ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 20-02-43
298

j.inst.Korean.electr.electron.eng.Vol.24,No.2,669~672,june 2020
http://dx.doi.org/10.7471/ikeee.2020.24.2.669

사이버물리시스템에 대한 사이버공격 경호위협 분석 - 지능형건물관리시스템을 중심으로 -

Analysis on Presidential Security Threat of Cyber Physical System by Cyber Attack Focusing Intelligent Building System

최 준 성*, 이 삼 열*★

Junesung Choi*, Sam Youl Lee*★

Abstract

In this paper, we analyzed the characteristics of cyber attacks and major threat scenarios that could occur around intelligent building management Systems(IBS) by cyber attack security threats against cyber physics systems. Generally determined that lowering the likelihood of aggression against predictable threats would be a more realistic approach to attack response. The countermeasures against this need to be applied to multi-layered defense systems, and three alternatives were proposed: preliminary cyber safety diagnosis for protection targets and the establishment of mobile security control systems.

요 약

본 논문에서는 사이버물리시스템에 대한 사이버공격 경호위협 중 지능형건물관리시스템(IBS)을 중심으로 발생할 수 있는 사이버공격의 특성과 주요 위협 시나리오를 분석했다. 분석한 결과 일반적으로 예측이 가능한 위협에 대해 공격의 성공 가능성을 낮추는 것이 현실적인 공격의 대응방법이 되는 것으로 판단하였고, 구체적인 대응방안으로는 다계층 방어시스템의 적용과 보호대상 시스템에 대한 사이버안전진단 사전점검, 이동식 보안관제 시스템과 같은 방안들을 제시하였다.

Key words : CPS, IBS, Cyber-Security, Detection, Prevention

Ⅰ. 서론

기존의 일반적인 사이버공격들은 주로 정보의 탈취나 파괴만을 목적으로 하였고[1-5], 피해의 범위가 사이버 공간으로 한정되어 사회적 영향이 제한적으로 평가되었다[1, 3]. 그러나 네트워크를 통해 물리시스템이 사이버시스템에 연결되어 상호작용을 하는 범위가 확대되었다[3, 6-10]. 이런 과정에서 사이버공격에 인한 피해가 현실 세계의 물리적 공간에 확장되 직접적이고 실체적 피해로 전환되어 사회적 영향이 증대되고 있다[6-10]. 경호위협들에 대한 대응 측면에서 전통적인 경호위협은 물리적 무기에 의한 위협이었으나 최근 사우디 드론 테러 사례는 미래경호위협의 변화를 예고하게 되었다. 본 논문에서는 미래경호위협진단의 일환으로 사이버물리시스템에 대한 사이버공격 경호위협 중

* Ph.D, Professor, Yonsei University
★ Corresponding author
E-mail : samyoul@yonsei.ac.kr Tel : +82-2-2123-2958
Manuscript received May, 31. 2020; revised Jun. 14, 2020; Accepted Jun. 22, 2020.

지능형건물관리(IBS)에서 발생할 수 있는 사이버 공격의 특성과 시나리오를 분석하고 대응방안을 모색한다.

II. 사이버 물리시스템의 현황

1. 사이버물리시스템

사이버물리시스템은 실제 물리적 장치(센서, 구동기, 로봇) 등을 정보통신 기반 제어기기와 연결시킨 통합체계이며[6], 물리시스템의 상태를 관찰하고, 연산-제어-작동으로 운영되는 정보-물리 융합체계이다[6, 7]. 사이버물리시스템을 분류해보면, 산업 제어시스템에는 발전과 생산 설비 등으로 사용되는 제어시스템 등이 있다. 무인이동체에는 자율주행차, 선박, 무인기과 이를 통제하기 위한 시스템 등이 있다. 스마트 그리드에는 전력망, 수도망, 가스망 등의 사회기반 공급 제어망 등이 있다. 군용시스템에는 방공시스템, 지휘통제시스템, 전투체계시스템, 무인기와 무인기 통제시스템 등이 있다.

문헌별로 표현이나 분류가 다를 수도 있으나[6-9], 사이버물리시스템의 계층을 분류 해보면 그림 1과 같이 물리계층-네트워크계층-응용계층의 3계층으로 구성할 수 있다.

사이버물리시스템은 가용성과 실시간 반응성을 중시하는 반면, 기밀성과 무결성 같은 보안성 확보와 준수에는 상대적으로 관심과 적용이 적은 편이다[6, 7]. 사이버물리시스템의 제어, 센서, 네트웍에는 전용통신프로토콜이나 전용장비가 적용된 경우가 많았으며, 이러한 사이버물리시스템은 현재 표준화, 성능평가, 사고예방 등에서 미흡하다. 특히 90년대 이전에 제작된 노후한 전용장비와 통신프로토콜 등이 현재까지 사용되는 경우도 있다[6-9].

2. 사이버물리시스템에 대한 사이버위협

사이버물리시스템에 대한 사이버위협은 2000년 이후에 전세계적으로 발생하고 있는 것으로 알려지고 있다. 2007년 시리아 군방공망의 무력화에 사용된 시니어슈터공격은 레이더 센서의 신호를 역으로 활용하여 방공망과 지휘통제망에 악성코드를 침투시켜 정보의 조작을 통해 방공망의 전투 불능 상황을 만들어낸 것으로 알려져 있다. 또한 2010년 이란 원전에 대한 스턱스넷 사건과 2011~2012년의 미군, 이스라엘 군 정찰드론에 대한 하이재킹

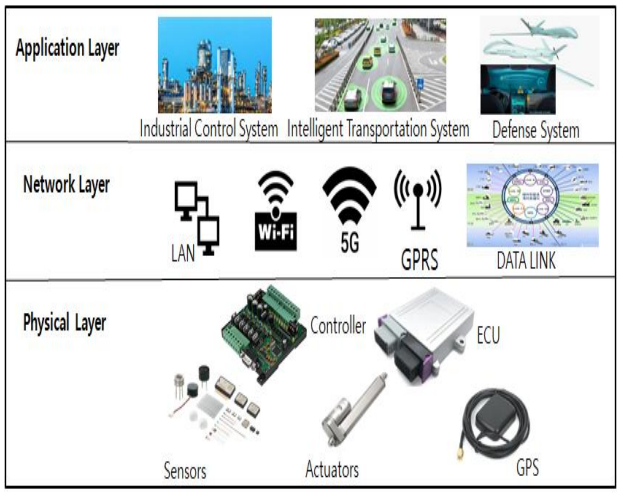

Fig. 1. Cyber Physical Systems Layer.
그림 1. 사이버물리시스템 구성 계층

사건은 사이버물리시스템에 대한 사이버위협의 실체화와 위험성이 일반에도 널리 인식되었다[3-5].

III. 대상 시스템의 분석

1. IBS의 현황과 특성

지능형 건물관리시스템 IBS(Intelligent Building System) 또는 BAS(Building Automation System)은 건물의 에너지 관리효율을 비롯하여 주요제어대상 기기인 공조설비(HVAC), 엘리베이터, 에스컬레이터 등의 이동설비, 통신 및 보안설비, 전기시설 등으로 구성된다. 건물관리시스템은 망분리 형태로 운영하는 것이 가능하지만, 일반 인터넷망에 노출되어 있는 경우도 있다. 대상시스템은 보안업데이트 또는 보안관제 등의 관리 대상으로 인지되고 있지 않는 경향이 있다. 그러나 경호목적의 사전점검은 시설에 국한되는 경우가 많아 지능형 건물관리시스템이나 이와 연계된 장비에 대한 진단 절차나 방법론이 명확하지 않다.

2. 발생 가능한 사이버 공격 유형 분석

사이버물리시스템에 특성화 공격유형은 부채널 공격과 사이버물리시스템 내부논리기반 정밀공격의 2가지라고 볼 수 있다. 그러나 이러한 2가지 공격유형은 공격자 입장에서도 실행하기가 어렵기 때문에 일반적으로 예측 가능한 위협에 대해 공격가능성을 먼저 대응하는 것이 현실적인 선택이 된다. 공격대상 사이버물리시스템의 물리계층-네트워크계층-응용계층에 대해 계층별로 발생 가능한

사이버공격의 유형을 분류하여 표 1과 같이 정리하였다. 여기에 분류한 공격유형은 사이버물리시스템에 공통적으로 적용 가능한 분류이다.

Table 1. Cyber-Phisical cal Systems Attack Types.
표 1. 사이버물리시스템에 대한 공격 유형

Cyber Threat	Security Factor	Application	Network	Physical
Key Deception Attack	Confidentiality	-	√	-
Data Deception Attack		-	√	√
Sub-Channel Attack		-	√	√
CPS Internal Logic Precision Attack	Integrity	√	√	√
Malicious code execution attack		√	-	-
SW Vulnerabilities Exploitation		√	-	-
Spoofing		-	√	√
Data Fake Modulation Attack		-	√	√
Replay Attack		-	√	√
Denial of Service Attack	Availability	-	√	√

3. 예상 위협 시나리오

테러조직은 ○○컨벤션센터에서 개최예정인 정부○○기념행사 중 행사장 혼란을 야기하고, 대피과정에서 주요인사 공격을 계획 중이다. 주요 침투예상 경로는 센서 망 및 통신망에 대한 원격 침투, 통신망에 대한 서비스거부공격, IBS의 시스템악성코드 유입이며, 악성코드는 버퍼오버플로우 등의 동적 불안정성을 활용하여 IBS에 침투한다. 테러조직은 사이버공격으로 건물관리시스템의 제어 권한을 획득하기 위하여 공격대상 IBS에 시스템악성코드를 유입시키고 IBS의 권한을 획득하였고, 이를 통하여 출입통제기기 및 CCTV 무력화, 이동설비 가동 권한을 획득한다. 그리고 건물의 이동설비, 통신설비, 건물의 소등 및 정전과 공조기 미작동 등으로 혼란을 발생시킨다. 이런 과정에서 예상되는 주요 경호위협은 건물 내의 공조 기능을 조작하고, 물리적으로 가스설비와 전기설비에서 화재 등을 발생시킨 다음 경비망과 이동제어 등을 통제하고 화재경보와 화재방화벽을 통해 경호 병력과 경호 대상을 분리하여 경호 병력의 집결을 제한시키고 경호 대상에 대해 위해를 가하는 위협이 발생할 수 있다.

4. 대응방안

지능형 건물관리시스템(IBS)에 대한 사이버-경호위협을 진단하고 예상 위협 시나리오를 예상한 결과 IBS는 평상 시 방어시스템의 구성과 적용이 필요하다. 방어시스템은 기본적으로 사이버물리시스템의 물리계층-네트워크계층-응용계층의 3계층에 대해서 다계층 심층방어의 개념 적용이 필요하다. 기존 사이버물리시스템은 보안을 위한 방어시스템이 구성되어 있지 않은 경우가 많으며, 이에 대한 기본적인 대응은 다계층 방어시스템의 적용이다. 기본적인 대응이 이루어지지 않은 시스템은 취약하기 때문이다. 다음의 그림 2는 다계층 방어시스템의 탐지와 이에 따른 예방 통제 방안(공격차단)의 기본적인 구성을 보였다. 각 계층별로 침입을 탐지하고 공격시도를 차단하는 다계층 방어는 사이버위협 공격의 경제성을 낮추는 현실적인 대안이 될 수 있다.

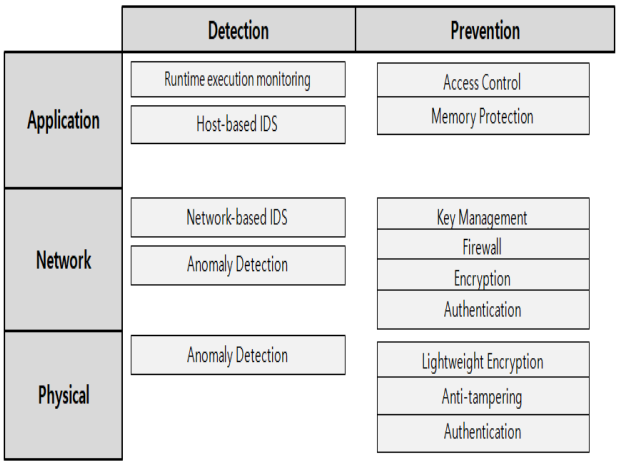

Fig. 2. Detection and Prevention of Cyber Attacks on Cyber Physical Systems.
그림 2. 사이버물리시스템의 공격 탐지와 차단

한편 대상 건물의 IBS 시스템에 대해 사전에 사이버안전진단을 하여 안전성이 확보된 시스템인지 사이버물리시스템에 의한 위험이 있는 시스템인지에 대한 사전점검과 검토가 필요하다. 한편으로 해당 시스템의 점검 결과를 보완하고, 발생 가능 사이버 경호 위협의 대응과 관리를 위한 이동식 보안관제 시스템 구축하여 적용하는 것이 필요하다. 보호대상 지능형 건물관리시스템(IBS)에 대한 사전 사이버안전진단의 방법론은 기존 사이버안전진단 방법론과 스마트빌딩 사이버안전진단에 대한 방법

론을 참고하여 적용할 수 있다. 사이버-경호위협대응을 위한 이동식 보안관제 시스템 구축을 별도의 규모가 있는 보안관제 시설이나 설비로 오해하기도 하는데 그런 의미가 아니라, 여기서 의미하는 이동식 보안관제 시스템은 보호대상 시설에 대해 네트워크 원격제어나 최소한의 네트워크 및 보안장비를 전개하고 이를 보호대상 시설의 IBS에 접속하여 보안관제할 수 있는 약식의 보안관제 체계 적용을 의미한다.

Ⅳ. 결론

사이버물리시스템에 대한 사이버공격의 경호위협 중에서 지능형건물관리(IBS)을 중심으로 발생할 수 있는 사이버공격의 특성과 주요 위협 시나리오를 분석했다. 분석한 결과 일반적으로 예측 가능한 위협에 대해 공격 성공가능성과 공격의 경제성을 낮추는 것이 현실적인 대응방법이 되는 것으로 판단되며, 이를 위해서는 다계층 방어시스템의 적용이 필요하며, 보호대상에 대한 사전 사이버안전진단과 이동식 보안관제 시스템의 구축이 필요하다.

References

[1] Jeffrey Carr, Inside Cyber Warfare : Mapping the Cyber Underworld, O Relly, 2009.

[2] Richard Clarke, Cyber War : The Next Threat to National Security and What to Do About, 2011.

[3] Junesung Choi, “C4ISR Systems IDS Performance Enhancing Method,” *Convergence security journal,* vol.12, no.4, pp.57-69, 2012.

[4] Junesung Choi, “The Analysis of the Malware Trend and the Prediction on the Defense Service and Industry,” *Convergence security journal,* vol.12, no.4, pp.97-108, 2012.

[5] Junesung Choi, “Evaluation Method Using Analytic Hierarchy Process for C4I SW Secure Coding Rule Selection,” *The Journal of Korea Information and Communications Society.* vol.38C, no.8, pp.651-662, 2013.
DOI: 10.7840/kics.2013.38C.8.651

[6] Raj Rajkumar, Dionisio de Niz, Mark Klein, “Cyber-Physical Systems,” *Addison-Wesley Professional,* 2017.

[7] Pascal Ackerman, Industrial Cybersecurity : Efficiently secure critical infrastructure systems, *Packt Publishing*, 2017.

[8] Abdulmalik Humayed, “Cyber physical systems security A survey,” *IEEE Internet of Things Journal,* 2017. DOI: 10.1109/JIOT.2017.2703172

[9] Yosef Ashibani, “Cyber physical systems security : Analysis,” *challenges and solutions. Computers & Security Journal.* 2017.
DOI: 10.1109/ACC.2013.6580348

[10] Murat Fiskiran, “Runtime execution monitoring (REM) to detect and prevent malicious code execution,” *IEEE International Conference on Computer Design 2004 Proceedings,* 2004.
DOI: 10.1109/ICCD.2004.1347961