안전한 스마트빌딩 운영을 위한 내부자 패턴 모니터링 시스템 연구

김정호*, 정하규*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:kimpocjstk@naver.com
standard@ssu.ac.kr
mjun@ssu.ac.kr

Study on Insider Pattern Monitoring System for Secure Smart Building Operations

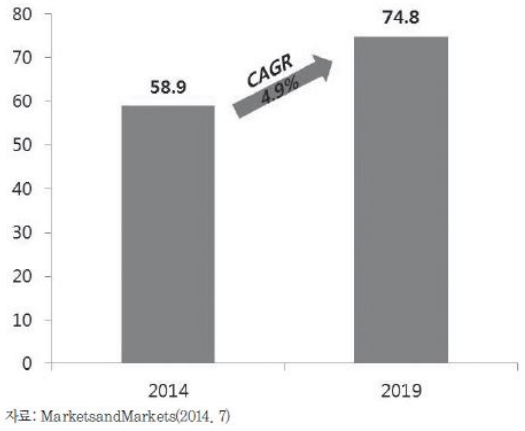
Jeong-Ho Kim*, Hague Chung*, Moon-Seog Jun*
*Dept of Computer Science & Engineering, Soongsil University

요 약

최근 사물인터넷(Internet of Things)의 발달로 인해 사물과 사물간의 통신을 이용해 사용자가 어느 곳에서나 집 또는 사무실 등의 장소의 정보를 얻을 수 있게 되었다. 하지만 IoT기기들을 스마트빌딩에 활용하는데 있어서 내부에서 공격이 발생했을 경우에 효과적으로 방어할 수 있는 방어체계가 갖추어져 있지 않아 위험하다는 점이 존재한다. 따라서 본 논문에서는 IoT 네트워크를 구축한 스마트빌딩에서 내부 사용자 접근에 대한 누적 정보를 바탕으로 스마트빌딩 내부에서 발생할 수 있는 불법적인 내부자 공격에 대하여 스마트빌딩을 안전하게 운영할 수 있는 내부자 패턴 모니터링 시스템을 제안한다.

1. 서론

최근 IoT의 발달로 인해 사물과 사물간의 통신을 이용하여 다양한 분야(스마트홈, 스마트빌딩 등)에서 사람이 그 장소에 있지 않아도 원하는 정보를 사물들의 통신을 통해 장소의 정보들을 제공받을 수 있게 되었다. 특히 스마트빌딩의 경우 IoT를 활용하여 정보 전달뿐 아니라 편리성/안정성/친환경성을 최적화하는 자동제어 시스템을 구축할 수 있게 되었다. 이에 따라 IoT 네트워크를 활용한 스마트빌딩은 편리하게 운용할 수 있다는 장점으로 인해 크게 각광받고 있다[1].



(그림 1) 스마트빌딩 시장 발전 전망[1]

이러한 IoT 네트워크를 활용하여 시스템을 구성하게 되면 건물 내부를 인력의 도움 없이 무인 방식으로도 효율적으로 관리할 수 있다는 장점은 있지만, 여전히 보안적인 면에서 '내부자 공격에는 취약하다'라는 문제점이 존재하기 때문에 이에 대한 내부자 공격에 대한 방어체계가 필요하다[2].

본 논문의 구성은 다음과 같다. 2장에서는 스마트빌딩 및 내부자 위협 그리고 이에 따른 접근 제어모델에 대해서 기술하고, 3장에서는 이러한 접근 제어모델을 활용하여 스마트빌딩을 안전하게 관리하는 방법을 제안한다. 4장에서는 결론을 맺는다.

2. 관련연구

2.1 스마트빌딩

스마트빌딩이란 과거에는 지능형 빌딩 시스템(IBS)으로도 불리며, 초기에는 오피스 자동화(OA), 빌딩자동화(BA), 통신(TC)과 건축 등의 기능이 융합된 빌딩을 의미했다. 하지만 현재에는 더 나아가 고도의 정보통신 기능과 더불어 건축, 통신, 사무자동화, 빌딩 자동화 등의 4가지 시스템을 유기적으로 통합하여 첨단 서비스 기능을 제공하고, 경제성, 효율성, 쾌적성, 기능성, 신뢰성, 안전성을 추구하는 첨단 정보 빌딩을 말한다.

※ 이 논문은 2016년도 중소기업청의 산학연구마을 지원사업의 지원을 받아 수행된 연구임.

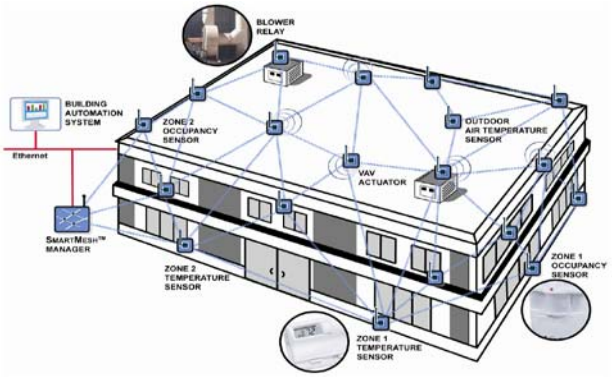
2.2 내부자 위협

내부자는 내부 네트워크를 통하여 내부 서버 또는 데이터 등의 정보통신 네트워크를 접근하는데 있어 합법적인 접근 권한을 가지고 언제든지 컴퓨터 및 네트워크의 구성, 프로그램, 데이터 등에 대한 내부 정보를 열람하거나 변경할 수 있는 고용인을 의미한다. 이는 정식 직원, 임시/계약직 직원, 계약자, 하청업자 등에 해당되는데, 이러한 내부자들이 자신의 경제적 이익이나 회사의 이직 등을 동기로 회사의 내부 정보시스템에 접근하여 악의적으로 행동을 하게 된다면, 외부자의 침입에 의한 공격보다 효과적으로 더 막심한 피해를 입게 될 수 있다. 내부자 침입에 대한 유형은 다음과 같은 세 분류로 설명할 수 있다[3].

- 개인의 이익을 위하여 기업의 중요한 기밀사항을 악의적으로 변경하거나 유출하는 경우
- 사업적 이득이나 외국 정부/조직에게 정보를 빼돌리기 위해 고객의 거래 및 개인 정보를 유출하는 경우
- 조직 내부의 네트워크, 시스템, 데이터 등을 기술적으로 정교하게 파괴하는 경우

최근에는 시스템보다는 데이터, 전자문서, 고객정보를 대상으로 내부 공격자 자신이 사용할 수 있는 권한을 이용해 데이터에 불법적으로 접근하는 사례가 점차적으로 늘어나고 있다. 또한, 내부 공격자는 접근이 가능한 객체간의 불법적으로 정보의 흐름을 발생시켜 중요한 정보를 유출시킬 수 있다. 내부자는 자신의 역할과 직무에 합법적인 접근권한을 이용하여 서버에 접속한 후 데이터를 파괴, 변경, 유출한다. 대부분 내부자의 시스템 접근 보안정책은 소속, 역할, 직책 등의 그룹별로 접근권한을 부여함으로써 내부자의 데이터에 대한 불법적인 정보 유출을 효과적으로 차단하지 못한다. 또한, 기존의 접근제어 모델도 역할, 직무, 역할-직무, 상황 등의 두 가지 이상의 구성요소로만 접근권한을 승인하고 있어 내부자에 대한 강력한 보안통제가 어렵다[4].

3. 제안



(그림 2) 제안하는 스마트빌딩 모니터링 시스템 구성도

위 그림은 IoT 네트워크를 활용하여 건물 내에 설치한 스마트빌딩 모니터링 시스템 구성도이다. 위와 같이 스마트빌딩의 각 구역에 설치된 IoT 센서들을 활용하여 네트워크를 구성해 내부에서 사용자들이 스마트빌딩을 이용하면서 발생하는 다양한 정보들을 수집하여 통합 관리센터로 전달하여 연결되어 있는 서버에 수집 정보들을 누적시켜 저장한다.

관리센터에서는 지속적으로 누적수집한 내부자 이용 정보들을 빅데이터화하여 내부자들의 시설 이용 관련 정보들을 나열하여 패턴화시킨다. 가공된 패턴화된 정보는 관리센터의 서버에 감시시스템에 주기적으로 업데이트하여 적용시킨다. 이를 활용하여 사전에 적용시킨 각각의 사용자들의 권한등급 정보를 통해 내부자의 패턴에 해당하는 권한등급과 대조를 통하여 지속적으로 내부자들이 스마트빌딩을 이용하는데 있어서 사용자에게 권한이 승인되어 있지만 평소와 다른 수상한 행동을 하지 않는지 감시를 통해 내부자 공격이 이루어지지 않는지 감시를 하게 된다. 만약 지속적으로 업데이트되는 가공된 정보와 다른 패턴의 내부자 접근에 대한 이상 징후가 발생하게 된다면 신속하게 불법적으로 발생하는 내부자 공격에 대응할 수 있도록 조치를 취하게 함으로써, 내부자의 공격에 대하여 방어한다.

4. 결론

스마트빌딩 관리에 대하여 지속적으로 업데이트가 이루어지는 저장된 내부자 패턴 정보를 통하여 안전하게 운영할 수 있으며, 만일의 사태에 대비하여 내부자 보안 취약점이 또한 관리 권한을 등급에 따라 부여함으로써 각각의 사무실에서 불법적인 내부자 공격이 발생한다고 해도 효과적으로 이를 인지하고 대처할 수 있다. 향후 새로운 방식으로 발생할 수 있는 내부자 공격패턴에 대하여 본 논문을 기반으로 추가적인 분석 및 연구를 통하여 예방하는 방안이 필요하다.

참고문헌

[1] 김은숙, “[전송통신] 스마트빌딩 구축 관련 표준화, TTA, 2011-18

[2] Jaykumar Vijayan, "스마트빌딩, 사물인터넷으로 보안 위협에 노출", ITworld, , May 2014

[3] 송지훈, “내부자 위협을 고려한 정보보호 대책 요구사항 분석 연구”, 한국인터넷정보학회 2010년도 학술발표대회, 2010

[4] David F. Ferraiolo and D. Richard Kuhn, Ramaswamy Chandramouli, Role-Based Access Control, Artech House, 2003.