제어시스템 위협분석을 위한 Event Log 상관분석에 관한 연구

김종민* · 김민수* · 이동휘**

요 약

제어시스템은 공공 네트워크와의 통신망 융합에 따라 다양한 루트를 통해 정보유출 및 변조 등의 위협이 제어시스템에서도 그대로 나타날 수 있다. 최근 다양한 보안에 대한 이슈와 새로운 공격기법에 의한 침해 사례가 다변화됨에 따라서, 단순히 차단 및 확인 등의 학습을 통해 정보를 데이터베이스화하는 보안 시스템으로는 새로운 형태의 위협에는 대처하기 힘들어지고 있으며, 보안 접근 권한을 가진 내부자에 의한 보안위협에 대해서도 기존의 보안장비로는 대응하기가 어렵다. 내부자에 의한 위협에 대응하기 위해 내부 시스템에서 실시간으로 발생한 Event Log를 수집하고 분석하여야 한다. 이에 따라 본 연구에서는 제어시스템에서 실시간으로 발생한 Event Log들을 토대로 상관분석을 통해 Event Log간 요소들의 상관관계의 여부를 알 수 있었으며, 분석결과를 바탕으로 이 분야의 연구에 기여할 수 있을 것으로 판단된다.

A Study on Event Log Correlation Analysis for Control System Threat Analysis

Jongmin Kim* · Minsu Kim* · DongHwi Lee**

ABSTRACT

The control system can have such threats as information leakage and falsification through various routes due to communications network fusion with public network. As the issues about security and the infringe cases by new attack methods are diversified recently, with the security system that makes information data database by simply blocking and checking it is difficult to cope with new types of threats. It is also difficult to respond security threats by insiders who have security access authority with the existing security equipment. To respond the threats by insiders, it is necessary to collect and analyze Event Log occurring in the internal system realtime. Therefore, this study could find out whether there is correlation of the elements among Event Logs through correlation analysis based on Event Logs that occur real time in the control system, and based on the analysis result, the study is expected to contribute to studies in this field.

Key words : Information Security, Event Log, Log Analysis, Correlation Analysis, Control System

접수일(2017년 11월 30일), 수정일(1차: 2017년 12월 22일), 게재확정일(2017년 12월 27일)

* 경기대학교 융합보안학과

** 동신대학교 융합정보보안학과(교신저자)

1. 서 론

제어시스템은 일반적으로 독립 폐쇄망으로 구성으로 구축되어 있으나 최근에는 업무상 편의성 및 대외기관과의 협력이 증가됨에 따라 범용 프로토콜과 Windows 기반의 운영체제를 이용한 제어시스템 도입 비율이 높아지고 있다[1][2]. Windows 운영체제의 도입 증가로 인해 해당 운영체제의 보안패치 및 제어시스템 패치를 위해 내부 관리자 계정을 이용해 작업을 하는 사례들이 빈번하게 이루어지면서 제어시스템 내부위협이 새로운 노출요소가 되고 있다.

본 논문에서는 이렇듯 Windows 운영체제를 기반으로한 제어시스템의 Event Log 데이터를 수집하여 상관관계를 분석함으로써 각 Event Log들의 상관관계를 연구하려한다. 2장에서 제어시스템 보안위협 및 Event Log, 3장에서는 제안한 연구대상과 변수에 대해 데이터를 정량화한다. 4장에서는 데이터들을 SPSS 18.0을 이용하여 나온 결과를 토대로 5장에서 결론을 맺는다.

2. 관련연구

2.1 제어시스템 위협사례

세계적으로 주요 기반시설에 적지 않은 피해를 주었던 악성코드들은 제어시스템을 대상으로 시스템 파괴나 운영방해를 목적으로 제작된 것으로 알려져 있다. 2010년 6월 이란에서 발견된 스턱스넷(Stuxnet) 바이러스는 이란의 핵시설에 대한 사이버공격을 목적으로 제작되었고 전 세계에 걸쳐 10만개 이상의 제어시스템을 감염시키는 결과를 초래하였다. 이 바이러스는 입출력 장치(HMI)에 설치된 소프트웨어 명령어를 교란, 제어시스템을 공격하도록 설계된 특정코드를 가지고 있었다. 또 다른 악성코드로는 2012년5월에 발견된 플레임(Flame) 바이러스로 사이버 사보타주 형태로 이란의 전력제어시스템을 손상시켰다. 플레임은 이란 오일회사와 관련 정부조직을 공격 대상으로 삼았고 HMI 기능과 관련된 제어명령과 수행 업무를 복제함으로써 컴퓨터 네트워크 감시의도를 가지고 제작된 것으로 알려져 있다. 스턱스넷과 플레임 바이러스는 제어시스템을 대상으로 하는 사이버 공격이 현실적으로 가능하다는 것을 입증한 사례가 되었다. 최근에는 '드래곤플라이(Dragonfly)'로 알려진 러시아 해커 집단이 2011년부터 유럽과 미국 에너지기업들을 대상으로 지속적인 사이버 스파이 활동을 펼친 사실이 포착되었다. 에너제틱 베어로 알려진 악성코드는 에너지 기업들을 직접공격 대상으로 하는 것이 아니라 제어시스템 장비 제조사 내부시스템에 우회로 침투하여 에너지기업에 납품되는 소프트웨어를 조작하여 원격에서 해커가 접속 할 수 있도록 만든 것이 특징이다[3].

2.2 Event Log

Windows 시스템은 Application Log, Security Log, System Log와 같이 세 가지 로그를 이벤트에 기록하며, OS 구성에 따라 Directory Service Log, File Replication Service Log, DNS Server Log가 추가될 수가 있다[4]. 주요 이벤트 별 특징은 <표 1>과 같다.

<표 1> 윈도우 시스템 Event Log 종류[4][5]

Event Log	설 명
Application	응용 프로그램이 기록한 다양한 이벤트가 저장되며, 기록되는 이벤트는 해당 제품의 개발자에 의해 결정된다. ex) 안티바이러스 제품의 경우 악성코드 탐지 및 업데이트를 기록한다. 일반 응용프로그램의 경우 활성화 여부와 성공 여부 등에 대한 정보를 기록한다.
Security	유효하거나 유효하지 않은 로그온 시도 및 파일 생성, 열람, 삭제 등의 리소스 사용에 관련된 이벤트를 기록한다. 감사로그 설정을 통해 다양한 보안 이벤트 저장이 가능하다.

System	Windows 시스템 구성요소가 기록하는 이벤트로 시스템 부팅 시 드라이버가 로드 되지 않는 경우와 같이 구성요소의 오류를 이벤트에 기록한다.

2.3 상관관계분석

2개의 변수 와 y가 있을 때에, x의 변화에 따라서 y도 변화하는 관계를 상관관계라고 한다.

변수 간 상관관계가 있는지를 수치적으로 판단하는 데는 상관계수라고 불리는 지표를 이용한다.

상관계수는 통상 r이라는 기호로 표기되고, -1에서 1까지의 값을 취한다.

$$-1 \quad r \quad 1$$

상관계수의 부호가 양(+)일 때에는 양의 상관관계가 있다는 것을, 음(-)일 때에는 음의 상관관계가 있다는 것을 나타내고 있다. 상관관계의 강도는 상관계수의 절대 값 $|r|$ 또는 자승 값 r으로 평가한다. 어느 쪽도 1에 가까울수록 상관이 강하다는 것을 의미한다. 상관관계가 존재하지 않을 때에는 상관계수의 값은 0에 가까운 값이 된다.

변수 x와 y의 상관계수는 다음과 같은 순서로 산출할 수 있다[6][7][8].

① x의 편차제곱의 합 (xx)를 계산한다.

$$xx) = \sum_{=1}^{n} (x_1 - x)^2 = \sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i \right)^2 / n$$

② y의 편차제곱의 합 $S(yy)$를 계산한다.

$$S(yy) = \sum_{i=1}^{n} (y_1 - y)^2 = \sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i \right)^2 / n$$

③ x와 y의 편차곱의 합 $S(xy)$를 계산한다.

$$xy) = \sum_{=1}^{n} (x_1 - x)(y_1 - y) = \sum_{i=1}^{n} x_i y_i - \left(\sum_{i=1}^{n} x_i \right) \left(\sum_{i=1}^{n} y_i \right) / n$$

④ 상관계수 r을 계산한다.

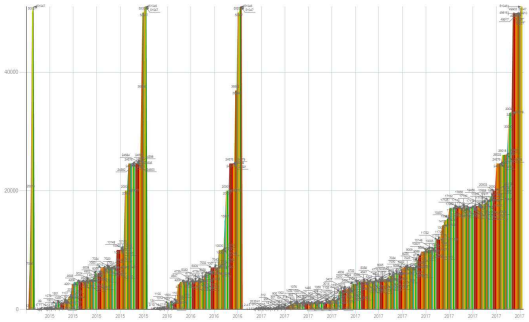
$$r = \frac{S(xy)}{S(xx)S(yy)}$$

3. 제안하는 방법

본장에서는 제어시스템에서 수집된 데이터를 토대로 Event Log들 간의 상관관계를 분석하고자 한다.

3.1 연구의 대상 및 변수

본 연구에서 사용된 데이터는 015년 06월 01부터 2017년 08월 03일까지 발생한 Event Log들을 데이터로 사용하였고 (그림 1)은 의 총 발생 현황을 나타낸 것이다.

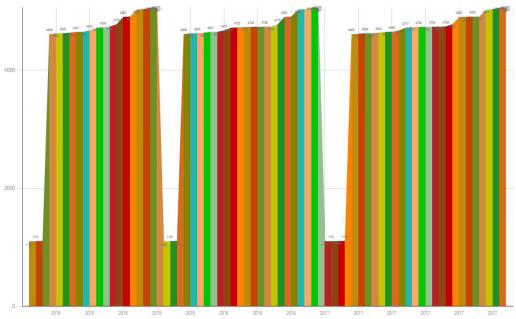


(그림 1) Event Log 총 발생 현황

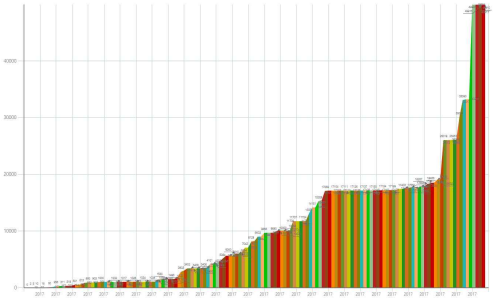
3.2 변수

(그림 2), (그림 3), (그림 4)는 Event Log(Security Log, Application Log, System Log)들에 대한 각각의 발생현황을 나타낸 것이다.

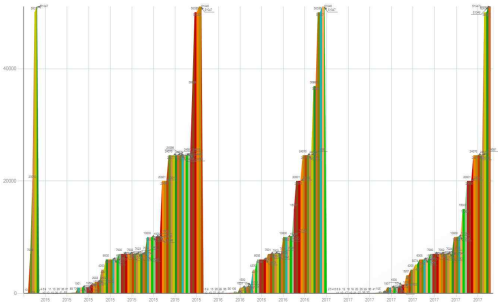
.



(그림 2) 2015~2017 Security Event Log 발생현황



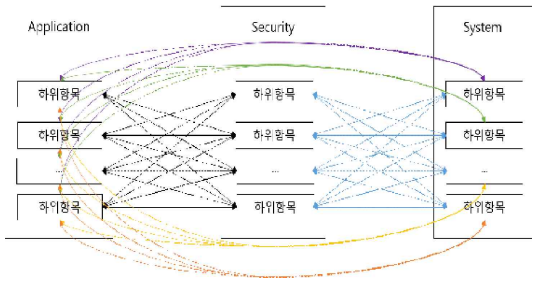
(그림 3) 2015~2017 Application Event log 발생현황



(그림 4) 2015~2017 System Event log 발생현황

3.3 연구 분석 모형

(그림5)는 상관관계를 분석하기 위한 연구모형이다.



(그림 5) 분석모형

3.4 연구 분석 방법

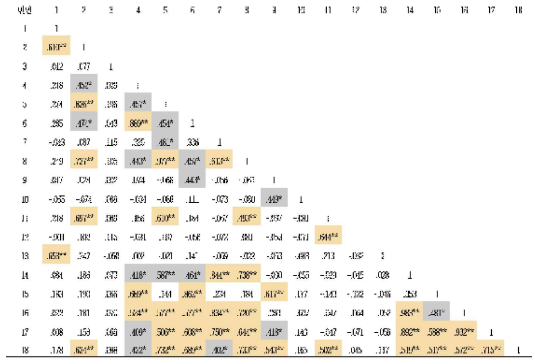
본 연구에서는 제어시스템에서 수집한 Event Log 데이터를 토대로 SPSS18.0을 이용하여 Event Log간의 상관관계를 도출하였다.

4. 연구결과

4.1 상관관계 분석

제어시스템에서 수집한 Event Log들에 대해 상관관계를 분석한 결과 <표 2>와 같다.

<표 2> Event Log 상관분석



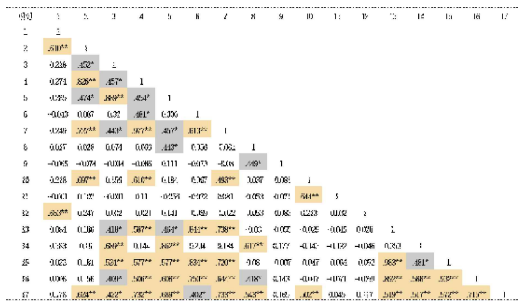
*. 상관계수는 0.05수준(양쪽)에서 유의.
**. 상관계수는 0.01수준(양쪽)에서 유의.

상관분석을 실시한 결과 변인별로 유의수준별로 정리한 것은 <표 3>과 같으며, 변인 3만 다른 변인과 상관관계가 나타나지 않았으며, 변인 3을 제외하고 다시 상관관계를 실시하였다.

<표 3> 변인 간 상관관계 결과

변인	*. 0.05 수준에서 유의	**. 0.01 수준에서 유의
1	-	1, 2, 13
2	4	5, 6, 8, 11, 18
3	-	-
4	2, 5, 8, 14, 17, 18	6, 15, 16
5	4, 6, 7, 14	2, 8, 11, 16, 17, 18
6	2, 5, 8, 9, 14	4, 15, 16, 17, 18
7	5, 18	8, 14, 16, 17
8	4, 6	2, 5 7, 11, 14, 16, 17, 18
9	6, 10, 17	15, 18
10	9	-
11	-	2, 5, 8, 12, 18
12	-	11
13	-	1
14	4, 5, 6	7, 8, 16, 17, 18
15	-	4, 6, 9, 16, 17, 18
16	15	4, 5, 6, 7, 8, 14, 17, 18
17	4, 9	5, 6, 7, 8, 14, 15, 16, 18
18	4, 7	2, 5, 6, 8, 9, 11, 14, 15, 16, 17

<표 4> 변인3을 제외한 Event Log 상관분석



<표 5> 변인3을 제외한 상관관계 결과

변인	*. 0.05 수준에서 유의	**. 0.01 수준에서 유의
1	-	2, 12
2	3, 5	1, 4, 7, 10, 17
3	2, 4, 7, 13	5, 14, 15, 17
4	3, 5, 6	2, 7, 10, 13, 15, 16, 17
5	2, 4, 7, 8, 13	3, 14, 15, 16, 17
6	4, 17	7, 13, 15, 16
7	3, 5	2, 4, 6, 10, 13, 15, 16, 17
8	5, 9, 16	14, 17
9	8	-
10	-	2, 4, 7, 11, 17
11	-	10, 17
12	-	1
13	3, 5	4, 6, 7, 15, 16, 17
14	15	3, 5, 8, 16, 17
15	14	3, 4, 5, 6, 7, 13, 16, 17
16	3, 8	4, 5, 6, 7, 13, 14, 15, 17
17	6	2, 3, 4, 5, 7, 8, 10, 13, 14, 15, 16

상관분석을 실시한 결과 <표 5>와 같이 모든 요소가 유의수준(양쪽)에서 0.01 또는 0.05 수준에서 유의한 상관관계가 있는 것으로 나타났다.

5. 결 론

지금까지의 보안위협에 대한 대처는 보안장비를 이용한 방법이 주를 이루었지만 최근에 들어서는 시스템의 Event Log를 활용한 보안기법들

이 적용되고 있다.

본 연구에서 Event Log 요소들간의 상관관계 분석을 하였고, 이 결과 본 연구에서 Event Log 요소들간의 상관관계를 알 수 있었다. 내부 시스템에서 어떠한 행위를 하게되면 Event Log에 로그 데이터들이 수집되고 수집된 Event Log들을 분석하여 보안에 문제가 있는지를 판단하게 됨으로써 내부자의 보안위협을 감소 및 예방정책에 기여할 수 있을 것이라 기대된다.

또한, 차후 이 결과를 토대로 시나리오 개발을 통해 패턴분석을 하여 위협을 탐지할 수 있는 시스템 연구가 수행되기를 기대한다.

참고문헌

[1] 이동휘, 최경호, “제어망에서 화이트 리스트 기법을 이용한 이상 징후 탐지에 관한 연구”, 융합보안학회논문지, Vol. 12, No. 4, 2012, pp. 77-84.

[2] 이경문, “발전제어시스템 악성코드 방어를 위한 보안관제 모델 연구”, 석사학위논문, 2017. 02.

[3] 이건행, “한전의 ‘배전지능화 시스템’ 현행 보안대책 및 향후전망”, 전기저널, 2015. 5, pp. 34-40.

[4] Minasi, Mark, Gibson, Darril, Finn, Aidan, Henry, “Mastering Windows Server 2008 R2”, Wiley, 2012. 08, p. 921.

[5] 김현우, “보안을 고려한 DRS(Disaster recovery system) 구현 방안 연구”, 석사학위논문, 2014. 08.

[6] Seong S. Chae, Chansoo Kim, Jong-Min Kim, William D. Warde, "Cluster analysis using different correlation coefficients", Statistical Papers Vol. 49, No.4, 2006, pp.715-727.

[7] Ali Abbas, "Statistical Signal Processing Technique for Identification of Different Infected Sites of the Diseased Lungs", Journal of medical systems Vol. 36, No.3, 2010, pp.1537-1541.

[8] 김종민, 김민수, 김귀남, “기상변화 및 불쾌지수에 따른 범죄발생 예측 모델”, 융합보안학회논문지, Vol. 14, No. 6, 2014, pp. 89-95.

〔저자소개〕

김 종 민 (Jongmin Kim)
2010년 체육학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : dyuo1004@gmail.com

김 민 수 (Minsu Kim)
2004년 컴퓨터공학사
2012년 경호안전학석사
2015년 산업보안학박사
현 재 경기대학교 융합보안학과 초빙교수

email : fortcom@hanmail.net

이 동 휘(DongHwi Lee)
2007년 경기대학교 정보보호박사
2011년~2012년 University of Colorado Denver, Dept. of Computer Science and Engineering
현 재 동신대학교 융합정보보안학과 교수

email : dhclub@dsu.ac.kr