Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.4, Aug. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.4.745

PLC 로그의 사고조사 활용 가능성에 관한 연구

장 엽,[1†] 김 태 연,[2] 김 우 년[3‡]
[1,2,3]ETRI 부설연구소(선임연구원, 연구원, 실장)

A Study on the Possibility for Incident Investigation Using PLC Logs

Yeop Chang,[1†] Taeyeon Kim,[2] Woo-Nyon Kim[3‡]
[1,2,3]The Affiliated Institute of ETRI(Senior Researcher, Researcher, Manager)

요 약

산업제어시스템이란 전력, 수처리, 교통과 같은 주요기반시설이나, 자동화 공장, 화학 플랜트와 같이 산업분야의 프로세스를 안전하고 효율적으로 모니터링 및 제어하는 시스템을 말한다. 이러한 산업제어시스템을 대상으로 하는 사이버 공격이 성공한다면 큰 인명 피해, 경제적 피해를 유발할 수 있어, 국가단위 해커 집단들의 주요 공격 대상이 될 가능성이 높다. Stuxnet, Industroyer, TRITON과 같은 사이버 공격은 이러한 우려가 실제 현실로 드러난 사례이며, 사이버 공격으로 실제 물리적 피해를 발생시키기 위해 대상 제어시스템에 대한 깊은 지식을 기반으로 개발된 것으로 확인되었다. 따라서 산업제어시스템의 사고조사를 위해서는 사고분석가 역시 제어시스템 운영 프로세스에 대한 지식을 보유하고 제어시스템에 특화된 사고조사 기술을 확보해야 한다. 이를 위해 사이버와 물리적 경계에 위치한 임베디드 제어기기와 같이 사이버 공격의 대상이 될 수 있지만, IT분야에서 사용되지 않아 즉시 활용할 기술이 없는 장치들을 대상으로 하는 사고조사 기술 개발이 필요하다. 이러한 연구 개발의 첫 단계로써 대표적인 임베디드 제어기기인 PLC(Programmable Logic Controller) 4종을 대상으로 PLC의 로깅 기능 및 본 논문에서 제안한 공격 시나리오에서 사고조사에 활용 가능한 로그 생성 여부를 분석한 결과를 제시한다.

ABSTRACT

An ICS(industrial control system) is a complex system that safely and efficiently monitors and controls industrial processes such as electric power, water treatment, transportation, automation plants and chemical plants. Because successful cyber attacks targeting ICS can lead to casualties or serious economic losses, it becomes a prime target of hacker groups sponsored by national state. Cyber campaigns such as Stuxnet, Industroyer and TRITON are real examples of successful ICS attacks, and were developed based on the deep knowledge of the target ICS. Therefore, for incident investigation of ICSs, inspectors also need knowledge of control processes and accident investigation techniques specialized for ICSs. Because there is no applicable technology, it is especially necessary to develop techniques and tools for embedded controllers located at cyber and physical boundaries. As the first step in this research, we reviewed logging capability of 4 PLC(Programmable Logic Controller)s widely used in an ICS area, and checked whether selected PLCs generate logs that can be used for digital investigation in the proposed cyber attack scenario.

Keywords: ICS Security, PLC, ICS Forensic

Received(06. 10. 2020), Modified(07. 21. 2020), Accepted(07. 21. 2020)

† 주저자, ranivris@nsr.re.kr
‡ 교신저자,wnkim@nsr.re.kr(Corresponding author)

I. 서 론

산업제어시스템(ICS: Industrial Control System)은 전력, 교통, 철도, 수처리 시설과 같은 기반시설이나 공장과 같은 생산 공정에 설치되어 물리적 장치들을 안전하고 효율적으로 모니터링 및 제어하는 시스템을 말한다. 현대인의 편리한 삶의 기반에는 산업제어시스템이 있음은 자명하다. 한동안 산업제어시스템은 폐쇄망으로 운영되어 왔으며, 내부기기 간에도 제조사가 독자적으로 개발한 필드버스 프로토콜이 사용되어 사이버 위협으로부터 안전한 것으로 생각되었다. 그러나 유지보수성과 효율성을 위하여 이더넷 통신, 무선기술과 같은 IT 기술들이 산업제어시스템 내 적용됨에 따라, 제어시스템의 접근성과 연결성이 증가하였고, 사이버 보안 위협 역시 따라 늘어나게 되었다.

만약 산업제어시스템에 사이버 공격이 발생한다면 경제적인 손실과 생활의 불편, 혹은 큰 인명 피해가 발생할 수 있다. Stuxnet[1], Industroyer[2], TRITON[3]과 같은 사이버 공격은 제어시스템을 공격하여 물리적 피해를 일으킨 대표적인 사례이며, 산업제어시스템 특성상 공개되지 않은 크고 작은 사이버 사고 사례는 더욱 많을 것으로 생각된다. 산업제어시스템을 대상으로 하는 사이버 공격들의 일반적인 특징은 다음과 같다.

첫째, 사이버 공격 수행을 위해서 국가 단위 규모의 지원이 있다는 점이다. 성공적인 사이버 공격을 위해서는 대상 시스템과 유사한 환경을 구축하고 개발된 공격을 실증해야 한다. 이는 많은 인력과 비용이 필요하므로 개인이 수행하기 어렵다. 둘째, 물리적 피해를 일으키기 위해 PLC(Programmable Logic Controller), IED(Intelligent Electronic Device), RTU(Remote Terminal Unit)와 같은 산업현장에서 사용하는 임베디드 제어기기까지 공격의 대상으로 삼고 있다는 것이다. 셋째, 피해 시설의 운영자나 보안 분석가가 공격자들의 공격 방식, 최종 목적을 확인하는데 장시간이 소요되었다는 점이다. 많은 시간이 소요된 이유는 '보안 전문가의 제어시스템 지식 부족', '제조사들의 협조 미진', '제어S/W, 제어기기의 사고조사에 활용할 수 있는 도구 부재' 등이 원인이라 할 수 있다.

산업제어시스템을 대상으로 하는 사이버 공격은 앞으로도 꾸준히 증가할 것으로 예상한다. 따라서 제어시스템 특화 사이버 공격을 탐지하고 차단하기 위한 보안 기술을 개발하고 적용해야 하며, 그럼에도 불구하고 사이버 사고가 발생한 경우 유사한 사고가 재발하지 않도록 보안대책을 마련하기 위해 철저한 사고조사가 필요하다. 그러나 현재 산업제어시스템 사고조사에서 활용가능한 기술이 부족한 실정이다. 이에 우리는 산업제어시스템 사고조사 기술개발의 첫 걸음으로써 국내 점유율이 높은 산업용 임베디드 제어기기인 PLC 4종을 대상으로 PLC가 생성하는 로그들이 사고조사에 활용 가능한지 분석하였다. PLC가 제공하는 로그 관련 기능들이 사이버 보안 관점에서 적절하게 구현되었는지, 실제 공격 사례에 기반한 다양한 공격 시나리오에서 유의미한 로그를 생성하는지 실험하였다. 실험 결과 우리는 PLC가 생성하는 로그들이 일부 부족한 면이 있지만, 사고조사에서 활용 가능함을 확인하였다.

본 논문의 분석 결과는 향후 제어시스템 내 제어기기를 대상으로 하는 사이버 공격의 사고조사 시 활용 가능할 것으로 보이며, 제어기기를 개발하는 제조사들 또한 부족한 보안 기능을 인지하고 강화하는 데 도움이 될 수 있을 것이다.

II. 관련연구

산업제어시스템에 사이버 사고가 지속해서 발생하고 있으나 현장에서 활용 가능한 사고조사 기술이 부족하여 산업제어시스템 특화 사고조사 기술의 필요성이 증가하고 있다. Awad[4]는 현존하는 사고조사 기술 수준을 분석하고, 제어시스템에 활용 가능 여부를 검토하였다. 제어시스템을 제어센터(Control Center), 제어 네트워크(Control Network), 제어기기(Field Device)로 구분하고, 이 중 제어 센터를 대상으로 하는 사고조사 기술은 기존의 IT 대상 사고조사 기술로 일부 활용이 가능하나 제어 네트워크와 제어기기를 대상으로 하는 사고조사 기술은 아직 부족한 상황인 것으로 판단하였다.

산업제어시스템에 특화하여 진행된 사고조사 연구들은 주로 비공개인 제어시스템 프로토콜을 분석에 초점을 맞추었고, 사고조사를 위해 기기 혹은 트래픽으로부터 정보를 획득하는 연구를 진행하였다. 예를 들어 Senthivel[5]은 RA(Rockwell Automation)의 소형 PLC인 MicroLogix1400이 사용하는 제어 프로토콜인 PCCC(Programmable Controller Communication Commands)의 구조, 동작 방식을 분석하여, 네트워크 트래픽으로부터 PLC의 구성설

정이나 제어로직을 추출할 수 있는 도구인 Cutter를 개발하였다. Denton[6]은 GE의 구형 PLC 모델인 Fanuc 90-30을 대상으로, 해당 PLC가 사용하는 비공개 제어프로토콜인 SRTP(Service Request Transport Protocol)를 분석하여 PLC로부터 정보를 읽을 수 있는 사고조사 도구를 개발하였다. 이 도구를 활용하면 사고분석가는 동작 중인 PLC로부터 실시간으로 로그 정보(Fault Table)나 제어로직 변수(Tag) 값을 읽어와 사고조사에 활용할 수 있으며, 네트워크 트래픽 분석을 통해 기기와 소프트웨어 간 발생한 통신 오류 또한 식별할 수 있다.

현재까지 진행된 연구들을 분석한 결과, 산업제어시스템 사고조사 기술은 네트워크 트래픽에 기반하여 제어기기 및 제어시스템에서 일어난 행위를 분석하거나, 비공개 프로토콜을 분석하여 제어기기들로부터 정보를 획득하는 방법에 초점이 맞추어져 있었다. 이러한 연구들은 제어기기로부터 획득할 수 있는 정보(제어로직, Tag 값, 로그 등)의 내용에 대해서 심도 있는 연구를 수행하지는 않았다. 우리는 제어기기가 생성하는 로그 자체에 초점을 맞춰, 로그의 내용, 로그관리 기능, 그리고 본 논문에서 제안한 공격 시나리오에서 제어기기가 로그를 생성하는지 분석하였다.

III. 분석 대상 소개

3.1 산업제어시스템(ICS)

제어시스템은 효율적, 안정적으로 대상 프로세스를 제어하기 위해서 센서, 액추에이터, 제어기기, 제어 애플리케이션 등의 다양한 구성요소들이 유기적으로 구성되어 있다. Fig. 1.은 제어시스템의 구성요소 간의 관계를 개략적으로 표현하고 있다. EWS (Engineering WorkStation), HMI(Human Machine Interface) 이외에도 제어시스템 동작 이력을 기록하는 Historian 등 다양한 제어시스템 애플리케이션들이 유기적으로 동작하고 있다. 임베디드 제어기기로는 DCS(Distributed Control System) controller, PLC, RTU, IED 등의 기기들이 목적에 따라 다양한 산업제어시스템에서 활용되고 있다. 각 구성요소에 대한 개략적인 설명은 다음과 같다.

- 임베디드 제어기기: 센서로부터 신호를 받아, 현재 상태에 기반하여 액추에이터들을 구동하는 장치로 DCS, PLC, IED, RTU 등이 존재
- EWS: 임베디드 제어기기의 하드웨어, 네트워크 설정 및 제어로직을 작성하는 등 제어기기를 관리하는 애플리케이션이 설치된 장비
- HMI: 대상 프로세스를 운전원이 식별할 수 있도록 화면에 출력하는 기능을 가진 애플리케이션
- 센서: 실제 물리적 현상을 측정하여 디지털 혹은 아날로그 신호로 변경하는 장치
- 액추에이터: 시스템을 움직이거나 제어하는데 사용되는 기계 장치

3.2 PLC

산업제어시스템 현장에서 널리 사용되는 임베디드 제어기기인 PLC는 현장에서 제어를 담당하고 있는 산업용 컴퓨터로 환경적 요인에 강인하게 설계되며

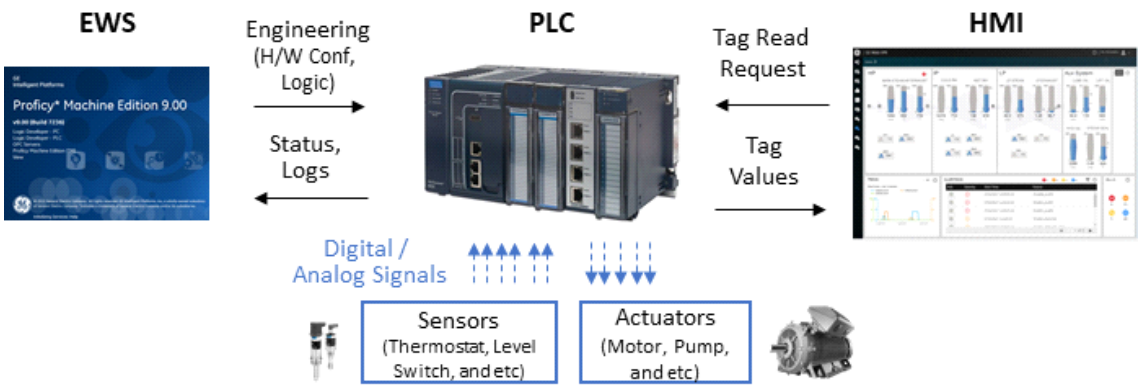

Fig. 1. Overview of ICS Components

실시간성과 가용성을 특징으로 한다. PLC는 범용성이 높아 다양한 곳에서 활용되며, 타 제어기기 대비 환경 구축이 쉬워 공격자들로부터 공격 우선순위가 높다. 따라서 우리는 PLC를 대상으로 사고조사에 활용 가능한 기술 연구를 먼저 진행하고자 한다.

PLC는 다양한 산업현장에서 사용될 수 있으므로, 현장의 요구에 유연하게 대응할 수 있도록 모듈 형태로 구성하게 된다. PLC 모듈 전체를 관리하는 CPU 모듈, 센서나 액추에이터와 신호를 주고 받는 디지털/아날로그 입출력 모듈, 필드버스 통신 혹은 실시간 통신을 지원하기 위한 통신 모듈, 초정밀 제어를 수행하기 위한 모션 제어 모듈 등 다양한 모듈들이 존재한다. 로그 생성 등 PLC 관리와 관련된 기능 대부분은 CPU 모듈에서 제공하므로 우리는 CPU 모듈이 생성하는 로그를 중심으로 분석을 수행하였다.

국내 산업시설 점유율을 고려, 사고조사 관점에서 제어기기 로그 분석을 위해 Siemens, RA, Emerson[1], LS ELECTRIC[2] 4개 회사의 현재 판매 중인 4종 모델(S7-1500, ControlLogix, RX3i, XGT)을 선정하였다. 각 PLC의 세부모델과 PLC의 설정 및 기능 확인 등에 사용된 엔지니어링 S/W(TIA-Portal, Studio 5000, PME(Proficy Machine Edition), XG5000)의 버전은 다음과 같다.

Table 1. Description of Analysis Target (PLCs and Engineering S/Ws)

Vendor	PLC (Model, Firmware)	Engineering S/W(Version)
Siemens	S7-1500 (1516F-3PN/DP, v1.8.1)	TIA-Portal (v13 Sp1 Up9)
RA	ControLogix (1756-L71/B, v21.11)	Studio 5000 Logix Designer (v21.11)
Emerson	RX3i (IC695CPE305, v8.75)	Proficy Machine Edition (v9.0)
LS ELECTRIC	XGT (XGR-CPUH/T, v.2.74)	XG5000 (v4.29)

1) GE의 자동화사업분야는 2019년 Emerson에 인수합병

2) LS 산전에서 LS ELECTRIC으로 2020년 사명 개정

IV. PLC 로그관리 기능 및 보안 수준 검토

이번 장에서는 4종의 PLC가 생성하는 로그관리 기능과 특징에 대해서 살펴보도록 한다. PLC가 생성하는 로그는 일반적으로 PLC 관리 소프트웨어인 엔지니어링 S/W를 이용하여 조회할 수 있다. 제조사 별로 '진단 이벤트', '시스템 이력', 'fault table'과 같이 다른 용어를 사용하고 있지만, 본 논문에서는 기기의 특정 기능을 언급하지 않는 한 'PLC 로그' 혹은 '로그'라는 용어를 사용한다. 또한, 국내외 제어시스템 보안요구사항에 기반하여 PLC들의 로그관리 기능 구현의 보안수준을 검토한다.

4.1 PLC 로깅 기능 분석

S7-1500. Siemens S7-1500이 생성하는 로그는 전용 엔지니어링 S/W인 TIA-Portal에서 '진단 버퍼(Diagnostics buffer) 조회' 기능을 이용하여 Fig. 2.와 같이 로그를 조회할 수 있다. 개별 로그 항목을 선택하면 하단 부에 상세 내용(Details on event)을 통해 구체적인 이벤트 내용을 추가로 확인할 수 있다. S7-1500의 로그는 TIA-Portal에서 조회만 가능하며 수정하거나 초기화할 수 없고, 물리적인 공장 초기화 방식을 통해서만 로그의 초기화가 가능하다. S7-1500은 제조사 매뉴얼에 '옳지 않은 비밀번호 사용 시도', '조작된 펌웨어 업데이트 시도', '보안 수준 변경' 등 보안업무에 활용 가능한 로그들을 별도로 명시하고 있어, 타 제조사 대비 보안에 많은 관심을 기울이고 있음을 알 수 있다.

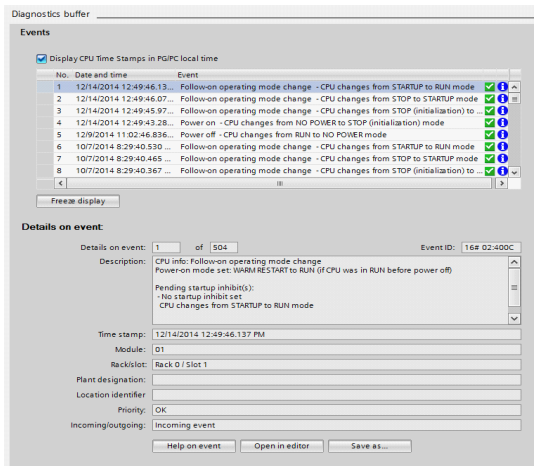

Fig. 2. Diagnostics Buffer of S7-1500

ControlLogix. RA의 ControlLogix는 다른 PLC들과 달리 로그를 Studio 5000에서 조회를 할 수 없으며, CPU 모듈에 삽입된 SD카드를 탈착하여 안에 저장된 로그 파일을 확인해야 하는 특징을 가지고 있다. 이는 공격자가 로그를 위변조하기 어렵지만, 로그 분석을 위해 자동화된 수집환경을 구축하기 어려운 단점을 가지고 있다. 또한, 로그 생성 및 기록을 자동으로 제공하는 다른 PLC들과 달리 제어 로직 상에서 '자동 로그 저장 기능(AutoWriteSet)'을 활성화하거나, '수동 로그 저장 명령(WriteLog)'을 실행해야만 SD카드에 로그를 기록한다. 따라서 기능을 활성화하지 않았을 때 사고가 발생한다면 사고 관련 로그 획득 및 분석이 어려울 수 있다.

ControlLogix는 로그 파일을 1MB 단위로 SD 카드에 저장하게 되며, 최대 1000개까지 저장할 수 있다. 로그 파일은 Fig. 3.과 같이 탭으로 구분된 텍스트 형태를 보인다. 다른 PLC들과 달리 로그에서 사용자 정보를 확인할 수 있으며, 시간 정보는 초 단위까지만 기록하고 있다.

```
remark  "TSV-Controller-Log"
remark  "Date = Jan-01-1998 06:45:28"
remark  "Controller = 1756-L71/B"
remark  "Serial-Number = 16#00D6_4A53"
remark  "Revision = 21.11"
"2.0"

Record Number   Time    Entry Description   User Name
Workstation Name    Factory Talk Login ID   Extended Information
Change Detection Audit Value

 1  Jan-01-1998 00:00:57    Project download    AB-PC\02AB
AB-PC   AB-PC\02AB  Project AB_PLC
16#050A_12CD_D863_73A1

 2  Jan-01-1998 00:01:12    Remote mode change  AB-PC\02AB
AB-PC   AB-PC\02AB  Old mode Remote Program, New mode Remote Run
16#050A_12CD_D863_7465

 3  Jan-01-1998 06:22:45    Keyswitch mode change   Local   None
None    Old mode Run, New mode Program
16#050A_12CD_D863_7BBD
```

Fig. 3. Log file contents in a SD card (RA ControlLogix, Re-formmated)

RX3i. Emerson의 RX3i 로그는 PME를 이용해서 조회할 수 있다. RX3i는 'Fault Table'과 'I/O Table' 두 종류로 로그를 구분하여 관리한다. 시스템 운영과 관련된 정보는 Fig. 4.와 같이 Fault Table에 저장되며, 이 로그 테이블에서 일부 보안과 관련된 로그를 확인할 수 있다. 각각의 로그는 최대 64개까지 저장되며, PLC에 접속 권한이 있다면 로그 테이블을 초기화할 수 있다. 독특한 점이 로그의 수량이 64개가 초과할 경우, 오래된 로그인 1~32번째 로그는 그대로 유지되고 33~64번째

0.2	Password access failed	2020-02-17 19:38:43
0.4	Extra option module	2020-02-17 19:30:42
0.4	Extra option module	2020-02-17 19:30:31
0.2	Memory access rejected due to Access Control List violation	2020-02-17 19:29:30

Fig. 4. Fault Table of RX3i (Partial)

영역에만 순환 저장되는 특징을 갖고 있다. RX3i의 PLC 로그는 재부팅될 때 모든 로그가 사라지기 때문에 사고조사 시에 현장에서 전원이 인가된 채로 즉시 로그를 수집해야 한다.

XGT. XG5000은 PLC 로그 정보를 Fig. 5.의 대화창과 같이 '에러 이력', '모드 전환 이력', '시스템 이력', '전원 차단 이력'으로 구분하여 제공하고 있다. 항목별로 최근에 발생한 100개씩의 로그를 기본적으로 제공하고 있으며, 더 오래된 이력을 보고 싶으면 '전체 읽기' 혹은 '파일 저장'을 통해 PLC에 저장된 모든 이력을 읽어올 수 있다. PLC 로그는 유형별로 최대 1024개(모드 전환 이력, 전원 차단 이력), 2048개(에러 이력, 시스템 이력)까지 저장된다. XGT에 접근할 수 있는 권한이 있는 사용자라면 '지우기'를 선택해 특정 유형의 로그 혹은 로그 전체를 삭제할 수 있다.

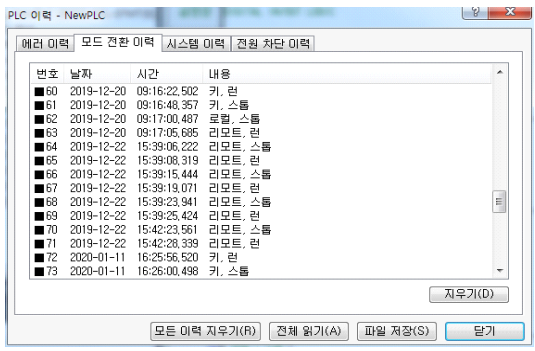

Fig. 5. PLC History of XGT (Mode Change)

4.2 PLC 로그관리 기능의 보안 수준 검토

앞서 살펴본 PLC들의 로그관리 기능의 보안 수준을 검토하기 위해 우리는 미국의 제어시스템 보안 가이드라인 문서인 NIST-SP 800-82[7]와 국내 제어시스템 보안 요구사항 표준 문서인 "산업제어시스템 보안 요구사항 - Part 3: 제어계층[8]"에서 명시된 보안 요구사항을 활용하였다. 감사 로그와 관련

된 보안 요구사항에서 관리적 요구사항을 제외한 기술적인 요구사항 6종류(로그 조회, 로그 삭제 방지, 로그 정보, 로그 저장 용량, 로그 저장 실패 대응, 원격소 로그 저장)를 도출하였다. 기기별로 로그 관리기능이 보안 요구사항을 만족하는지 검토한 결과는 Table 2.와 같으며 각각의 보안 요구사항에 대한 설명 및 검토 기준은 다음과 같다.

1. Log View. PLC가 생성한 로그를 관리자가 조회할 수 있는지 확인한다. 또한, 네트워크를 통한 로그 조회 시 최소한의 권한을 요구하는지 확인한다.

2. Log Delete. PLC가 생성한 로그를 관리자 권한이 없는 사용자가 삭제할 수 있는지 확인한다. 또한, 관리자 여부와 관계없이 원격 삭제를 항상 제한한다면 보안 수준이 높은 것으로 판단한다.

3. Log Content. 각 이벤트 로그가 언제 발생했는지, 어느 PLC 모듈에서 발생했는지, 어떠한 형태의 보안 이벤트인지, 어느 시점에서 오류가 발생했

Table 2. Security Analysis Result of PLC Log Management Function (O: Good, △: Partial, X: Bad)

PLC	Security Requirement	Result	The Basis for the Analysis Result
S7 -1500	1. View	O	Logs can be viewed from the engineering S/W.
	2. Delete	O	Logs cannot be deleted from the engineering S/W.
	3. Content	△	Each log entry provides detail information except user information.
	4. Capacity	O	S7-1500 can store up to 3200 logs.
	5. Fail. Resp.	△	When the capacity is exceeded, old logs are overwritten without notice.
	6. Remote	O	S7-1500 provides remote log storage. Configuration is done within the control logic.
ControlLogix	1. View	△	An incident inspector must remove a SD card from PLC to view logs.
	2. Delete	O	Logs cannot be deleted from the engineering S/W.
	3. Content	△	Each log entry shows the type and time of the event that occurred by whom.
	4. Capacity	O	ControlLogix can store up to 1GB of logs.
	5. Fail. Resp.	X	When the capacity is exceeded, logs are no longer stored.
	6. Remote	X	ControlLogix does not provide remote log storage.
RX3i	1. View	O	Logs can be viewed from the engineering S/W.
	2. Delete	X	Anyone connected to the PLC can delete the log. Also, all logs disapper after re-boot.
	3. Content	△	Each log entry shows the type and time of the event that occurred.
	4. Capacity	X	The RX3i's two log tables have only 64 log entries.
	5. Fail. Resp.	O	When old logs are overwritten, a log indicating that capacity has been exceeded is generated.
	6. Remote	X	RX3i does not provide remote log storage.
XGT	1. View	O	Logs can be viewed from the engineering S/W.
	2. Delete	X	Anyone connected to the PLC can delete the log.
	3. Content	△	Each log entry shows the type and time of the event that occurred.
	4. Capacity	O	XGT can store up to 1000~2000 logs per log category.
	5. Fail. Resp.	△	When the capacity is exceeded, old logs are overwritten without notice.
	6. Remote	X	XGT does not provide remote log storage.

는지, 관련된 사용자는 누구인지 등 사고조사를 위해 필요한 정보를 모두 획득할 수 있는지 확인한다.

4. Log Capacity. 제어기기가 얼마나 많은 제어기기 로그를 저장할 수 있는지 확인한다. 로그 저장 용량에 대해서는 명시적인 평가 기준이 없어 임의로 검토 기준(1,000개)을 선정하였다.

5. Failure Response. 로그 저장 용량보다 더 많은 로그가 발생할 때 오래된 로그부터 덮어 쓰여야 하며 관리자에게 알람이 발생해야 한다. 그리고 로그 저장에 실패한 때에도 관리자에게 알림이 가능해야 한다.

6. Remote Storage. Syslog 등의 기능을 활용해 외부에 로그를 저장할 수 있는지 확인한다.

6가지 보안 요구사항에 대해 PLC들의 보안수준을 검토한 결과 Siemens의 S7-1500이 다른 PLC 대비 전체적으로 보안을 고려한 로그관리 기능을 제공하는 것으로 판단되었다. 그리고 계정관리 기능이 없는 타 PLC와 달리 ControlLogix는 RA가 제공하는 제어시스템 운영환경(FactoryTalk Platform)의 계정 관리기능에 기반해, 로그 세부내역에 사용자, 장비 정보, FactoryTalk ID 등의 정보를 기록한다. 이는 사고조사에 매우 유의미한 정보가 될 수 있다. RX3i와 XGT의 경우 원격에서 PLC에 접속할 수 있다면 로그 초기화가 가능하여 공격자가 로그를 삭제할 가능성이 있으므로 사고조사에 로그를 활용하기 위해서는 로그 삭제 명령을 네트워크 수준에서 차단하는 등의 노력이 필요하다.

V. PLC 공격 시나리오

실제 제어시스템 사고 사례와 공격 연구 사례들에 기반해 PLC 공격 시나리오를 도출하였다. 우리는 제어기기가 지닌 사이버 보안 취약점을 이용하여 버퍼 오버플로우와 같이 공격자가 원하는 코드를 PLC에서 실행시킬 수 있는 공격은 제외하였다. PLC가 제공하는 기능들에 초점을 맞춰 공격 시나리오를 제시하고 실험을 수행한 이유는 다음과 같다.

- 첫째, 공격자들은 제어시스템의 오동작으로 인한 물리적 피해를 발생시키고자 한다. 이를 위해서는 PLC가 공격자의 의도대로 현장장치들의 제어를 수행해야 한다. 따라서 PLC가 지닌 고유의 기능들을 활용하여 대상 시스템에 대한 정보를 획득하고, 공격을 수행하기를 선호할 것이다.
- 둘째, 제조사들은 시스템 레벨의 로그를 획득하는 방법을 제공하고 있지 않다. 일차적인 사고조사는 PLC의 애플리케이션 수준에서 제공하는 로그에서 진행될 수밖에 없다.
- 셋째, 현재 CVE DB[9]나 ICS-CERT[10]에 많은 제어시스템 취약점이 등록되어 있지만, 대부분의 취약점이 HMI나 통신 라이브러리와 같은 소프트웨어 쪽에 치중되어 있다. PLC를 대상으로 하는 일부 취약점이 존재하지만 PLC별로 유사한 취약점들을 개발하고 로그 생성 여부를 확인하는 것은 많은 노력과 시간이 필요하다.

따라서 공격 시나리오는 공격자가 엔지니어링 S/W 혹은 HMI가 설치된 시스템의 권한을 획득하거나, 혹은 악성코드가 정상 S/W인 것처럼 동작하여 네트워크를 통해 PLC에 대한 제어를 시도하는 것으로 제한한다. 각 공격 시나리오에서 사용되는 PLC의 주요 기능에 대한 설명은 다음과 같다.

1. Login. 이더넷 또는 USB나 제조사 전용 시리얼 인터페이스를 통해 PLC에 접속하여 세션을 맺는 것을 말한다. 보안을 고려하지 않고 개발되었던 이전 세대 PLC들은 접속만 하면 관리자 권한을 획득하도록 구현되어 있었으나, 최근의 PLC는 패스워드 설정이 가능하도록 구현되어 있다. 아직 다수의 PLC가 엔지니어링 세션을 위한 계정 관리를 수행하고 있지는 않으나 태그 값 변경, 제어로직 변경, 펌웨어 업데이트 등의 작업을 수행할 때 권한 수준을 확인하기 위해 비밀번호를 설정하는 기능을 제공하는 PLC가 늘고 있다.

2. Tag Write. 태그(Tag)란 PLC에서 사용하는 변수를 의미한다. 센서, 액추에이터와 연결하는 신호선에 붙이는 꼬리표에서 유래된 이름으로 제조사에 따라 용어가 다르며, 일반적인 프로그래밍과 동일하게 변수라는 용어를 사용하기도 한다. 태그는 목적 및 쓰임새에 따라 입출력 접점과 1:1로 맵핑되는 I/O 태그, 프로그램 내부에서 사용하는 프로그램 태그, 컨트롤러의 정보를 담고 있는 시스템 태그 등이 존재한다. 제어시스템 운전원들은 제어로직 내 설정

된 특정 태그 값(예: 희망온도)을 변경하는 것으로 PLC 제어를 수행한다.

3. Forcing I/O. Forcing 기능은 강제로 입력 값이나 출력 값을 on/off 시키는 가능으로 제어시스템의 초기 구축 단계에서 장치 정상 동작 시험을 목적으로 사용하거나, 특정 센서가 고장이 났을 때 공정을 계속 가동하기 위해 임시로 사용할 수 있는 기능이다. 이 기능은 제어로직과 무관하게 기기를 동작시킬 수 있으므로 매우 조심히 사용해야 함을 모든 제조사가 경고하고 있다.

4. Operation Mode Change. 운전모드 변경은 PLC의 운영에 특화된 기능으로 제조사마다 다양한 운전모드를 제공한다. 대부분의 PLC는 딥(DIP) 스위치 혹은 키(Key) 스위치 형태로 운전모드를 변경할 수 있는 기능을 제공하고 있으며, Run/Stop 모드 2종류 혹은 Run/Remote/Stop 3종류 모드를 제공하고 있다. 제조사마다 운전모드에서 가능한 작업이 조금씩 다를 수 있으나, 일반적으로 제어로직이나 하드웨어 설정 변경은 Remote-Stop 상태에서, 펌웨어 업데이트는 Stop 상태에서만 가능하다.

5. Control Logic. 제어로직은 제어기기가 어떻게 동작할지를 명세한 프로그램이다. 즉 제어로직을 분석하면 대상 제어시스템이 어떻게 구성되어 있는지, 어떻게 동작하는지를 확인할 수 있다. 엔지니어링 S/W들은 IEC61131-3[11]에서 정의한 PLC 프로그래밍 표준인 래더, 펑션블록 다이어그램, Structured text(ST) 형태를 제공한다. 공격자는 제어로직 변조를 통해 제어시스템에 물리적 피해를 야기할 수 있다.

6. Hardware Configuration. PLC는 다양한 모듈들로 구성이 될 수 있으므로, 어떠한 모듈들이 장착되었는지 PLC CPU 모듈에 하드웨어 구성 설정이 되어 있어야 한다. 만약 하드웨어 구성이 실제와 일치하지 경우 PLC CPU 모듈이 폴트 상태에 빠져 DoS 상태가 될 수도 있으며, 통신 설정이 맞지 않으면 네트워크가 끊어질 수도 있다.

PLC의 주요 기능들을 활용하여 제어시스템을 공격하는 공격 5종, 펌웨어 위변조 공격 1종, 공격 흔적을 숨기기 위한 로그 초기화 공격 1종을 추가하여 Table 3.과 같이 7종류의 공격 시나리오를 제안하였다. PLC의 제어로직을 변조한 Stuxnet[1] 같은 실제 공격 사례나 PLC Worm[12]과 같이 제어기기를 대상으로 하는 공격 기법 연구 사례들은 모두 Table 3.에서 제안한 공격 시나리오들을 하나 이상 포함하고 있으므로, PLC가 제안한 시나리오에서 유의미한 로그를 생성한다면 사고조사에 활용할 수 있을 것이다.

Table 3. Attack Scenarios for PLC

ID	Attack Scenario	Description
1	Login Trial	In order to acquire information and perform an attack, an attacker will first attempt to connect to a target PLC. He/She may perform brute force attacks.
2	Tag Write	An attacker who successfully infiltrate into the PLC can change operation of it by changing the PLC tag value such as setpoint
3	Forcing I/O	If I / O Force function is used by an attacker, an equipment may malfunction regardless of the control logic.
4	Operation Mode Change	To change the behavior of the PLC, an attacker must change PLC operation mode as engineering-enable state(ex: remote-stop mode)
5	Control Logic/Hardware Configuration Download	By changing control logic or hardware configuration settings, the attack remains permanently on the PLC
6	Firmware Upgrade/Downgrade	Install the old version of the firmware where the vulnerability exists, or the firmware crafted by the attacker on the PLC.
7	Log Clear/Overwrite	The PLC logs may be cleared over the network to hide the traces of the attack.

VI. 생성된 PLC 로그 분석을 통한 사고조사 활용성 검토

5장에서 제시한 공격 시나리오를 PLC에 직접 수행하고, PLC들이 생성한 로그가 사고조사에 활용 가능한지 검토한 결과를 제시한다. 공격 시나리오에서 제안한 행위가 명시적으로 로그로 남는 경우 'O'로, 여러 행위 중 일부만 확인할 수 있거나 혹은 가능성을 유추할 수 있는 경우는 '△'로, 관련 로그가 전혀 생성되지 않는 경우는 'X'로 표시하였다. 예외적으로 공격 시나리오 7은 물리적인 접근 없이 로그 초기화가 가능 여부를 확인하였다. 시나리오별로 로그 생성 확인 실험 결과는 Table 4.와 같다. 안타깝게도 XGT는 제조사 측에서 펌웨어 업데이트 기능을 일반 사용자에게 제공하고 있지 않고, 태그 권한관리 기능을 제공하고 있지 않아 해당 항목에 대한 실험을 수행하지 못하였다. 또한, 변조된 펌웨어 업데이트 등 실제 공격을 수행하기 어려운 항목에 대해서는 제조사 매뉴얼을 참조하였다.

공격 시나리오에 대해 실험을 수행한 결과 RX3i를 제외한 PLC는 운영과 관련된 주요 변경사항(제어로직 변경, 운전모드 변경, 구성설정 변경)을 기록하고 있으나, 접근제어와 관련된 로깅은 다소 부족한 것으로 판단되었다. S7-1500과 RX3i는 잘못된 비밀번호를 이용한 접근 시도 확인이 가능하나, 읽기 권한만 있는 태그에 쓰기 행위 등을 수행할 경우 관련 로그를 발생하는 경우는 오직 RX3i에서만 확인할 수 있었다.

I/O Forcing은 제어로직이나 프로세스 상태와 무관하게 기기가 동작할 수 있어 제조사들이 극도로 조심히 사용해야 함을 당부하고 있음에도 불구하고 ControlLogix에서만 해당 기능이 활성화/비활성화 되었음을 로그로 남기고 있음을 확인하였다. 펌웨어 업데이트 또한 기록해야 하는 중요한 로그가 될 수 있음에도 불구하고, S7-1500과 RX3i는 이를 확인할 수 있는 로그가 남지 않았다. 다만 매뉴얼 상 S7-1500은 인증서 값이 일치하지 않는 조작된 펌웨어일 때 이를 로그로 남기는 것을 명시하였다.

Table 4. PLC Log Analysis Result According to Attack Scenarios (O: Good, △: Partial, X: Bad)

PLC	Attack Scenario ID	Analysis Result	The Basis for the Analysis Result
S7-1500	1	O	Both of 'Login Success' and 'Login Fail' are recorded.
	2	X	S7-1500 provides access control of PLC Tags. Unfortunately, no record of attempts to change tags remains.
	3	X	Forcing activation does not leave any log records.
	4	○	Records of manually changing the operation mode in front of the panel or changing the operation mode in the EWS remain.
	5	△	Before logic download or H/W configuration, the PLC must stop and an inspector can check this record. Notably, PLC keeps a record of changes to security configuration settings.
	6	△	Log records are generated only when the PLC is updated with manipulated firmware.
	7	○	Log records are not initialized until physical access and factory reset.
ControlLogix	1	X	ControlLogix does not provide record about access to the PLC.
	2	X	PLC blocks tag write without a right privilege. But it doesn't record this event.
	3	○	When Forcing I/O activated or deactivated, PLC generates logs.
	4	○	All history about mode-changes physically or softwarely are stored.
	5	○	Whenever control logic or hardware configuration changed, all changes were record.
	6	○	When new firmware installed, a folder is created with the firmware version name in SD card. And new logs are stored in the folder.
	7	○	New logs will not be added when the maximum capacity is reached. However, 1GB is a very large capacity. In order to delete the log, it is necessary to remove the SD card through physical access.

Table 4. Continued

PLC	Attack Scenario ID	Analysis Result	The Basis for the Analysis Result
RX3i	1	△	RX3i records every 'Login fail' trial
	2	○	PLC blocks tag write without a right privilege. And PLC record this privilege violation.
	3	X	Enabling and disabling of I/O Forcing do not generate any logs.
	4	X	Mode change history are not managed.
	5	X	When control logic is downloaded to RX3i, this action does not generate log records.
	6	X	When new firmware installed, all logs are lost.
	7	X	Logs can be cleared by a person with the least privilege, and also 64 log entries are too small.
XGT	1	△	Both of 'Login Success' and 'Login Fail' are not recorded. But connection and disconnection are recorded
	2	N/A	XGT does not provide any access control for tags
	3	X	I/O Forcing histories are not recorded
	4	○	All history about mode-changes physically or softwarely are stored. EWS provides an UI for mode change history only
	5	○	H/W configuration changes and control logic changes are recorded.
	6	N/A	The company does not provide firmware update to normal clients.
	7	X	Old logs are deleted according to the circular queue method. But attackers can clear all or a part of logs.

본 연구에서 제안한 7종의 공격 시나리오에 대해 로그 생성 여부를 검토한 결과, ControlLogix가 사고조사에 활용 가능한 로그를 가장 많은 시나리오에서 생성하는 것으로 판단하였으며 RX3i나 XGT는 생성하는 로그가 다소 부실한 것으로 판단하였다.

VII. 결 론

이 연구에서 우리는 국내외 제어시스템 보안 요구사항에 기반해 국내 도입률이 높은 4종의 PLC의 로그관리 기능의 보안수준을 평가하고, PLC를 대상으로 하는 7종의 공격 시나리오에 대해 PLC가 생성하는 로그들이 사고조사에 활용 가능한지 확인하였다. 제어기기들이 생성하는 로그들은 주로 하드웨어 구성 설정이나 제어 및 통신 과정에서 발생하는 오류에 관한 것들이지만, 일부 로그는 사이버 사고 관점에서도 활용 가능함을 확인하였다. 또한, ControlLogix와 같이 사고조사 시에 로그를 활용하기 위해서는 로그 저장 기능 활성화와 같은 사전작업이 필요함을 식별하였다.

본 연구는 사고조사 관점에서, 사이버 위협에 따라 PLC들이 생성하는 로그들의 활용 가능성을 검토한 연구로 특정 제어기기의 보안 수준이 높고 낮음을 평가하기보다는 제어기기가 생성하는 로그들로부터 정보를 수집하고자 하는 보안 솔루션 개발에 도움을 주기 위해 수행되었다. 제어기기들의 로그 정보를 수집하는 보안 솔루션을 구축한다면, 사고조사 뿐만 아니라 실시간으로 발생하는 제어시스템 내 이상행위를 탐지할 수 있을 것으로 기대된다. 향후 제어기기가 생성하는 로그들을 자동으로 수집할 수 있는 도구를 개발하여 사고조사에 활용할 예정이다.

References

[1] N. Falliere, L.O. Murchu, and E. Chien, "W32.STUXNET dossier v1.4," Whitepaper, Symantec Security Response, Symantec Corp., Feb. 2011.

[2] R. Lee, J. Slowik, B. Miller, A. Cherepanov, and R. Lipovsky,

"Industroyer/crashoverride: Zero things cool about a threat group targeting the power grid," Black Hat USA, 2017.

[3] A.A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The first ICS cyber attack on safety instrument systems," Black Hat USA, 2018.

[4] R.A. Awad, S. Beztchi, J.M. Smith, B. Lyles, and S. Prowell, "Tools, Techniques, and methodologies: A survey of digital forensics for scada systems," Proceedings of the 4th Annual Industrial Control System Security Workshop, pp. 1-8, Dec. 2018.

[5] S. Senthivel, I. Ahmed, and V. Roussev, "SCADA network forensics of the PCCC protocol," Digital Investigation 22 (2017), pp. 57-65, Aug. 2017.

[6] G. Denton, F. Karpisek, F. Breitinger, and I. Baggili, "Leveraging the SRTP protocol for over-the-network memory acquisition of a GE fanuc series 90-30," Digital Investigation 22 (2017), pp. 26-38, Aug. 2017.

[7] K.A. Stouffer, J.A. Falco, and K.A. Scarfone, "Guide to industrial control systems(ICS) security," SP 800-82 rev. 2, NIST, May 2015.

[8] "Security requirements for industrial control System - Part 3: control layer," TTAK.KO-12.0307-part3, Jun. 2012.

[9] https://cve.mitre.org/

[10] https://www.us-cert.gov/ics

[11] K.H. John, and M. Tiegelkamp. "IEC 61131-3: programming industrial automation systems," Springer, 2005.

[12] R. Spenneberg, M. Brüggemann, and H. Schwartke, "PLC-blaster: a worm living solely in the PLC," Black Hat Asia, 2016.

〈저자소개〉

장 엽 (Yeop Chang) 정회원
2005년 2월: 고려대학교 컴퓨터학과 졸업
2007년 2월: 포항공과대학교 컴퓨터공학과 석사
2007년 3월~2010년 2월: LS산전 주임연구원
2010년 3월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 기반시설 보안, ICS 보안, 소프트웨어 공학

김 태 연 (Taeyeon Kim) 정회원
2014년 2월: 아주대학교 정보컴퓨터공학과 졸업
2016년 2월: 한국과학기술원 전산학부 석사
2016년 3월~현재: ETRI 부설연구소 연구원
〈관심분야〉 기반시설 보안, ICS 보안, 빅데이터

김 우 년 (Woo-Nyon Kim) 정회원
1996년 2월: 안동대학교 컴퓨터공학과 졸업
1998년 2월: 경북대학교 컴퓨터과학과 석사
2000년 2월: 경북대학교 컴퓨터과학과 박사수료
2000년 3월~2003년 12월: ㈜니츠 선임연구원
2003년 12월~현재: ETRI 부설연구소 책임연구원
〈관심분야〉 기반시설 보안, ICS/CPS/IIoT 보안, ICS 보안성/안전성 평가