교통신호제어기 해킹 방지 기술에 관한 연구

이희조*, 김명우*, 최종현**, 강혁**
*고려대학교 컴퓨터정보통신대학원
**미륭에이스
e-mail:yagami99@korea.ac.kr

A Study on Traffic Signal Controller Hack prevention technology

Yi-HeeJo*, Kim-MyungWoo*, Jong-hyen Choi**, Kang-Hyeug**
*Department of Computer and Information Communication graduate
**Miryung Ace

신호등을 제어하는 교통신호제어기는 차량의 흐름을 제어하는 중요한 역할을 하는 장치이다. 만약 도심지에서 교통신호제어기가 침해되었을 경우 교통마비 현상이 발생하거나 자칫 교통사고까지 유발할 수 있다. 하지만 현 교통신호제어기는 물리적 보안 이외 인증, 행위제어, 통신구간에 대한 보안이 무척 취약하다. 따라서 이를 보안하기 위해 각각의 위험 요소에 대해 분석하고 그에 맞는 대응방안을 마련할 필요가 있다. 본 논문에서는 신호등 교통신호제어기의 취약점을 분석하고 각각의 취약점에 대해서 대응책을 제시하고자 한다.

1. 서론

지능형 교통시스템(ITS, Inteligent Transport System)이란 교통체계의 구성요소에 정보통신 기술을 접목시켜 교통정체, 사고 등의 각종 교통문제를 체계적으로 대처하여 효율적인 교통운영을 통해 국가적인 물류비 증가 등 경제적 손실 대응과 현장의 정보통신설비(검지기, CCTV, 기상정보시스템 등)로부터 수집된 교통정보를 교통센터에서 분석·가공처리하여 유·무선 통신망으로 교통정보를 제공함으로서 도로이용자에게 안전 및 편리성을 도모하기 위한 종합교통 정보관리시스템이다.[1] 국내에선 1993년 4월 대통령직속 사회간접자본(SOC)투자기획단에서 ITS 도입을 시작으로 과천시 ITS 시범사업, 수도권남부지역 국도3호선등 6개 노선 ITS 구축, 지능형교통체계(ITS) 국가표준화 계획 수립 등을 하였다. 서울, 경기, 인천, 관천, 대전, 고양, 안산, 광주, 울산, 군산, 수원, 경주, 창원, 안양, 여수, 충주 등으로 기본계획 수립을 하였고, 한국도로공사에서 추진한 ITS의 한 분야인 고속도로 교통관리시스템(FTMS : Freeway Traffic Management System)을 구축 운영 중에 있다[2]. 이 같은 확산으로 인해 교통체계를 제어하는 교통신호 제어기에 대한 보안에 대한 우려가 높아져 가고 있다. ITS 설비는 교통관리운영 센터설비와 교통정보수집 현장설비로 이루어져 있으며, 교통정보수집 현장설비는 교차로 또는 횡단도로에 설치되어 신호등을 제어하는 전자 교통신호제어기, 폐쇄회로텔레비전(CCTV) 시스템, 자동차량인식시스템(AVI), 영상검지 시스템 등으로 나누어져 있다. 본 논문에서는 신호등을 제어하는 전자 교통신호 제어기의 문제점을 파악 및 이에 대한 대응 방안에 대해 제시하려 한다.

2. 현 교통신호 제어기 시스템 현황

최근 정보통신기술의 급격한 발전으로 교통, 전력, 발전소, 댐 등 대규모 플랜트시설들을 운영하기 위한 제어시스템은 발전된 정보통신기술을 이용하여 다양한 형태의 개방형시스템으로 진화하였다. 제어시스템은 원격지의 장비, 센서, 제어기, 변환기 등으로부터 자료를 수집하고, 수집된 자료는 중앙관리시스템으로 전송되어 저장 및 분석 단계를 거쳐 화면으로 표시하며, 시스템구성요소들을 실시간으로 감시 및 제어를 한다. 그리고 장치마다 상호간 또는 외부기기와 연결하여 각각의 장치에 대한 원격접근과 제어가 가능하고, 여러 명령 및 조작이 가능하도록 양방향 통신서비스 환경이 구축되어 있다. 통신 프로토콜 측면에서 초기에는 제조 회사 고유의 프로토콜을 사용하였으나 상호 연계의 필요성이 증가되어 점차 표준화된 시스템으로 전환되었다.

현재 Windows 운영체제 및 TCP/IP 기반의 Ethernet 통신을 적용하는 시스템이 주로 도입되고 있으며, 제어시스템 상호간 및 현장의 센서 등 필드장치와의 연결방식도 기존의 실선방식에서 필드버스 등 표준 네트워크 프로토콜이 적용되었다.

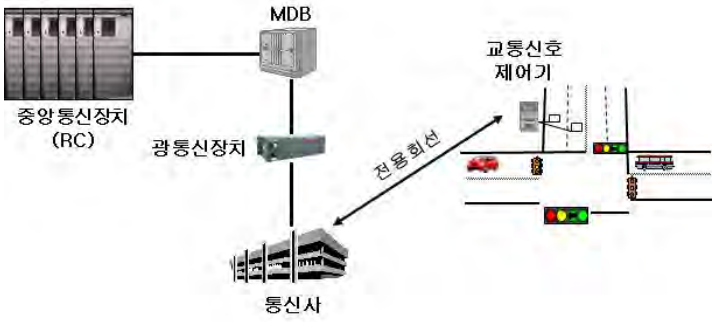
업무효율 향상을 위해 제어시스템에서 처리하는 데이터를 자재, 경영, 생산, 구매 등의 업무용 정보시스템과 연계를 위한 시도가 증가하고 있는 추세이다.

제어시스템 중 신호등 교통신호제어기의 구성도는 아래 <그림-1>과 같다.

교통신호제어기는 각 교차로에 설치되어 있는 Local 신호등의 신호를 제어한다. 통신사는 각 Local의 교통신호제어기 신호를 하나의 전용망으로 통합 전송하고 현장 교

통신호의 전반적인 유지보수 관리를 하고 있다.

광통신장치는 광통신 신호로 변환하여 교통정보센터 중앙통신장치(RC)와 Local 교통신호제어기 사이에서 광케이블로 전송한다.[3]



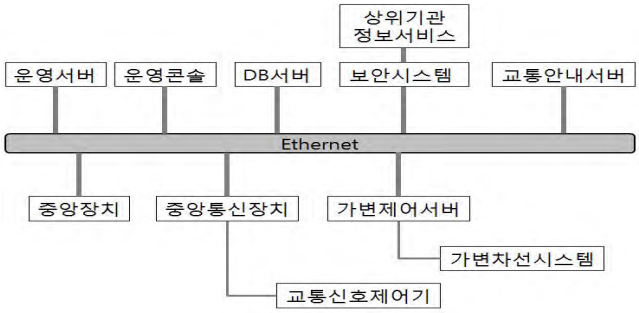
<그림-1> 일반적인 교통신호 제어시설 구성도

MDB는 광통신 장비의 아날로그 신호를 통합정보센터의 각 부분에 분배하며 낙뢰 방지 역할도 수행한다.

중앙통신장치(RC)는 하나의 모뎀이 하나의 Local 교통신호제어기의 아날로그 신호를 받는 단순 모뎀 역할을 수행한다. 1대의 RC 장비에 여러 개의 모뎀이 존재한다.

기반시설로 지정되어 지속적인 위험관리를 해야 하는 교통신호제어시스템은 제어설비, 제어설비를 관리 및 운영하는 정보시스템, 네트워크, 응용시스템 등으로 이루어져 있다. 교통신호제어시스템을 구성하는 제어망은 업무망과 별도의 망으로 구성되어 있으며, 신호운영서버, 중앙통신장치, 운영콘솔, 방화벽 등의 시스템이 연결되어 있다.

교통신호제어시스템의 구성은 아래 <그림-2>와 같다.



<그림-2> 교통신호제어시스템 구성도

3. 취약점 분석 및 피해 사례

파주, 고양, 광명, 수원, 부천, 안산 등 교통제어시스템의 경우 자가망을 활용하고 있으며 자가망과 인터넷이 연결되어있는 형태로 운영중이여서 해킹에 대한 보안이 매우 취약하다. 교통신호제어시스템의 유지보수를 수행했던 업체는 특히 교통제어시스템에 관련된 정보를 보유하고 있으므로 특별한 보안조치가 없는 경우 언제든지 시스템에 접근이 가능하기 때문이다.[4] 또한, 공격자가 교통신호제어기에 통신 포트(LAN)를 통해 접속하여, 악의적인 목적으로 신호제어 SW를 변형/삭제 등의 행위를 하여도 이를 제한하는 기능 또한 없다. 게다가 피씨로 통신포트에 접속할 경우, 포트 제어 기능이 없어 인터넷 사용이 바로 가능할 정도로 보안이 취약하다.

대도시 및 일부 신도시에는 교통신호제어기를 교통 센터에서 원격으로 감시 및 제어를 하기 위해 하나의 폐쇄망으로 연결하여 보호하고 있다. 하지만, 제어시스템을 운영하는 콘솔 PC는 모두 OS를 사용하며 제어시스템은 일반 PC와 마찬가지로 바이러스에 감염되며, 하나의 교통신호제어기를 통해 센터로 침입할 경우, 전체의 교통체계를 혼란시킬 수도 있다.

다음으로 접근 제어 부분이 취약하다. 교통신호제어기에서 별도의 접근제어 통제가 적용되지 않아 제3자 누구나 접근이 가능하여 교통신호제어기를 제어할 수 있다. 교통신호제어기에 접근 후 정해진 권한 또한 없어 일반 운영자 또는 공격자가 관리자 권한으로 접속이 가능하여 심각한 보안사고가 발생할 우려가 있다.

위에서 본 바와 같이 교통신호제어기에서 접속하는 경우 사용자 인증 등의 계정관리를 위한 보안조치가 없는 상태이므로, 악의적인 의도를 가지고 교통신호제어기에서 제어시스템으로 접근하여 제어시스템의 관리자 PC에도 접근이 가능하다.

마지막으로 제어시스템에서 교통신호제어기와의 통신 시 인증이나 암호화가 제공되지 않아 제어시스템에 불법적인 접근 및 데이터 조작이 가능한 점이 문제가 된다.

실제 교통신호제어 시스템에 대한 공격으로 발생한 국외의 피해사례로 <표-1>을 들 수 있다.

시기	발생국	피해내용
2003. 8	미국	· 동부지역의 철도신호시스템이 소빅-F웜에 감염 · 수시간 동안 운행 중단
2007. 11	미국	· 미국 캘리포니아주 Tehama Colusa Cana Authority사의 전직 직원이 SCADA시스템을 침해 · 악성소프트웨어로 인해 Sacramento River의 수로 제어 컴퓨터 마비
2008. 1	폴란드	· 14세 소년이 TV리모컨을 개조하여 트램 교차로 불법 조작 · 4대의 트램 탈선 및 12명 부상

<표-1> 국외 교통 관련 제어시스템 피해사례[5]

4. 취약점 대응방안

3절에서 교통신호제어기의 취약점을 분석하였다. 취약점은 다음과 같이 네 가지로 요약될 수 있다.

접속자 인증, 포트 제어, 행위 제어, 행위 추적, 데이터 암호화이다.

각각의 취약점에 대하여 대응 방법은 다음과 같다.

4.1 접속자 인증에 대한 대응방안

현 신호등 교통신호제어기는 클라이언트가 접속 시 Ethernet Port, Serial Port(RS232C)를 사용한다. 아무 제한없이 접속이 가능하기 때문에 이에 대한 대응 방안이 필요하다. 가장 먼저 아이디/패스워드를 이용하여 클라이언트를 제한할 수 있는 방법을 생각해 볼 수 있다. 여기에 보안성을 높이기 위해 아이디/패스워드를 전송 할 때, 요청 클라이언트의 유니크한 값(예, HostID)과 섞어 Message Digest를 만들어 요청함으로 중간에서 데이터를 가로채더라도 아이디/패스워드가 유출되는 것을 방지할 수 있다.

4.2 포트 제어에 대한 대응방안

다음으로 교통신호제어기에 접속 할 수 있는 Lan Port의 취약점에 대한 대응방안을 마련할 필요가 있다. 인증되지 않은 기기라도 교통신호제어기에 있는 Lan Port에 접속하면 인터넷이 사용 가능하기 때문이다. 이를 방지하기 위해 인증된 클라이언트만이 인터넷을 사용가능하도록 하는 방안을 생각해 볼 수 있다. Lan Port를 제어하기 위해 Embedded 보드를 Add-On하고 추가한 보드 안에서 Lan Port를 제어하도록 프로그래밍 하는 방법을 생각해 볼 수 있다. 즉, 교통신호제어기에 바로 접근하는 방식이 아닌, Add-On된 보드를 통해 접근함으로써, Lan Port를 인증된 사용자(인증 방법은 4.1절에서 논의)만이 사용하도록 하는 방식을 제안한다.

4.3 행위 제어에 대한 대응방안

셋째로 현재 교통신호제어기에 접속한 클라이언트는 모든 명령어(관리자 명령 포함)를 사용할 수 있다. 그러므로 인증 절차를 거친 클라이언트 또한 관리자 권한의 명령을 사용할 수 있다. 이런 취약점을 방지하기 위해 관리자가 관리자 전용 페이지에서 계정별 권한을 세팅하는 식의 접속자별 권한을 따로 두는 방법을 제안한다. 즉, 접속한 클라이언트는 인가된 명령어 이외 명령어를 수행하지 못하도록 하는 기법이다.

4.4 행위 추적에 대한 대응방안

넷째, 현재는 교통신호제어기에 접속을 해서 작업을 했을 경우 접속한 사용자 누구인지, 무엇을 하는지에 대한 기록이 전혀 남지 않는다. 이는 추후 문제가 생겼을 경우 추적을 불가능하게 만든다. 이를 방지하기 위해 클라이언트가 교통신호제어기에 접속하여 작업을 할 경우, 접속한 클라이언트 정보, 시간 정보, 명령어 수행 및 수행 결과 등의 정보를 로그를 통해 기록해놓고 관리자 툴에서 로그를 볼 수 있도록 해야 한다.

4.5 데이터 암호화에 대한 대응방안

마지막으로, 현재 클라이언트와 교통신호제어기와의 통신시 전송 데이터가 암호화되지 않아서 데이터를 가로 챘을 경우 주고받는 데이터 내용이 전부 노출이 된다. 그러므로 이를 위해 구간 암호화 기법을 적용할 필요가 있다. SSL을 이용하여 통신 채널을 암호화 하는 방법과 비밀키를 공개키로 암호화해서 교환 후 대칭키로 데이터를 암복호화해서 서로 주고받는 즉, 공개키 기반 암호화와 대칭키 기반 암호화를 섞어서 통신하는 방법[6]을 사용할 수 있다.

5. 결론

교통제어 신호기와 같은 주요 기반시설이 사이버 공격 등으로 인해 가동이 중단될 경우 교통마비로 인한 사회·경제적 손실을 초래할 뿐 아니라 교통사고와 같이 인명피해 또한 발생할 수 있다.

요 몇 년간 2011년 4월 농협 금융사고, 2013년 방송사, 은행에서 일어난 3·20 전산 대란 등의 사이버 테러가 발생함에 따라 교통신호제어시스템의 경우에도 예외에 해당될 수 없다. 또한 교통신호 제어시스템 환경이 폐쇄망이 아니라 다양한 외부 서비스 및 관리를 위해 외부망과 연결되고 있는 환경이라 이에 대한 보안 위협이 커지고 있다.

이에 따라 본 연구에서는 신호등 교통신호제어시스템에 대한 취약점을 분석 하고 각각의 취약점에 대한 대응방법을 제시하였다.

교통신호제어시스템은 일반 시설과 다른 교통신호제어시스템에 특화된 점검 기준 마련이 필요하다. 보안 담당자의 잦은 보직 변경으로 인한 보안관리 업무의 연속성 문제 및 외주업체를 통한 운영업무 수행으로 인한 인적 보안 또한 필수적이다. 하지만, 교통신호제어 시스템을 관리하는 기관에서 내부적으로 보안 정책을 수립하는 것은 현실적으로 조금 힘들다. 이를 위해 한국 인터넷 진흥원과 같은 정보보호 관련 기관의 지원 및 정보보호 활동 강화를 위한 교육, 정보제공 등 지속적인 관심 및 지원 체계가 필요하다.

교통신호제어시스템 보안 관련 담당자들은 교통신호제어시스템의 중요성을 인지하고 시스템이 침해당하지 않도록 보안 강화에 많은 관심을 가져야 한다.

참고문헌

[1] 한국정보통신공사협회,ITS(지능형 교통시스템)

[2] 국토해양부, 도시교통관리를 위한 ITS 필수교육 교육과정 코스.

[3] 대구광역시청, “교통신호제어시스템 구축”, 2009년.

[4] Antone Gonsalves, 미시건대 연구진, ″도시 신호등 해킹, 너무나도 쉬웠다″, 2014년 9월

[5] 한국인터넷진흥원, 국가정보보호백서, “정보보호 활동 - ISIS 인터넷통계정보시스템”, 2013년

[6] RSA Laboratories, PKCS#07, Cryptographic Message Syntax Standard, pp17