편집위원 : 유희정, 박용완(영남대)

무선통신기반 SCADA시스템 공격기법과 위협사례 및 연구 동향분석

김지훈, 이성원, 윤종희
영남대학교

요 약

국가 및 사회 기반 시설의 제어를 하는 컴퓨터 시스템을 SCADA(Supervisory Control And Data Acquisition)이라 한다. 대부분의 SCADA 시스템은 과거 폐쇄망과 비공개 통신프로토콜을 사용하기 때문에 비교적 안전하다고 고려되어 시스템보안 및 침해사고 대응 강화는 등한시 되었던 것이 사실이다. 하지만 최근 발생되고 있는SCADA 시스템의 침해사고들은 SCADA 시스템들이 보안위협에 노출되어있음을 의미하며 통신기술이 발전함에 따라 무선통신을 사용하는 SCADA 시스템의 통신망을 통한 불법적인 접근경로는 더욱더 확대될 수 있다. SCADA 시스템은 국가 및 사회 기반 시설의 제어를 담당하는 시스템이기 때문에 침해사고 발생시 심각한 문제가 초래될 수 있기 때문에 관련 보안기술 및 정책 연구가 필요하다. 본고에서는 이를 위해 SCADA 시스템의 구조 및 발전 단계를 소개하여 전반적인 시스템 이해를 돕는다. 또한 무선통신 기반 SCADA 시스템의 공격 기법을 소개하고 최근 몇 년간 발생한 보안위협 사례와 관련 연구 동향을 분석한다.

Ⅰ. 서 론

산업제어시스템(Industrial Control System, ICS)은 산업 부문 및 제어 시스템을 다루는 전반적인 용어들을 포함하는 용어이며, 일반적으로 전기, 수도, 수송, 석유, 가스와 같은 주요 기반 시설을 제어하는 컴퓨터 시스템을 말한다.

본고에서 주로 다룰 SCADA(Supervisory Control And Data Acquisition) 시스템은 DCS(Distributed Control System)와 함께 대표적인 산업제어시스템의 종류로 포함되어 있으며 SCADA시스템은 데이터수집을 기반한 대규모 분산 된 기기 및 장치 따위를 제어 및 감시하는 시스템을 말하며 분산처리시스템 즉, DCS는 일반적으로 제어를 위해 상호 연결된 통신 프로토콜을 사용하여 비교적 근거리 내의 시스템을 제어한다. 하지만 현대에 들어 정보 통신 기술(Information & Communic0ation Technology, ICT)의 발전으로 인해 이 두 가지 대표적인 산업제어시스템들의 차이는 모호해졌다.

SCADA 시스템은 발전소, 배전, 공항, 방공 등 공공기관이나 사회기반시설 및 국가기반시설을 관리하기 때문에 다른 어느 시스템들보다 위협에 대한 보안을 강화해야 하며 침해사고에 즉각 대응할 수 있는 매뉴얼이 필요하다.

SCADA 시스템은 독립된 폐쇄망 환경과 공개되지 않은 프로토콜을 사용해 운용되기 때문에 보안위협이 부각되지 않을 뿐더러 이러한 특성 때문에 보안위협에 대한 대응책이 다소 등한시 되고 있다. 하지만 최근 국, 내외 SCADA 시스템에 대한 침해사고가 증가하고 있으며 2014년 한국수력원자력의 정보유출 사고는 대표적인 사례가 될 수 있다. 이러한 침해사고들로 인해 폐쇄된 내부망을 사용하는 SCADA시스템은 더 이상 안전하다고 맹신될 수 없는 시스템으로 고려 되고 있다.

더욱이 최근 통신기술의 발전 덕분에 유선통신이 아닌 무선통신기술이 적용된 SCADA 시스템이 등장하였으며 SCADA 시스템을 운용하는 기관들은 제어 시스템의 접근 효율성이나 제어 유연성 향상의 이유로 무선통신을 기반한 SCADA시스템 도입이 증가되고 있다.

하지만 대부분의 무선통신기반 SCADA 시스템들은 유, 무선통신을 모두 사용하여 운용되기 때문에 네트워크 및 통신프로토콜을 이용한 보안위협은 더욱더 취약하다고 할 수 있다.

본고에서는 무선통신을 기반한 SCADA시스템의 전반적인 보안위협에 대해서 다루고자 하며 이를 위해SCADA 시스템의 구조 및 발전 과정을 언급하고 국, 내외 SCADA 시스템 사고 사례와 관련 연구 동향을 소개하고자 한다.

Ⅱ. 본 론

1. SCADA시스템

1.1 SCADA 시스템의 구조

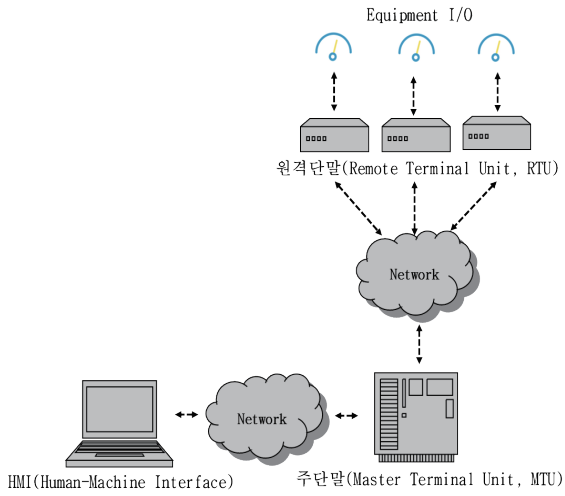

그림 1. SCADA 시스템 구조

〈그림 1〉과 같이 일반적인 SCADA 시스템은 데이터 수집 및 제어를 담당하는 주단말(Mater Terminal Unit, MTU), 데이터 전송을 담당하는 원격단말(Remote Terminal Unit, RTU), 그리고 HMI(Human-Machine Interface) 및 네트워크 등으로 구성된다[1].

MTU는 통신망을 통하여 RTU로부터 데이터를 수집하고 수집된 데이터를 바탕으로 전체 SCADA시스템 통신을 감시하고 제어한다. RTU는 SCADA 시스템의 센서 등과 같은 데이터 수집 장치들로부터 정보를 실시간으로 수집하고 MTU로 전송한다. HMI는 운용을 담당하고 있는 담당자와의 효율성 있는 커뮤니케이션을 위해 수집된 데이터를 텍스트 및 그래프 형식으로 시각화하여 표시하는 기능을 담당하고 있다.

SCADA 시스템의 데이터 및 감시제어는 다양한 네트워크를 통해 이루어지고 있으며 과거는 근거리통신망(Local Area Network, LAN) 이나 원거리통신망(Wide Area Network, WAN)을 기반한 Ethernet 유선망을 기초로 이루어지고 있었다면 최근에는 Bluetooth, Zigbee, GPS와 같은 무선통신과 같은 다양한 통신망을 이용하고 있다.

1.2 SCADA 시스템의 발전

과거 SCADA은 단순히 데이터를 표시하는 장치를 통해 정보를 수집하고 그를 바탕으로 시스템을 감시 및 제어하였다. 하지만 관련산업이 발전하고 함에 따라 세계적으로 SCADA시스템의 수요가 증가함에 따라 SCADA 시스템은 대형화 및 자동화되었다.

SCADA 시스템의 발전은 크게 1세대 모놀리식, 2세대 분산처리, 3세대 네트워크 순으로 발전해왔으며[2] 최근 통신기술의 발전으로 4세대 무선통신 및 클라우드 환경을 기반한 SCADA 시스템이 추가되어 발전되고 있다[3].

1.2.1 1세대 SCADA 시스템 : 모놀리식

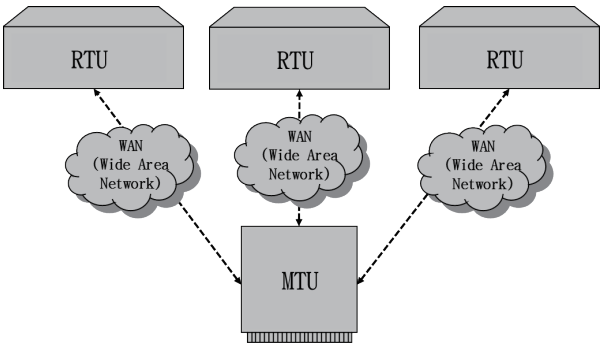

그림 2. 1세대 SCADA 시스템 : 모놀리식

〈그림 2〉는 1세대 SCADA 시스템 즉, 모놀리식 시스템의 구조적인 모습니다. 과거 SCADA 배치1세대 극 초기 단계에서는 네트워크라는 개념이 정립되지 않은 상태였기 때문에 SCADA 시스템 또한 상호 연결 없이 독립적으로 운용되었다. 산업이 발전되면서 네트워크 기술이 SCADA시스템에 접목되었다 하더라도 1세대에서는 원거리통신망 만이 RTU와의 통신에 사용되었다.

1.2.2 2세대 SCADA 시스템 : 분산처리

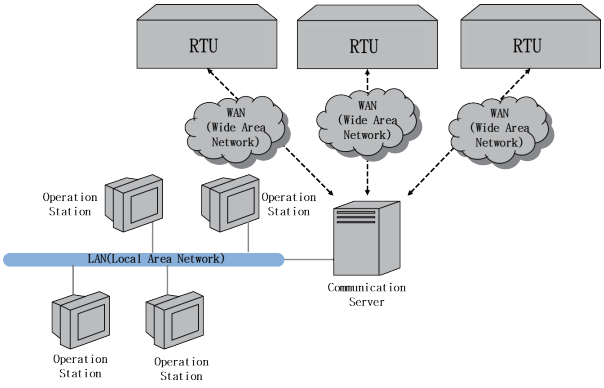

그림 3. 2세대 SCADA 시스템 : 분산처리

네트워크 기술의 발전으로 인해 2세대 SCADA 시스템에서는 근거리통신망에 기초한 분산 처리 시스템이 적용되었으며 〈그림 3〉에서 2세대 SCADA 시스템의 구조를 나타내었다. 2세대의 분산처리 SCADA 시스템은 1세대의 SCADA 시스템보다 처리 능력, 안정성 측면에서 높은 성능을 향상시켰으며 유지, 보수 비용 또한 감소되었다.

1.2.3 3세대 SCADA 시스템 : 네트워크

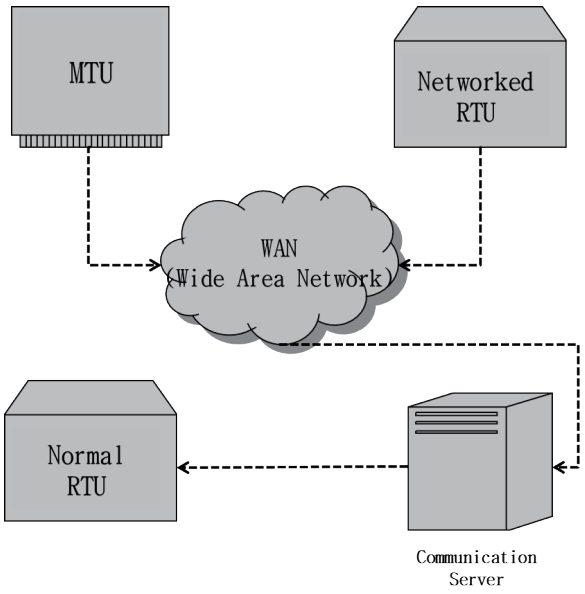

그림 4. 3세대 SCADA 시스템 : 네트워크

2세대 SCADA 시스템과 비교하였을 때3세대 SCADA 시스템의 가장 큰 차이점은 통신을 위한 인터넷 프로토콜(Internet Protocol, IP)의 사용이다. 이전의 SCADA 시스템이 폐쇄적인 독점 시스템을 사용하는 데에 비해 3세대 SCADA 시스템은 오픈 소스를 사용한다. 〈그림 4〉와 같이 원격단말에 네트워크가 사용되어짐에 따라 즉, 인터넷 표준 프로토콜이 사용되어짐에 따라 수많은 SCADA 시스템에 인터넷으로 접근 가능해졌으며 네트워크 침투 행위를 통한 위협이 잠재적으로 취약하다고 할 수 있다.

1.2.4 4세대 SCADA 시스템 : 무선통신 및 클라우드[3]

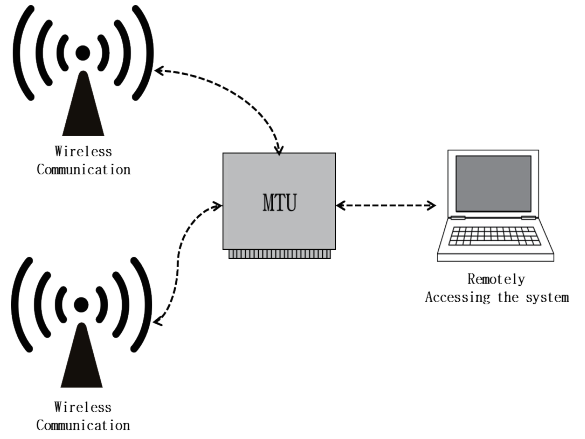

그림 5. 4세대 SCADA 시스템 : 무선통신 및 클라우드

〈그림 5〉와 같이 최근 SCADA 시스템은 무선네트워크, IoT(Internet of Things) 기술 및 클라우드 컴퓨팅 서비스를 통합하고 있다. 유선망을 사용하지 않으며 무선네트워크 기반 SCADA 시스템은 이전의 세대보다 유지 보수 및 통합이 용이해졌으며 제어 데이터의 접근 효율성, 유연성 또한 보장되지만 3세대 SCADA시스템과 마찬가지로 네트워크 취약성을 통한 보안위협이 존재하고 있다.

1.3 SCADA 시스템의 보안 위협

과거의 SCADA 시스템은 유선 통신 기반 표준 프로토콜을 사용하였다. SCADA 시스템이 처음 등장 하였을 때는 단순히 해당 시스템에 대한 프로세스를 모니터링하고 제어하기 위한 목적이었으며 시스템 자체 또한 수치가 표시되는 미터기 형태로 데이터를 취득하였기 때문에 관리자는 시스템 보안에 대하여 큰 관심을 둘 필요가 없었다.

산업 과 기술이 발전되면서 SCADA 시스템 또한 네트워크 기술이 접목되면서 네트워크를 통해 SCADA 시스템에 접근이 가능하게 되었으며 SCADA 시스템 자체가 전력, 가스, 수도, 교통 등 국가 및 사회 주요 기반시설의 제어시스템을 담당하고 있기 때문에 자연스레 공격자에 의해 흥미로운 공격대상이 되었다.

이전의 SCADA시스템은 대부분 물리적으로 외부 네트워크와 분리되었으며 전용 하드웨어와 소프트웨어를 사용하는 폐쇄망을 사용하고 있기 때문에 안전하다고 맹신되어 왔다. 하지만 산업의 발달로 인해 IP 기반 디바이스 보급량이 늘어나면서 SCADA 시스템 또한 네트워크 프로토콜을 사용해 구현되어 네트워크를 통한 SCADA 시스템으로의 접근이 가능해졌으며 대부분의 SCADA 시스템의 업데이트 또한 인터넷 혹은 USB 메모리를 사용하여 실행[4]되기 때문에 완전한 폐쇄망을 가진 SCADA 시스템의 의미는 더 이상 모호한 표현이 될 수 밖에 없게 되었다.

2. 공격기법

〈그림 6〉은 SCADA 시스템에서의 일반적인 공격방법에 대한 통계를 도식화 한 그림이다[5]. 그림을 토대로 살펴 악성코드(Malicious Code)에 의한 위협이 가장 높은 수치를 나타내고 있으며 다음으로 서비스 거부 (Denial of Service attack, DoS) 공격이 그 뒤를 잇고 있다.

본 항에서는 현재의 통계를 기반으로 무선통신 기반 SCADA 시스템의 공격기법들을 소개하고자 한다.

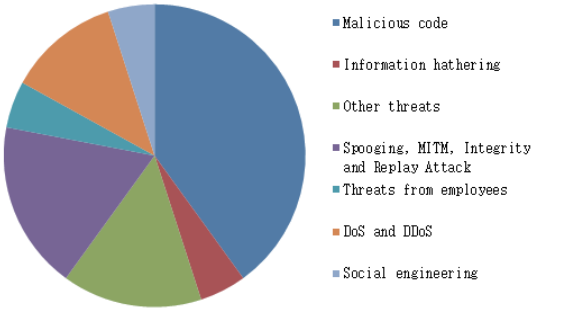

그림 6. SCADA 시스템 공격방법

2.1 Brute force Attack, Dictionary Attack

Brute force Attack은 암호나 암호화된 데이터를 해독화 하기 위하여 공격 가능한 모든 값을 대입하는 공격기법이다. 예를 들어 4자리의 숫자로 된 암호의 경우의 수는 실제로 1만개이며 무차별 대입 공격 방법은 이를 0000부터 9999까지 모든 경우의 수를 대입하여 공격한다. 이와 같이 가능한 모든 경우의 수를 대입하여 공격하기 때문에 대부분의 암호화 방식은 무차별 대입 공격에 대하여 안전하지 않으며 충분한 시간이 존재한다면 이론적으로는 해당 암호화된 데이터를 해독화 할 수 있는 확률이 높다. 또한 실제로 SCADA 시스템에서의 Brute force Attack 이 급격이 증가하는 보고서가 발표된 바가 있다[6].

무차별 대입 공격방법과 유사하게 미리 정의된 용어나 사전에 포함된 단어를 목록화하여 해독하는 방법을 Dictionary Attack 이라 한다. 해당 공격기법은 모든 경우의 수를 대입하는 무차별 대입공격과는 달리 미리 정의된 용어나 사전의 단어를 순차적으로 입력하여 해독화 한다.

2.2 Replay attack[7]

Replay attack은 공격자가 네트워크 통신 패킷을 수집, 저장하여 악의적인 용도로 재사용하는 공격기법을 말한다. 예컨대, 사용자가 패스워드를 입력할 때 패스워드가 저장된 패킷이 전송된다. 이 경우 공격자는 해당 패킷을 저장하여 재전송함으로써 공격자는 사용자의 패스워드를 악의적인 용도로 사용할 수 있다. 이 공격기법을 SCADA 시스템에 적용한다면 SCADA 시스템에 보내진 일련의 명령 패킷을 저장한 공격자는 후에 해당 명령을 Replay attack으로 재사용할 수 있다. 해당 기법은 공격자가 단순히 SCADA 시스템에서의 송수신되는 네트워크 패킷을 저장한 후 재 전송 하는 방법을 사용하므로 해당 네트워크 프로토콜에 대한 자세한 이해할 필요도 없으며 재사용된 패킷 또한 정상적인 패킷과 동일한 효과를 가지므로 공격자의 불법적인 접근이나 제어가 발생할 수 있다.

2.3 Man In The Middle(MITM) Attack

중간자(Man-In-The-Middle) Attack에서의 공격자는 통신을 연결하는 사용자 혹은 장비 사이에 침입하여 도청하는 공격기법이다. 해당 공격방법이 가해짐으로써 상호 연결된 사용자나 장비는 공격자가 중간에 연결되었다는 사실을 인식하지 못하며 송, 수신되는 네트워크 정보는 중간자(공격자)에 의해 도청되어 악의적으로 조작되어 사용된다. 해당 공격기법은 상호 연결매체에 대한 취약한 인증과정을 악용하고 있으며 공격자는 중간과정에서 허위 데이터를 삽입하여 해당 시스템에 대한 연결 제어권을 획득할 수도 있다.

2.4 Denial-of Service(DoS) Attack

Denial-of Service(DoS) Attack은 해당 시스템에 대한 자원을 부족하게 하여 의도된 시스템의 용도를 무력화 하기 위한 공격기법이다. 해당 공격기법은 흔히 특정 서버에 수많은 접속 시도를 만들어 해당 시스템의 과부화를 이끌어 낸다. 해당 공격기법을 확장한 공격기법이 DDoS(Distributed DoS) 공격기법이다. DDoS공격기법은 여러 대의 공격자를 분산적으로 배치해 동시에 DoS공격을 가한다. 과거 전력시스템과 같은 SCADA 시스템은 해당 공격기법의 많은 대상이 되었으며 최근 국, 내외의 사회 기반 시설이 해당 공격기법에 위협을 받고 있다[8]. 해당 공격기법은 네트워크 장비를 사용하여 공격하는 기법에 한정되지 않으며 프로세스의 과부하를 이끄는 악성코드의 사용 또한 하나의 DoS 공격이라 할 수 있다.

2.5 War Dialing[9]

과거의 War Dialing 공격 기법은 조직 내부의 모뎀을 식별, 탈취하기 위한 목적을 가지고 있었으며 조직 내부의 가능성 있는 모든 전화번호에 조직적으로 전화를 건 후 응답을 통해 모뎀을 식별하는 무차별 공격 기법의 형태였다. 최근 해당 공격기법은 무선 네트워크에 활용되고 있다. 공격자는 해당 네트워크의 가능성 있는 모든 IP 주소나 포트에 대한 응답을 요구하며 성공적으로 응답이 재전송되면 해당 정보를 바탕으로 기기의 장치 유형, 제조업체 및 위치와 같은 정보를 수집 할 수 있다.

2.6 Spoofing

Spoofing은 자기 자신의 식별 정보를 속여 다른 대상 시스템을 공격하는 기법이다. 네트워크 상의 공격자는 네트워크 프로토콜 상의 취약성을 기반으로 공격시도 시 자신의 시스템 정보를 위장함으로써 역 추적이 어렵게 한다. 이러한 공격방법은 여러 가지 공격형태로 세분화 할 수 있다. 첫째, IP Spoofing은 말 그대로 IP 정보를 속여 다른 시스템을 공격하는 방법이다. IP Spoofing을 통해 DoS공격을 수행 할 수 있으며 공격 대

상 시스템의 연결을 해제할 수도 있다. 둘째, ARP Spoofing은 ARP 프로토콜에 대한 변조를 하는 공격기법이다. 32비트 IP 주소를 48비트 네트워크 카드 주소(Mac address)로 대응시켜 주는 프로토콜을 ARP 프로토콜이라 하는데 실제로 시스템이 네트워크 연결을 시도할 때 해당 IP에 해당하는 네트워크 주소를 찾아 연결하게 한다. 이러한 프로토콜이 변조 되면 공격 대상 시스템 내부의 네트워크 정보를 공격자의 시스템으로 우회할 수 있으며 이러한 정보는 공격자에 의해 악의적으로 사용될 수 있다.

3. 사례 및 관련연구

본 항에서는 무선통신을 기반한 SCADA 시스템의 보안 위협 사례와 관련 연구의 동향에 대해서 소개한다.

3.1 사례

3.1.1 GPS 교란

매년 북한에서는 2010년 ~ 2012년 사이 매년GPS 교란(jamming) 공격을 시도 하였으며, 최근 2016년 3월 또한 GPS 교란을 통한 사이버 공격을 감행하고 있다[10]. 2016년에 발생한 공격을 살펴 보면, 상용 채널인 1575.42MHz 와 군용 채널인 1227.6MHz 에 대한 공격을 감행하였는데 인천, 경기, 강원도를 대상으로 광범위한 공격이 이뤄졌다. 항공(962대), 선박(어선 포함 694척), 통신(1786개 기지국) 등 다양한 분야에서 교신 신호 유입이 확인되었으며 다행이 물리적인 피해는 발생하지 않았다.

국외의 GPS 교란 사례는 다양한 무선 SCADA 시스템에 대한 피해 사례를 확인 할 수 있다[11].

2001년 미국 캘리포니아주 모스랜딩 에 있는 작은 항구에서 전파 위협 신호가 검출되었다. 이로 인해 GPS 신호를 통한 정보에 의존하는 선박들이 안개가 낀 상황에서 항구를 통과하는 과정에서 장애를 초래 했으며, 동년 에리조나 주에서는 약 6일 동안의 전파교란 이 발생하여 주변 333km 이내에서는 휴대형 GPS 수신기가 작동되지 않았고, 항공기 내 GPS 또한 동작하지 않아 운행에 불편을 초래했다.

2003년 이라크 전쟁 당시 이라크 군에서는 미국에서 사용하는 유도탄의 정밀도를 떨어뜨리기 위해 GPS 교란기를 사용하였다. 미군이 사용한 유도탄은 사전에 입력된 GPS 좌표를 좇아 명중하는 방식인데, 당시 전파 교란을 당했는지 감지하지 못한 미군은 유도탄을 당초 목표로 했던 장소가 아닌 지역에 떨어뜨려 민간인 피해가 발생하였다.

2007년 1월, 샌디에고 항구에서는 해군 함정에서 계획된 통신 재밍 훈련이 진행 되었다. 훈련은 2시간 가량 진행 되었으며, 사용한 무선신호 방해가 의도치 않게 도시 전역의 GPS 신호를 차단하고 말았다. 이로 인해 해군 의료센터의 긴급 호출기와 휴대전화 는 작동을 멈추었고, 항구 교통관리 시스템 및 공항 교통통제 시스템에 영향을 미치는 사건이 발생하였다. 훈련은 2시간 가량 진행되었지만 피해 신고는 약 4시간 이상 지속되었다고 한다.

2010년 과 2011년에 독일의 하노버 지역의 공항에서 GPS 전파 교란이 발생하여 항공기 이륙 등에 장애를 초래 하였다[12].

2013년에는 Newwark 국제 공항에서 고용주의 눈을 속이기 위해 자신의 픽업트럭에 설치한 불법 GPS 재밍 장치가 공항의 위성 추적 시스템을 방해하는 사건이 발생하였다. 차량에서 발생하는 신호가 항공 교통 관제 시스템에서 사용하는 GPS 신호를 차단하였으며, 이와 비슷한 사건이 2009년에도 발생했었다. 두 사건 모두 차량에 설치한 값싼 GPS 재머 에 방해를 받은 것이며 GPS 의존도가 높은 공항이었다[11].

이 외에도 2011년 영국에서는 6개월간 동일 장소에서 67건의 재밍 신호를 확인, 대만의 카오슝 국제공항에서는 하루 최대 117건의 전파 교란이 발생했다는 보고가 발표되기도 하였다[13].

3.1.2 호주 퀸즈랜드 오폐수 처리 제어시스템 침해사고[14]

2000년도 호주 퀸즈랜드 오폐수 처리 제어시스템이 회사의 전직 직원에 의한 침해사고가 발생하였다. 전직 직원은 차에 도난 무선 장비와 컴퓨터 등을 설치하여 War-driving 방식으로 오폐수처리 제어시스템을 공격하였다. 악성 프로그램을 펌프장치 제어프로그램에 설치하여 오작동을 야기하였다. 이와 같은 방식으로 총 46번의 공격이 이루어 졌으며, 이로 인해 80만 리터의 폐수가 무단으로 방출되었다.

3.1.3 폴란드 우츠시 트램 시스템 교란[15]

2008년 1월에는 14세 소년에 의해 폴란드 우츠 시에서 트램 시스템의 교란으로 4대의 트램이 탈선하는 사고가 발생하였다. 소년은 트램시스템에 평소 흥미를 가지다가 관련 지식을 바탕으로 TV 리모컨을 개조한 시스템 교란기기를 제작하였다. 이 사고로 12명이 부상당하고 운행이 중단되는 등의 피해가 발생하였다.

3.1.4 미국 텍사스 차량 이모빌라이저 해킹[16]

2010년 3월 미국 텍사스에서 원격 이모빌라이저 시스템이 적용된 차량을 대상으로 해킹이 발생하였다. 원격 이모빌라이저 시스템이란 차량 의 도난방지를 위한 원격 시스템이다. 해킹 사고 당시 차량 100대 가량의 차량이 시동이 걸리지 않거나 경적이 울리는 등의 상황이 발생하였으며, 조사결과 자동차 판매점에서 해고된 직원이 악의를 가지고 공격을 시도한 것으로 확인되었다. 결국 사고 차량은 정비소에서 수리를 통해 복구되었다

고 한다.

3.1.5 미국 지프체로키 해킹[17]

2015년 미국에서는 달리는 지프 체로키를 해킹하여 라디오와 와이퍼를 조종하고 차를 멈추게 하는 사건이 발생했다. 이 사건은 2명의 해커가 자동차 내부에 있는 UConnect 기능의 치명적인 보안취약점을 발견했기에 능하였다. Uconnect 기능은 전화 및 자동차 내부 엔터테인먼트, 와이파이 핫스팟 등을 제공하는 기능인데 이 기능을 이용하여 자동차의 IP 를 알아내고 미국 전역 어디서든 무선 원격 조종이 가능하였다고 한다. 이 취약점으로 인해 피아트 크라이슬러 사는 140만대가 넘는 자동차를 리콜 조치 하였다.

3.2 관련연구

3.2.1 신호등 및 교통 제어 시스템

2014년 Michigan 대학 연구진에 의해 발표된 연구는 당국의 허가를 통해 진행된 연구로 영화에서 본 법한 교통 신호 해킹이 실제 상황에서도 실현 가능함을 보였다[18].

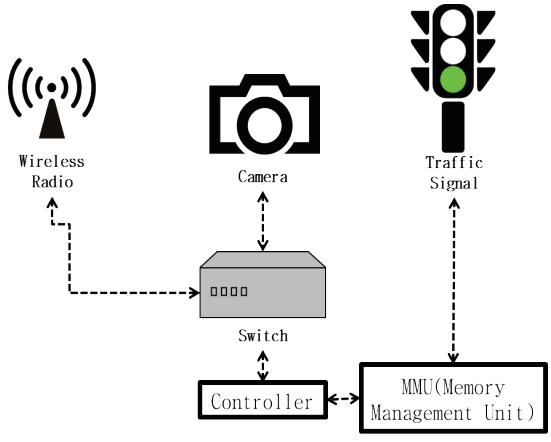

그림 7. 일반적인 신호등의 구조도

〈그림 7〉은 해당 연구에서 연구 대상으로 설정한 교차로 신호등의 구조를 해부한 조직도 이다. 전형적인 교차로의 신호등에서 무선 라디오는 스위치에 연결되어 컨트롤러, 실시간 비디오와 기타 정보를 수집한다. 수집된 정보는 도로통제를 담당하는 기관으로 전송되며, MMU(Memory Management Unit)는 컨트롤러와 신호등 사이에 위치하여 기기들의 결함을 제어하는 장치의 역할로 위치한다.

본 연구에서는 신호등이 사용하는 암호화 되지 않은 무선신호와 초기 설정된 장비의 아이디와 패스워드가 변경되지 않았기 때문에 교통신호 등을 제어하는 컨트롤러에 쉽게 접근할 수 있었다.

해당 연구에서는 간단한 암호와 와 기초적인 보안 만으로도 상당수 개선할 수 있는 부분이 많지만 가장 큰 문제점은 보안의식의 결여와 명확히 규정화 되어 있지 않는 표준 이라고 말한다.

3.2.2 자동차 시스템

2010년 발표된 해당 연구는 차량 내부의 무선 네트워크에 대한 보안 위협을 위해 진행되었으며 공격 대상은 자동차 내부의 타이어 공기압 체크 시스템이다[19]. 〈그림 8〉과 같이 타이어의 공기압 체크 시스템은 타이어의 공기압이 문제가 있을 시 운전자에게 알려주는 시스템으로, 차와 타이어 간에 무선통신으로 정보를 주고 받는다. 해당 연구에서는 정보를 주고 받는 과정을 차량 에서 무려 40m 나 떨어진 곳에서도 도청이 가능하며, 역공학을 통해 알아낸 바로는 이 데이터 안에는 각 차량들의 고유번호가 존재한다고 한다. 이를 악용한다면, 차량의 공기압 수치를 조작하여 운전자에게 거짓 경고를 줄 수 있으며, 각 차량의 고유 번호를 통해 차량 추적이 가능할 수 있다고 설명한다.

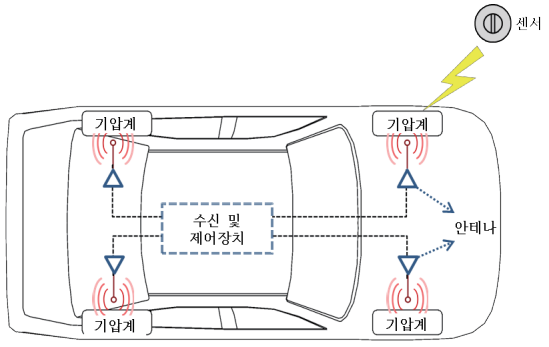

그림 8. 무선통신 기술이 접목된 자동차 타이어 공기압 체크 시스템

이러한 문제점 또한 교통 제어시스템의 문제와 같이 인증되고 규격화된 프로토콜의 부재로 발생한 취약점이라고 말한다.

또 차량과 스마트 키를 공격 대상으로 하는 연구가 2010년에 발표되었다[20]. 최근에 출시되는 차량들은 대부분 스마트 키를 이용하여 Passive Keyless Entry and Start 시스템을 적용한다. 스마트 키를 소지한 채 차량 근처에 가면 바로 차문을 열고 시동을 걸 수 있는 시스템이다. 〈그림 9〉와같이 기존의 스마트 키와 차량 사이의 통신에서 신호를 전달할 수 있는 무선 장치를 중간 다리로 사용함으로 키와 차량이 아무리 멀리 있어도 신호를 훔쳐 차량에 전달할 수 있으며 이를 Relay attack이라 정의한다. 예를 들어 집에 놓아둔 스마트 키의 신호를 무선 장비를 통해 주차장에 있는 차와 실시간으로 통신할 수 있게 하는 것이다. 이러한 공격 기법은 매우 단순하면서도 인증 및 암호화, 사용 프로토콜의 존재와는 상관없이 적용 가능함을 증명하였다.

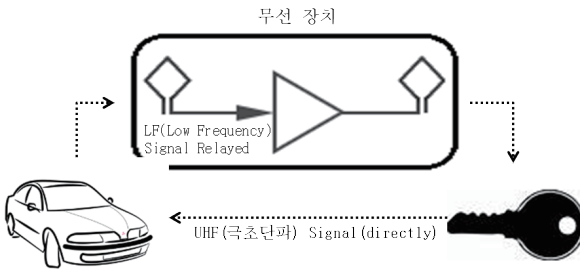

그림 9. 무선장비를 이용한 스마트키 Relay attack

해당 연구에서는 기술적이나 정책적인 보안 방법에 대하여 제시하면서 실생활 에서도 보안의식을 가지고 작은 알루미늄 키 케이스에 보관을 하거나 사용하지 않을 때 배터리를 빼는 식의 간단한 조치 만으로도 피해를 예방할 수 있다고 설명한다.

3.2.3 의료장비

2011년 BlackHat 에서는 의료 장비SCADA 시스템에 대한 무선 해킹을 발표하였다[21]. 무선 통신기술은 사회 기반 시설뿐만 아니라 장난감, 의료 장비, 산업 장비 등과 같은 다양한 분야에 접목되면서 그에 대한 다양한 연구 역시 진행되고 있다. 해당 발표 에서는 의료 기기의 무선 보안 취약성에 대해 연구 하였으며, 실제 공격 대상으로는 혈당 측정기 와 인슐린 펌프를 대상으로 진행하였다. 장비에서 사용하는 무선 통신을 도청하여 개인 정보들을 획득할 수 있을 뿐만 아니라 조작된 명령을 전달하여 사용자를 속이는 것까지 가능하다고 설명한다.

Ⅲ. 결 론

본고에서는 산업 및 사회 기반 시설의 제어하는 시스템인 SCADA(Supervisory Control And Data Acquisition)의 전반적인 이해와 보안위협의 사례와 연구 동향에 대해서 소개하였다. 과거의 SCADA 시스템은 폐쇄적인 내부망과 비공개 통신 프로토콜을 사용하는 까닭에 타 시스템들 보다 보안 위협 및 침해사고에 안전하다고 맹신되었다. 하지만 본고에서 다룬 SCADA 시스템 관련 침해사고들은 폐쇄망이 더 이상 안전하지 않은 통신망이 될 수 있음을 증명할 수 있다.

더욱이 산업이 발전됨에 따라 공장 및 사회 주요 기반 시설들은 대형화 되고 자동화 되었으며 이는 자연스레 제어시스템의 환경 변화로 이어졌다. 그 결과 최근의 SCADA 시스템들은 운용의 효율성과 접근의 자율성의 이유로 Bluetooth, GPS, Zigbee와 같은 무선통신을 결합한 시스템의 출현으로 발전되었다. 이와 같은 변화는 SCADA 시스템의 접근 경로가 더욱더 넓어짐을 의미하기도 한다.

통신기술의 발전은 사회전반적인 수준을 높이는데 큰 기여를 했지만, 기술의 발전에만 관심을 가지는 풍조는 정보보호강화를 등한시하며 침해사고 시 미흡한 대처로 이어지고 있다. 특히 국가 및 사회 주요기반 시설을 제어하고 있는 SCADA 시스템의 침해사고 발생 시 심각한 악영향을 초래할 수 있으며 이를 위해 관련 보안 기술 연구와 개발이 필요하다.

참 고 문 헌

[1] Baker, George H., and Allan Berg. “Supervisory control and data acquisition (SCADA) systems.” The Critical Infrastructure Protection Report 1.6 (2002).

[2] Shahzad, A., et al. “The SCADA review: system components, architecture, protocols and future security trends.” American Journal of Applied Sciences 11.8 (2014): 1418.

[3] Sajid, Anam, Haider Abbas, and Kashif Saleem. “Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges.” IEEE Access 4 (2016): 1375-1384.

[4] Lüders, Stefan. Control systems under attack?. No. CERN-OPEN-2005-025. 2005.

[5] H. M. N. Al Hamadi, C. Y. Yeun, and M. J. Zemerly, A novel security scheme for the smart grid and SCADA networks,” Wireless Pers. Commun., vol. 73, no. 4, pp. 1547_1559, 2013. ,

[6] U.S. Department of Homeland Security, “ICS-ALERT-13-016-02: Offline Brute-Force Password Tool Targeting Siemens S7,” ICS-CERT, December 2013. Available: https://ics-cert.us-cert.gov/alerts/ICSALERT-13-016-02.

[7] Syverson, Paul. “A taxonomy of replay attacks [cryptographic protocols].” Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings. IEEE, 1994.

[8] H. M. N. Al Hamadi, C. Y. Yeun, and M. J. Zemerly, A novel security scheme for the smart grid and SCADA networks,” Wireless Pers. Commun., vol. 73, no. 4, pp. 1547_1559, 2013. ,

[9] Baker, George H., and Allan Berg. “Supervisory

control and data acquisition (SCADA) systems." The Critical Infrastructure Protection Report 1.6 (2002).
[10] http://www.etnews.com/20160405000068, 전자신문 etnews, 2016.04.05
[11] Coffed, Jeff. "The threat of GPS jamming: The risk to an information utility." Report of EXELIS, Jan (2014)
[12] 3. 신천식. "GPS 전파교란 대응기술 동향." TTA Journal 149 (2013): 92-99.
[13] New Technologies deployed to counter the threat of GPS Jamming,' Cellular-news, 2013. 2. 13
[14] 임종인, and 장규현. "전자적 제어시스템 침해 위협에 따른 법적 대응방안." 정보보호학회지 20.4 (2010): 52-65.
[15] http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html, The telegraph, 11 Jan 2008, By Graeme Baker
[16] Poulsen, Kevin. "Hacker disables more than 100 cars remotely." Internet]. Available: www. wired. com/threatlevel/2010/03/hacker-bricks-cars (2010).
[17] Greenberg, Andy. "Hackers remotely kill a jeep on the highway—With me in it." Wired 7 (2015): 21.
[18] Ghena, Branden, et al. "Green Lights Forever: Analyzing the Security of Traffic Infrastructure." WOOT 14 (2014): 7-7.
[19] Ishtiaq Roufa, Rob Millerb, et al. "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study." 19th USENIX Security Symposium, Washington DC. 2010
[20] Francillon, Aurélien, Boris Danev, and Srdjan Capkun. "Relay attacks on passive keyless entry and start systems in modern cars." Proc. Network and Distributed System Security Symp.
[21] Radcliffe, Jerome. "Hacking medical devices for fun and insulin: Breaking the human SCADA system." Black Hat Conference presentation slides. Vol. 2011. 2011.

약 력

김 지 훈

2014년 영남대학교 공학사
2014년 영남대학교 컴퓨터공학과 석사과정
관심분야: 디지털포렌식, 악성코드분석

이 성 원

2011년~현재 영남대학교 컴퓨터 공학과 학사과정
관심분야: 임베디드 해킹 및 보안

윤 종 희

2003년 경북대학교 전자전기공학부(학사)
2011년 서울대학교 전기컴퓨터공학부(박사)
2011년~2012년 강릉원주대학교 컴퓨터공학과 강의전담교수
2012년~2013년 한국전자통신연구원 부설연구소 연구원
2013년~현재 영남대학교 컴퓨터공학과 조교수
관심분야: 사이버 보안, 컴파일러, 소프트웨어 최적화, 임베디드 시스템