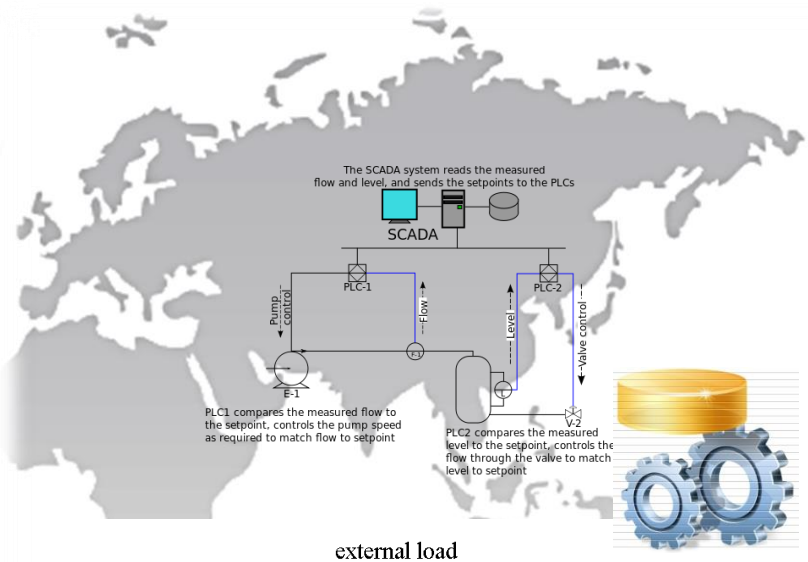
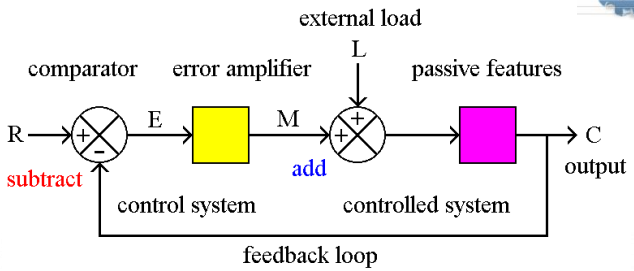
Industrial IoT 보안 기술

– 산업 제어 시스템 중심 –



SMARTGRID



Howon Kim
(Pusan National University)

CONTENTS

순 서

산업 제어 시스템 개요

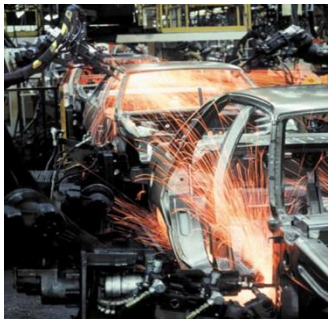
- 산업 제어 시스템:
  - SCADA, PCS, DCS, Automation, PLC등 다양한 통신 프로토콜, OS, 응용 기술로 구성됨
  - 발전소, 전력망, 철도, 정유공장, 공장 자동화 등 다양한 응용 환경에서 사용됨

Supervisory Control And Data Acquisition (SCADA)

Distributed Control Systems(DCS)

Process Control Systems (PCS)

Programmable Logic Controller(PLC)



Automation

그림 참고[1]

산업 제어 시스템 개요

- SCADA(Supervisory Control and Data Acquisition)
  - 산업 공정이나 인프라, 생산설비/공정을 모니터링하고 제어하는 시스템
    - 제조 공정, 발전소, 파워 그리드, 상하수 관제 시스템, 정유 공정, 공장에서의 작업 공정, HVAC 냉난방 시스템 등에 적용됨

- DCS(Distributed Control System)
  - 제조 시스템 및 공정 제어 시스템으로서 SCADA는 데이터수집/모니터링에 중점을 두는 반면, DCS는 공정 제어에 중점을 둠

산업 제어 시스템 개요

- 산업 제어 시스템의 주요 특성
  - 비표준화된 proprietary 기술 사용
  - 특정 응용을 위한 vertical solution을 제공하며 응용별 customized 됨
  - 응용에 따라 특정한 통신/네트워크 방식/프로토콜 사용
    - 유선 통신, 광 통신, serial 통신, dialup, microwave 등
    - 수백 종류의 통신/네트워크 프로토콜이 존재
    - 실시간성, 신뢰성 등, 응용 환경에 따라 각각 다른 특성을 중요하게 생각함
  - 오랜 기간동안 사용됨
  - 초기 단계에서 security를 고려하지 않고 개발됨

산업 제어 시스템 개요 – IP/web service 연동

- 기존 proprietary 통신 + IP network + Web Service 기술

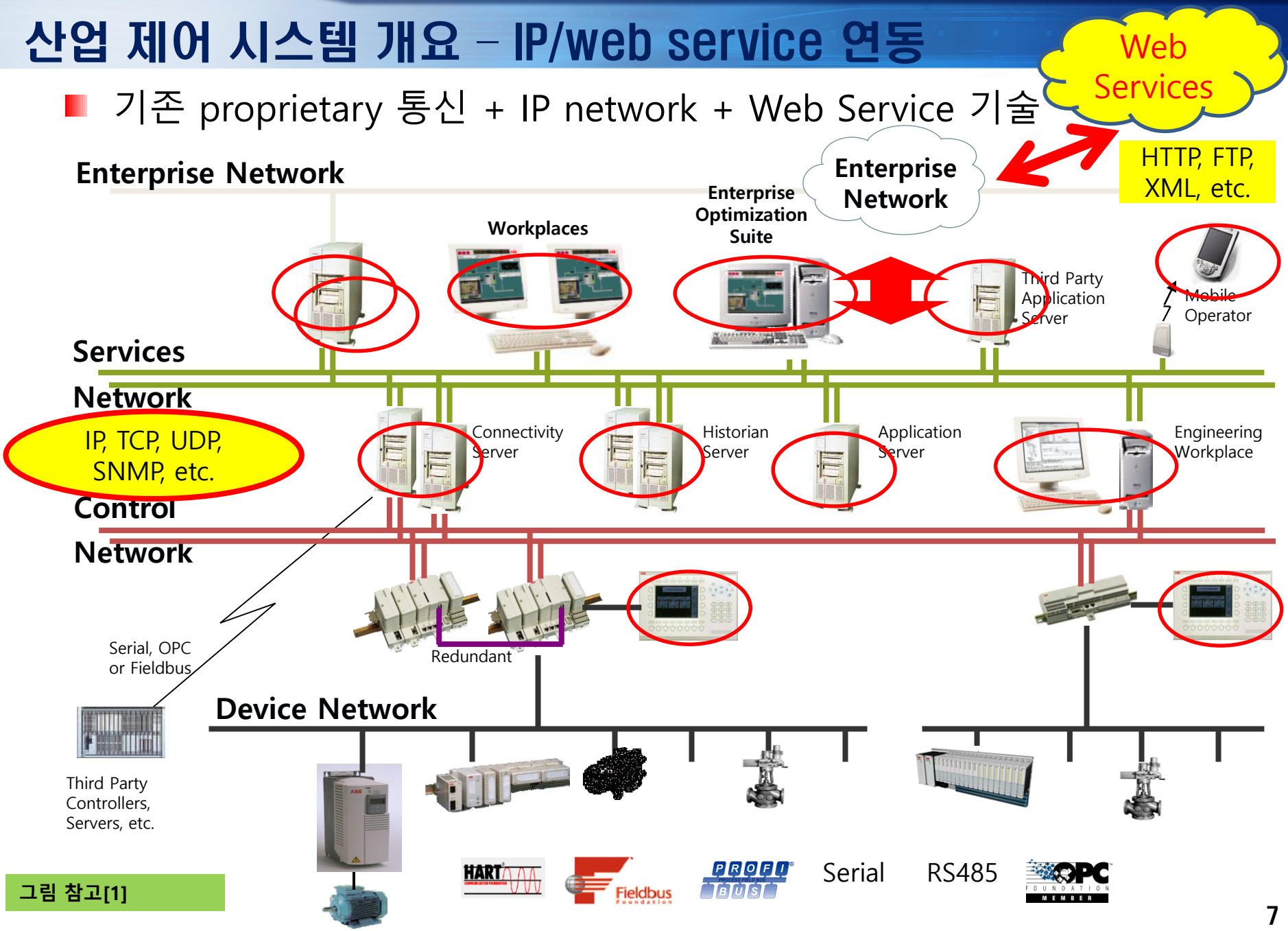


그림 참고[1]

산업 제어 시스템과 인터넷 연결 – 보안 취약성 증대

- 전통적인 제어 시스템 통신 기술 + IP 네트워크 → 보안 취약성 증대
- 산업 제어 시스템에서의 가능한 보안 취약성/공격 유형

• Worms and Viruses	• Legacy OSes and applications
• DOS and DDOS	• Inability to limit access
• Unauthorized access	• Inability to revoke access
• Unknown access	• Unexamined system logs
• Unpatched systems	• Accidental misconfiguration
• Little or no use of anti-virus S/W	• Improperly secured devices
• Limited use of host-based firewalls	• Improperly secured wireless
• Improper use of ICS workstations	• Unencrypted links to remote sites
• Unauthorized applications	• Passwords sent in clear text
• Unnecessary applications	• Default passwords
• Open FTP, Telnet, SNMP, HTML ports	• Password management problems
• Fragile control devices	• Default OS security configurations
• Network scans by IT staff	• Unpatched routers / switches
• Cloning attack	• Unprotected firmware
• Unprivileged access to the I/O interfaces	• Gateway to attack applications/monitoring services

참고[1]

순 서

II. 제어 시스템 보안 특성

(제어 시스템과 보안과 IT 시스템 보안 환경 차이)

산업 제어 시스템 보안 요구 사항 특성

- 기존 IT 시스템 보안 요구 사항(CIA triad)
  - Confidentiality: 정보에 대한 기밀성(비밀성) 보장
  - Integrity: 정보에 대한 위변조 감지
  - Availability: 서비스의 가용성 제공

- 산업 제어 시스템의 주요 보안 요구 사항 **– 우선순위 존재**
  - Availability(가용성)과 Integrity(무결성)은 산업제어 시스템의 정상 동작 및 신뢰성(reliability) 높은 동작을 위해 더욱 중요함
  - Confidentiality(기밀성)에 대한 요구는 상대적으로 낮음
  - 많은 산업 제어시스템에선 six 9 가용성을 추구함
    - 99.9999%의 가용성 제공을 추구함
  - 높은 가용성 제공의 어려움
    - 암호를 통한 기밀성, 인증/인가시 가용성 떨어질 수 있음
    - DoS 공격 방지 기법, rate limiting, monitoring, log 저장, resource 관리, 추가된 프로토콜 보안 단계, 추가된 redundancy 등은 가용성을 떨어뜨릴 가능성 높임
    - 보안성 강화시, 가용성을 동시에 제공해야 함

산업 제어 시스템 특성과 보안 취약성 (1/3)

- 보안 취약성이 있는 통신 프로토콜을 사용
  - 산업 제어 시스템에서는 telnet, ftp, snmp 등 보안 취약성이 높은 프로토콜을 사용하는 경우가 많음
  - 또한, DNP3(Distributed Network Protocol), Modbus, ICCP(Inter-Control Center Communications Protocol) 프로토콜에도 보안 취약성이 존재함

- 제어 시스템에 사용되는 OS의 보안 취약성
  - 제어 시스템에는 보안 취약성이있는 embedded OS와 구버전의 Windows OS를 사용하는 경우가 많음
  - 특히 DOS를 사용하는 경우, 원격 reset 및 rebooting 공격이 용이함

- 제어 시스템의 응용 소프트웨어 보안 취약성
  - 제어 시스템 상에서의 응용 소프트웨어는 성능 및 기능 위주로 개발되는 경우가 많으므로 보안 취약성이 많음
    - 제어 시스템 세부 동작을 모르는 경우라도 fail-open, fail-close 출력만을 변경하여 공격 가능
    - Buffer overflow 공격 등, 다양한 공격이 가능함

참고[2]

산업 제어 시스템 특성과 보안 취약성 (2/3)

- 공격이 용이한 제어 시스템 firmware
  - 제어 시스템 firmware는 일반적으로 OTA(Over the Air) 업데이트가 용이함
  - Firmware에 virus 혹은 worm을 심는 공격도 용이함

- Web service와 연결되는 제어 시스템
  - 제어 시스템은 운용 및 관리를 위해 web 인터페이스 혹은 web server를 구현하는 경우 많음 → 웹 보안 취약성을 가짐

- 기본 OS 혹은 제어 프로그램상에서의 부족한 access control 기법
  - 제어 시스템에는 Linux 혹은 Windows OS 등에서 가지는 kernel mode access control 등이 부족함

참고[2]

산업 제어 시스템 특성과 보안 취약성 (3/3)

- Ethernet-to-serial 연결이 용이함
  - 대부분의 제어 시스템은 serial 인터페이스와 Ethernet 연결망을 가짐
  - Ethernet 연결망을 통해 원격으로 제어 시스템을 모니터링 및 명령어 전송
  - 전송된 명령어는 serial 인터페이스를 통해 장치까지 제어 가능(참고: IEC 61850에선 Ethernet과 제어 시스템 end-device간 연결 인터페이스 제공)

- 불완전한 IDS
  - 제어시스템 proprietary 프로토콜을 사용할 경우, snort 등으로도 비정상 트래픽 혹은 event를 감지 못하는 경우가 많음

- 방화벽 등, 네트워크 보안 기술 부족
  - 제어 시스템 통신 프로토콜에 특화된 방화벽 기술 등이 부족한 상황

참고[2]

산업 제어 시스템 vs. IT 시스템(1/2)

- 산업 제어 시스템과 IT 시스템 비교 1

특성	IT 시스템	산업 제어 시스템
기밀성	High	Low
무결성	Low to moderate	Very high
가용성	Low to moderate	Very high
인증	Moderate	High
시간 적시성	Delays tolerated	Critical
현재의 보안기술	Good	Usually poor
S/W patch 특성	Frequent	Slow or impossible
시스템 life cycle	3~5 years	15+ years
소프트웨어 변경 빈도	Frequent, formal, documented	Rare, informal, not always documented
자동화된 툴	Widely used	Limited, used with care
상호 운용성	Not critical	Critical, security often not a consideration

참고[2]

산업 제어 시스템 vs. IT 시스템(2/2)

- 산업 제어 시스템과 IT 시스템 비교 2

특성	IT 시스템	산업 제어 시스템
통신 프로토콜	TCP/IP, UDP	DNP, ICCP, Modbus, Fieldbus, Profibus 등
통신 기법	Telco, Wi-Fi	Telco, radio, satellite, PLC, serial, Wi-Fi
컴퓨팅 연산 능력	비제한적	매우 제한적
통신 대역폭	넓음	좁음
보안 표준	ISO 17799, 27001, NIST SP8000-53	ISA 99, NERC CIP 002-009, NIST SP800-53, NIST SP800-82
포렌직	사용 가능	제한적
보안 테스팅	Pen-Testing	Pen-Testing with HMI
관리 기법	중앙 집중형	지역적
운영 체제	Windows, Unix, Linux 등	RTOS, embedded Linux 등
보안 침해 영향	Business 영향	Business 영향, 장비 파괴, 환경 영향, 개인 안전에 영향 등

참고[2]

산업 제어 시스템 보안 취약성 영향

- 산업 제어 시스템에 대한 공격 영향
  - 대규모 인명 손실(상해, 사망)
  - 국가 인프라 손상
  - 생산 차질
  - 소송
  - 기업체에 대한 신뢰 상실
  - 시장에서의 경쟁력 상실
  - 물리적/경제적 손실
  - 환경 파괴 등

Bushehr Nuclear Plant (Iran)

Stuxnet target:

SIEMES PLC system

순 서

III. 제어 시스템 보안 기술 동향

제어 시스템 통신 프로토콜 보안 기술

- DNP3 프로토콜 보안 취약성 연구 사례
  - DNP3 제어 시스템 프로토콜에 대한 보안 취약성 연구(국가보안기술연구소)
  - DNP3 프로토콜은 제어 시스템상에서 OSI 관점에서보면, L2(데이터링크), L4(트랜스포트), L7(응용) 계층을 정의
    - 중앙제어 장치에 연결된 다수의 RTU(Remote Terminal Unit), IED(Intelligent Electronic Device) 연결 정의
  - DNP3 프로토콜 보안 취약점 연구 결과
    - DNP3 프로토콜에 비인가 제어 명령을 전송하여 대량의 응답 패킷을 제어 시스템 서버로 전송, 재시작, 정지, 상태값 변경 등을 수행함
    - 다수의 보안 취약점이 존재함을 확인하며, 실제 테스트베드에서 공격 실험 수행
    - DNP3 보안 취약성을 해결하기 위해선 인증 기법을 강화하거나 비정상 행위 탐지/대응 기법이 존재해야 함

참고[3]

제어 시스템 통신 프로토콜 보안 기술

- DNP3/Modbus 프로토콜 보안 취약성 연구 사례
  - DNP3와 Modbus 프로토콜 보안 취약성 연구(이탈리아 IPSC 연구센터)
  - DNP3와 Modbus 주요 문제점 확인
    - DNP3와 Modbus 프로토콜의 명령어 패킷에 대한 integrity 확인 부재
    - Master와 slave 사이의 인증 매커니즘 부재 (어떤 entity도 Master 형태로 command를 전송할 수 있음)
    - Anti-repudiation과 anti-replay 공격에 대한 대응책 부재
  - DNP3와 Modbus 프로토콜 공격 유형
    - Unauthorized command execution: master와 slave사이의 인증 부재때문
    - SCADA-DOS 공격: 공격자는 master로 위장하여 대량의 명령어 전송 가능
    - Man-in-the-Middle attack 공격: 공격자가 네트워크에 접근하여 MITM 공격 가능
    - Replay 공격: 공격자가 capture한 패킷을 사용하여 재생 공격 용이함
  - 본 연구에서는 IDS 기반으로 위 공격 탐지 및 대응함
    - State 기반 IDS 기반으로 비정상 명령어 탐지 및 대응, 비인가 entity 개입 방어

참고[3]

내부망 비인가 명령어 전송 탐지

- Signature 기반 비인가 명령어 탐지
  - Smart Grid 구성 내부망에서의 signature 기반 비인가 명령어 실행 탐지/대응 (국내)
  - 제어 시스템의 proprietary 프로토콜에 대해서도 적용 가능
  - 특정 명령어에 대한 필터링 수준에서의 보안 기능 제공
    - 허용된 명령어를 사용한 공격 행위 탐지/대응 불가
    - Behavior 기반 Anomaly detection 기술 필요

제어 시스템상에서의 암호 구현 기술

- 제어 시스템 엔터티간 기밀성/무결성/인증 제공 기술
  - 경량 암호 구현 기술 (국가보안기술연구소, 부산대)
  - 경량 암호 S/W 구현 기술
    - 제어 시스템 프로토콜상에서 기밀성/무결성/인증에 사용될 가용성을 고려한 경량 구현 연구
    - Target platform: MSP 430, Atmega, ARM9, Cortex M3
    - 연구 결과 사례(25MHz, MSP430) : SHA-1(1ms), SH-256(1.9ms), AES 128(100us), LEA 64(64us)
  - 경량 암호 H/W 구현 기술
    - 타원곡선 암호 칩(Binary field B233, B283, Prime field P224, P256, NIST curve)
    - RSA 암호 칩
    - AES, LEA 암호 칩
    - 디바이스용 공개키 인증서 기반 디바이스 인증, 키 분배 등 가능
    - 연구 결과 사례(33MHz 동작시): ECC B233(~4msec)

제어 시스템상에서의 안전한 암호 구현 기술

- 부채널 공격(Passive EM 공격) resistant 암호 구현 기술
  - Passive EM 공격을 통한 제어 시스템내 암호 키 유출(부산대)

2 Near field Probe (LANGER EMV-Technik사)

4 USRP (Universal S/W Radio Peripheral)

Signal Analysis GNU Companion

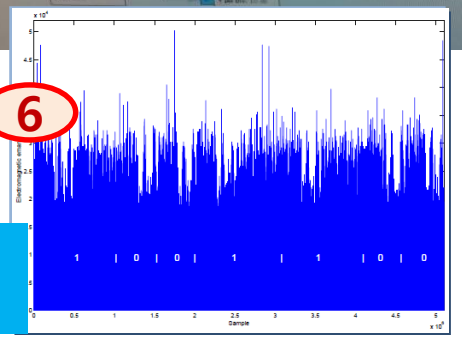
5

1 Smart Meter

3 Radio Receiver

Require: EC point $P = (x, y)$, integer k, $0 < k < k = (k_{l-1}, k_{l-2}, \cdots, k_0)_2$, $k_{l-1} = 1$ and M
Ensure: $Q = (x', y') = [k]P$

```
1: Q ← P
2: for i from l − 2 downto 0 do
3:     Q1 ← 2Q
4:     Q2 ← Q1 + P
5:     if k_i = 1 then
6:         Q ← Q2
7:     else
8:         Q ← Q1
9:     end if
10: end for
```



6

ECC Scalar Multiplication Algorithm

ECC Scalar Multiplication Waveform → Private Key

순 서

IV. 맺음말

Summary

- 산업 제어 시스템에 높은 보안성을 제공하기 위해선 다음 사항을 고려해야 함
  - CIA에서 가용성의 비중이 큼
  - 산업 제어 시스템의 구성 요소(프로토콜, OS, 응용 소프트웨어, 웹 서비스 등)에 많은 보안 취약점 존재
  - Proprietary 프로토콜을 많이 사용하므로 기존 보안 솔루션(IDS, Firewall 등)의 완성도는 떨어짐

- 산업 제어 보안 기술 연구
  - 산업 제어 프로토콜 보안성 강화
  - 제어 시스템 망에 대한 IDS, IPS 연구
  - 디바이스 인증/인가 연구
  - 경량 암호 기술 연구
  - 다양한 통신 방식, OS, 동작 특성, 구성 요소에 대한 공격 방식 및 대응 기술 연구

Thank you !
Q&A

howonkim@pusan.ac.kr

참고 자료

[1] Andrew Wright, Cyber Security for the Power Grid: Cyber Security Issues & Securing Control Systems, ACM CCS, Nov. 2009

[2] Joseph Weiss, Protecting Industrial Control System, 2010

[3] 장문수 외 5명, DNP3 제어 시스템 프로토콜 취약점 실험, 보안공학연구논문지, 2010년2월