情 報 保 護 學 會 誌
第22卷 第5號, 2012. 8

제어시스템 네트워크 보안기술 동향

윤 정 한*, 김 우 년*, 서 정 택*

요 약

제어시스템에 대한 사이버테러는 사회적, 경제적으로 큰 혼란을 발생시킬 수 있기 때문에 최근 제어시스템은 사이버테러의 제 1목표로 부각되고 있다. 이에 발맞추어 제어시스템 보안을 위한 연구 및 제품 출시가 많이 이루어지고 있다. 특히 제어시스템 가용성에 영향을 주지 않을 수 있는 제어시스템 네트워크 보안기술이 그 중심에 있다고 하겠다. 본 논문에서는 제어시스템 네트워크 보안에 대한 연구 및 제품의 동향을 살펴본다. 그리고 앞으로 제어시스템 네트워크 보안기술 연구 시 필요한 사항들을 짚어본다.

Ⅰ. 서 론

최근 사이버 공격의 목적과 주체가 변하고 있다. 그동안 사이버 공격의 주요 목적이 금전적 이득이었다면 최근 주요 사이버 공격은 정치적 목적으로 이용되고 있다. 사이버 공격의 주체 또한 개인이 아닌 특정 단체 및 국가 단위로 거대해지고 있다.

제어시스템은 일반 공장에서부터 교통, 발전, 전력, 항공 등의 국가기반시설까지 우리 생활 전 영역에서 사용되고 있다. 제어시스템에 대한 사이버테러는 사회적, 경제적으로 큰 혼란을 일으킬 수 있기 때문에 제어시스템은 사이버공격의 제 1목표로 부각되고 있다.

최근 들어 등장한 제어시스템을 타겟으로 한 Stuxnet, Duqu, Night dragon, Flame과 같은 악성코드들은 이러한 경향을 잘 보여주고 있다. 또한 카스퍼스키랩이 선정한 “최고 악성프로그램 15선”[1]에 Stuxnet(2010년), Duqu(2011년), Flame(2012년)이 포함되기도 하였다.

제어시스템은 정보의 기밀성을 최우선으로 하는 일반 IT 시스템과 달리 가용성 유지가 가장 우선시되는 시스템이다. 그러므로 보안을 위해 가용성을 저해할 수 있는 소프트웨어를 제어기기에 설치하기는 현실적으로 매우 어렵다.

네트워크 보안기술은 제어시스템에 직접 설치되어 운영되지 않으므로 가용성 저하를 최소화할 수 있기 때문에 제어시스템 보안에 적합하다. 따라서 제어시스템 보안을 위한 네트워크 보안기술에 대한 많은 연구와 제품 개발이 진행 중이다.

본 논문에서는 제어시스템 네트워크 보안기술에 대한 동향을 제어시스템 보안 제품을 중심으로 알아본다. 그리고 제어시스템 네트워크 보안기술 개발이 앞으로 지향해야 하는 방향에 대해 제안하고자 한다.

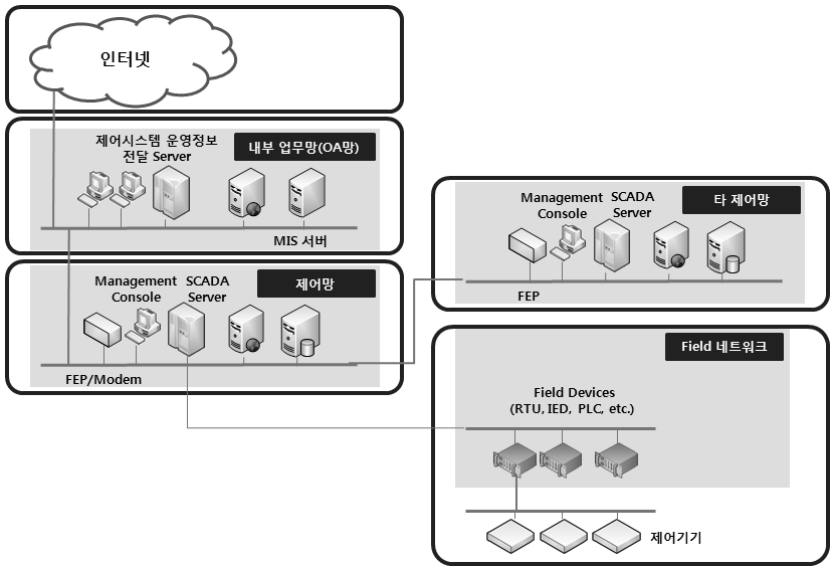
본 논문의 구성은 다음과 같다. 2장에서는 일반적인 제어시스템 네트워크 구조를 소개하고, 3장에서는 여기서 일어날 수 있는 보안위협을 정리한다. 4장에서는 제어시스템 네트워크 보안을 위한 제품들을 알아보고, 5장에서 앞으로 제어시스템 네트워크 보안기술 연구 시 고려해야 하는 사항들을 제시한다. 마지막으로 6장에서 결론을 내린다.

Ⅱ. 제어시스템 네트워크 구조

제어시스템은 하나의 독립된 제어망으로 운영되기도 한다. 하지만 제어기기들이 물리적으로 멀리 떨어져 있거나 제어시스템의 기능 단위로 제어망이 나뉠 경우 제어망들이 서로 네트워크로 연결되기도 한다. 필요에 따라 내부 업무망과 연동되어 운영되기도 한다. [그림 1]은 일반적인 제어시스템 네트워크 구조를 나타낸 것이다.

하나의 제어망 내에는 여러 가지 제어기기들이 존재한다. 각 제어기기들은 사용되는 제어망에 따라 수행하는 역할이 조금씩 다를 수 있다. 제어망에서 생성한 정

* ETRI 부설연구소 (dolgam, wnkim, seojt@ensec.re.kr)



〔그림 1〕 일반적인 제어시스템 네트워크 구성

보를 내부 업무망에서 모니터링 하여 비즈니스 업무에 활용할 수 있다. 이 때 제어망에 대한 보안관제 시스템이 내부 업무망에 존재하기도 한다.

Ⅲ. 제어시스템 네트워크 보안위협

여기서는 제어시스템 네트워크 구조에서 제어시스템 네트워크를 통해 발생 가능한 보안위협을 구분해 보았다.

〔T1〕 **보안정책 관리** : 내부 업무망 및 외부기관과의 연계, 제어망 내 시스템 간 통신 등 많은 연계 접점 및 시스템이 운영되고 있지만 이에 따른 보안정책을 수립하지 않거나 관리가 잘 되지 않는 곳이 많다.

〔T2〕 **제어망 간 연동** : 제어시스템은 다른 망과 분리하여 운영하는 것이 원칙이다. 그러나 현재 많은 제어시스템은 내부 업무망 및 외부기관과 물리적으로 연결되어 데이터를 송수신하고 있으며, 네트워크 연계구간에 정보보호시스템을 운영하고 있다 하더라고 정보보호시스템 설정 부주의에 의해 비인가 접근이 가능할 수도 있다.

〔T3〕 **제어망 내부 사이버침해 전이** : 제어시스템은 단일망이 아닌 다수의 서브넷(Subnet)과 중앙 네트워크로 구성되는 경우가 많다. 따라서, 제어망 내부의 한 시스템에서 발생한 장애나 침해가 전체 제어시스템으로 전이될 위험이 있다. 또한, 한 부분에 대한 제어 권한을 가지는 운영요원이 다른 부분도 제어할 수 있는 내부자에 의한 위협도 상존한다.

〔T4〕 **제어명령 및 감시정보 위변조** : 제어망까지 침입한 해커 또는 악의적 내부자는 제어시스템의 제어명령, 감시정보를 위·변조하여 물리적·경제적 큰 피해를 입히고, 사회적 혼란을 야기할 수 있다. 널리 사용되는 Modbus 등과 같은 제어 프로토콜은 보안에 대한 인식이 낮았던 시기에 설계되어 패킷 위·변조 공격에 매우 취약하다.

〔T5〕 **제어시스템 취약점** : 많은 경우, 사이버 침해는 네트워크 장비 및 시스템의 원격접속 서비스, 응용프로그램의 취약점을 이용하여 이루어진다.

〔T6〕 **취약한 인증 시스템** : 제어시스템은 긴급 상황에 신속히 대응하기 위해 인증 절차를 사용하지 않는 경우가 많다. 또한 인증을 위해 비밀번호를 사용하는 경우에도 제어 소프트웨어에 하드코딩 되어 있거나 현장 관리자들이 쉽게 기억할 수 있도록 기관명, 단순 숫자 조합, 장비명 등 취약한 비밀번호를 사용하는 경우가 많다.

〔T7〕 **서비스 거부 공격에 취약** : 임베디드 장비를 포함한 제어시스템은 한정된 자원에 의해 서비스 거부 공격에 취약하다.

Ⅳ. 제어시스템 네트워크 보안제품 동향

이 장에서는 제어시스템 네트워크 보안을 위해 개발된 제품들에 대해 알아본다. [표 1]은 각 보안제품들이

해결하고자 하는 보안위협들을 나타낸다.

〔표 1〕 보안제품이 해결하고자 하는 보안위협

보안제품 분류	관련된 보안위협
제어시스템 방화벽	T2, T4, T5, T6, T7
일방향 자료전달 장치	T2
침입탐지 시스템	T3, T4, T5, T6, T7
보안제품 중앙 관리	T1

4.1 제어시스템 방화벽

제어시스템 방화벽은 IT 기반 방화벽과 크게 다르지 않다. 제어시스템을 위해 제어프로토콜(Modbus, DNP, ICCP 등)을 지원하며, 해당 프로토콜에 대해 방화벽 정책을 프로토콜 스펙 수준에서 적용할 수 있도록 해 준다.

이들을 활용하여 제어망 간 연동(T2), 트래픽 위변조(T4), 서비스 접근 제한(T5), 패치되지 않은 취약점 공격 트래픽 또는 허가되지 않은 서비스 제한(T6), 외부망에서의 서비스 거부 공격 탐지(T7)및 차단이 가능하다.

관련 제품으로 Secure Computing社의 Secure Firewall[2], Plantdata technologies社의 patriot SCADA[3], Bayshore networks社의 SCADA Firewall[4] 등이 있다.

4.2 일방향 자료전달 장치

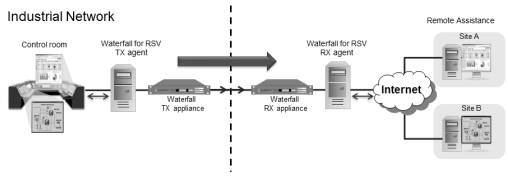
방화벽은 관리자가 설정을 잘못하는 경우 등 외부에서 내부로의 침투가 가능한 경우가 발생할 수 있다.

이러한 방화벽의 문제점을 보안하기 위한 일방향 자료전달 장치는 네트워크 트래픽이 한 방향으로만 전달될 수 있도록 만든 네트워크 보안장치이다.

악성코드가 업무망에서 제어망으로 전파되는 것은 막으면서 제어망의 정보를 업무망에서 사용할 수 있도록 하기 위해 일방향 자료전달 장치가 제어망 연계 구간에 도입되어 사용되고 있다(T2).

일방향 자료전달 기술은 물리적인 일방향 자료전달 기술과 공유 스토리지를 이용한 일방향 자료전달 기술로 나누어진다.

물리적인 일방향 자료전달 기술은 일방향 네트워크 장치를 이용하여 역방향의 물리적 경로를 제거하여 네트워크를 분리하는 기술이다. 물리적인 일방향 자료전달 기술은 Owl Technologies社(미국)의 “Dual Diode”[5], Waterfall社(이스라엘)의 “Unidirectional Security Gateway”[6]와 Fort Fox社(네덜란드)의 “Data Diode”[7], Tenix Datagate Inc社(호주)의 “Data Transfer, IL-DDD”[8]의 제품과 같이 일방향 자료전달 기능, 일방향 자료수신 기능이 각각 분리된 네트워크 카드 혹은 네트워크 장치를 제공한다.

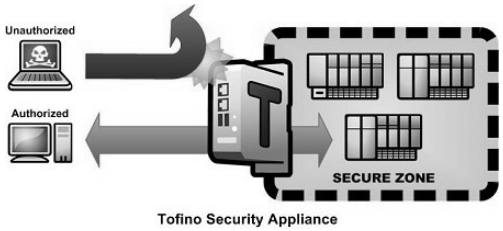


〔그림 2〕 Waterfall社의 Unidirectional Security Gateway 구성도

공유 스토리지를 이용한 일방향 자료전달 기술은 공유 스토리지의 쓰기 기능과 읽기 기능 제한을 이용한 기술이다. 대표적인 제품으로 Hitachi社(일본)의 “HRX (Hitachi RapidXchange)[9]”와 SQI 소프트社(대한민국)의 “ssbridge[10]” 등이 있다.

4.3 침입탐지 시스템

침입탐지 시스템은 망 간 연계구간 뿐 아니라 내부망에 대한 감시(T3)를 포함한다. 트래픽 감시라는 입장에서는 방화벽과 기술영역이 겹치기도 한다.



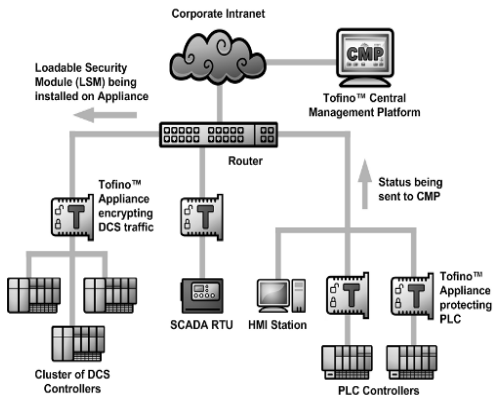
〔그림 3〕 Tofino社의 Tofino Security Appliance

제어시스템을 위한 침입탐지 시스템에 관한 연구는 제어시스템에 허용된 제어명령의 특성 등을 스펙으로 작성하고, 해당 스펙이 지켜지는지 감시하는 형태로 진행되고 있다[11][12][13]. 이러한 스펙은 제어기기 간의 통신에 있어 각 기기들의 권한을 표현할 수 있어 인증의 효과가 있다. 대표적인 제품으로 Tofino社의 Tofino Security Appliance[14], Innominate社의 mGuard 시리

즈[15]가 있다. 그 외 Cisco社의 CGR2010[16] 라우터는 제어프로토콜을 지원하는 IPS 기능을 제공한다.

4.4 보안제품들의 중앙 관리

제어시스템 보안제품들 중에는 네트워크에 설치된 전체 보안 솔루션들을 중앙에서 관리할 수 있도록 한다. 이러한 중앙관리는 일관된 보안정책 적용 및 유지보수의 편의성(T1)을 제공한다.



〔그림 4〕 Tofino Security Solution

침입탐지 시스템에서 언급한 Tofino社 Innominate社도 각각 전체 보안솔루션[17][18]을 제공하고 모두 중앙관리시스템을 포함하고 있다.

Ⅴ. 제어시스템 네트워크 보안기술 개발시 제안사항

앞서 살펴 본 보안기술 제품들은 제어시스템 네트워크 보안위협에 대해서 [표 1]과 같이 대응하고 있으나, 제어시스템 보안을 위해서는 이외에도 추가적으로 고려할 사항들이 있다. 이들 제품의 기술방향을 정리하고, 향후 제어시스템 네트워크 보안기술 개발 및 적용을 위해서 필요한 사항들을 정리해보면 다음과 같다.

5.1 Whitelist 기반 보안감시

제어시스템과 관련된 보안 취약점이 계속 발견되고 있다. 제로데이 취약점을 이용한 공격, 내부자에 의한 공격 등 특정 제어시스템을 목표로 한 사이버공격을 탐지하기에는 기존 공격 시그니처를 탐지하는 Blacklist 기반 감시는 한계를 나타내고 있다. 이에 제어시스템의 정상적인 특성을 Whitelist로 나타내고 이를 기반으로 한 보안감시가 더욱 효율적일 수 있다.

Whitelist 기반 보안감시에 있어 가장 핵심은 보호하고자 하는 제어시스템의 특성을 정확히 White -list로 작성하는 것이다. 이를 위해서는 제어시스템의 특성을 잘 나타낼 수 있는 Whitelist 모델 개발이 필수적이다. 또한 하나의 제어시스템은 그와 관련된 정보가 너무나 방대하여 사람이 모든 Whitelist를 정확히 작성하는 것은 현실적으로 불가능한 경우가 많다. 그러므로 Whitelist 모델을 기반으로 제어시스템을 위한 Whitelist 구축지원방안에 대한 연구도 필요하다.

5.2 보안정책 반영 및 관리

사실상 제어시스템 공격 경로의 많은 부분은 관리상의 실수로 인한 경우가 대부분이라 할 수 있다. 이로 인한 피해를 줄이기 위해서는 보안정책 변경 시 해당 사항을 신속히 모든 보안제품에 반영할 수 있는 방안이 필요하다.

하나의 제어시스템에서 사용하는 보안제품은 여러 개가 될 수 있다. 제어시스템을 위한 보안정책이 일관되게 모든 보안기기에 적용할 수 있는 방안을 고려해야 한다.

5.3 추후 분석을 위한 보안로그 생성 및 관리

모든 사이버공격을 실시간으로 막거나 감지하지 못할 가능성은 존재한다. APT(advanced persistent threat) 공격과 같이 장기간 동안의 공격일 경우 수개월 또는 수 년 간의 추이를 분석해야 할 수도 있다. 실시간으로 공격을 탐지하는 것만큼이나 이미 공격을 당했는지 아닌지를 파악할 수 있는가도 중요한 사항이다.

이를 위해 보호 대상 제어시스템의 운영에 대한 분석이 가능하도록 구체적인 정보가 담긴 보안로그를 생성하고 관리할 필요가 있다. 그러나 일반적으로 제어시스템은 제한된 성능과 저장용량을 지니고 있어, 이러한 한계를 극복할 수 있는 제어시스템에서의 보안로그 생성과 관리에 대한 연구가 필요하다.

5.4 제어망과 보안관제망의 분리

시스템 관리 기능 및 보안 기능은 시스템 서비스와 분리하여 운영되어야 한다. 분리 운영되지 않을 경우 시스템 서비스 권한을 획득한 비인가자는 시스템 관리 기능 및 보안 기능의 권한까지 획득 할 수 있다.

보안관제는 지속적으로 많은 정보를 활용하게 될 것이다. 앞에서 제안한 보안로그 생성 및 관리를 생각해 보더라도 대량의 보안로그가 로그서버 또는 보안관제시스템으로 전송될 필요가 있다. 보안로그는 제어기기 간의 트래픽이 증가함에 따라 비례해서 증가할 가능성이 높다. 이 때 보안로그 자체가 제어망 트래픽양의 많은 부분을 차지하면서 제어망 성능에 악영향을 끼칠 위험이 존재한다.

그러므로 보안제품을 개발함에 있어 보안관제망을 제어망과 분리하여 운영할 수 있도록 설계하는 것이 필요하다. 이러한 보안관제망의 분리는 보안제품 및 보안관제망 자체가 제어시스템 사이버공격의 경로로 활용되는 것도 방지하는데 기여할 것으로 판단된다.

Ⅵ. 결 론

본 논문에서는 제어시스템 네트워크 보안기술 동향을 제어시스템 네트워크 보안을 위한 제품 위주로 알아보았다. 그리고 각 제품들의 기술방향을 바탕으로 앞으로 제어시스템 보안기술 연구에 있어 나아갈 방향을 제시하였다.

참고문헌

[1] http://www.etnews.com/news/computing/security/2615591_1477.html.

[2] Secure Firewall, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1107.pdf.

[3] patriotSCADA, http://www.controlglobal.com/whitepapers/wp_001_SCADApollet.pdf.

[4] SCADA Firewall, http://www.bayshorenetworks.com/inc/pdf/SingleKeyIE_Data_Sheet.pdf.

[5] Dual Diode, http://www.owlctl.com

[6] Waterfall SCADA Monitoring Enabler, http://waterfallsecurity.com.

[7] Data Diode, http://datadiode.eu/home

[8] IL-DDD, http://www.tenix.com

[9] HRX-AOSP, http://www.hds.com/kr/products/storage-system-universal-storage-platformvm.html?_p=V.

[10] ssBridge, http://www.sqisoft.com/product/ssbridge

[11] I. Nai Fovino, A. Carcano, T. Murel, A. Trombetta, M. Masera, “Modbus/DNP3 State-based Intrusion Detection System”, 24th IEEE International Conference on Advanced Information Networking and Applications, April 2010.

[12] A. Carcano, I. Nai Fovino, M. Masera, “Modbus/DNP3 State-based Filtering System”, 2010 IEEE International Symposium on Industrial Electronics, July 2010.

[13] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, “Using Model-based Intrusion Detection for SCADA Networks”, SCADA Security Scientific Symposium, 2007.

[14] Tofino Security Appliance, http://www.tofinosecurity.com/products/tofino-security-appliance.

[15] mGuard, http://www.innominate.com/en/products.

[16] CGR2010, http://www.cisco.com/en/US/prod/collateral/routers/ps10967/ps10977/data_sheet_c78_593509.html.

[17] Tofino Security Solution, http://www.tofinosecurity.com/products/overview.

[18] Innominate Industrial Security Solution, http://www.innominate.com/en/solutions/industrial-network-security.

〈著者紹介〉

사 진

윤 정 한 (Jeong-Han Yun)
정회원

2001년 2월: KAIST 전산학과 졸업
2003년 2월: KAIST 전산학과 석사
2011년 2월: KAIST 전산학과 박사
2011년 3월~현재: ETRI 부설연구소 연구원
<관심분야> 프로그램 분석, 제어시스템 네트워크 침입탐지

사 진

김 우 년 (Woon-Nyon Kim)
정회원

1996년 2월: 안동대학교 컴퓨터공학과 졸업
1998년 2월: 경북대학교 컴퓨터과학과 석사
2000년 2월: 경북대학교 컴퓨터과학과 박사수료
2000년 3월~2003년 12월: (주)니츠 선임연구원
2003년 12월~현재: ETRI 부설연구소 선임연구원/과제책임
<관심분야> 정보보호, 제어시스템 보안

사 진

서 정 택 (Jung-Taek Seo)
종신회원

1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학과 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학과 박사
2000년 11월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안연구실장
<관심분야> 스마트그리드시스템 및 통신보안, 제어시스템 보안, 취약성 분석평가, DDoS 공격탐지 및 대응