OT 네트워크에서 자산 식별을 위한 네트워크 트래픽 특성 분석

2023 차세대컴퓨팅 춘계 학술대회

박민수, 안석현, 조성제, 김홍근

INDEX

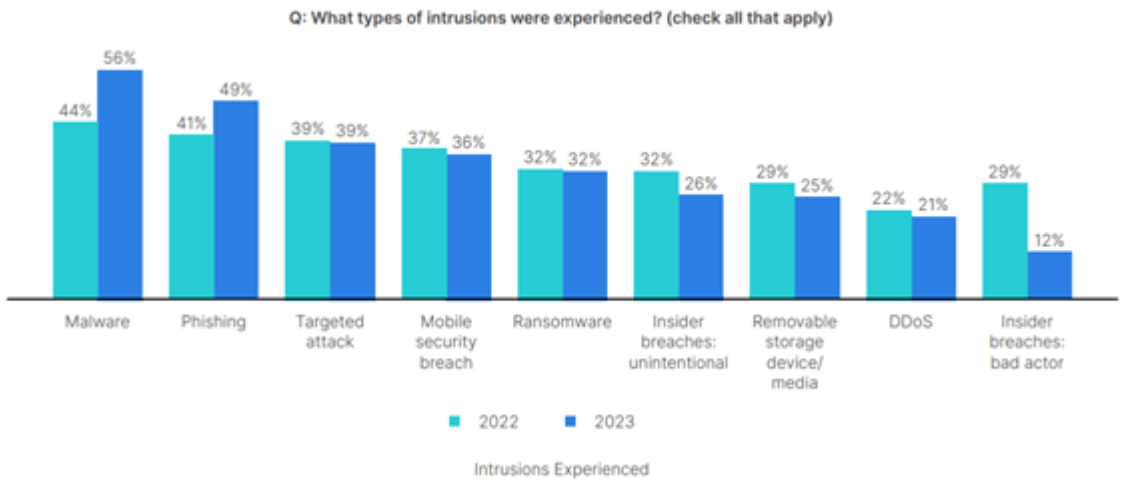
01 연구 배경

연구 배경

❖배경

- 디지털 전환으로 인해 스마트 전력망, 스마트 빌딩, 스마트 팩토리 등 **‘스마트 x’ 기술의 등장**으로 인터넷과 격리되어 있던 OT(Operational Technology) 네트워크가 인터넷과 연결
- 격리되어 있던 네트워크의 인터넷 연결로 인해 **사이버 공격 위협이 지속**

포티넷, ‘2023 글로벌 운영기술(OT) 및 사이버보안 현황 보고서’ 발표



출처: 포티넷 코리아 뉴스, 2023년 6월 5일

연구 배경

❖OT 환경에 대한 사이버 공격 대응 방안

- 사이버 공격에 대한 위협을 효율적으로 방어하기 위해서는 중요 인프라에 있는 **자산 식별**, **취약점 탐지 및 완화** 조치가 필요
- 하지만, OT 장비들의 **가용성 중요도**와 **자원의 한계**로 인해 기존 IT 시스템에서 자산을 식별하기 위해 사용하던 **네트워크 스캐닝(Network Scanning) 기법을 적용하기에 어렵다**는 문제가 있음

❖해결 방안

- 본 논문에서는 위 문제를 해결하고자 OT 네트워크인 스마트 공장 네트워크에서 **자산 식별**을 위해 트래픽 정보를 수집하고, 장치 별 **고유한 특징 정보를 식별**하는 연구를 수행

02 관련 연구

관련 연구

❖ Network Scanning 기법
- Active Scanning: 네트워크에 직집적인 쿼리를 요청해 자산을 식별하는 방식
- Passive Scanning: 네트워크에 직접적인 쿼리를 발생하지 않고 트래픽 관찰만으로 자산을 식별하는 방식

구분	ICS/SCADA 장치 식별: 하이브리드 통신 패턴과 패시브 핑거프린팅 접근 [7]	장치의 특별한 Modbus 정보를 활용한 원격 필드 장치 핑거프린팅 [8]	BACnet 장치 검색 및 속성 식별 자동화에 대해 [추가 문헌]
연구 대상	싱가포르(iTrust)의 수처리 SCADA(supervisory Control and Data Acquisition) 테스트베드 등 공개데이터 3개	Wago PLCs, MegaTec SNMP Card for UPS(Uninterruptible Power Supply), ElectroIndustries/GaugeTech, Eaton Corporation on Internet.	Siemens Desigo CC Building management, DXR, QMX, QAM Series 3개의 기기
식별 특징 정보	총 20개의 특징정보(프레임 길이, 공급업체 MAC ID, TCP Segment Length, IP Packet Length, TTL 등)	제조사 별 Modbus의 레지스터 주소 활용	빌딩 전용 프로토콜(BACnet 객체, BACnet 속성)의 정보 특성 활용
식별 방법	Passive Scanning	Active Scanning	Active Scanning

관련 연구

❖ [7] Al Ghazo, Alaa T., and Ratnesh Kumar**. "Ics/scada device recognition: A hybrid communication-patterns and passive-fingerprinting approach."** *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2019.

❖ [8] Keliris, Anastasis, and Michail Maniatakos. **"Remote field device fingerprinting using device-specific modbus information."** *2016 IEEE 59th international Midwest symposium on circuits and systems (MWSCAS)*. IEEE, 2016.

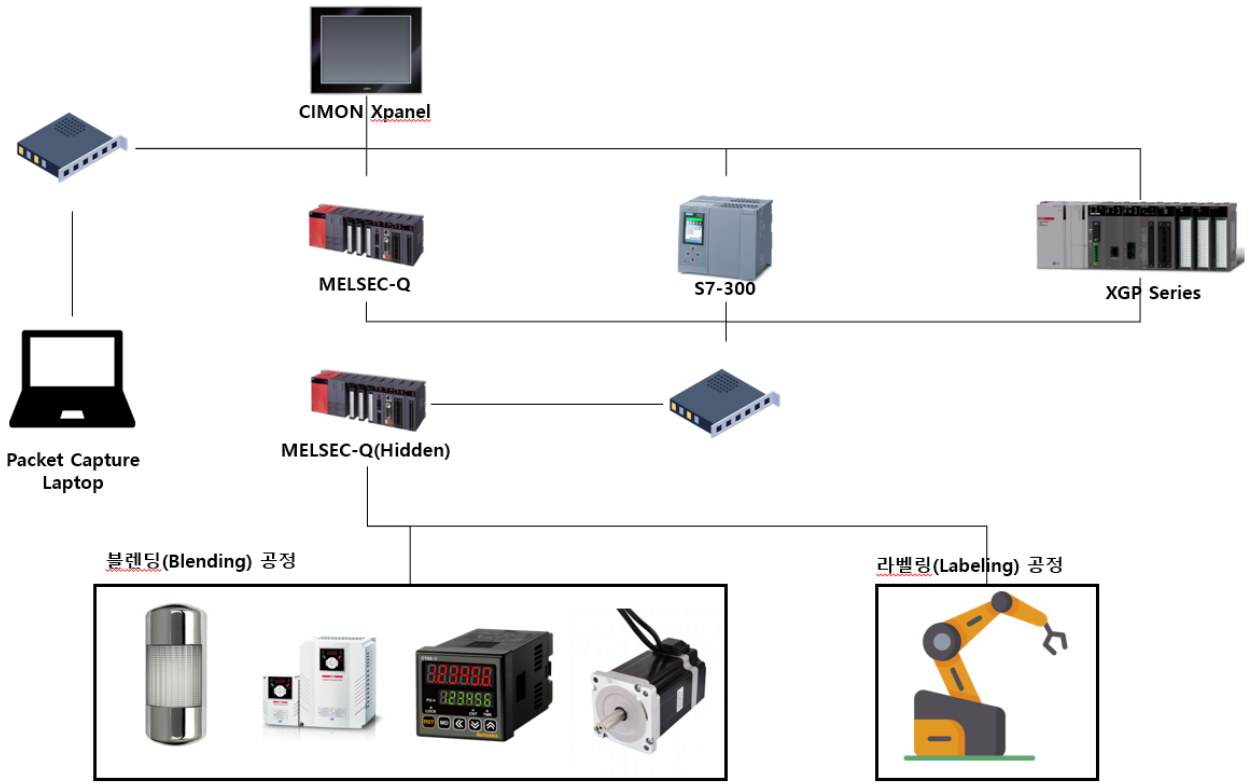
❖ [추가 문헌] Cash, Michael, et al. **"On Automating BACnet Device Discovery and Property Identification."** *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021.

03 실험 환경 및 설계

실험 대상 및 설계

❖실험 환경
- KISA 스마트 팩토리 보안 리빙랩(안산)

❖실험 대상
- 4개의 제조사(LS Electric, Mitsubishi, Siemens, CIMON)
- 5개의 장비(PLC 4개, HMI 1개)



❖실험 설계
- Wireshark를 통한 트래픽 수집
- Passive scanning 방식 접근
  - 공정을 제어하는 경우(6시간)
  - 공정을 제어하지 않는 경우(6시간)

장비	모델명
LS Electric PLC	XGT Series
Mitsubishi PLC	MELSEC-Q
Siemens PLC	S7-300
CIMON HMI	Xpanel

04 실험 결과 분석

실험 결과 분석

❖실험 결과 분석

- OSI 7 계층의 응용 계층, 전송 계층, 네트워크 계층 관점에서 특징 정보 추출
  - **응용 계층**: 장치 별 사용하는 프로토콜 및 산업 전용 프로토콜
  - **전송 계층**: TCP Window size, TCP Segment Length, UDP Data Length
  - **네트워크 계층**: TTL(Time To Live)

실험 결과 분석

❖응용 계층 분석

- OT 장치는 자동 제어를 위해 제조사마다 독립적인 프로토콜을 사용

장비	프로토콜
MELSEC-Q	Modbus
Xpanel	Modbus
S7-300	S7comm
XGT Series	XGT 전용
MELSEC-Q(Hidden)	MELSEC 전용

❖응용 계층에서의 특성

- 공정을 제어하는 경우 & 제어하지 않는 경우 **모두 동일한 결과**를 확인할 수 있음
  - XGT Series, MELSEC-Q, S7-300은 **제조사 별 전용 프로토콜**을 사용
  - MELSEC-Q의 경우 산업에서 자동제어를 위해 만들어진 Modbus 혹은 MELSEC 전용 프로토콜을 사용하지만, 다른 제조사 장비도 Modbus를 사용할 수 있음
  - **제조사 별 전용 프로토콜**을 확인하는 것은 일부 **장치를 식별**하는데 **유용한 정보**가 될 수 있음

실험 결과 분석

❖전송 계층 분석

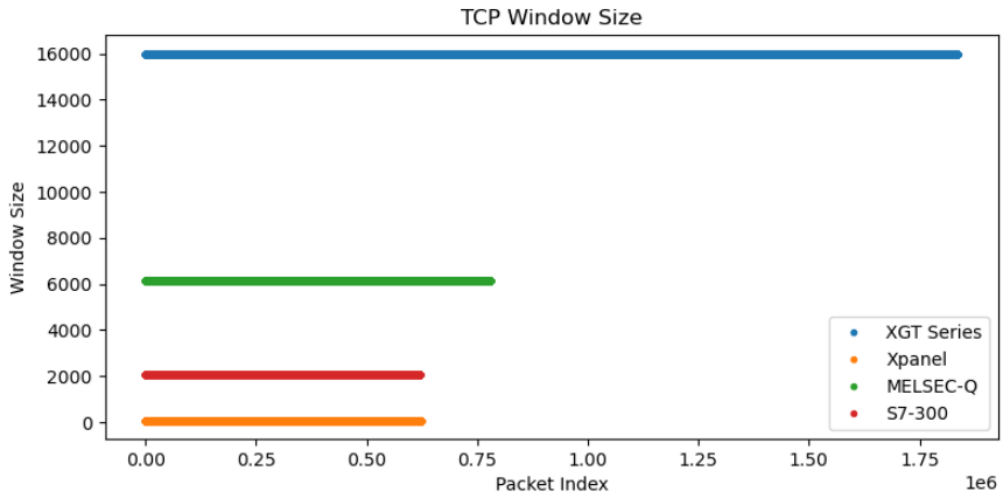
- TCP Window size, TCP Segment Length, UDP Data Length의 최소, 최대, 평균 값을 확인**(단위: byte)**

구분	모델명	TCP Window Size			TCP Segment Length			UDP Data Length		
		최소	최대	평균	최소	최대	평균	최소	최대	평균
공정 제어	XGT Series	16000	16000	16000	54	64	56.1	0	0	0
	MELSEC-Q	6132	6144	6138	30	83	32	0	0	0
	MELSEC-Q(hidden)	0	0	0	0	0	0	18	1472	484
	S7-300	2048	2048	2048	26	45	35.5	0	0	0
	Xpanel	62	86	65.1	54	64	56	40	40	40
공정 미제어	XGT Series	16000	16000	16000	54	64	56	0	0	0
	MELSEC-Q	6132	6144	6138	30	80	32.5	0	0	0
	MELSEC-Q(hidden)	0	0	0	0	0	0	18	1472	484
	S7-300	2048	2048	2048	26	45	35.5	0	0	0
	Xpanel	0	8192	65.1	33	61	60.4	40	40	40

실험 결과 분석

❖장치 별 TCP Window Size 변화

- 공정을 제어하는 경우 TCP Window Size의 변화



❖전송 계층에서의 특성

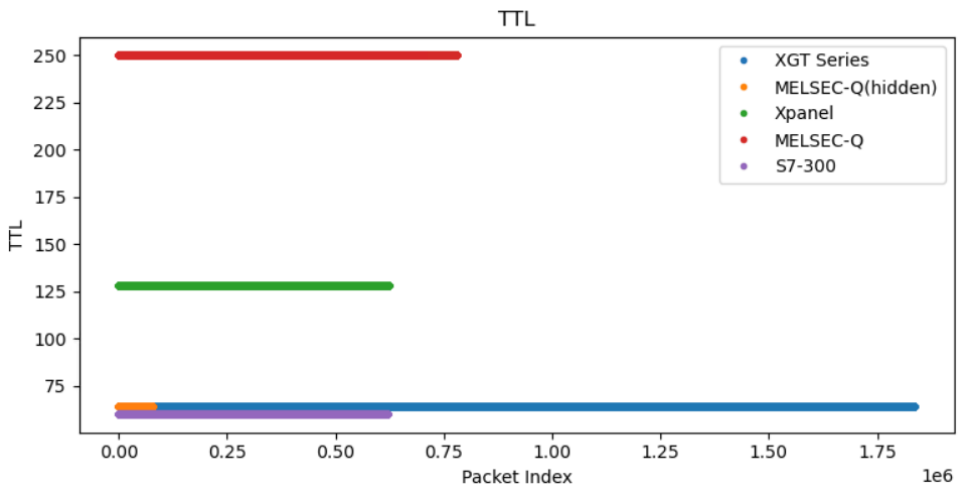
- 공정을 제어하는 경우& 제어하지 않는 경우 **일부 차이(TCP Segment Length)가 발생**
  - **TCP Window Size**의 평균값은 **모든 장치가 동일**
  - **TCP Segment Length**의 평균은 차이가 발생했으며, 4, 0.5, 0.1 바이트 크기로 **차이가 발생**
  - **UDP Data Length**는 CIMON Xpanel, Mitsubishi MELSEC-Q PLC 만 확인 가능
    - 공정을 제어하는 경우& 제어하지 않는 경우 **동일한 결과 값**을 보여줌

실험 결과 분석

❖네트워크 계층 분석

- TTL(Time To Live) 값은 PC 운영체제를 식별하던 특징 정보로도 활용

장비	공정 제어 시 TTL 값			공정 미 제어 시 TTL 값		
	최소	최대	평균	최소	최대	평균
XGT Series	64	64	64	64	64	64
MELSEC-Q	250	250	250	250	250	250
MELSEC-Q (Hidden)	64	64	64	64	64	64
S7-300	60	60	60	60	60	60
Xpanel	128	128	128	128	128	128



❖네트워크 계층에서의 특성

- 공정을 제어하는 경우 & 제어하지 않는 경우 **TTL 값은 같음**
  - XGT Series, MELSEC-Q(Hidden) PLC는 같은 TTL 값인 64를 사용
  - MELSEC-Q PLC는 같은 장치임에도 TTL 값이 64와 250을 사용
  - 세 개의 장비에서 TTL 값이 달라, TTL 값이 **일부 자산 식별에 활용할** 수 있음

실험 결과 분석

❖계층 특징 정보 별 한계점 파악

장비	특징 정보	내용
응용 계층	제조사 전용 프로토콜	**장치의 제조사**를 알 수 있으나, **장치 유형** 혹은 **개별 장치**를 **식별은 할 수 없음**
	산업 전용 프로토콜	**장치의 제조사**를 알 수 없지만, **관련 연구**에서 **Modbus**의 경우 **메모리 필드 정보**를 활용해 **일부 장치를 식별하는데 활용**될 수 있음
전송 계층	TCP Window Size	장치별로 크기가 다르고, 값이 일정하여 **일부 장치의 고유한 식별 정보로 활용**될 수 있음
	TCP Segment Length	공정을 제어하거나 제어하지 않는 경우 일부 차이가 발생하여 **고유한 식별 정보로 활용**될 수 **없음**
	UDP Data Length	장치별로 크기가 다르고, 값이 일정하여 **일부 장치의 고유한 식별 정보로 활용**될 수 있음
네트워크 계층	TTL(Time To Live)	값이 일정하여 장치의 고유한 특징 정보로 활용될 수 있으나, 값이 겹치는 경우가 존재하기에 **일부 장치 식별에 활용**될 수 있음

❖논의

- 공정을 제어하는 경우&제어하지 않는 경우에 **TCP Segment Length의 값에서만 차이**가 발생
- 다섯 개의 장치를 **각각 식별할 수 있는 단일 특징 정보는 없음**
- TCP Window size는 MELSEC-Q(hidden) PLC를 제외하고 모든 장치를 식별할 수 있음
- UDP Data Length는 MELSEC-Q(hidden) PLC를 식별할 수 있음

05 결론 및 향후 연구

결론 및 향후 연구

❖결론

- 본 논문에서는 OT 네트워크에서 자산을 식별하기 위해 OSI 7 계층 중 응용 계층, 전송 계층, 네트워크 계층을 기준으로 **확인한 특징 정보를 활용해 자산을 식별할 수 있음**을 확인

❖한계점

- 실험에 사용된 **장치의 수가 적음**
- 장치의 수가 많아지면 확인한 특징 정보가 **고유하지 않을 수 있음**

❖추가적으로 사용 가능한 특징 정보

- **장치 유형** 식별에 사용되는 특징 정보: 흐름 볼륨(Flow Volume), 패킷 간 도착 시간(Inter Arrival Time) …
- **개별 장치** 식별에 사용되는 특징 정보: 클록 스큐(Clock Skew)
- **기타**: Application Port Numbers, MAC Address …

결론 및 향후 연구

❖향후 연구

- OT 제품 분석 **대상 확대**할 계획
- 광범위한 OT 제품에 적용 가능한 **자산 식별 기법 개발**할 계획

Q&A