Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 4 pp. 669-676, 2017

https://doi.org/10.5762/KAIS.2017.18.4.669
ISSN 1975-4701 / eISSN 2288-4688

BAS의 보안 특성 및 취약점에 관한 연구

최연석
호서대학교 컴퓨터정보공학부

A Study on security characteristics and vulnerabilities of BAS(Building Automation System)

Yeon-Suk Choi
Department of Computer Engineering, Hoseo University

요 약 최근 정보 보안의 중요성으로 인하여 신규 빌딩은 물론 기존 빌딩에서도 사이버 공격에 대한 대비책으로 보안 취약점 분석, 정보 보호 기술 및 시스템이 도입되는 추세이며, 초고층 건축물에 대한 정보 보안 연구들도 이루어지고 있다. 그러나 일반적인 IT 시스템의 관점 및 보안 정책에 따라 보안 시스템 도입과 연구들이 이루어지다 보니, 빌딩의 기반 시설에 대한 고려가 미비한 편이다. 특히, 빌딩 기반 시설인 BAS는 일반적인 IT 시스템과 달리 폐쇄적 시스템이지만 개방형 기능들을 수용하는 독특한 구조적 특징을 가지고 있다. 빌딩 보안 정책을 수립할 때 이러한 시스템 구조와 기능에 대한 이해가 부족하면 BAS에 대한 정보 보안 정책이 미진하게 되고 이로 인해 빌딩 전체 구성 요소들이 BAS를 통한 악의적인 사이버 공격에 노출될 가능성이 커진다. 본 논문은 공급 업체별로 상이한 BAS 구조를 3단계 레벨로 통합 분류한 구조 참고 모델을 제시하였고, 레벨별로 정보 보안 특성 및 취약점을 도출하였다. 본 연구를 통해 도출된 BAS 구조와 레벨별 보안 취약점 및 특성들은 BAS 특징을 반영한 보안 정책 수립과 빌딩의 안전 관리 능력 향상에 기여할 것으로 사료된다.

Abstract Recently, due to the importance of information security, security vulnerability analysis and various information protection technologies and security systems are being introduced as a countermeasure against cyber-attacks in new as well as existing buildings, and information security studies on high-rise buildings are also being conducted. However, security system introduction and research are generally performed from the viewpoint of general IT systems and security policies, so there is little consideration of the infrastructure of the building. In particular, the BAS or building infrastructure, is a closed system, unlike typical IT systems, but has unique structural features that accommodate open functions. Insufficient understanding of these system structures and functions when establishing a building security policy makes the information security policies for the BAS vulnerable and increases the likelihood that all of the components of the building will be exposed to malicious cyber-attacks via the BAS. In this paper, we propose an architecture reference model that integrates three different levels of BAS structure (from?) different vendors. The architectures derived from this study and the security characteristics and vulnerabilities at each level will contribute to the establishment of security policies that reflect the characteristics of the BAS and the improvement of the safety management of buildings.

Keywords : BAS, cyber attack, information security, security characteristic, security policy, vulnerability

1. 서론

최근 건물의 추세를 보면 대형화, 고층화 및 IT 기술로 최첨단 기능을 구현한 스마트 빌딩이 많이 건설되고 있다. 이러한 스마트 빌딩들은 건축, 통신, 사무 자동화, 빌딩 자동화 등의 4가지 시스템을 유기적으로 통합하여

*Corresponding Author : Yeon-Suk Choi (Hoseo Univ.)
Tel: +82-41-540-5977 email: changwah@hoseo.edu
Received November 17, 2016 Revised (1st February 1, 2017, 2nd February 27, 2017, 3rd March 28, 2017, 4th March 29, 2017)
Accepted April 7, 2017 Published April 30, 2017

첨단 서비스 기능을 제공함으로써 경제성, 효율성, 쾌적성, 기능성, 신뢰성, 안전성을 추구하고 있다. 특히 스마트 빌딩의 BAS(Building Automated System, 빌딩 자동화 시스템은 크게 전력, 조명 및 기계설비 3가지로 분류되고, 이들은 건물 운영 관리를 위한 인건비와 사용 에너지 절감, 건물 수명 증가, 쾌적한 근무 환경을 제공하는데 핵심적인 구실을 하고 있다.

또한, 다양한 최신 IT 기술들이 건축물의 차별화를 위해 도입되고 있는데, 이러한 IT 기술들은 건물의 기술적, 대외 이미지 향상에 많은 기여를 하고 있다. 그러나 건물 자체 및 내부 시설물들에 대한 물리적인 보안 정책은 수립되어 있지만, 건물 운영 부분에 적용되는 제어설비와 같은 기기들에 대해서는 기기 특성을 반영한 정보 보안 정책이 수립되지 않은 상태에서 IT 기술들이 적용되다 보니, 이러한 기기들에 대한 외부 공격자의 사이버 공격 노출 가능성이 커지고 있다. 만약, 건물을 제어하는 시스템에 악의적인 사이버 공격이 발생하면, 이로 인해 건물의 운영 환경(빛, 온도, 안전 등)의 급격한 변화가 발생하게 되고, 이러한 급격한 환경 변화는 건물 내 있는 사람들에게 큰 혼란을 야기할 수 있다.

최근 적용되고 있는 사물인터넷(IoT) 기기 및 근거리 무선 통신 장비들과 복수의 건물을 통합하여 효율적인 시설 및 에너지를 관리하고자 적용되는 군 관리 시스템 기술들도 건물의 사이버 공격에 대한 가능성을 더욱 높이고 있는 요인으로 작용하고 있다[1].

정보시스템의 안전을 위해 시작된 정보 보안 연구는 정보시스템과 다른 특징을 가지는 산업 제어 시스템 및 IT 기술이 접목된 스마트 자동차 분야까지 그 영역을 확대하고 있다[2-5].

건물 특히 초고층 건물에 대한 보안 및 안전 관련 연구는 초고층 건물의 화재 및 테러와 같은 재난재해에 대한 위험요소 도출 및 방지 부분에 관한 연구들[6-9]과 IT 기술이 융합된 스마트 빌딩에 대한 물리적인 보안 및 사이버 공격에 관한 연구들이 진행돼 왔다[1, 10-11].

그러나 기존 건물에 대한 정보 보안 연구들은 BAS를 지칭하는 건물의 제어 설비에 대한 구성 요소 및 시스템에 대한 이해 없이 일반적인 IT 정보 보안 정책을 적용한 연구가 주를 이루다 보니, BAS에 대한 세부적인 보안 특성 및 취약점 연구가 미진한 상태이다.

이에 무형적인 정보 객체의 처리를 위한 IT 시스템과는 달리 유형적인 객체의 정보 처리를 위한 BAS는 정보 객체 이용에 근본적인 차이를 가지고 있기 때문에 건물의 보안 및 안전을 강화하기 위해서 BAS에 적합한 보안 특성 및 침해 요소 도출 연구에 대한 필요성이 도출됐다.

본 논문은 건물의 기반 시설인 BAS에 대한 시스템 구조 분석을 통해 BAS에 적합한 보안 특성 및 취약점을 도출하였고 그에 대한 대책을 주제로 삼아, 2장에서 다양한 BAS 구성요소들을 표준화된 구조로 표현되도록 구성된 BAS 구조 참고 모델에 대한 도출 배경과 구성요소들의 세부 내용을 기술하였고, 3장에는 도출한 BAS 구조의 레벨(level)별 보안 특성과 그에 따른 취약점을 그리고 4장에는 도출한 취약점을 고려한 보안 대책을 제시하였다.

2. BAS 구조(BAS Architecture)

2.1 개요

일반적으로 건물에서 운영되는 BAS는 공급 업체별로 시스템의 경제성 확보, 효율성 증대 및 차별화를 위해 독자적인 관리 체계 및 구성 요소들을 가지고 있다. BAS는 다양한 구조로 표현될 수 있는데, 제어 구조로 분류해보면, 집중형 제어 구조, 분산형 제어 구조로 나눌 수 있으며, 최근에는 IT 기술의 발전에 따라 표준화된 프로토콜 수용 및 최신 IT 기술 수용이 이루어지는 개방형 시스템 구조(Open System Architecture)로 진화하고 있다.

분산된 BAS 시스템 구성 요소들에 대해 수직적인 기능 관점으로 분류하면 프로세스 레벨, 단말 제어 레벨, 전송 레벨, 중앙 처리 맨 머신 레벨, 관리 계획 레벨의 5개 계층을 가지는 수직 계층 구조로 표현할 수 있으며, 물리적인 요소보다는 논리적인 기능을 중심으로 하는 수평적인 기능 관점 분류를 적용하면 BAS 구성요소들은 검출 요소, 조직 요소, 처리 요소, 신호 요소, 맨 머신(Human Machine Interface) 요소의 구조로 일반화하여 표현될 수 있다[12].

2.2 표준화된 BAS 구조 참고 모델

본 연구에서는 적용되는 기술, 제품 및 솔루션의 조합에 따라 다르게 표현될 수 있는 BAS 구성 요소들을 기능적으로 분류한 후 동치류 집합을 구성하고, 집합 요소들을 계층으로 가지는 트리를 보안 취약점 연구를 위한

BAS 구조 참고 모델로 모델링 하였다.

다양한 BAS 주요 제품과 시스템의 구조들을 표준적인 구성 체계로 전환하기 위해 본 연구에서는 다양한 프로토콜을 가진 BAS 제품 간의 호환성 확보를 위해 개발된 국제 표준 ISO 16484 문서에 정의된 BACnet(Building Automation Control Network) 프로토콜 체계 및 Field, Automation, Management Level의 3개 Level로 표준화된 시스템 개념[13][14]을 기반으로 하였다. 개념화된 시스템 구조 위에 BAS를 구성하는 각종 요소를 기능 관점으로 구분하여 아래와 같이 3개의 동치류 집합을 생성하였다.

- Level 1 동치류: 센서 및 액추에이터 레벨
- Level 2 동치류: 현장기기 제어 레벨
- Level 3 동치류: 통합 및 관리 레벨

본 연구에서 제시하는 BAS 구조는 상기 3개 Level을 계층적으로 구성한 트리 구조이며, 조명, 전력 및 기계설비 시스템의 구성 요소들을 포함하는 계통도를 Fig. 1에 도시하였다.

2.3 Level 별 구성 요소 특징

2.3.1 Level 1 : 센서 및 액추에이터 레벨

제어 장치와 연결되어 설비 제어, 환경 감시를 수행하며, 공조/열원/위생 장비의 제어 및 감시를 위한 조작기(댐퍼, 밸브), 감지기(온도, 습도, 압력, 유량, 풍량) 들에 대하여 현장 상황에 따른 다양한 신호 방식을 적용하여 상호 연결을 한다. Level 1에서 사용되는 연결 방식은 hard wiring과 같은 전기적 신호 연결 방식과 시리얼 통신, 유무선 네트워크 등 현장 설치 환경 및 기계에 따라 제어 장치와 다양한 형태의 연결 구성을 하고 있다. 최근에는 표준화 및 개방화된 프로토콜 기반의 센서 네트워크 및 IoT 기반 센서 등을 구비함으로써 현장 기기 레벨에서의 네트워크화, 자동화, 지능화가 진행되고 있다.

2.3.2 Level 2 : 현장기기 제어 레벨

현장 제어 장치인 DDC(Direct Digital Controller)는 현장(기계실, 공조실)에 설치돼, 공조 /열원 /위생 설비를 직접 제어하며, 장비별로 각종 운전 프로그램을 탑재 및 운영하는 기능이 있어 현장 제어 설비라 한다. 이러한 DDC는 독립 운영(stand alone) 기능을 주 기능으로 가짐으로써 단독 DDC만으로도 각종 설비 제어 및 에너지 최적화 운전 프로그램 및 제어 로직을 수행하며, 중앙 감시 장치와의 통신 단락이나 DDC 간 통신 두절 시에도 연결된 DDC들은 상호 통신을 계속하여 데이터 통신 기능을 수행하는 분산처리 기능도 가지고 있다. 또한. 제어 대상 설비에 대한 데이터 관리 및 백업 기능을 가짐으로써 정전 등 비상시 데이터를 백업하고 복구 시 연속 운

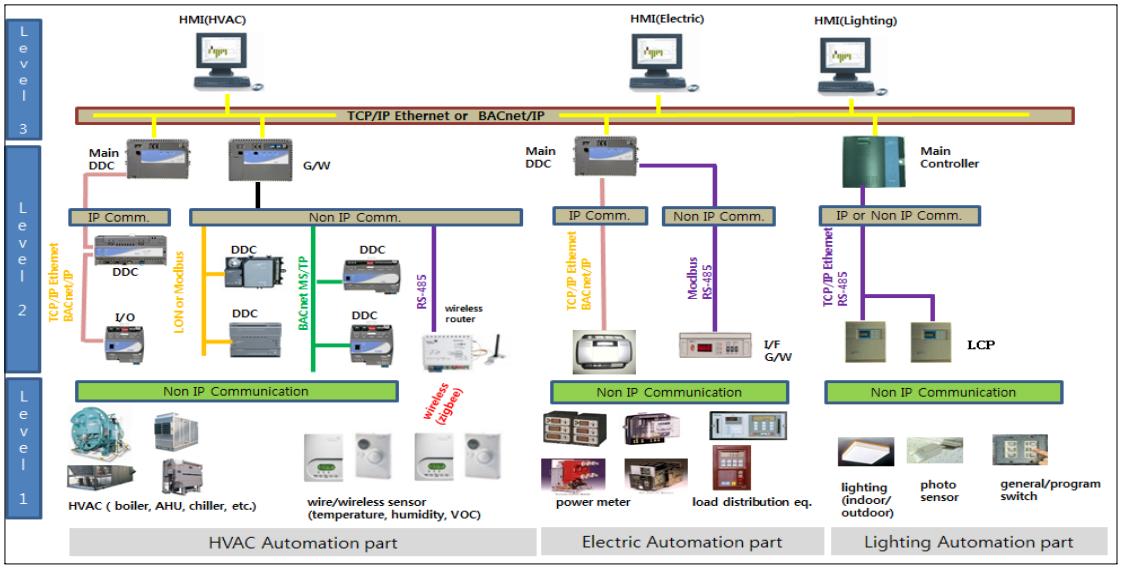

Fig. 1. Generalized 3-tier BAS architecture

전 기능 수행도 가능하다. 또한, DDC 자체에 내장된 주요 제어 프로그램은 공조/열원/위생 설비의 운영 시나리오에 따른 자동 운전 프로그램(쾌적한 실내를 위한 댐퍼/밸브 제어 등), 자체 에너지 절약 프로그램(최적 기동/정지 제어, 절전 운전 제어, 엔탈피 제어, 이산화탄소 제어, 공실 제어, 각종 스케줄 제어, 수요전력 피크 부하제어 연동, 정전/복전 연동 제어) 등이 탑재돼 지능화된 제어 서비스를 제공하고 있다. 이렇듯 DDC는 초기 단순 기기 제어 수준 단계에서 통신 네트워크 기능이 탑재되는 보편화 단계를 지나 인터넷/웹 기술이 탑재되어 자체적으로 외부와 연결되는 단계까지 진화하고 있다.

2.3.3 Level 3 : 통합 및 관리 레벨

Level 3 는 Level 1과 Level 2에 속한 기기들에 대한 통합 관리 기능을 담당하며, 통합 관리를 위해서는 빌딩 설비들의 제어 및 환경·상태 정보를 운전자 및 시설 관리자가 인지하기 쉽도록 Graphic User Interface(GUI)를 가진 HMI(Human Machine Interface)를 사용하고 있다.

빌딩용 제어설비 기기의 모니터링과 제어 기능들을 HMI에 부여하기 위해 각 제조사는 다양한 프로그래밍 언어(C, C++,Java, Basic, C#등)를 활용하여 HMI S/W를 구현하여 제공한다. 그러나 컴퓨터에 대한 전문적인 지식이 적은 빌딩설비 운전원이 상태 감시 및 제어를 쉽게 할 수 있도록 구현된 HMI들이 BAS 제조업체들 자신만의 시스템에만 적용되도록 또는 자사의 프로토콜만 지원하게 되어있어서, 타 시스템들과의 연동 및 같은 회사의 다른 제품들과도 호환성을 가지기 어려웠다. 최근에는 이러한 특성에 따른 시장 확대 걸림돌을 제거하기 위해 통합 및 관리 레벨의 통신방식에는 BACnet 및 표준 인터넷 통신 규약들이 적극적으로 적용되고 있으며, 이를 통해 BAS 원격 감시나 이기종 제어 설비 간 상호 연동이 원활해져 최적화된 빌딩 제어 및 군 관리 감시 서비스가 가능해졌다[12][13].

3. Level 별 보안 특성과 취약점 도출

IT 시스템은 “무형적인 정보 객체를 처리하기 위해 유형적인 사물 객체를 이용”하지만 BAS는 “유형적인 사물 객체를 처리하기 위해 무형적인 정보 객체를 이용”하는 근본적인 차이가 존재하기 때문에, 기존 IT 시스템을 위한 보안 기술이 BAS의 보안을 위한 필요조건은 될 수 있지만, 충분조건은 되지 못한다. 본 장에서는 빌딩 에너지 및 시설관리의 기반 시설을 구성하고 있는 BAS의 보안 특성에 대한 충분한 이해를 얻기 위하여 BAS 구조의 Level 별 보안 특성과 취약점을 도출하였다.

3.1 Level 1 보안 특성과 취약점

3.1.1 Level 1 보안 특성

BAS 구성요소 중 특히, Level 1 위치인 현장에서 사용되는 기기 간의 통신은 전기적 신호를 주고받는 접점 방식 및 시리얼 통신 방식을 전통적으로 사용하고 있는데, 특히 시리얼 기반의 신호들은 기본적으로 어떠한 보안도 적용되어있지 않는 평문 데이터를 많이 사용하는 특성이 있으며 구성 요소에 대한 위협 요소는 다음과 같다.

- 현장 제어기에 연결된 유무선 센서, 액추에이터는 사용자와 방문자에게 쉽게 노출되어 물리적 접속을 통한 전기적 신호 변경에 취약하며, 아날로그, 디지털 입출력 신호 조작, 시리얼 통신 신호 조작이 가능
- 최근 무선 네트워크의 적용으로 전파에 대한 보안 취약 사항이 공통으로 적용되며, IoT 기기들과 같이 배터리를 주전원으로 사용하는 무선 소형 기기들은 트래픽 발생 시 배터리가 단시간에 방전되어 쉽게 기능이 정지
- 무선 메시 네트워크를 통신 토폴로지로 사용하는 WSN(Wireless Sensor Network)에서는 무선 노드의 신규 추가 및 기존 노드의 고장 등에 따라 라우팅 테이블 변경이 필수적이며 이를 위한 각 노드 간 통신으로 인한 트래픽이 증가됨
- 위장된 무선 노드의 공격 시 전체 네트워크 기능 저하가 유발됨

이러한 BAS 현장 기기들의 보안 특성을 고려하여 도출된 Level 1의 보안 취약점은 다음과 같다.

3.1.2 Level 1 보안 취약점

- 운영 환경 부분 위협: 긴 거리의 배선 및 배관으로 인한 물리적 또는 전기적인 공격에 취약
- 설치 환경 부분 위협: 단자대에 신호 연결 정보가 표시되어 있어 연결 정보 유출에 취약
- 통신 패킷 스니핑(sniffing)위협: 전기적 신호 취득 및 패킷 스니핑을 통한 평문 데이터 구조, 네트워크 키 등 중요 정보 유출에 취약

- 통신 패킷 인젝션(injection) 및 무선채널 고갈 위협: data playback, data fuzzing을 통한 Dos 공격과 무선 채널 선점을 통한 채널 자원 고갈 공격에 취약
- WSN 노드 라우팅 테이블 공격 및 배터리 소모 위협: 메시 네트워크를 지원하는 센서 망의 라우팅 테이블 전송 방해 공격, 빈번한 송·수신 트래픽 발생 유도 및 무선 라우팅 변경을 위한 트래픽 발생 유도에 취약

3.2 Level 2 보안 특성과 취약점

3.2.1 Level 2 보안 특성

Level 2의 핵심 구성요소인 DDC는 센서로부터 입력을 받는 입력 기능, 로직을 수행하는 로직 기능, 액추에이터로 출력을 내보내는 출력 기능의 3가지 기능 모듈을 이용하여 현장 기기들을 제어 및 감시하는 특징을 가진다. 또한, 통신 네트워크를 이용하는 구성 특징과 부여된 기능을 수행하기 위해 DDC는 소프트웨어 프로그래밍이 요구되는 특징을 가지고 있다.

대부분의 네트워킹 기능을 가진 DDC의 제어 설비 신호 흐름은 Fig. 2에서 도시된 사례와 같이 현장에 설치된 각종 계측기에서 감지한 신호가 DDC I/O 모듈로 인입된다. 이들 전송된 신호는 DDC의 로직 모듈에서 프로그래밍 된 절차에 따라 연산 되며, 결과는 통신 네트워크를 통해 관리자가 사용하는 컴퓨터인 HMI 시스템으로 전달되고, HMI 시스템에서 GUI 형태로 디스플레이 된다. 또한, 빌딩 설비 관리자가 조작한 신호는 이와 역순으로 다시 DDC 제어기를 거쳐 Level 1의 현장 기기인 액추에이터에 전달되어지는 양방향 통신 특성이 있다.

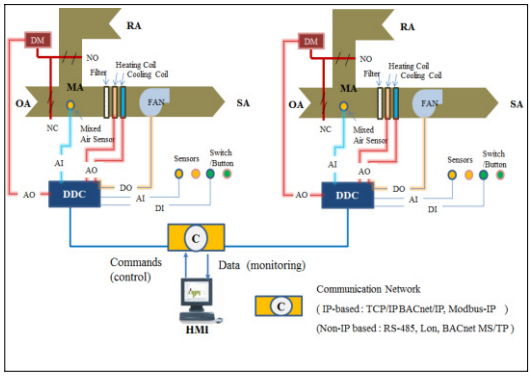

Fig. 2. Typical configuration of multiple DDC

지금까지 DDC는 제조사 별로 하드웨어와 소프트웨어가 규격화돼 왔지만, 점차 개방형·표준 플랫폼을 적용하는 형태로 발전되고 있다. 그러나 개방화 또는 표준화를 위해 사용된 프로토콜이나 인터페이스 등의 기술 자료는 인터넷상에 공개되거나 비교적 저렴하게 배포되어 누구나 쉽게 입수할 수 있는 경우가 많으므로, 그러한 기술정보는 공격 방법을 짜내는 힌트가 될 수 있다. 즉, 완전히 같은 코드로 만들어진 모듈을 내장한 제어시스템이 다수 존재한다는 것은 공격자가 그 코드에 대한 공격 도구를 별도로 만들어 내지 않고도 같은 도구를 사용해 다수의 제어시스템을 표적으로 하는 공격이 가능하게 되는 것을 의미한다.

한정된 메모리 공간과 상대적으로 저속의 CPU를 사용하는 DDC는 외부 공격자가 프로그램의 특성을 파악하여 관제점 등 많은 데이터를 확보하게 되면 외부 및 원격에서 빌딩 내의 제어 시스템 오동작을 쉽게 유도할 수 있다. 또한, DDC의 통신 환경은 저속 무선 네트워크, 저속 시리얼 네트워크(RS-485, Lon, RS-232) 및 저속 이더넷(Ethernet) 등으로 이루어져 통신 속도에서 제약이 따르는데, 이러한 통신 환경은 다량의 통신 트래픽 공격에 쉽게 시스템의 기능이 정지된다는 취약점을 가지고 있다. 이러한 위협 요소들을 가지는 DDC의 보안 특성을 고려하여 도출된 Level 2의 보안 취약점은 다음과 같다.

3.2.2 Level 2에서의 보안 취약점

- 메모리 덤프 위협 : 동일 모델 기기의 프로그램 메모리 덤프를 통한 프로그램과 중요 데이터 추출에 취약
- Host interface를 이용한 MCU 덤프 위협 : 마이크로 컨트롤러(MCU)에서 제공되는 host interface (JTAG, I2C, SPI, etc.)를 통한 프로그램 덤프를 통한 공격에 취약
- 서비스 거부(DoS) 공격 위협 : 현장 제어기기를 대상으로 한 통신 패킷 반복 전송 및 인위적인 브로드캐스팅 패킷 발송을 통한 한정된 자원의 임베디드 시스템 기능 정지 유도 공격에 취약
- 허위 존재 및 허위 부재 위협 : 관제 시스템으로 위장하여 제어 명령을 발송함으로써 오동작을 유도하는 유형과 전기적 신호를 취득하는 패킷 스니핑을 통한 평문 데이터 구조, 네트워크 키 등 주요 정보 유출에 취약

- 원격 악성 펌웨어 업데이트 위협 : 원격 펌웨어 업데이트 기능을 사용하여 현장 제어기에 악성 펌웨어를 다운로드하는 공격에 취약

3.3 Level 3 보안 특성과 취약점

3.3.1 Level 3 보안 특성

Level 3의 주 구성요소인 HMI들은 HMI들 간 또는 하부 Level 2의 현장 제어 설비들과의 통신 신뢰성 확보 및 시스템 안전성을 유지하기 위하여 전용 네트워크로 구성되어 있으며, 한번 설치되면 가동을 중단하기 곤란한 특성 때문에 유지보수 과정에서의 시스템의 업그레이드마저 쉽지 않은 환경에서 운영되는 특성을 내재하고 있다. 이러한 환경은 매시간 출현하는 사이버 공격의 새로운 위협에도 불구하고 악성코드에 대비한 운영 소프트웨어의 패치가 거의 이루어지지 않고 있으며, 단순한 비밀번호의 변경에서부터 새로운 보안 소프트웨어 설치까지 보안성을 높이기 위한 추가적인 통제 적용이 곤란한 조건을 가지고 있으며, 이미 설치된 시스템에 새로운 소프트웨어 및 하드웨어를 추가할 경우 제어시스템을 제공하는 제조사로부터 시스템의 오작동 등 장애가 발생하면 유지 보수 지원을 받지 못할 가능성마저 존재하고 있어 보안에 매우 취약한 잠재적인 리스크를 내재하고 있다. 이러한 보안 특성을 고려하여 도출된 Level 3의 보안 취약점은 다음과 같다.

3.3.2 Level 3에서의 보안 취약점

- 건물 건축 당시 OS를 사용하며, OS 패치 나 보안 업그레이드 작업이 이루어지지 않고 있는 상황 (관리자의 IT 수준이 낮아 초기 설치된 버전을 그대로 사용)으로 보안 취약
- 무차별 대입 공격 : 무차별 공격을 이용한 관리자 권한(아이디 & 패스워드) 유출에 취약
- 시스템 운영자의 낮은 보안의식 수준 : 디폴트 패스워드 미변경 등 적절하지 못한 계정 관리로 정보 유출에 취약
- 스피어 피싱(spear phishing) 위협 : 관리자의 IT 수준이 낮아 보안 관리 의식이 부족할 때 공격 (웜이 첨부된 이메일을 생성하여 외부 연결 통로 제공 프로그램 생성 및 실행) 노출
- DB 및 웹 서버 취약점 공격 위협 : SQL injection 공격 또는 워터링 홀(watering hole) 공격에 취약
- 앱(App) 서비스 취약점 공격 위협 : 스마트 기기와의 연동을 위한 앱 서비스의 취약점 분석을 통한 공격에 취약
- 허위 존재 및 허위 부재 : 패킷 스니핑을 통한 평문/표준화 데이터 구조, 네트워크 키 등 중요정보 유출에 취약
- 통신 패킷 Playback 및 인젝션 위협: data playback, 허위 부재/허위 존재 정보 공격 및 data fuzzing을 통한 DoS 공격에 취약

4. 보안 대응책

본 장에서는 기업이 BAS를 정보 보안 대상으로 포함하여 정책을 수립할 때, BAS 특성에 따른 보안 취약점 연구결과를 고려하여 기존 대책에 추가되거나 확대 적용할 수 있는 대응책을 다음과 같이 3가지로 분류하여 응용 사례로 제시하였다.

4.1 보안 정책 강화 대책

◎ BAS 보안정책 수립

- BAS 네트워크와 구성 요소를 위한 보안 정책을 개발하여야 하며, 현재 도출된 레벨별 보안 특성, 취약점을 반영하여 주기적으로 점검하는 보안 운영 프로세스 수립
- BAS 관리자와 운영자의 보안 교육 강화 정책 수립 : 보안 교육을 통한 OS 패치, 보안 업그레이드 및 개인 계정 관리 강화

◎ 잘못된 의식의 전환

- 제어 시스템 및 프로토콜은 자체 프로토콜 기술 및 기반 제어 시스템이며 기존 제어 시스템 동작에 대한 공개 정보가 없었기 때문에 해커의 침입은 있을 수 없다는 의식을 BAS 시스템 개발 단계부터 전환함
- 도출된 레벨별 취약점을 시스템 기획 및 개발 시에 적극적으로 반영하는 시스템 개발 및 운영 정책을 수립

4.2 자원과 서비스에 대한 접근 제어 대책

◎ BAS 네트워크 분리 운영

- 건물에 입주한 기업들이 사용하는 업무용 네트워크

(사내 망)와 제어 설비용 BAS 네트워크(BAS 망)를 분리하여 운영하도록 함

- BAS 망과 사내 망 사이에 연결에 대한 문서화 규칙과 최소한의 액세스 포인트 유지
- BAS와 빌딩 내 유·무선 LAN 사이의 통신방법은 서로 직접 통신하지 않도록 중간에 방화벽에 연결된 DMZ 네트워크를 설치하고 이를 경유하여 제한된 특정 통신만 이루어지도록 통제

◎ 침입탐지 및 악성 행위 탐지 시스템 운영

- 로그 파일의 정기적인 감시를 위한 침입탐지 시스템을 BAS 네트워크 혹은 BAS 운영 호스트에서 운영

4.3 레벨별 공격 가능성 완화 대책

◎ 공격 가능성 완화

- 레벨별로 도출된 보안 취약점이 이용될 수 없도록, 필터 설정, 특정 구성(배열)을 가진 서비스와 응용의 운영 등을 통하여 취약성에 대한 접근을 통제
- 물리적인 보안을 결합한 융합보안 구비 : 운영 환경 부분 위협 공격(긴 거리의 배선 및 배관으로 인한 물리적 또는 전기적인 공격)과 설치 환경 부분 위협 공격(단자대에 신호 연결 정보가 표시되어 있어 연결 정보 유출) 완화를 위한 통신실 출입보안 강화 및 패치 상태 감시가 가능한 배관 및 통합 배선 관리 시스템 운영
- 소프트웨어 취약성 갱신 및 패칭과 같은 핵심 보안 문제를 해결 : 소프트웨어 허점이 있는 곳에는 관리자가 적용할 수 있도록 공급자나 개발자로부터 완화 기법 받음

5. 결론

우리 주변에 생기고 있는 건축물들이 점점 대형화, 복합화 및 초고층화되면서, 빌딩의 안전 문제는 911테러의 경험으로 비추어 볼 때 빌딩 하나에서 그치는 문제가 아니라 빌딩 주변 지역 및 도시 전체에 영향을 미칠 수 있음을 알 수 있다.

본 논문에서는 대형 및 초고층화되는 현대 건물에 대해 체계적이고 강화된 보안 정책이 수립될 수 있도록, 건물의 기반 시설로 여러 구성요소가 혼합돼 적용되는 BAS를 기능적으로 분류한 후, BAS 구성 요소가 노드가 되는 3단계 Level의 트리 구조를 모델링 하였으며, Level 별로 BAS 특성을 반영하는 보안 취약점을 도출하였다.

건물 기반 시설로서 각종 제어 기기들로 구성된 BAS는 하나의 보안 제품, 보안 기술 또는 보안 솔루션으로 적절히 보호될 수 없다. 그러나 본 논문에서 도출한 레벨별 보안 취약점을 통한 공격 벡터의 철저한 이해가 반영된 정보 보안 정책을 수립한다면 기업들의 정보보안 강화에 크게 기여할 것으로 사료된다.

향후에는 건물의 출입통제, 소방 및 전관방송 시스템까지 보안 취약점 분석 대상을 세분화함으로써, 스마트 빌딩의 다양한 제어 설비들에 대한 보안 취약점 도출 및 대응 기술에 관한 심층 연구를 진행하고자 한다.

References

[1] Pramod E. F. Dribble, Raphael Imhof, Udo Drafz, “Cyber security in Smart Buildings: Preventing Vulnerability While Increasing Connectivity”, CABA Intelligent & Integrated Buildings Council(IIBC), 2015.

[2] Cheol-Won Lee, "Major Control Facilities Cyber Security Trends", NST, 2007.

[3] Sung-Mo Jung, Jae-gu Song, Tai-Hoon Kim, Yo-Hwan So, Seok-Soo Kim, “Design of Idle-time Measurement System for Data Spoofing Detection”, Journal of the Korea Academia-Industrial cooperation Society, Vol. 11, No. 1, pp. 151-158, 2010.
DOI: http://dx.doi.org/10.5762/KAIS.2010.11.1.151

[4] Young-Doo Kang, Kil-To Chong, "Development of Cyber Security Assessment Methodology for the Instrumentation & Control Systems in Nuclear Power Plants", Journal of the Korea Academia-Industrial cooperation Society, Vol. 11, No. 9, pp. 3451-3457, 2010.
DOI: http://dx.doi.org/10.5762/KAIS.2010.11.9.3451

[5] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, Oakland, CA, pp. 16–19, May 2010.
DOI: https://doi.org/10.1109/sp.2010.34

[6] Ministry of Public Safety and Security, “Report on the development of high-rise building safety management standard manual”, 2007.

[7] Man-Chul Choi, Byung-Suk Kim(2011),
“A Study on the general direction of Fire-Fighting Safety management in high-rise buildings”, Journal of the Korea Safety management & Science, Vol. 13, No. 2, pp. 67-75, 2011.

[8] Bin Sung, Yoon-Ho Lee ,"Review on Prior Evaluation

for Terrorism Risk of High-rise Buildings", Journal of KSSA, Vol. 36, pp. 293-316, 2013.

[9] Sang-Hwan Bae,"A study of vertical airflow and smoke control technique for high-rise building, Daerim Technical Review, pp. 89-95, Jun. 2013.

[10] IT Security Group, “Best Practices for Securing an Intelligent Building Management System”, Schneider Electric Buildings BU, Apr. 2011.

[11] David J. Brooks, “Intelligent buildings: an investigation into current and emerging security vulnerabilities in automated building systems using an applied defeat methodology“, The Proceedings of the 4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th – 7th Dec. 2011.

[12] Hong Won-Pyo, “Building Automation System”, The Proceedings of the Korean Institute of Illuminating and Electrical Installation Engineers, Vol. 12, No. 3, pp. 56-66, 1998.

[13] Wolfgang Kastner, Georg Neuschwandtner, Stefan Soucek and H. Michael Newman, “Communication Systems for Building Automation and Control”, Proceedings of the IEEE, June, Vol. 93, No. 6, pp. 1178-1203, 2005.
DOI: https://doi.org/10.1109/jproc.2005.849726

[14] Building Automation and Control Systems (BACS)－Part 2: Hardware, ISO Std. 16484-2, 2004.

최 연 석(Yeon-Suk Choi) **[정회원]**

- 1990년 2월 : 성균관대학교 기계공학과 (공학사)
- 1992년 2월 : KAIST 정밀공학과 (공학석사)
- 1992년 2월 ~ 1995년 8월 : 대우전자 연구소 주임연구원
- 2005년 9월 ~ 현재 : 호서대학교 컴퓨터정보공학부 정보보호학과 부교수

<관심분야>

MEMS, Smart Building, Indoor Wireless Location System, Sensor for Security