сервери запускаються з-під окремо створеного в системі користувача з обмеженими правами. Так працює, наприклад, apache або nginx. Однак, веб-сервер ThingsPro Suite вже запущений з-під користувача root в системі, тому, отримавши можливість виконання довільних команд, зловмисникові підвищувати привілеї не треба.

Вектор атаки: [AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N]. Загальна оцінка: 9.0.

У висновках можна сказати, що технологія «Інтернет речей» ще дуже молода, тож більшість загроз, що існують через те, що розробники занадто швидко випускають нові продукти, та не тестують їх належним образом. У всіх на меті лише якомога швидше стати лідерами у цій сфері. То ж, де, як не в цій сфері потрібен добрий аналіз загроз та повне розуміння ризиків інформаційної безпеки. Як було виявлено в атестаційній роботі, облікові дані для перевірки автентичності в хмарі, які використовуються в процесі настройки та експлуатації розгортання IoT, мабуть, являють собою найсерйознішу уразливість, яку зловмисники можуть легко використовувати, щоб отримати доступ до системи IoT і скомпрометувати її. Для захисту облікових даних рекомендується регулярно міняти пароль і намагатися не використовувати ці облікові дані на загальнодоступних комп'ютерах.

З аналізу можна зробити такі висновки. Компаніям треба більш ретельно підходити до тестування свого програмного забезпечення та приладів, та розраховувати усі ризики, що можуть бути. Так як, усі загрози, що були виявлені – це лише результати занадто швидкої розробки продукту.

Щоб забезпечити належний рівень безпеки для інфраструктури IoT, необхідна стратегія всебічного захисту. В рамках неї забезпечується захист даних в хмарі, захист цілісності даних при передачі в Інтернет, а також безпечне виробництво пристроїв. І все це дуже залежить від доброго аналізу усіх вразливостей та ризиків.

Список використаних джерел:

1. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Електронний ресурс]. – 2002. – Режим доступу до ресурсу: <http://csrc.nist.gov/publications/nistpubs/>.

