ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

КВАЛІФІКАЦІЙНА РОБОТА

МОДЕЛЬ ГЕНЕРАЦІЇ АТАК І МАРКУВАННЯ НАБОРІВ ДАНИХ ПРО АТАКИ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

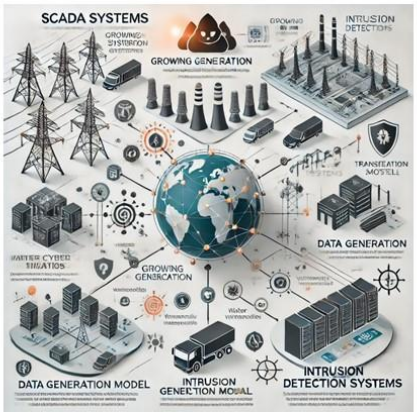
ВИКОНАВ:
•Студент гр КСМм-23-1 Пасічнюк Р. Р.

КЕРІВНИК:
доц. Ільїна І.В.

ХАРКІВ
2025р.

Актуальність дослідження

Розробка моделі генерації атак дозволяє створювати реалістичні сценарії атак на основі специфіки SCADA-протоколів, таких як DNP3 і MODBUS, а також враховувати унікальні характеристики кожного середовища. Це дозволяє не лише тестувати існуючі системи виявлення вторгнень, але й формувати нові стратегії захисту, які враховують сучасні загрози.

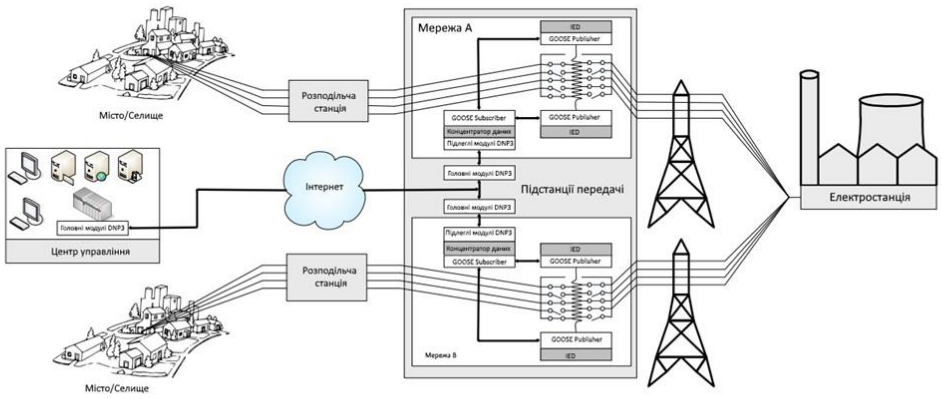


Мета та завдання

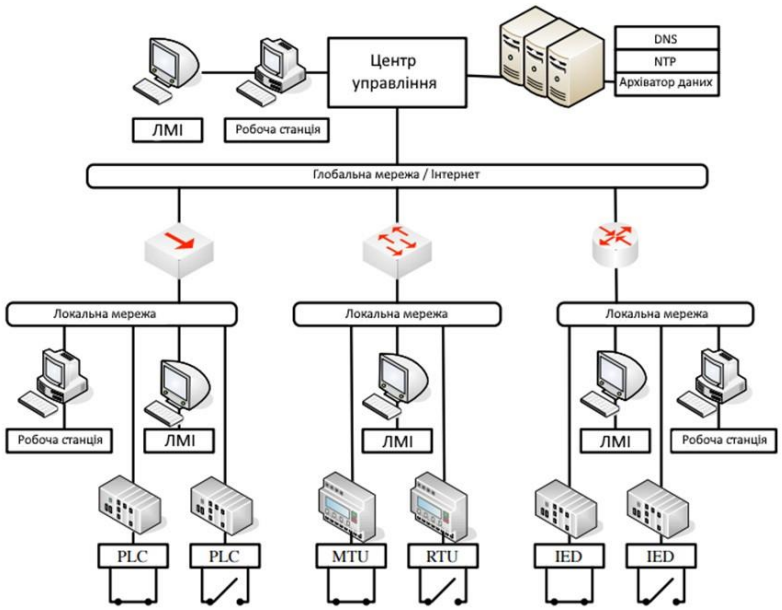
Мета роботи:
Розробка моделі генерації атак і маркування наборів даних про атаки для систем виявлення вторгнень, яка забезпечує можливість створення реалістичних сценаріїв атак на основі специфіки SCADA-протоколів і дозволяє підвищити ефективність роботи систем виявлення вторгнень у критичних інфраструктурах.
Завдання роботи:
1.Провести аналіз сучасних загроз і вразливостей SCADA-систем.
2.Визначити ключові вимоги до генерації даних про атаки, орієнтованих на специфічні протоколи автоматизації (DNP3, MODBUS тощо).
3.Розробити архітектуру фреймворку для моделювання кібератак та створення маркованих наборів даних.
4.Реалізувати модулі для ін’єкції, маскування, флудингу, атак типу "людина посередині" (MITM) і відтворення атак (replay).
5.Забезпечити можливість розвідки мережевих пристроїв і маніпуляції даними в реальному часі.
6.Провести тестування фреймворку на віртуальному стенді з використанням протоколу DNP3 та оцінити його ефективність.
7.Розробити рекомендації щодо використання фреймворку для вдосконалення систем виявлення вторгнень.
Ця робота спрямована на підвищення кібербезпеки критичних інфраструктур шляхом створення інструменту для моделювання і аналізу потенційних атак.

3

Абстрактний вигляд мережі передачі електроенергії



4



5

Список атак на SCADA-системи

- Атака типу "людина посередині" (MITM)
- Ін’єкція (Injection Attack)
- Маскування (Masquerading)
- Флудинг (Flooding)
- Відтворення атак (Replay Attack)
- Розвідка мережі (Reconnaissance)
- Атака на відмову в обслуговуванні (Denial of Service, DoS)
- Підміна команд (Command Injection)
- Спуфінг (Spoofing)
- Зміна даних (Data Manipulation)
- Евесдропінг (Eavesdropping)
- Привласнення ресурсів (Resource Hijacking)
- Використання вразливостей (Exploitation of Vulnerabilities)
- Сканування портів (Port Scanning)
- Зловживання функціями (Function Abuse)

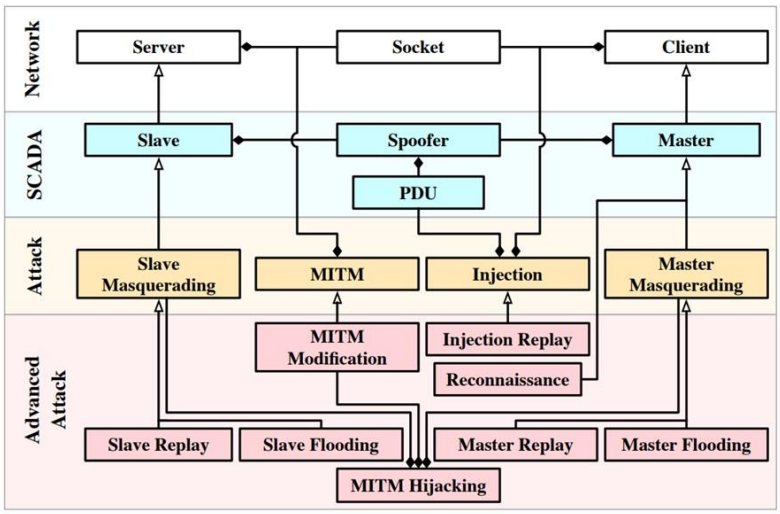
6

Вимоги для генерації даних атак SCADA

1. здатність розбирати повідомлення протоколів SCADA.
2. здатність відтворювати стек протоколів SCADA.
3. здатність прослуховувати локальний трафік SCADA-мережі.
4. здатність впроваджувати аномальні повідомлення протоколу SCADA у мережу
5. здатність змінювати дані протоколу в режимі реального часу.
6. надання сервісу майстра протоколу для маскування.
7. надання сервісу веденого протоколу для маскування
8. надання функцій розвідки SCADA-мереж для виявлення додатків SCADA.
9. здатність відтворювати попередні повідомлення протоколу SCADA.
10. здатність перевантажувати сервіс SCADA аномальними повідомленнями.

7

UML діаграма класів представленого фреймворку генерації даних про кібератаки SCADA



8

```
1: packet ← {ethernet, ip, tcp}
2: pdu ← PDU()

3: procedure INJECT
4:     sequence ← packet_tcp_seq + len(pdu) + len(mal_pay)
5:     packet_tcp_seq ← sequence
6:     SOCKET.SEND({packet, pdu, mal_pay})

7: procedure UPDATE(p)
8:     packet_ethernet_src ← p_ethernet_src
9:     packet_ethernet_dst ← p_ethernet_dst
10:    packet_ip_src ← p_ip_src
11:    packet_ip_dst ← p_ip_dst
12:    packet_tcp_src ← p_tcp_src
13:    packet_tcp_dst ← p_tcp_dst
14:    packet_tcp_seq ← p_tcp_seq
15:    packet_tcp_ack ← p_tcp_ack
16:    if PDU ∈ p then
17:        pdu_src ← PPDU_src
18:        pdu_dst ← PPDU_dst
19:        pdu_seq ← (PPDU_seq+1)

20: procedure SNIFF
21:    while running do
22:        p ← SOCKET.RECV
23:        if p ≠ ∅ then
24:            UPDATE(p)
```

9

Лістинг 1 – Процедура автоматизації маскування для Master пристроїв

```
1: spoofer ← Spoofer()
2: running ← True
3: queue_out ← Queue()

4: procedure AUTOMATION
5:     while running do
6:         request1 ← SPOOFER.REQUEST(message1)
7:         request2 ← SPOOFER.REQUEST(message2)
8:         request3 ← SPOOFER.REQUEST(message3)
9:         sleep(interval)
10:        queue_out(request1)
11:        queue_out(request2)
```

Лістинг 2 – Процедура автоматизац маскування для Slave пристроїв

```
1: spoofer ← Spoofer()
2: trigger ← False

3: procedure AUTOMATION
4:     while running do
5:         if trigger then
6:             unsolicited ←
SPOOFER.UNSOLICITED(message)
7:             queue_out(unsolicited)
8:             trigger ← False
```

10

Лістинг 3 – Алгоритм визначення адреси

```
1: src ← 0
2: dst ← 0
3: rsp ← False
4: while ¬rsp ∧ src ≤ MAX_ADDRESS do
5:     while ¬rsp ∧ dst ≤ MAX_ADDRESS do
6:         PDU_src ← src
7:         PDU_dst ← dst
8:         SEND(PDU)
9:         dst ← dst + 1
10:    src ← src + 1
```

11

Атака повторного відтворення (Replay Attack)

Суть атаки:
Зловмисник перехоплює легітимні повідомлення, що використовуються в SCADA-системі, та повторно відправляє їх, щоб викликати небажані дії у системі.

Цілі:
Маніпуляція станом системи.
Виклик збоїв у роботі обладнання.
Виконання старих команд або дублювання процесів.

Механізм атаки:
Перехоплення трафіку між майстром (master) та підпорядкованим пристроєм (slave).
Збереження перехоплених повідомлень.
Повторна відправка легітимних повідомлень у потрібний момент.

Наслідки:
Порушення роботи систем автоматизації.

12

Атака флудинг (Flooding Attack)

•**Суть атаки:**
Зловмисник надсилає велику кількість повідомлень до SCADA-сервісу з метою перевантаження його ресурсів або примушення до виконання небажаних дій.
•**Цілі:**
•Перевантаження мережевих або обчислювальних ресурсів.
•Заважання обробці легітимних запитів.
•Примус цільового пристрою перейти в небажаний стан.
•**Механізм атаки:**
•Генерація та відправлення великої кількості запитів.
•Маніпуляція пам'яттю або регістрами пристроїв SCADA.
•Використання швидкого відправлення критичних повідомлень.
•**Наслідки:**
•Відмова в обслуговуванні (Denial of Service).
•Порушення нормального функціонування SCADA-систем.
•Потенційна небезпека для обладнання та інфраструктури.
•**Захист:**
•Впровадження лімітів на кількість запитів за певний час.
•Використання систем виявлення аномальної активності (IDS).
•Захист на мережевому рівні, зокрема фільтрація трафіку.

13

Лістинг 4– MITM Forwarding

```
1: procedure FORWARDING(packet)
2:     if packet_ether_dst ≡ Attacker_mac then
3:         if packet_ip_src ≡ Master_ip then
4:             packet_ether_dst ← Master_mac
5:             SOCKET.SEND(packet)
6:         else if packet_ip_src ≡ Slave_ip then
7:             packet_ether_dst ← Slave_mac
8:             SOCKET.SEND(packet)
9:         else Drop packet
```

14

Висновки

У даній кваліфікаційній роботі була представлена розробка фреймворку для генерації даних про кібератаки SCADA, який враховує сучасні виклики та вимоги до захисту систем критичної інфраструктури. Основна увага приділялася розробці модульного підходу, який дозволяє забезпечити гнучкість та масштабованість у процесі створення тестових даних для виявлення та аналізу атак.

У рамках роботи було виконано:

– аналіз існуючих таксономій атак на протоколи SCADA та їх впливу на критичну інфраструктуру;
– визначено 10 основних вимог до фреймворку генерації атак, які дозволяють створювати реалістичні дані для тестування;
– розробка та імплементація модулів фреймворку, таких як PDU, спуфер, модулі ін'єкції, маскування та MITM, для реалізації атак на мережевому рівні.

Подальший розвиток фреймворку може включати розробку експериментального стенда для перевірка роботи фреймворку на тестовому середовищі DNP3, що продемонструє практичну цінність реалізованого підходу.

Апробація результатів:

Пасічнюк Р.Р., Ільїна І.В.,МОДЕЛЬ ГЕНЕРАЦІЇ АТАК І МАРКУВАННЯ НАБОРІВ ДАНИХ ПРО АТАКИ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ // Проблеми інформатизації : XII міжнародна науково-технічна конференція. - 21-22 листопада 2024. –с.105. doi: https://doi.org/10.32620/PI.24.t2