Додаток А

(Рекомендований)

КОПІЇ ПРЕЗЕНТАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

Аналіз методів забезпечення безпеки в IoT системах

Виконав: Клімашевський Р.О.

Керівник: ст.викл. PhD. Мерзлікін А.О.

ВСТУП

Інтернет речей (IoT) стає все більш поширеним і важливим аспектом сучасних технологій, проникаючи в багато сфер життя, від розумних будинків до промислових систем. Однак зі збільшенням кількості підключених пристроїв і обсягу зібраних даних зростає ризик вразливості та кібератак; забезпечення безпеки в системах IoT стає ключовим викликом для забезпечення конфіденційності, цілісності та доступності даних.

Метою цієї кваліфікаційної роботи є аналіз методів забезпечення безпеки в системах Інтернету речей, щоб виявити існуючі вразливості та запропонувати ефективні рішення для їх усунення. Для досягнення поставленої мети було проведено огляд існуючих методів забезпечення безпеки, виявлено типові вразливості в системах IoT, проаналізовано методи їх виявлення та усунення, а також запропоновано рекомендації щодо підвищення рівня безпеки систем IoT.

ОГЛЯД НАЯВНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В IOT СИСТЕМАХ

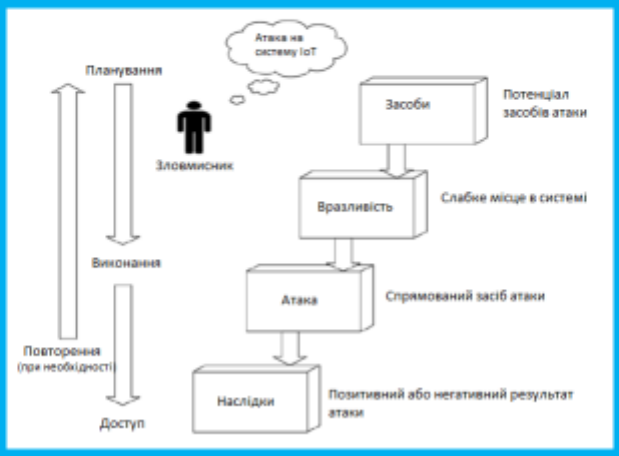
Автентифікація та авторизація пристроїв є важливими аспектами безпеки в системах Інтернету речей. Автентифікація пристрою - це процес перевірки автентичності пристрою, який гарантує, що пристрій дійсно є тим, за кого себе видає. Авторизація, з іншого боку, визначає права доступу пристрою до ресурсів і функцій системи після успішної автентифікації.

Шифрування даних відіграє важливу роль у забезпеченні безпеки систем IoT. Воно допомагає захистити конфіденційність інформації, що передається між пристроями та процесорами даних.

Моніторинг та аналіз безпеки відіграють ключову роль у забезпеченні безпеки систем Інтернету речей. Ці процеси допомагають виявити вразливості, аномальну поведінку і потенційні загрози, що дозволяє швидко реагувати і запобігати інцидентам безпеки.

Вразливості IoT систем

Вразливості в системах Інтернету речей (IoT) становлять серйозну загрозу їхній безпеці та можуть мати різноманітні негативні наслідки, включаючи витік даних, порушення конфіденційності та доступності інформації, а також негативний вплив на фізичні об'єкти, що контролюються пристроями IoT.



МЕТОДИКА З БЕЗПЕКИ В IOT

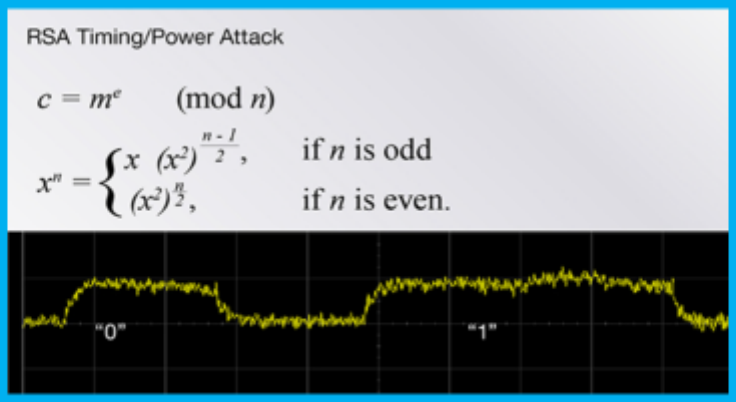
Екосистема IoT-технологій являє собою комбінацію різних технологічних зон: зона IoT-пристроїв, мережева зона і хмарна зона. Ці зони можуть бути джерелом цифрових даних. Тобто дані можна збирати з розумного пристрою або датчика з внутрішньої мережі, такого як брандмауер або маршрутизатор, або із зовнішніх мереж (хмара чи додаток. Ці технологічні зони є і об'єктом кримінального інтересу кіберзлочинців.

Способи захисту від загроз

Способи захисту	Опис
Управління інформаційною безпекою та управління ризиками	Заходи безпеки, що стосуються аналізу ризиків безпеки інформаційної системи, політики, акредитації, показників та аудиту, а також безпеки людських ресурсів
Управління екосистемами	Заходи безпеки щодо картування екосистем і відносин екосистем
Архітектура інформаційної безпеки	Заходи безпеки, що стосуються конфігурації систем, управління активами, поділу систем, фільтрації трафіку та криптографії
Адміністрування інформаційної безпеки	Заходи безпеки щодо адміністративних облікових записів та адміністративних інформаційних систем
Керування ідентифікацією та доступом	Заходи безпеки щодо аутентифікації, ідентифікації та прав доступу
Технічне забезпечення інформаційної безпеки	Заходи безпеки щодо процедур технічного забезпечення IT безпеки та віддаленого доступу
Управління інцидентами комп'ютерної безпеки	Заходи безпеки щодо аналізу та реагування на інциденти безпеки в інформаційній системі, а також звіт про інциденти

Атака за енергоспоживанням на алгоритм RCA

Більшість шкідливих програм можна виявити за перериванням живлення через побічні канали. Запропонована система відстежує енергоспоживання пристрою і використовує машинне навчання для виявлення можливої аномальної поведінки. Такі методи можуть бути використані для автентифікації та авторизації IoT-пристроїв у ненадійних мережах.



Розробка програми для перевірки вразливостей у системах Інтернету речей (IoT)

Програма, яку ми розробили, призначена для перевірки вразливостей у системах Інтернету речей (IoT) на основі даних про температуру, одержуваних із пристрою. Ось короткий опис цієї програми:

Мета програми: Очікування приходу даних про температуру з пристрою IoT і перевірка їх на вразливості, як-от різка зміна температури або несподівана зміна інтервалу надсилання даних.

Опис роботи програми:

Програма очікує приходу даних кожні 5 секунд.

Якщо дані надходять, їх перевіряють на різку зміну температури. Якщо зміна понад 2 градуси, виводиться повідомлення про злом.

Якщо дані не надходять протягом 5 секунд, програма також виводить повідомлення про злом.

Використання програми: Програму можна використовувати для виявлення потенційних вразливостей у системах IoT, пов'язаних із моніторингом і керуванням температурою, і вжиття заходів для їх виправлення.

Результати роботи програми

```
Checking for vulnerabilities...
Received temperature data: 22 degrees Celsius
Received temperature data: 23 degrees Celsius
Received temperature data: 27 degrees Celsius
Temperature spike detected and unusual data sending interval. Possible intrusion!
```

Наш алгоритм перевірки вразливостей у системах IoT являє собою простий, але ефективний підхід до виявлення потенційних загроз безпеки. Ось кілька причин, чому його використання може бути корисним:

Простота й ефективність: Наш алгоритм простий у реалізації та не вимагає складних обчислень або налаштування. Він заснований на принципі виявлення різких змін даних, що робить його ефективним для швидкого виявлення можливих загроз безпеки.

Швидка реакція на загрози: Алгоритм працює в реальному часі, що дає змогу виявляти та реагувати на вразливості негайно після їх виникнення. Це дає змогу оперативно вживати заходів щодо захисту системи.

Низьке навантаження на систему: Алгоритм очікує приходу даних кожні 5 секунд, що не створює значного навантаження на систему. Це дає змогу використовувати його навіть на ресурсно-обмежених пристроях IoT.

ВИСНОВКИ

У кваліфікаційній роботі ми зосередили увагу на аналізі та забезпеченні безпеки в системах Інтернету речей (IoT). Розділ 1 роботи присвячений огляду існуючих методів забезпечення безпеки в IoT системах, таких як аутентифікація та авторизація пристроїв, шифрування даних, моніторинг та аналіз безпеки, а також уразливості IoT систем.

У розділі 2 ми детально розглянули методи забезпечення безпеки в системах Інтернету речей, звернувши увагу на методи аналізу та забезпечення безпеки, шифрування даних, фізичну безпеку та захист від атак DoS і DDoS.

Завершальний розділ роботи присвячений методиці забезпечення безпеки в IoT, зокрема інформаційній безпеці пристроїв IoT з використанням апаратної підтримки та розробці програми для перевірки вразливостей у системах Інтернету речей.

Додаток Б

(Обов’язковий)

ВІДОМОСТІ АТЕСТАЦІЙНОГО ПРОЕКТУ

№ п/п	Позначення	Найменування	Додаткові ві-домості
		Текстові документи	
		Пояснювальна записка	57с.

					ГЮІК.467957.000Д2		
Зм	Арк.	№ докум.	Подп.	Дата			
Розроб.		Климашевський			Аналіз методів забезпечення безпеки в IoT системах. Відомість атестаційного проекту	Літера	Аркуш	Аркушів
Перевір.		Мерзлікін				У	1	1
Н. контр.		Бітченко				ХНУРЕ Кафедра РТІКС		
Затв.		Зарудний						