Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1223

안전한 제어시스템 환경을 위한 트래픽 분석망 설계*

이 은 지,[1†] 곽 진[2‡]
[1]아주대학교 컴퓨터공학과 정보보호응용및보증연구실, [2]아주대학교 사이버보안학과

Traffic Analysis Architecture for Secure Industrial Control System*

Eun-Ji Lee,[1†] Jin Kwak[2‡]
[1]ISAA Lab., Department of Computer Engineering, Ajou University,
[2]Department of Cyber Security, Ajou University

요 약

제어시스템은 국가기반시설 및 산업분야 전반에 걸쳐 이용되기 때문에 사이버 공격을 받게 될 경우 공공분야에 직접적인 피해가 발생할 수 있다. 이러한 이유로, 제어시스템에 대한 보안요구사항이 제안되고 있으며 전자제어시스템보안 가이드라인에 따라 외부망과 분리된 환경으로 운용되고 있다. 그럼에도 불구하고 스턱스넷(Stuxnet)과 같이 제어시스템을 겨냥한 악성코드가 지속적으로 발견되고 있으며, 신·변종 악성코드의 등장으로 실시간 탐지의 어려움과 자료유출 등의 보안위협이 지속적으로 발생되고 있다. 본 논문에서는, 안전한 제어시스템 환경 제공을 위한 트래픽 분석망 도입에 대해 제안한다. 이를 위해 제어시스템에서 발생 가능한 보안위협들을 분석하고, 이러한 보안위협에 대응하기 위한 보안기능들에 대하여 도출한다.

ABSTRACT

The Industrial control system is adopted by various industry field and national infrastructure, therefore if it received cyber attack, the serious security problems can be occured in the public sector. For this reason, security requirements of the industrial control system have been proposed, in accordance with the security guidelines of the electronic control system, and it is operated by separate from the external and the internal network. Nevertheless, cyber attack by malware (such as Stuxnet) targeting to control system have been occurred continuously, and also the real-time detection of untrusted traffic is very difficult because there are some difficulty of keeping up with quickly evolving the advent of new-variant malicious codes. In this paper, we propose the traffic analysis architecture for providing secure industrial control system based on the analyzed the security threats, the security requirements, and our proposed architecture.

Keywords: Control system, Malware, Analysis, Security

I. 서 론

제어시스템은 주요 국가기반시설을 운용할 뿐만 아니라 산업분야의 공정 제어, 감시 등에 이용되고 있다. 따라서 제어시스템이 사이버 공격을 받게 될 경우 산업분야 전반에 걸쳐 피해가 발생할 수 있다.

이러한 이유로, 제어시스템은 전자제어시스템 보안 가이드라인에 따라 외부망과 제어망이 분리된 환경으로 운용되고 있다[1]. 또한, 인터넷의 확산과 제어 설비들의 효율적 관리를 위해 제어 설비들의 정보를 외부망과 공유할 필요성이 늘어나면서 외부망과 제어망이 연계된 형태로 운용되고 있다.

이러한 망분리 환경으로부터 제어시스템이 안전할

Received(08. 04. 2016), Modified(09. 30 2016), Accepted(10. 06. 2016)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).
† 주저자, heo160@ajou.ac.kr
‡ 교신저자, security@ajou.ac.kr(Corresponding author)

것이라는 인식에 반해, 스턱스넷(Stuxnet), 가우스(Gauss) 등 제어시스템을 겨냥한 악성코드 공격과 같은 보안위협이 지속적으로 발견되고 있으며[2], 특히 2003년 미국 원자력 발전소의 웜 감염 사고, 2011년 미국 휴스턴 상수도 제어시스템 해킹 등 제어시스템에 대한 사이버 공격이 계속해서 발생하고 있다[3].

이에 따라, 현재 안전한 제어시스템 환경 구축을 위한 솔루션 및 보안기능들이 제시되고 있다. 특히, 제어시스템에 특화된 침입탐지 시스템 기술에 대한 연구가 활발히 진행되는 등 제어시스템을 겨냥한 악성코드 분석의 필요성이 높아지고 있다[2].

따라서, 본 논문에서는 안전한 제어시스템 환경 제공을 위한 트래픽 분석망 모델을 제안한다. 기존 제어시스템 보안요구사항이 있음에도 보안위협이 지속적으로 발견되는 상황에서 트래픽 분석망 도입을 통해 제어시스템에서 발생하는 보안위협에 대한 대응을 목표로 한다.

본 논문의 구성은 다음과 같다. 2장에서는 제어시스템 망분리 아키텍처, 제어시스템을 위한 침입탐지, 보안요구사항을 설명하고. 3장에서는 제어시스템 환경에서 발생하는 보안위협들을 분석한다. 4장에서 트래픽 분석망 모델 제안 및 특징과 보안기능들을 도출하고, 제안하는 시스템 도입 시 만족되는 보안요구사항을 분석하며, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 제어시스템 망분리 아키텍처

미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)에서 제정한 ICS 보안을 위한 가이드 문서에 따르면[4], 제어시스템의 네트워크는 외부와 분리된 형태로 구축함으로써 민감한 정보들의 접근을 최소화 할 수 있다.

이 문서는 민감한 트래픽으로부터 망을 보호하기 위해서는 망간 경계 구간에 대한 보호를 권고하고 있으며, 경계 구간 보호 장비를 통해 악성코드 공격 및 비 악성코드 에러 등으로부터 제어시스템을 보호함으로써 트래픽을 제어한다. 망간 경계 구간 보호 제어는 방화벽, 네트워크 기반 악성코드 분석, 침입탐지 시스템 등을 포함하고 있다.

망 경계에는 중립 구간인 DMZ(Demilitarized Zone) 구간이 존재하며, 이는 보안 정책을 통해 망간 자료 전송 시 외부 위협으로부터 내부망 보호를 목적으로 한다. 이를 위해 망 중계 구간에 방화벽 도입을 권고하고 있으며, 이는 트래픽의 무단 유출을 방지하고, 트래픽 전송 시의 취약점을 식별하는 등의 역할을 한다.

분리된 망간 자료 전송은 단방향 게이트웨이를 통한 자료 전송을 권고한다. 단방향 게이트웨이는 외부망과 내부망 사이 경계에 배치되며, 트래픽을 단방향으로 전송함으로써 원치 않는 곳으로 부터의 트래픽 유입을 차단하여 망을 보호한다.

이때, 내부망에서 유입되는 트래픽에 대한 모니터링 및 로깅, 감사가 이루어질 수 있다. 이는 전송된 트래픽에 대하여 정책 위반 또는 시스템의 동작 방해 여부 등을 감시한다. 모니터링으로 이상행위가 감지되면 시스템을 정밀 분석할 필요가 있다.

아래 Fig. 1.은 망이 분리된 형태의 제어시스템 네트워크 아키텍처를 보여주며[5], Fig. 2.는 보안정책에 의한 트래픽의 흐름도를 나타낸다. 또한 아키텍처 구성에 대한 설명은 다음과 같다.

- Enterprise Zone
  업무망인 Enterprise zone은 외부 네트워크와 연결되어 외부와 통신이 가능한 영역이다.
- Manufacturing Zone
  실제 제어시스템이 구성되는 제어망으로 외부와의 통신이 차단되어 운용되는 영역이다.
- DMZ(Demilitarized Zone)
  업무망과 제어망 사이에 존재하며, 보안 정책, 방화벽 등을 통해 망간 자료 전송 시 발생할 수 있는 외부 위협으로부터 내부망을 보호한다.
- firewall
  방화벽은 망 중계구간에 위치하며 보안 정책을 통해 이상트래픽을 차단하는 등의 망간 전송되는 트래픽을 제어한다.
- IDS(Intrusion Detection System)
  침입탐지 시스템은 망간 전송되는 트래픽 중 이상트래픽을 탐지하여 차단함으로써 제어시스템에 대한 공격을 사전에 방지한다.
- Monitering Zone
  업무망과 제어망 각각에 존재하는 영역으로 Log Collector를 통해 각 망에서 발생한 이벤트들에 대한 로그를 수집하고, SIEM(Security Information & Event Management)으로 보안정보 및 이벤트를 관리함으로써 각 망에서 발

생하는 보안위협을 찾아내기 위한 모니터링 영역이다.

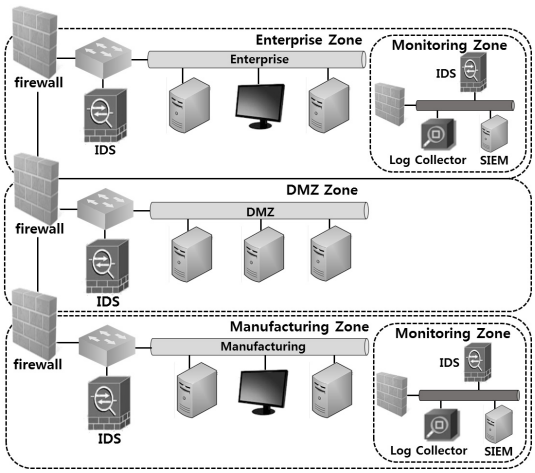

Fig. 1. Networks architecture of controlled system[5]

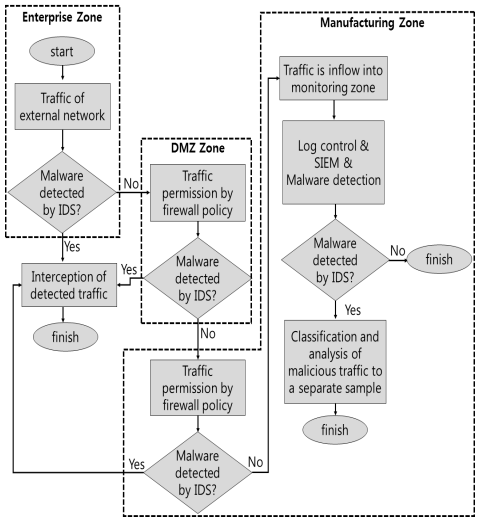

Fig. 2. Traffic flow of Networks architecture of control system[5]

2.2 제어시스템 침입탐지 기술

제어시스템을 겨냥한 악성코드가 지속적으로 등장함에 따라 침입탐지 기술 연구가 활발히 진행되고 있으며, 제어시스템 환경의 특성을 고려한 제어시스템 특화 침입탐지 시스템에 대한 기술 연구는 다음과 같다[2].

2.2.1 네트워크 침입탐지 기술

제어시스템 네트워크는 물리적인 망분리 환경으로 제어망과 외부망이 연계된 형태로 운용되고 있다. 또한, 제어시스템 네트워크 구조는 일반적인 네트워크 구조에 비해 소규모로 구성되어 있으며, 제어 명령에 대한 실시간 응답과, 현장장치의 실시간적인 데이터 전송을 요구한다. 이러한 특성에 따라 제어시스템에 특화된 침입탐지 기술이 제시되고 있다.

Smart-grid, IEC61850 등의 전력 및 SCADA 시스템 분야를 대상으로 연구가 진행되고 있으며, 이에 대한 탐지 기술로는 제어시스템의 특성에 따른 동작 상태 정보를 이용한 상태기반(State-based) 탐지 기술과 오용 기반과 비정상기반 탐지 기반의 혼합형(Hybrid) 기반 탐지 기술 등이 있다.

2.2.2 통신 프로토콜별 침입탐지 기술

통신 프로토콜 별 침입탐지 기술 연구는 Modbus over TCP와 DNP3, BACnet(빌딩 제어시스템), IEC 60870-5-104(전력 제어시스템) 등을 대상으로 제어시스템에 주로 사용되는 통신 프로토콜에 관련하여 진행되고 있다.

통신 프로토콜 별 탐지 기술은 인공 신경망(Artificial neural network)과 베이지안 네트워크(Bayesian network) 분석법과 같은 기계학습(Machine learning) 알고리즘이 사용되고 있다. 또한, 트래픽의 패턴에 따른 규칙 기반 및 행위 기반의 개념을 도입한 혼합 기술이 사용되고 있다.

2.3 보안요구사항

2.3.1 제어시스템 보안요구사항

ISA/IEC 62443은 제어시스템에 대한 보안 국제표준이다. ISA(International Society of Automation)는 전기 기술에 대한 국제 표준 제정을 목적으로 하는 국제전기표준회의인 IEC (International Electronical Committee) 의 표준들 중 컴퓨터 및 계측시스템에 대한 설계 및 규격을 제정한다. 제어시스템에 대한 ISA/IEC 62443 보안요구사항은 다음과 같다[6].

- R1.1. 식별 및 인증 제어
  디바이스, 데이터 등에 대한 비인가 접근에 대한 접근 제어
- R1.2. 사용 제어
  전송되는 데이터에 대하여 비인가된 디바이스의 운용, 데이터의 사용 등에 대한 보호를 위한 데이터 무결성 보장
- R1.3. 시스템 무결성
  전송되는 데이터에 대하여 허가되지 않은 변조 등에 대한 보호를 위한 무결성 보장
- R1.4. 데이터 기밀성
  전송되는 데이터에 대한 도청 등으로부터 보호하기 위한 데이터 기밀성 보장
- R1.5. 제한된 데이터 흐름
  허가되지 않은 근원지로부터 전송되는 데이터 보호를 위한 데이터 흐름 제한
- R1.6. 이벤트에 적시 응답
  보안 정책 위반 시 적절한 권한 자동 알림, 시정 조치를 통한 보안 위반에 대한 응답 보장
- R1.7. 자원 가용성
  서비스 거부 공격 방지를 위한 모든 네트워크 가용성 보장

2.3.2 망간 자료전송 제품 보안요구사항

국가정보원의 망간 자료전송 제품 보안요구사항은 국가·공공기관의 망간 자료전송 제품에 대한 자료 및 서버 스트림 등 보안요구사항을 정의한 문서이다. 국가 및 공공기관에 사용되는 망간 자료전송 제품은 이 문서에 정의된 기준에 따라 국가정보원으로부터 인증을 받아야 사용 가능 하다. 이 문서에 정의된 보안요구사항은 다음과 같다[7].

Table. 1. Security requirements for control system in ISA/IEC 62443 and information security products for data transmission between networks in NIS

	NO.	Security Requirements	Explanation
ISA/IEC 62443	R1.1	Identification and authentication control	Control access to selected devices, information or both to protect against unauthorized interrogation
	R1.2	Use control	Data integrity to protect against unauthorized operation
	R1.3	System integrity	Data integrity to protect against unauthorized changes
	R1.4	Data confidentiality	Data confidentiality to protect against eavesdropping
	R1.5	Restricted data flow	Restrict the flow of data to prevent the publication of information to unauthorized sources
	R1.6	Timely response to events	Respond to security violations by notifying the proper authority, and taking timely corrective action
	R1.7	Resource availability	availability of network resources to protect against DoS
NIS	R2.1	Data transmission control	Data transmission according to the control policy, user authentication , malware inspection
	R2.2	Stream link	Control access to terminal, It can be requested only in non-secure areas
	R2.3	Maintain one direction	Managing Security for a one-way maintenance should be done only in the security area
	R2.4	Audit records	Audit data generation like identification
	R2.5	Identification and authentication	User identity verification, authentication information to prevent reuse
	R2.6	Security management	Security management of an authorized administrator
	R2.7	Transfer data protection	Encryption to maintain data confidentiality
	R2.8	Self test	Periodic self- tests during system operation
	R2.9	Session management	If undetected over a period of time, controls the session

- R2.1. 자료전송 통제
  통제 정책에 따른 자료전송, 사용자 인증, 비-보안영역에서 보안영역으로 전송되는 자료에 대한 악성코드 검사 수행, 통제 정책에 따른 패킷 흐름 허용 및 차단 등의 기능 포함
- R2.2. 스트림 연계
  인가된 업무서버에만 접근 가능하도록 단말에 대한 접근 통제를 해야 하며, 보안영역 전송통제서버에서 비-보안영역 전송통제서버로만 통신 요청 가능해야 하는 등의 기능 포함
- R2.3. 일방향성 유지
  일방향성 유지를 위한 보안관리는 보안영역에서만 이루어져야 하며, 비-보안영역 전송통제서버는 보안영역으로부터 정책을 수신하는 기능 포함
- R2.4. 감사기록
  식별, 인증, 보안기능 수행 내역과 같은 감사 데이터 생성하는 등의 기능 포함
- R2.5. 식별 및 인증
  관리자나 이용자 신원 검증, 패스워드 보안성 기준 검사, 인증정보 재사용 방지 등의 기능 포함
- R2.6. 보안관리
  인가된 관리자에 의한 보안기능, 보안정책, 중요 데이터 설정 및 관리하는 등의 보안관리 기능을 포함
- R2.7. 전송데이터보호
  전송 데이터에 대한 기밀성 유지를 위한 암호화 기능 포함
- R2.8. 자체시험
  시스템 운영하는 동안 주기적인 자체시험을 통한 정확한 운영 관리, 시스템 자체의 무결성 검사 등의 기능 포함
- R2.9. 세션관리
  일정시간 동작 미 감지되면 세션 통제, 동일 계정에 의한 재로그인 차단 등의 기능 포함

2.3.3 보안요구사항 도출

표준 ISA/IEC 62443의 제어시스템에 대한 보안요구사항 및 국가정보원의 망간 자료전송 제품 보안요구사항을 바탕으로 도출한 제어시스템 환경에서의 안전한 망간 자료전송을 위한 보안요구사항은 다음과 같다.

- R3.1. 접근제어 및 인증
  통제 정책에 따라 디바이스, 전송되는 데이터 및 사용자 등 비인가된 접근에 대한 접근제어를 의미하며, R1.1, R2.1, R2.5의 내용 및 R2.2의 일부 내용을 포함한다.
- R3.2. 기밀성
  도청과 같은 보안위협으로부터 망간 전송되는 데이터 보호를 위한 암호화 등의 데이터 기밀성 보장을 의미하며, R1.4와 R2.7의 내용을 포함한다.
- R3.3. 무결성
  망간 전송되는 데이터에 대하여 비인가된 시스템 접근에 의해 허가되지 않은 변조 등에 대한 보호를 의미하며, R1.2와 R1.3의 내용을 포함한다.
- R3.4. 가용성
  서비스 거부 공격과 같은 시스템 가용성을 침해하는 보안위협 방지를 위한 네트워크 가용성 보장을 의미하며, R1.7의 내용을 포함한다,
- R3.5. 데이터 흐름제어
  비-보안영역에서 보안영역으로 전송되는 자료에 대해 허가되지 않은 근원지로부터 전송되는 데이터를 보호하기위한 악성코드 검사, 통제 정책에 따른 데이터 흐름 제한을 의미하며, R1.5의 내용 및 R2.1의 일부 내용을 포함한다.
- R3.6. 일방향성
  보안영역 전송통제서버에서 비-보안영역 전송통제서버로만 통신 요청이 가능하고, 비-보안영역 전송통제서버는 해당 요청에 대한 정책을 수신함으로써 데이터전송이 일방향으로 이루어지도록 함을 의미하며, R2.2의 일부 내용과 R2.3의 내용을 포함한다.
- R3.7. 시스템 보안관리
  주기적인 보안 테스트를 통한 정확한 운영 관리와 안전한 시스템 운영에 필요한 보안정책, 세션 통제 등 보안기능 설정 및 관리를 의미하며, 보안기능 수행 내역과 같은 감사 데이터 생성 및 관리를 의미한다. 이는 R2.4, R2.6, R2.8, R2.9의 내용을 포함한다.

III. 보안위협 분석

본 절에서는 제어시스템에서 발생할 수 있는 보안위협을 분석하고 보안위협별 위협 수준과 공격 및 악성코드 유형의 특성으로 분류한다. 위협수준은 한국인터넷진흥원에서 발표한 “취약점 분석·평가 모

Table. 2. Classification of security threats

NO.	Security Threats	Threat Level	Malicious code/Attack Type
V1	Data Leakage	H	APT, Duqu, etc.
V2	Newly-born·Mutated Malicious	VH	Flame, Gauss, Shamoon, Skywiper, etc.
V3	Difficulty of Real Time Detection	VH	Zero-Day Attack, APT, etc.

델"[12]의 위협평가기준표를 바탕으로 분석하였다.

해당 문서는 위협에 의한 손실 및 업무에 미치는 영향 정도에 따라 보안위협을 낮음(L), 중간(M), 높음(H), 매우높음(VH) 4단계로 분류하고 있으며, 최근에도 여러 기업에서 취약점 분석 및 평가에 이 기준표를 활용하고 있다. Table.2.는 특성별 보안위협을 분류한 표이다.

3.1 V1. 자료유출

최근 급증하는 APT(Advanced Persistent Threat) 공격은 정부기관 내 기밀문서 탈취, 군 기밀문서 탈취, 국가기반시설에 대한 사이버 테러리즘 활동, 기업 영업 비밀 탈취, 금융기업에 대한 금융시스템 작동을 마비시켜 금융 자산 정보 탈취 등을 목표로 한다[1].

이는 내부망에 접근하여 내부 시스템을 감염시키고 C&C 서버와의 통신을 통해 내부 정보를 유출시킨다.

3.2 V2. 신종 및 변종 악성코드

2010년 제어시스템의 일부 구성 요소를 제어하는 스턱스넷 악성코드가 발견됨[9]에 이어 스턱스넷과 유사한 악성코드인 듀크(Duqu)가 발견되었다. 듀크는 Microsoft Word문서를 설치 프로그램 파일로 사용해 코드 실행을 허용하여 정보를 수집한다[10]. 이후에도 플레임(Flame), 가우스(Gauss) 등 스턱스넷이 진화된 형태의 악성코드들이 출현하였다.

또한, 제어시스템을 대상으로 한 악성코드로 데이터를 삭제하는 샤문(Shamoon) 뿐만 아니라 감염된 시스템으로부터 문서 및 녹음 기록 등을 수집하는 스카이와이퍼(SkyWiper), 마흐디(Mahdi) 등의 신종 및 변종 악성코드가 지속적으로 발견되고 있다[2,11].

3.3 V3. 실시간 탐지의 어려움

기존 망분리 환경은 전송통제서버가 위치하는 구간에 침입탐지 시스템을 두어 악성코드를 탐지한다. 이를 통해 탐지된 악성코드는 차단시키고 탐지 되지 않은 트래픽만이 정상 트래픽으로 간주되어 내부망으로 전송된다.

하지만, 취약점에 대한 패치가 나오지 않은 시점에서 공격이 이루어지는 제로 데이 공격(Zero-Day Attack)이나 잠복기를 거쳐 동작 하는 악성코드 등의 행위기반 악성코드는 침입탐지 시스템을 통해 실시간적인 탐지 및 차단이 불가하다.

IV. 제안하는 트래픽 분석망

국가정보원의 전자제어시스템의 보안가이드라인과 제어시스템에 특화된 침입탐지 기술 연구, 보안요구사항 등을 통해 안전한 제어시스템 환경 구축을 위한 방안들이 제시되고 있다.

하지만 이러한 방안에도 불구하고 제어시스템을 겨냥한 악성코드 공격으로 인한 자료유출과 같은 취약점이 지속적으로 발생하고 있다. 또한, 제어시스템 환경에서는 침입탐지 되어 수집된 악성 트래픽들로부터 악성코드 분석이 이루어지며[2], 탐지가 어려운 신·변종 악성코드의 등장으로 미탐지된 악성 트래픽에 대한 분석이 어렵다.

본 논문은 이러한 보안위협들로부터 신·변종 악성코드 공격에 즉각적 대응을 목표로 트래픽 분석망 모델을 제안한다. 이는 계측정보와 같은 실시간으로 변하는 현장장치의 정보를 전달해야 하는 제어시스템의 특성에 따라 모든 트래픽을 수집하여 분석한다. 침입탐지 시스템으로 탐지된 트래픽은 시그니처 정보와 같은 탐지된 정보를 이용해 분석하며, 미탐지된 트래픽은 이상행위 모니터링을 통해 모니터링된 동적 분석 정보를 이용해 분석한다. 모든 트래픽에 대해 악성여부 유형 및 행동패턴에 따른 군집화를 통해 새로

운 트래픽의 특성을 분석할 때 유사도를 기반으로 해당 유형으로 분류한다. 따라서 분석망에 전송되는 새로운 트래픽에 대한 악성여부 및 변종 또는 신종 여부를 검사할 수 있다.

제어시스템 환경에 이러한 트래픽 분석망 도입을 제안함으로써, 트래픽의 악성여부 및 신·변종 악성코드로 인한 이상행위에 대하여 심층적 분석을 통해 보안위협에 대응하기 위한 보안기능들을 도출한다.

4.1 트래픽 분석망 구성

제안하는 시스템은 일방향 전송장치를 사용하여 격리된 환경을 구축한다. 일방향 전송장치는 단방향 자료전송을 위해 물리적 계층에서 구현된 장치로써 데이터 다이오드라는 이름으로 사용되고 있다. 이는 주기적인 확인 과정 없이 자료를 즉시 전달하기 때문에 제어시스템 환경에서 실시간으로 발생하는 정보를 전달할 수 있어 실시간성을 보장한다.

제안하는 트래픽 분석망의 구성은 Fig. 3.과 같으며, 시스템의 각 구성요소에 대한 설명은 다음과 같다.

- C1. 일방향 전송장치
  - 망간 전송되는 모든 트래픽을 트래픽 분석망에 전송한다. 단방향으로만 전송되게 함으로써 다른 망과 격리된 환경에서 트래픽 분석이 가능하다.

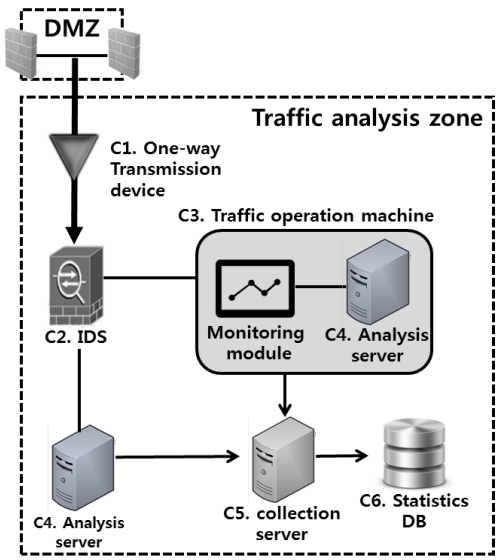

Fig. 3. The proposed Traffic analysis Architecture

  - 물리적 계층에서 H/W 기반으로 구현되어 데이터 전송의 실시간성이 높은 시스템으로 현재까지도 오류제어, 통신 프로토콜 기능을 탑재하는 등의 보안성이 강화된 일방향 전송장치 개발 연구가 활발히 진행되고 있다.
- C2. IDS
  - 전송된 모든 트래픽에 대해 침입탐지를 수행한다. 수행된 결과를 통해 탐지 및 미탐지 트래픽으로 각각 분류한다.
  - 침입탐지는 IDS 특성에 따라 호스트 기반, 네트워크 기반 등의 방식으로 시스템 로그, 네트워크 패킷 분석을 통해 데이터의 근원지와 침입경로를 파악한다.
  - 이후, 미리 지정해 놓은 이상행위와 비교하여 검사하는 오용기반, 정상 트래픽의 행위 궤적을 기록해 놓고 이와 비교하여 검사하는 이상기반 등의 방법을 통해 이상행위를 검사 및 탐지 한다[13].
- C3. 트래픽 동작 머신
  - 미탐지된 트래픽에 대해 모니터링 모듈을 사용하여 이상행위를 모니터링하고, 모니터링된 내용을 바탕으로 악성 트래픽을 분석한다.
  - 모니터링 결과는 무결성 및 가용성 침해, 자료유출 등 이상행위 특성별 분류한다.
- C4. 분석서버
  - IDS로 탐지된 트래픽에 대해서 시그니처와 같은 탐지된 내용을 바탕으로 악성 행위 정보를 분석한다.
  - 미탐지된 트래픽에 대해서는 모니터링된 내용을 바탕으로 동적 분석 정보를 통해 무결성 및 가용성 침해, 자료유출 등 이상행위 특성별 분류하여 분석한다.
- C5. 수집서버
  - 분석서버를 통해 분석된 트래픽 정보는 유형 및 행동패턴 별 유사도를 바탕으로 악성 행위 정도를 정상부터 악성까지의 범위로 통계치를 분석하여 통계치 별 트래픽을 분류한다.
  - 유사도 판별은 Jaccard Coeffifient[14]과 같이 현재까지도 악성코드 유사도 분석에 많이 사용되는 알고리즘들을 응용하여 유사도 판별의 실시간성을 높이는 방법을 사용한다[15].
- C6. 통계 DB
  - 통계치 별 분류된 트래픽 정보들을 수집한다. 수집된 정보는 새로운 트래픽 분석에 사용되

며, 분석된 내용은 통계 DB에 지속적으로 업데이트 된다.

4.2 트래픽 분석망 운용 단계

Fig. 4.는 제안하는 시스템에 대한 동작 흐름을 나타내며, 이에 따른 동작 단계를 설명한다.

step1. 트래픽 분석망에 모든 트래픽 전송
일방향 전송장치를 이용하여 망간 전송되는 모든 트래픽을 트래픽 분석망으로 전송한다.

step2. IDS를 통한 침입탐지여부 결정
침입 탑지 시스템으로부터 1차적인 침입탐지를 수행한다. 탐지된 악성트래픽은 분석서버에 전송되고, 탐지되지 않은 트래픽은 트래픽 동작 머신 내 모니터링 모듈에 전송한다.

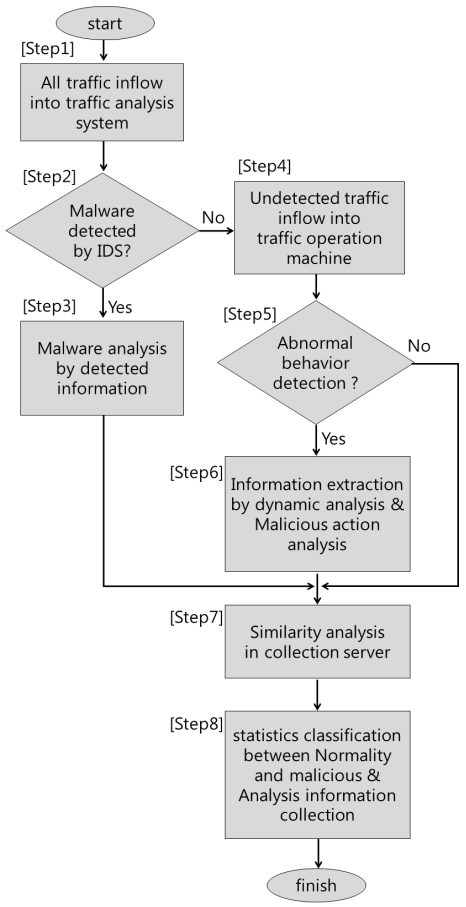

Fig. 4. Traffic operation flow of proposed Traffic analysis Architecture

step3. 탐지된 트래픽 분석
탐지된 악성 트래픽은 탐지된 정보를 기반으로 분석서버를 통해 분석한다. 분석된 정보는 수집서버로 전송한다.

step4. 미탐지된 트래픽 이상행위 모니터링
미탐지된 트래픽은 트래픽 동작 머신 내 모니터링 모듈에 전송된다. 모니터링 모듈을 통해 이상행위를 모니터링 한다.

step5. 이상행위 여부 결정
모니터링 모듈을 통해 이상행위가 발견되면 트래픽 동작 머신 내 분석서버에 전송하고, 이상행위가 탐지되지 않은 트래픽 정보는 수집서버에 전송한다.

step6. 이상행위가 탐지된 트래픽 분석
이상행위가 탐지된 트래픽은 트래픽 동작 머신 내 분석서버를 통해 동적 분석 정보를 추출하고, 악성 행위의 패턴을 분석한다.

step7. 악성행위 정도에 따른 유사도 분석
수집서버로 수집된 모든 트래픽에 대한 분석정보를 이용하여 악성행위 정도 및 행동패턴에 따른 유사도를 분석 및 측정한다.

step8. 유사도에 따른 통계치 별 분류
측정된 유사도 기반의 통계치를 바탕으로 트래픽을 유형 및 행동패턴 별 정상부터 악성까지의 범위로 분류한다. 분류되어 군집화된 트래픽의 각 정보는 통계 DB에 수집한다.

4.3 특징 및 보안기능 분석

본 절은 제안하는 시스템의 특징과 시스템 구성요소 각각의 특성을 분석하고, 분석된 특성들로부터 제어시스템에서 발생되는 보안위협들에 대응 할 수 있는 보안기능들을 도출한다.

4.3.1 제안하는 시스템 특징

샌드박스는 악성코드 분석에 주로 이용되는 기술로 샌드박스와 같은 기존의 악성코드 분석 연구는 수집된 악성코드 샘플을 이용하여 분석하기 때문에 이에 따른 분석 결과는 악성코드가 발생한 시스템과 악성코드 샘플간 상호작용에 의존한다[15]. 이로 인해, 시스템 운영 및 기능 확장 등의 이유로 기존 샘플로부터 분석된 바 없는 새로운 유형의 악성코드 공격이 발생할 경우 대응이 어렵다.

제안하는 시스템의 가장 큰 특징은 전송되는 모든 트래픽을 수집하여 정적 및 동적 분석을 통해 분석된 결과를 실시간으로 업데이트 시키고, 새로운 트래픽에 대한 악성여부 분석 시 업데이트된 정보를 활용하는데 있다.

이는 기존의 분석환경보다 신·변종 악성코드 판별에 유용한 특징을 가지며, 이와 더불어, 악성코드 특성에 따라 제어시스템에서 발생될 수 있는 무결성 침해, 자료유출 등의 보안위협에 대한 신속한 대응에 활용됨에 따라, 안전한 제어시스템 환경을 제공할 수 있다.

4.3.2 보안기능 분석

- 자료유출 방지
  - 일방향 전송장치를 통해 격리된 분석환경을 제공함으로써 분석 과정 중 발생할 수 있는 자료유출을 방지한다.
  - 트래픽 동작 머신을 통해 기존 침입탐지 시스템으로 탐지되지 않았던 자료유출 행위를 하는 트래픽을 발견하고 분석한다.
- 신종 및 변종 악성코드 탐지
  - 망간 전송되는 모든 트래픽을 수집하여 분석하며, 분석 정보는 통계 DB에 지속적으로 업데이트된다. 지속적으로 업데이트되는 정보는 새로운 트래픽 분석에 사용된다.
  - 수집서버는 트래픽에 대한 악성 행위 정도 및 행동패턴에 따라 트래픽을 유형별로 분석하여 군집화 한다. 유형별로 분석된 정보는 새로운 트래픽이 분석될 때 유사도를 바탕으로 해당 유형을 판별함으로써 신종 또는 변종 여부를 파악할 수 있다.
- 실시간 분석
  - 트래픽 동작 머신을 통해 실시간 탐지가 어려운 행위기반 또는 잠복기를 갖는 악성코드에 대하여 이상행위를 분석한다. 통계 DB에 이러한 분석 내용이 실시간으로 업데이트되어 다음 트래픽 분석에 적용된다.
- 무결성 및 가용성
  - 트래픽 동작 머신을 통해 미탐지된 데이터 무결성과 시스템 가용성을 침해하는 행위기반 악성코드를 탐지 및 분석한다.

4.4 보안요구사항 분석

본 절에서는 2.3.3절에서 도출한 보안요구사항을 바탕으로 제안하는 시스템 도입 시 만족되는 기존 제어시스템에서의 보안요구사항을 분석한다. 만족되는 보안요구사항들은 제안하는 시스템에서 각 구성요소들의 역할로부터 도출된다.

각 구성요소로 부터 만족시키는 보안요구사항은 Table. 3.과 같다.

- R3.3. 무결성
  - 수집서버는 실시간 전송되는 모든 트래픽을 수집하여 분석함으로써 미탐지 되었던 트래픽에 대해서 데이터 변조형 악성코드에 대한 추가적 분석이 가능하다.
  - 트래픽 동작·분석 머신은 망간 전송되는 데이터에 대해 무결성을 침해하는 악성코드 탐지가 가능하다.
- R3.4. 가용성
  - 트래픽 동작·분석 머신을 통해 탐지가 어려운 DDoS 등의 행위 기반 악성코드에 대한 행위 모니터링 및 분석으로 악성코드 탐지기능을 강화한다.
  - 수집서버는 악성행위 정도를 통계별로 분석함으로써 시스템의 가용성을 침해할 가능성이 있

Table. 3. satisfied security requirements by component of Traffic Analysis Architecture

		R3.3	R3.4	R3.5	R3.6	R3.7
		Integrity	Availability	Data Stream Control	One-Way	System Security Management
C1	One-Way Transmission device			√	√	
C3	Traffic Operation Machine	√	√	√	√	
C4	Analysis Server					√
C5	Collection Server	√	√			
C6	Statistics DB					√

는 트래픽을 판별한다.

- R3.5. 데이터 흐름제어
  - 일방향 전송장치를 통해 일방향 데이터 전송 정책에 따라 외부로의 패킷 흐름을 제한함으로써 격리된 분석환경 구축이 가능하다.
  - 트래픽 동작 머신은 미탐지된 트래픽에 대해 탐지되지 않았던 이상행위를 도출해내어 탐지가 어려운 신·변종 등의 악성코드에 대한 탐지가 가능하다. 탐지가 어려운 악성코드에 대한 심층적 분석을 통한 악성코드 검사 기능을 강화 한다.
- R3.6. 일방향성
  - 일방향 전송장치로 부터 격리된 분석환경을 구축함으로써 보안영역으로 통신 불가하기 때문에, 트래픽을 분석함에 있어서 분석환경에 전송되는 모든 자료에 대한 유출을 방지한다.
  - 트래픽 동작 머신을 통해 탐지가 어려운 행위기반의 악성코드 중 자료유출 형 악성코드에 대한 탐지가 가능하다.
- R3.7. 시스템 보안관리
  - 분석서버는 시스템이 운영하는 동안 분리된 망에서 트래픽을 실시간으로 분석한다. 분석된 정보가 지속적으로 통계 DB에 업데이트됨에 따라 이러한 정보로부터 보안 정책 및 설정 관리를 강화한다. 이에 따라 신·변종 악성코드 분석기능을 강화할 수 있다.

V. 결 론

본 논문은 기존 제어시스템 네트워크 아키텍처와 제어시스템에 특화된 침입탐지기술 및 보안요구사항을 분석하였다. 또한, 제어시스템 환경에서 발생되는 보안위협들에 대응하기 위한 추가적인 보안기능들을 도출하였다. 더불어, 보안기능들을 도출하기 위해 제어시스템의 특성에 따라 망간 전송되는 모든 트래픽을 분석하기 위한 트래픽 분석망 설계방안을 제안하였다. 제안한 시스템은 각 구성요소들의 역할들을 분석함으로써 기존 제어시스템에 대해 시스템 도입 시 필요한 보안요구사항을 만족시키는 것을 보였다.

최근 제어시스템에 특화된 침입탐지 기술로 사용되는 기계학습, 혼합기술 등은 트래픽의 행위 예측이 가능하고, 학습된 정보를 통한 분석이 가능하다. 따라서 본 논문에서 제안하는 시스템과 같은 실시간으로 트래픽을 분석하는 환경에 이러한 기술들을 도입함으로써, 신·변종 악성코드의 특성을 실시간으로 분석 가능할 것으로 기대한다.

또한, 본 논문에서 제안하는 시스템을 통해 제어시스템을 겨냥한 악성 트래픽에 대한 유형 분류 및 분석하는 기술 개발에 활용 될 것으로 기대한다.

References

[1] NIS, “Secure data transmission security guidelines between national public business networks and internet”, Aug. 2010.

[2] Seung-Oh Choi, Woo-Nyon Kim, “Research Trends on Intrusion Detection System Technique of Control System”, Jounal of The Korea Institute of Information Security & Cryptology VOL.24, NO.5, Oct. 2014.

[3] KISA, “Worm analysis of activities in industrial control systems”, May. 2014.

[4] NIST, ″Guide to Industrial Control Systems (ICS) Security″, NIST Special Publication 800-82, Jun. 2011.

[5] Luciana Obregon, ″Secure Architecture for Industrial Control Systems″, SANS Institute InfoSec Reading Room, Sept. 2015.

[6] IEC 62443-3-3, ″Industrial communication networks-Network and system security-Part 3-3: System security requirements and security levels″, Aug. 2013.

[7] NIS, “Security requirements for information security products for nation”, Feb. 2012.

[8] Dailysecu, http://dailysecu.com/news_view.php?article_id=131, Jun. 2011.

[9] Jae-Jun Heo, Sang-Choul Lee, “Infection process and countermeasures of Stunxnet”, Jounal of The Korea Institute of Information Security & Cryptology VOL.21, NO.7, Oct. 2011.

[10] Symantech, ttps://www.symantec.com/ko/kr/outbreak/?id=stuxnet, 2011.10.

[11] Ahnlab, http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsVie

w.do?curPage=&menu_dist=2&seq=24472&key=&dir_group_dist=&dir_code, Jan. 2016.
[12] KISA, "Vulnerability analysis·evaluation model", Dec. 2002.
[13] Yoonjeong Kim, Ki-Han Lee, " IDS technical standards trends of ISO/IEC", Journal of Korea Institute Of Information Security And Cryptology, Jun. 2004.
[14] Suphakit Niwattanakul, Jatsada Singthongchai,Ekkachai Naenudorn and Supachanun Wanapu, "Usingof Jaccard Coefficient for Keywords Similarity", Proceedings of the International MultiConference ofEngineering and Computer Scientists 2013, Vol I,IMECS 2013, (2013), Mar. 2013.
[15] You Joung Ham, Hyung-Woo Lee, "Malicious Trojan Horse Application Discrimination Mechanism using Realtime Event Similarity on Android Mobile Devices", Journal of Korean Society for Internet Information, Jun. 2014.
[16] Mariano Graziano, Corrado Leita, and Davide Balzarotti, "Towards Network Containment in Malware Analysis Systems", ACSAC '12 Proceedings of the 28th Annual Computer Security Applications Conference, Dec. 2012.

〈저자소개〉

이 은 지 (Eun-ji Lee) 학생회원
2016년 2월: 공주대학교 정보통신공학과 학사
2016년 3월~현재: 아주대학교 컴퓨터공학과 석사과정
〈관심분야〉 제어시스템 보안, 클라우드 컴퓨팅 보안, 암호프로토콜, 사물인터넷 보안

곽 진 (Jin Kwak) 종신회원
2000년 8월: 성균관대학교 학사
2003년 2월: 성균관대학교 석사
2006년 2월: 성균관대학교 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 1월~2009년 12월: 정보통신연구진흥원 주간기술동향 집필위원
2007년 1월~현재: 한국정보기술융합학회 이사
2007년 3월~2015년 2월: 순천향대학교 정보보호학과 교수
2008년 1월~현재: 한국정보보호학회 논문지편집위원
2008년 1월~현재: 한국정보보호학회 이사
2008년 4월~현재: 한국인터넷정보학회 논문지편집위원
2008년 12월~현재: 정보통신산업진흥원 기술평가위원
2009년 1월~2009년 12월: 순천향대학교 공과대학 교학부장
2009년 1월~2010년 12월: 순천향대학교 정보보호학과 학과장
2009년 5월~현재: TTA 표준화로드맵 기술표준기획전담반 위원
2010년 1월~2012년 12월: 순천향대학교 SCH BIT 창업보육센터장
2010년 3월~현재: 조달청 기술평가위원
2010년 5월~2010년 7월: 교육과학기술부 국가기술수준평가 위원
2011년 1월~현재: 한국정보처리학회 이사
2011년 1월~현재: JIPS 논문지 편집위원
2011년 2월~2012년 12월: 순천향대학교 중소기업산학협력센터 센터장
2011년 7월~현재: 지식경제부 지식경제기술혁신평가단 위원
2012년~현재: 한국암호포럼 운영위원
2012년~현재: 한국방송통신전파진흥원 평가위원
2013년~현재: 교육부 정책자문위원
2013년~현재: 금융보안연구원 보안기술 자문위원
2013년~현재: 금융감독원 인증방법평가위원
2015년 3월~현재: 아주대학교 사이버보안학과 교수
〈관심분야〉 자동차 보안, 암호프로토콜, 응용시스템보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가