스마트시티 보안 위협 분석 및 제로트러스트 기반 대응 전략 연구

강찬영[1], 이석준[2]
[1]가천대학교 스마트보안전공 학부생
[2]가천대학교 스마트보안전공 교수
1120cy@gachon.ac.kr junny@gachon.ac.kr

A Study of Security Threats and Zero Trust based Countermeasures in Smart Cities

ChanYoung Kang[1], Sokjoon Lee[2]
[1, 2]Dept. of Smart Security, Gachon University

요 약

21세기가 도래함에 따라 새로운 도시의 형태인 스마트시티는 다양한 기기들이 네트워크 상에 서로 연결되어 이용자에게 편리함을 제공한다. 하지만 사이버 공격 기법 또한 고도화되고 있다. 많은 IoT 기기들이 상호작용함에 따라 사이버 공격을 당하면 도시 전체가 피해를 입을 수 있다. 이에 따라 본 논문에서는 스마트시티에서 일어날 수 있는 보안 사고에 대해 분석하고 이를 대응하기 위한 제로트러스트 도입 전략에 대해 연구하고자 한다.

1. 서론

첨단 정보통신기술(ICT)을 이용해 도시 내의 다양한 문제를 해결하는 스마트시티는, 다양한 기기들이 네트워크 상에서 서로 연결되어 있고, 대량의 데이터를 수집하고 처리하는 과정에서 새로운 보안 문제가 발생할 수 있다. IoT 기기와 같은 네트워크 접점의 증가 등 다양한 공격 표면(Attack Surface)을 가지고 있으며, 도시 인프라와 직접 연결되어 있는 구조의 특성상 공격자가 시스템에 침투를 하면 도시 전체가 공격당할 수 있다.

따라서, 안전한 스마트시티 환경 구축을 위해서는 이에 대한 대비가 필수적이며, 2010년 J. Kindervag이 제안[1]한 제로트러스트(Zero Trust)는 대비 방안 중 하나로 고려할 수 있다. 제로트러스트는 접속 위치와 관계없이 모든 시스템과 기기를 신뢰할 수 없다는 가정하에 지속적인 인증을 통해 리소스에 대한 최소한의 접근 권한만 제공하는 보안 모델이다. 본 논문에서는 스마트시티에서 발생하는 보안 문제들을 살펴보고 이를 해결하기 위한 제로트러스트 기반 대응 전략에 대해서 제안하고자 한다.

2. 스마트시티에서 발생하는 보안 위협

2-1. IoT 취약점을 활용한 사이버 공격 및 해킹

스마트시티에서 활용되는 IoT 기기들은 제조사가 매우 다양하며, 모델마다 다른 보안 취약점을 가지고 있을 수 있다. 공격자들은 이 보안 취약점을 이용하여 IoT 기기·네트워크에 불법 침투한 후, 다양한 서비스와 인프라가 연결된 스마트시티로 공격을 확장할 수 있다. 만약, 랜섬웨어나 DDoS 공격 등으로 인한 장애가 발생하면 도시 전체의 기능에 영향을 미칠 가능성이 있다.

2-2. 개인정보 유출 및 오용

스마트시티는 다양한 센서나 IoT를 통하여 대량의 데이터를 생성·수집하고 분석·가공을 통해 사용자들에게 다양한 서비스를 제공한다. 그러나 이 과정에서 개인정보 유출 및 오용의 위험성이 존재하며, 사용자의 위치 정보나 건강상태 등 개인정보가 유출된다면 심각한 문제를 불러일으킬 수 있다.

2-3. 스마트시티에서 일어날 수 있는 사고

① 주요정보통신기반시설 랜섬웨어 공격

스마트도시법 제22조 등에 따르면 스마트도시기반시설 중 '스마트도시 통합운영센터'를 주요정보통신기반시설(Critical Information Infrastructure, CI)로 지정하도록 되어있다. 2021년 미국의 대표적 기반시설인 콜로니얼 파이프라인 회사는 가스와 기름을 운송하는 회사로 랜섬웨어 공격을 받아 시스템의 일부 기능이 마비되면서 가스와 기름 공급이 중단되는 사태가 발생했다[2].

② IoT 해킹 및 정보 유출

IoT 기술은 스마트시티에서 중요한 역할은 담당하고 있으며, 이에 따라 IoT 기술을 통한 해킹 및 정보 유출의 위험성 또한 높아지고 있다. 국내에서 최근 아파트의 월패드 중앙관리 서버와 아파트 세대에 설치된 월패드를 차례대로 해킹하여 권한을 얻는 방법으로 영상을 몰래 촬영한 후, 영상 일부를 유출하는 피해가 발생하였다[3].

③ 교통 분야

스마트시티에서의 교통 시스템으로 인한 교통마비는 가장 유력한 위협 시나리오 중 하나이다. 차량과 교통 시스템과의 메시지를 위·변조할 경우 교통 혼란을 초래하거나 인명피해까지 발생할 수 있다. 2017년 미국 캘리포니아에서는 지역 버스와 경전철을 운행하는 시스템이 랜섬웨어 공격을 당해 3천만 개의 파일이 삭제되었다[4]. 2018년 애틀랜타市는 '래번서스' 랜섬웨어 공격으로 교통 트래픽 시스템이 마비되어 지하철과 공항에서 혼란이 벌어지기도 하였다.

3. 제로트러스트 도입 전략

제로트러스트를 통하여 랜섬웨어 및 데이터 유출 공격에 대응하기 위한 방법은 <표 1>과 같다. 제로트러스트 보안 철학이 도입된다면, 공격자가 정상 사용자·기기의 인증 토큰을 훔쳤다 하더라도 접근 권한이 없는 리소스를 향해 횡적 이동하는 것을 막을 수 있으며, 정보유출 혹은 암호화를 위해 수많은 데이터를 접근하는 것을 실시간 감시를 통하여 이상 행위로 판단, 접근을 해제할 수 있다.

특히 데이터 유출의 경우 접속자의 물리적 위치 등 신뢰성을 확보할 만한 별도의 조치가 이루어지지 않으면 추가 인증을 요구하거나, 현재 세션에서 리소스 접근을 최소화함으로써 대응하는 것이 바람직하다.

4. 결론

본 논문은 스마트시티에서 발생할 수 있는 보안 위협과 사고에 대해 분석하고 이를 방지하기 위한 제로트러스트 모델을 검토하며, 이를 토대로 스마트시티의 보안 강화를 위한 방안을 제안하였다.

21세기 이후 정부의 스마트시티를 추진함에 따라 스마트시티의 보안이 더욱 중요해지고 있다. 제로트러스트의 적용을 통해 보안이 강화될 수 있으며 다양한 형태의 공격에 대해 현재 권한 이상의 추가적인 피해를 막을 수 있다는 장점이 있다.

그러나 제로트러스트는 모든 상황에서 최적의 모델은 아니며, 공격을 원천 차단하기 위한 철학이 아니라는 점은 유의해야 한다. 또한 제로트러스트 적용 과정에서의 과도한 정보 수집 및 제한은 개인의 사생활을 침해할 가능성이 있으므로, 앞으로 해결해 나가야 할 문제이다.

<표 1> 스마트시티 보안 사고사례 및 이에 대한 제로트러스트 기반 대응 전략

보안 사고 사례	보안 사고 유형	ZT 적용시 대응 방법
주요정보통신기반시설, 교통 분야	랜섬웨어	- Micro-Segmentation을 통해 서버 등 리소스들을 작은 구역으로 나누면, 다른 리소스에 대한 접근 권한이 없는 공격자가 네트워크를 통해 랜섬웨어를 다른 컴퓨터로 횡적 이동시키지 못하도록 하여 피해를 최소화 - 또한, 특정 서버의 모든 데이터에 접근 후 암호화 등 수정을 할 경우, 지속적인 감시를 통해 해당 행위를 이상 행위로 판단, 신뢰도를 낮추어 추가적인 데이터 접근 차단
IoT 해킹	데이터 유출	사용자에게는 강력하게 인증을 하며, 접속자의 물리적 위치, 네트워크 위치, 단말 상태 등 접속자 상황을 분석하여 충분히 신뢰하기 어려운 경우 추가 인증을 요구하거나, 리소스 접근을 최소화

5. Acknowledgement

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2022R1F1A1073211).

참고문헌

[1] J. Kindervag, Forrester. "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," 2010년 9월

[2] Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know", https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, 2022년 4월

[3] 경찰청, "월패드 해킹 사건 수사결과 발표", https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20221221091602934, 2022년 12월

[4] 양원모, "스마트시티에 닥칠 수 있는 보안 위협 6가지", https://www.boannews.com/media/view.asp?idx=79250, 2019년 5월