Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.531

지능형교통시스템의 보안취약점 개선방안에 관한 연구*

조 평 현,† 임 종 인, 김 휘 강‡
고려대학교 정보보호대학원

A Study on the Improvement of Security Vulnerabilities in Intelligent Transport Systems*

Pyoung Hyun Jo,† Jong In Lim, Huy Kang Kim‡
Graduate School of Information Security, Korea University

요 약

에너지·방송·통신·교통 등의 주요 기반시설의 파괴와 침해는 사회·경제적 손실 뿐 아니라 개인의 자유와 권리를 위협하는 결과를 초래할 수 있다. 특히 교통신호제어시설이 침해되었을 경우에는 시민들의 생활 불편 뿐 아니라 교통사고 등 사회 혼란을 유발시킨다. 최근의 제어시스템은 폐쇄망으로 운영하고 있어 안전하다는 생각으로 정보보호시스템이 구축되어 있지 않거나 보안 패치 및 바이러스 백신 업데이트 등이 제대로 이루어지지 않아 보안취약점을 이용한 사이버 공격에 노출되어 있다. 따라서, 사이버 공격 및 침해사고를 방지하기 위해서 지능형교통시스템의 특성을 파악하고 그에 맞는 대응방안을 마련할 필요가 있다. 본 논문에서는 지능형교통시스템에 대한 보안취약요인을 분석하고 보안취약점 개선방안을 제시하고자 한다.

ABSTRACT

The destruction and prejudice of major infrastructure such as energy, broadcast, communication and transportation could result in a threat to individual rights and liberties, as well as social and economic losses. If a traffic signal control facilities have been violated, the lives of the citizens discomfort as well as causing social disruption such as traffic accident. Because the control system is operating as a closed network and you think it is safe, the information protection system has not been built or security patches and anti-virus updates do not work properly. So, cyber attacks by security vulnerabilities are exposed. Therefore, there is a need to identify the characteristics of the system, and develop appropriate countermeasures in order to prevent cyber attacks and prejudices incidents. This paper examines the vulnerabilities of Intelligent Transport Systems and proposes the improvement of security vulnerabilities.

Keywords: Intelligent Transport Systems, Traffic Signal Control Systems

I. 서 론

ICS-CERT(Industrial Control Systems Cyber Emergency Response Team) 보고서에 따르면 2012년 산업제어시스템에 영향을 미치는 고유의 취약성을 171개 추적하였고, 이는 2011년 이후 신규 취약성이 지속적으로 증가하고 있는 추세이다[1]. 특히 에너지·방송·통신·금융·운송 등의 주요 사회 기반 시설은 긴밀하게 연계되어 정부와 국민이 이용하고

접수일(2013년 4월 17일), 수정일(2013년 5월 15일), 게재확정일(2013년 5월 15일)
* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT융합 고급인력과정 지원사업(NIPA-2013-H0301-13-3007)의 연구결과로 수행하였습니다.
† 주저자, withjph@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

있으므로 이러한 분야의 정보시스템의 파괴와 침해는 국가 기능 전반에 걸친 장애를 일으키고, 사회·경제적 손실 뿐 아니라 개인의 자유와 권리를 위협하는 결과를 초래할 수 있다. 이러한 이유로 정보통신기반보호법에 따라 국가적으로 중요한 정보시스템 및 정보통신망은 주요정보통신기반시설로 지정되어 취약점 분석·평가, 보호대책 및 보호계획 수립 등을 통해 전자적 침해사고를 예방하고 유사시 적절한 대응 및 복구를 할 수 있는 토대가 마련되었다[2]. 2012년도에 서울특별시와 6개 광역시 교통신호제어시스템이 신규 지정되었으며, 올해 또한 8개 시도 교통신호제어시스템이 추가 지정되는 등 교통신호제어시설의 보안에 대한 중요성이 갈수록 커지고 있는 상황이다. 도시 기반시설을 제어하는 컴퓨터 시스템은 전통적으로 폐쇄망으로 운영되고 있어 일반적인 개방형 네트워크에서의 바이러스, 악성코드 등과 같은 외부 위협으로부터 안전한 것으로 인식되어 왔으나 최근 이란 부셰르 원전을 감염시켜 발전 설비의 오동작을 일으킨 스턱스넷(stuxnet)이라는 신종 악성코드가 등장하여 각국의 보안전문가들이 주목하고 있다[3].

따라서, 본 논문에서는 교통신호제어시스템에 대한 취약점 분석·평가를 토대로 취약점 및 위협요인을 분석하여 문제점을 도출하고 이에 대한 교통신호제어시스템 환경에 적합한 대응방안을 제시하고자 한다. 2장에서는 선행연구로서 타 제어시스템의 보안 대응방안 연구결과를 분석하고, 3장에서는 지능형교통시스템의 구성 및 특징을 알아보고 이에 대한 보안 취약점을 알아본다. 4장에서는 교통신호 분야 기반시설 취약점 분석·평가를 토대로 관리·물리·기술 분야의 취약점을 분석하고, 5장에서는 교통신호 분야 기반시설이 갖고 있는 취약점에 대한 대응방안을 제시한다. 그리고, 6장에서는 연구결과를 종합하여 교통신호 분야 주요정보통신기반시설에 대한 향후 과제 제안으로 결론을 제시하였다.

II. 선행 연구

지능형교통시스템은 2012년도에 교통신호제어시스템이 기반시설로 신규 지정될 만큼 이전까지 보안취약점 및 대응방안에 대한 연구가 부족하였다. 따라서, 제어시스템, 철도관제시스템 등 유사한 타 제어시스템의 보안 대응방안 연구결과를 통한 보안취약점 대응방안에 대한 이해가 필요하다. 일반적인 제어시스템은 하나의 독립된 제어망으로 운영되기도 하지만 제어시스템의 기능단위로 나뉘어 네트워크로 연결되어 있으므로 이러한 제어시스템 네트워크 구조에서 발생 가능한 보안위협을 구분해보면 다음과 같다[4].

〔A〕 보안 정책 관리 : 내부업무망 및 외부기관과의 연계, 제어망 내 시스템 간 통신 등 많은 연계 접점 및 시스템에 대한 보안정책 수립과 관리 미비

〔B〕 제어망 간 연동 : 현재 많은 제어시스템은 내부 업무망 및 외부기관과 물리적으로 연결되어 데이터를 송수신하고 있으며, 네트워크 연계구간에 정보보호시스템을 운영하고 있다 하더라도 정보보호시스템 설정 부주의에 의해 비인가 접근이 가능함

〔C〕 제어망 내부 사이버침해 전이 : 단일망이 아닌 다수의 서브넷(Subnet)과 중앙 네트워크로 구성되는 경우가 많아서 제어망 내부의 한 시스템에서 발생한 장애나 침해가 전체 제어시스템으로 전이될 위험존재

〔D〕 제어명령 및 감시정보 위변조 : 제어망까지 침입한 해커 또는 악의적 내부자에 의한 제어시스템의 제어명령, 감시정보 위변조 가능

〔E〕 제어시스템 취약점 : 네트워크 장비 및 시스템의 원격접속 서비스, 응용프로그램의 취약점을 이용한 사이버 침해 가능

〔F〕 취약한 인증 시스템 : 긴급 상황 시 인증 절차를 사용하지 않거나 제어소프트웨어에 하드코딩되어 있는 비밀번호 사용 또는 단순 패스워드 사용 경우가 많음

〔G〕 서비스 거부 공격에 취약 : 임베디드 장비를 포함한 제어시스템은 한정된 자원에 의해 서비스 거부 공격에 취약

이와 같은 보안위협을 해결하기 위한 제어시스템 보안시스템은 〔표 1〕과 같다. 제어시스템 보안을 위해서는 이외에도 추가적으로 Whitelist 기반 보안감시, 보안정책 반영 및 관리, 추후 분석을 위한 보안로그 생성 및 관리, 제어망과 보안관제망의 분리 등이 향후 제어시스템 네트워크 보안기술 개발 및 적용을 위해 필요한 사항들이다.

철도관제시스템은 열차집중제어(CTC, Centralized

〔표 1〕 보안제품이 해결하고자 하는 보안위협

보안시스템 분류	관련된 보안위협
제어시스템 방화벽	B, D, E, F, G
일방향 자료전달 장치	B
침입탐지시스템	C, D, E, F, G
보안제품 중앙관리	A

〔표 2〕 CTC 시스템의 전반적인 보안 방안

구분	보안 방안
네트워크	- 방화벽(IPS) 설치 및 운영 - 특정 패킷에 대한 필터링 - 불필요한 데몬 및 서비스 제거 - 네트워크 로깅 관리
주컴퓨터	- 사용자 계정 및 패스워드에 대한 관리, 보안정책의 설정 - 시스템 접근 권한 제한 및 분리 - 파일 시스템에 대한 보안 강화 - 올바른 시스템 구성 및 패치 적용 - 시스템 로그 분석, 감사 및 접근통제
콘솔장치	- CMOS 암호설정, 화면보호기 기동 및 패스워드 설정 - 파일 공유시 패스워드 설정 - 백신 프로그램의 설치 및 운영
데이터베이스	- 비권한자의 데이터 접근 통제 - 사용자 및 업무 구분을 통한 계정 및 접근 권한 통제 - DBMS 고유의 보안 기능(Audit) 활용 및 핵심 정보 로깅
응용프로그램	- 업무구분을 통한 계정 및 권한 통제 - 응용 프로그램별 및 단위 업무별 권한 통제 - 특정 시간대별 접근 통제 - 응용 프로그램 사용 상태 관리

Traffic Control)장치라 칭하며 전 선구로부터 수집된 데이터를 바탕으로 중앙에서의 직접적인 열차운행 제어, 통제 및 감시를 수행한다[5]. 열차 운행 통제를 위한 관제시스템은 보호용 자가 통신망을 구축하여 외부로부터의 비정상적인 접근을 차단하고 있으며, CTC에 대한 접근은 연계되는 외부 시스템을 통한 접근과 사용자 인터페이스를 제공하는 콘솔 장치로의 접근 2가지 방법이 고려될 수 있다. 따라서, 2가지 경로에 대한 보안을 위해 콘솔장치 보안, 네트워크 보안을 강구함과 동시에 〔표 2〕와 같은 전반적인 보안방안을 수립하여야 한다.

III. 지능형교통시스템(ITS) 보안 취약점

3.1 지능형교통시스템 구성 및 특징

교통·전자·통신·제어 등 첨단기술을 도로·차량·화물 등 교통체계의 구성요소에 적용하여 실시간 교통정보를 수집·관리·제공함으로써 교통시설의 이용효율을 극대화하고, 교통 이용편의와 교통안전을 제고하며 에너지 절감 등 환경 친화적 교통체계를 구현하는 21세기형 교통체계를 지능형교통시스템 즉, ITS(Intelligent Transport System)라 한다. ITS는 전국의 도로, 차량, 운전자 및 여행객들을 대상으로 교통 관련 정보와 기상 정보, 도로 상태 정보 등을 수집, 처리, 가공하고 이를 유무선 통신수단을 이용하여 도로변 교통 단말기, 차내 단말기, 교통방송, 전화 등으로 차량 운전자 및 여행객들에게 전달함으로써 통행의 편의와 교통량의 원활한 소통을 이루기 위한 시스템이다[6]. ITS는 교통 이용자에 대한 서비스 제공과 서비스 제공을 위한 효율적인 공급체계 구축의 두가지로 분류할 수 있다.

〔표 3〕 ITS 제공서비스 분류 및 내용

서비스 분류		서비스 내용
교통관리 최적화	- 교통흐름 관리 - 돌발상황 관리 - 자동 교통단속 - 교통공해 관리지원 - 교통시설 관리지원	- 차량의 원활한 흐름 제공 - 돌발상황 대처 및 교통량 분산
전자 지불 처리	- 통행료 전자지불 - 요금 전자지불	- 정체 감소 및 이용자 편의 제공
교통정보 유통 활성화	- 교통정보 제공 - 교통정보 관리연계	- 연계를 통한 경제적 선택 기회 제공
여행자 정보 고급화	- 차량여행자 및 비차량여행자 부가 정보제공	- 합리적 의사 결정 도움 - 여행경로 및 편의시설 이용
대중교통 활성화	- 대중교통정보 제공 - 대중교통 관리	- 버스운행 조정, 도착정보 등 제공
화물운송 효율화	- 물류정보 관리 - 위험물 차량 관리 - 화물 전자 행정	- 신속한 화물 운송 및 안전 운행 유도
차량·도로 첨단화	- 안전 운전 지원 - 자동 운전 지원	- 위험요소 자동 감지 및 운전자 경고

첫째, 교통 이용자에 대한 서비스 제공에 따른 분류 및 내용은 〔표 3〕과 같이 교통관리 최적화, 전자 지불 처리, 교통정보 유통 활성화, 여행자 정보 고급화, 대중교통 활성화, 화물운송 효율화, 차량 및 도로 첨단화 등 7개 분야, 16개 사용 서비스, 63개 세부 서비스로 분류되어 있다. 개인 생활과 밀접한 관계가 있는 이러한 서비스의 파괴와 침해는 국가 기능 전반에 걸친 장애 뿐 아니라 사회적인 혼란을 초래할 수 있음을 알 수 있다.

둘째, 서비스 제공을 위한 효율적인 공급체계 구축

〔그림 1〕 ITS 제공서비스별 시스템 분류

에 따라 첨단교통관리시스템, 첨단운전자정보시스템, 첨단대중교통정보시스템, 물류운영시스템, 첨단차량도로시스템으로 분류할 수 있으며, 〔그림 1〕과 같이 각 시스템별로 다양한 서비스를 제공하고 있다. 각 시스템별 특징은 다음과 같다.

① 첨단교통관리시스템(ATMS, Advanced Traffic Management System) : 도로상에 차량 특성, 속도 등의 교통정보를 감지할 수 있는 시스템을 설치하여 교통상황을 실시간으로 분석하고, 이를 토대로 도로 교통의 관리와 최적 신호체계의 구현을 꾀하는 동시에 여행시간 측정과 교통사고 파악 및 과적 단속 등의 업무 자동화를 구현한다. 실시간 교통관리 및 제어, 돌발상황관리, 자동교통단속, 자동요금징수, 과적차량관리 등의 서비스를 제공한다.

② 첨단운전자정보시스템(ATIS, Advanced Traveler Information System) : 교통여건, 도로상황, 출발지에서 목적지까지의 최단경로, 소요시간, 주차장 상황 등 각종 교통정보를 FM라디오방송, 차량내 단말기 등을 통해 운전자에게 신속, 정확하게 제공함으로써 안전하고 원활한 최적 교통을 지원한다. 운전자정보시스템, 최적경로안내시스템, 여행서비스정보시스템 등이 해당된다.

③ 첨단대중교통정보시스템(APTS, Advanced Pub lic Transportation System) : 대중교통 운영체계의 정보화를 바탕으로 시민들에게는 대중교통수단의 운영스케줄, 차량위치 등의 정보를 제공하여 이용자 편익을 극대화하고, 대중교통 운송회사 및 행정부서에서는 차량관리, 배차 및 모니터링 등을 위한 정보를 제공함으로써 업무의 효율성을 극대화한다. 버스교통정보시스템, 대중교통관리시스템 등이 해당된다.

④ 물류운영시스템(CVO, Commercial Vehicle Op eration System) : 컴퓨터를 통해 각 차량의 위치, 운행상태, 차내 상황 등을 관제실에서 파악하고 실시간으로 최적운행을 지시함으로써 물류비용을 절감하고, 통행료 자동징수, 위험물 적재차량 관리 등을 통해 물류의 합리화와 안전성 제고를 도모한다. 전자통관시스템, 화물차량관리시스템 등이 해당된다.

⑤ 첨단차량도로시스템(AVHS, Advanced Vehicle and Highway System) : 차량에 교통상황, 장애물 인식 등의 고성능 센서와 자동제어장치를 부착하여 운전을 자동화하며, 도로상에 지능형 통신시설을 설치하여 일정간격 주행으로 교통사고를 예방하고 도로소통의 능력을 증대시킨다. 완전자동운전, 차량간격 자동제어, 도로용량 증대 등의 서비스를 제공한다.

3.2 지능형교통시스템 보안취약점 분석

ITS는 국가 기반시설로서 시민들에게 교통정보에 대한 안전한 서비스 제공을 목적으로 하기 때문에 기밀성, 무결성, 가용성, 책임성, 신뢰성 등의 보안요소별 정보보호 목적을 가지고 있다. 또한, 이러한 보안요소를 침해하는 주요 위협요소는 표준 프로토콜 및 잘 알려진 취약성을 가진 기술의 채택, 다른 네트워크와의 접점 증가, 안전하지 않은 연결의 증가, 제어시스템에 대한 기술적인 정보의 노출 등이다〔7〕. 이와 같이 제어시스템의 개방화에 따라 보안 침해 위협요소는 갈수록 증가하게 되어 다양한 공격 경로를 통한 해킹 가능성이 높아지고 있다. ITS에서 해킹 경로로 악용될 수 있는 구간은 시스템 내부 취약점, 타 시스템과 연계 상의 취약점, 시스템 외부 취약점의 세가지로 분류할 수 있다〔10〕.

3.2.1 시스템 내부 취약점

제어시스템에 대한 직접적인 접근 시도는 어렵지만 제어시스템을 관리하고 있는 운영 단말 PC의 취약점을 이용하거나 외부 인터넷상에 서비스를 제공하고 있는 DMZ 구간의 웹서버 등의 취약점을 이용한 내부 제어시스템에 대한 공격은 가능하다. 일반적으로 〔표 4〕와 같은 시나리오에 의한 공격이 이루어지는데 대부분의 제어망에서 24시간 가동되는 PC 및 시스템들은 보안패치를 하지 않거나 바이러스 백신을 설치 또는 업데이트를 하지 않고 있다. 또한 일부 단말의 경우 공유폴더가 적용되어 있고 공유폴더 내에 제어설비 운영프로그램 등의 중요정보가 포함되어 있어 이는 시급하게 개선해야 할 취약 요인 중 하나이다. 그리고, DMZ 구간의 웹서버 취약점을 이용한 접근 또한 가능

〔표 4〕 시스템 내부 공격 시나리오

구분		특징
1 단계	시스템 정보 및 취약점 수집	- TCP/IP의 구조적 결함이나 시스템의 결함, 각종 서비스 결함 등의 정보 수집
2 단계	관리자 권한 획득	- 취득한 정보를 기반으로 시스템 취약점을 이용하거나 악성코드 등을 통한 관리자 권한 획득
3 단계	악성 프로그램 설치	- 스니퍼(Sniffer) 등을 설치하여 아이디나 패스워드도청
4 단계	중요정보 취득	- 자료 변조 또는 파괴, 불법 유출 등의 실행
5 단계	공격 전이	- 타시스템으로의 접근 및 비인가자에 의한 제어시스템 조작 가능 여부 확인, 제어시스템 권한 획득에 의한 공격 시도

하다. 단순 패스워드 또는 디폴트 패스워드를 사용하는 취약한 계정관리를 통하여 웹서버 관리 권한 획득이 가능하며 권한 획득 후 웹서버 내에 존재하는 제어프로그램을 이용한 제어프로그램 관리 권한 및 DB 권한 획득이 가능하다. 이는 파일 업로드 시 무결성 검증 등의 프로세스 검증이 누락되어 악성 파일 업로드가 가능하였고, 웹서버 내에 제어프로그램 등의 중요정보가 존재하기 때문이다.

3.2.2 타 시스템과 연계상의 취약점

ITS는 각 연계 시스템 간 물리적, 논리적 데이터 흐름을 가지고 있으며 각각의 데이터 흐름은 출발지, 도착지, 연결방식, 위협요소, 보안요소로 연결될 수 있다. ITS는 7개 분야 16개 서비스를 제공하는 시스템이 있으며 본 절에서는 교통신호 제어와 관련된 TMS, TRMS, TRVS에 대한 특징 및 상호 데이터 흐름에 따른 취약점을 알아보고자 한다〔9〕.

- TMS(Traffic Management Subsystem) : TMS는 트래픽 처리, 사고 등의 데이터를 제공하는 중요한 서브시스템으로서 관리 기능과 다른 ITS 서브시스템과의 정보교환을 수행하고 있다. 또한 트래픽 흐름 모니터링 및 조정, 교통신호 우선순위, 긴급차량 우선 부여, 교통사고 감지 및 검증, 다른 ITS 서브시스템과의 데이터 신호 등을 조정한다. 그리고, 타 시스템과의 데이터 교환 시 유선 통신 체계를 사용하고 있다. TMS 신호 제어 소프트웨어가 동작하지 않거나 프로그램상 오류가 발생할 경우에 관리자는 트래픽 흐름을 확인하거나 제어할 수 없을 뿐 아니라 교통사고를 감지하거나 판별할 수도 없다.
- TRMS(Transit Management Subsystem) : TRMS는 운송 수단으로부터 운영 데이터를 수집하고 자동차와 운전자에게 교통 정보를 제공하는 중요한 서브시스템이다. 또한, 다른 ITS 서브시스템과 정보 교환할 때 유선과 무선 통신 체계를 모두 사용하고 있다. TRMS가 침해로 인해 동작이안될 경우에는 다른 ITS 서브시스템과의 통신이 끊기게 되어 교통운전자나 차량 등에 자동화된 경고나 운송신호에 대한 우선순위 정보를 실시간으로 전송할 수 없게 된다.
- TRVS(Transit Vehicle Subsystem) : TRVS는 승객들을 안전하고 효율적으로 운송하기 위한 센서, 프로세싱, 저장, 통신 기능 등을 제공하는 차량 서브시스템이다. TRVS는 TRMS에 운영데이터를 제공하고 네트워크 상태 업데이트 정보를 받고 여행자들에게 경로정보를 제공한다. 또한, 운전자와 승객 모두에게 보안 기능을 제공한다.
  TRVS의 침해로 인해 승객 수나 차량 운행 시간 등의 정보가 제공되지 않는다면 스케쥴 정보나 운송 계획 등을 수집할 수 없게 된다.

이와 같이 ITS 서브시스템 간 데이터 흐름과 그에 따른 보안 위협요소 및 보안요소를 분석한 결과는 〔표 5〕와 같다. 연결성의 증가로 인해 시스템이 거대화되고 접속점이 증가하면 그만큼 위협요인이 침입할 루트(route)가 많아지게 되고, 복잡성으로 인해 특정 위협에 대한 일관된 보안정책을 적용하는 것이 힘들어지게 된다〔10〕. 일반적으로 모든 데이터 플로우는 DoS 공격을 받기 쉽지만 대부분의 서브시스템들은 이에 대한 대응 방안이 마련되어 있다. 또한, 개인정보 등 민감한 정보를 담고 있지 않은 서브시스템 간 데이터 플로우는 정보 유출에 대한 위협이 있는 걸로 간주하지는 않는다. 예를 들어 TRVS에서 TRMS로 제공되는 "vehicle probe data"와 같은 데이터플로우는 link time과 위치 등의 정보를 제공할 뿐 개인정보 등의 민감정보는 담고 있지 않다. 하지만, 개인정보 등을 포함하는 데이터 플로우 상의 정보 유출에 대한 위협은 기밀성에 해당하는 보안요소로 적절하게 제공되어

〔표 5〕 ITS 서브시스템 간 데이터플로우 분석

출발지	데이터 흐름	목적지	통신 방식	위협요소						보안요소			
				DoS	Dis	Man	Mas	Rpy	Rpd	Aut	Con	Int	NRp
TMS	signal priority status	TRMS	w	○			○			○			
TMS	trffic information	TRMS	w	○			○			○			
TRMS	request for transit signal priority	TMS	w	○			○			○			
TRMS	transit system data	TMS	w	○			○			○			
TRVS	emergency notification	TRMS	u1t	○	○	○	○			○	○	○	
TRVS	transit vehicle condition	TRMS	u1t	○	○		○			○	○		
TRVS	traveler information request	TRMS	u1t	○	○	○	○	○	○	○	○	○	○
TRMS	emergency acknowledge	TRVS	u1t	○		○	○			○			
TRMS	request for vehicle measures	TRVS	u1t	○			○			○			
TRMS	schedules, fare info request	TRVS	u1t	○	○	○	○	○	○	○	○	○	○
TRMS	traveler information	TRVS	u1t	○	○	○	○		○	○	○	○	○

※ 약어 설명
- 통신방식 : w(wireline), u1t(2-way wide area wireless)
- 위협요소 : DoS(Denial of Service), Dis(Disclosure), Man(Manipulation), Mas(Masquerading), Rpy(Replay), Rpd(Repudiation)
- 보안요소 : Aut(Authentication), Con(Confidentiality), Int(Integrity), NRd(Non-Repudiation)

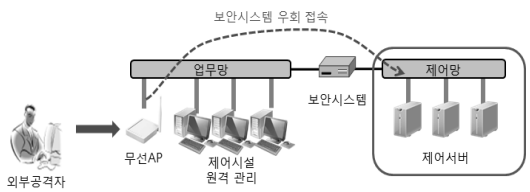
야 한다. 또한, 재정, 긴급, 사고, 안전 정보 등을 담고 있는 데이터플로우는 데이터 조작에 상당히 취약하다. 차량 통행에 직접적인 영향을 미치는 이러한 데이터 정보들은 다양한 시그널이나 메시지 등을 통해 운전자에게 전달되기 때문에 데이터 조작 등의 발생 시 큰 사고로 이어질 수 있다. 정상적인 도구를 가진 비인가자는 합법적인 서브시스템의 하나로 가장할 수가 있다. 따라서, 거의 모든 데이터 플로우는 수신된 메시지가 정상적으로 인증된 서브시스템으로부터 전송되었다는 것을 확신할 수 있어야 한다. 일반적인 운영 데이타플로우는 부인방지에 취약하다고 볼 수 없지만 시설 관리자들은 이러한 데이터플로우에 대해서도 부인방지에 대한 보안사항을 고려해야 한다. 예를 들어 TMS과 TRMS 사이의 "signal priority status" 데이터플로우는 도로 상의 신호 우선순위 요청 기능의 상태 정보를 제공하는데 비록 이러한 정보들에 대한 부인방지는 가능하지 않거나 관련 없이 보일 수 있지만 교통관리 시설 관리자는 법적, 관리자적 측면에서 이 정보가 교통 관리 작업을 보호하는데 중요하다고 보기 때문이다.

3.2.3 시스템 외부 취약점

일반적으로 제어망과 업무망은 물리적으로 분리되어 있으나 업무상 관리를 위해 연결되어 보안시스템을 통해 통제하고 있다. 이 때 업무망에는 업무망 무선 AP를 사용하는 경우가 있다. 무선 환경은 유선 네트워크와 달리 기본적으로 모든 단말에 데이터를 전송하는 브로드캐스팅 망이므로 AP의 비콘(Beacon) 프레임 수신 영역 내에 있는 모든 단말은 해당 AP로 접속을 시도할 수 있다. 따라서, 해당 무선 LAN 시스템이 사용자 인증과 관련된 보안 기능을 수행하지 못한다면 비인가 사용자의 접근이 가능할 것이며, 이는 보안상 중대한 위협요인이 되는 것이다. 외부공격자는 〔그림 2〕에서와 같이 취약한 무선AP 해킹을 통해 업무망에 접근하고 보안시스템을 우회하여 제어망의 제어서버로 침투할 수 있다.

무선랜 환경의 취약점은 다음과 같다.

① Rogue AP : Rogue AP가 무선 LAN에 위치하면 공격자는 AP에 대해 인증없이 네트워크 접근이



〔그림 2〕 무선 AP를 통한 제어망 침투

가능하게 되며 내부망에 설치된 AP가 암호화 기능을 사용하지 않거나 WEP 등과 같은 약한 수준의 보안설정일 경우 해당 AP는 내부 네트워크에 접속할 수 있는 출입구 역할을 하게 된다.

② IP 스푸핑(Spoofing) : IP 스푸핑은 기밀성에 대한 위협으로 TCP/IP 프로토콜의 설계상 문제로 인하여 허가되지 않은 사용자가 내부망에서 외부망으로 전송되는 패킷으로부터 발신처를 도용하여 허가된 사용자인 것처럼 위장하여 시스템을 공격하는 방법이다.

③ 데이터 변조(Injection and Modification of Data) : 전송 중인 데이터에 변형을 가하여 수신자로 하여금 잘못된 데이터를 수신하게 하는 공격 방법을 데이터 변조라 한다. 데이터 변조 공격은 정당한 송수신 채널을 마비시킬 수 있으며, 특히 DoS(Denial of Service) 공격에 사용될 수 있는 강력한 위협 요인이다.

④ 통신 방해(Communication Jamming) : 무선 네트워크에서 흔히 겪게 되는 통신 장애 중의 하나로 의도된 공격자에 의한 간섭현상이 있다. 전파 특성을 고려한 통신 방해를 일컫는 재밍은 무선 LAN 환경에서도 주요한 위협요인이 될 수 있다.

IV. 교통신호분야 기반시설 보안취약점

4.1 기반시설 보안취약점 분석·평가

기반시설 관리기관은 기반보호법에 의거, 보유중인 기반시설에 대한 취약점 분석·평가 및 보호대책을 매년 수립해야 한다. 본 절에서는 「주요정보통신기반시설 취약점 분석·평가 기준('11.5월, 행안부)」을 토대로 주요 7개 도시의 교통신호제어시스템에 대한 보안 취약점을 비교·분석하여 교통신호제어시스템 관리기관의 공통적인 특징을 파악하고 개선방안을 제시하고자 한다. 관리적 취약점 점검항목은 정보보호정책, 정보보호조직, 인적보안, 외부자보안, 자산분류, 매체관리, 교육 및 훈련, 접근통제, 운영관리, 업무연속성관리, 사고대응, 감사 영역의 총 12개 영역 90개 세부항목으로 구성되어 있고, 물리적 취약점 점검항목은 접근통제, 감시통제, 전력보호, 환경통제 영역의 총 4개 영역 25개 세부항목으로 구성되어 있다. 기술적 취약점 점검항목은 서버(UNIX, Windows), 제어시스템, 네트워크 장비, 보안시스템별로 점검 대상을 분류하였고, 취약점 결과는 다음과 같다.

관리분야의 주요 취약점을 살펴보면 대부분 시스템

〔표 6〕 관리분야 주요 취약점

분류	주요 취약점
정보보호정책	- 교통신호제어시스템에 특화된 정보보호체계를 갖추고 있지 못함
정보보호조직	- 교통신호 제어시설의 보안전담 조직 및 인력이 없음
매체관리	- 관리콘솔 PC의 USB 포트가 노출되어 있으며, USB 포트 접근 용이함
교육 및 훈련	- 내부직원과 외부용역 대상 정보보호 교육 미수행
접근통제	- 공통계정을 사용하여 공유함
운영관리	- 취약점조치미흡 및 일부 백신미설치

유지보수 및 운영 업무를 외부에 위탁하고 있어서 외부자 보안 및 내부정보 유출방지에 대한 철저한 보안이 필요하며 기존 보안대책도 잘 수립되어 있는 상태이다. 그러나, 전반적인 보안관리체계에 대한 점검이 이루어지지 않아 관리지침 수립, 정보보호 교육 등 기본적인 부분에서도 미비한 부분이 많았다. 관리분야 주요 취약점은 〔표 6〕과 같다.

물리분야의 주요 취약점을 살펴보면 교통신호제어시스템은 경찰청에 위치하거나 별도 교통정보센터에 구성되어 있는데, 교통정보센터의 경우 경찰청에 비해 물리적으로 다소 취약하여 외부 출입자에 대한 출입통제가 제대로 이루어지지 않거나 CCTV 등의 보안 대책이 미비하다. 물리분야 주요 취약점은 〔표 7〕과 같다.

기술분야 중 제어시스템 취약점을 살펴보면 계정관리 영역에서는 제어시스템 운영관리 계정을 공유하여 사용하고 있어 사고 발생 시 추적이 어렵고, 일부 제어시스템의 경우에는 아이디와 패스워드가 하드코딩되어 있어 주기적인 변경이 어렵다. 패치관리 영역에서는 OS 패치 등을 위한 사전 테스트 절차가 없고, 보안패치 등을 수행하지 못하여 취약점이 노출되어 있는 상태이다. 접근통제 영역에서는 운영자 권한이 분리되어 있지 않아 일반 운영자도 관리자 권한으로 접

〔표 7〕 물리분야 주요 취약점

분류	주요 취약점
접근통제	- 출입통제시스템이 없거나 사용하지 않아 비인가자의 출입이 가능함
감시통제	- CCTV가 설치되어 있지 않고, 출입자 관리가 수행되지 않음
환경통제	- 전산실이 업무공간과 분리되어 있지 않으며 통제 방안이 없음

〔표 8〕 기술분야 제어시스템 주요 취약점

분류	주요 취약점
계정 관리	- 제어시스템 운영관리 계정을 공유 하고 있어 사고 발생시 추적 어려움
패치 관리	- OS 패치 등을 위한 사전테스트 절차가 없고, 보안 패치 등을 수행하지 않아 취약점에 의한 공격 발생 가능
접근 통제	- 제어시스템 운영자 권한이 분리되어 있지 않아 일반 운영자의 실수 등을 통한 사고 및 비인가자의 접근 용이 - USB 포트 등이 물리적으로 차단되어 있지 않아 이동식 저장 매체를 통한 악성코드 유입 가능
보안 관리	- 발생된 취약점에 대한 조치가 즉각적으로 이뤄지지 않아 보안취약점이 노출되어 있음

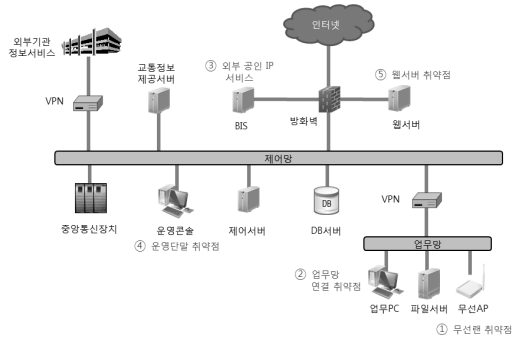
속이 가능하여 운영자 실수나 계정 탈취 시 심각한 보안사고가 발생할 우려가 있다. 기술분야 제어시스템 주요 취약점은 〔표 8〕과 같다. 이와 같이 7개 기관별 관리적/물리적/기술적 취약점 분석·평가 결과를 비교해보면 〔표 9〕와 같다. 각 기관별 공통적으로 가장 취약한 항목은 교육 및 훈련 시행과 자체보안 점검 활동, 제어망 내 접근통제 항목이고, 서버시스템과 응용시스템 계정 보안이 취약하여 지속적인 조치및 보안활동이 필요함을 알 수 있다.

교통신호제어시스템을 구성하는 제어망은 교통신호 제어 업무의 가용성 확보가 중요하기 때문에 외부로부터의 불법적인 접근을 차단하고, 안정적인 서비스 제

〔표 9〕 7개 기관 취약점 분석평가 결과 비교

분류		A	B	C	D	E	F	G
관리적	정보보호정책 존재	△	×	△	×	○	△	△
	정보보호직무 포함	×	×	△	×	△	△	△
	외부자 보안 통제	△	△	△	△	△	△	△
	교육 및 훈련 시행	×	×	×	×	×	×	×
	매체 보안 통제	△	×	×	×	×	×	△
	운영관리 인력상주	△	×	×	△	△	△	△
	자체점검/감사수행	×	×	×	×	×	×	×
물리적	외곽 출입 통제	○	○	×	×	△	×	×
	내부 출입 통제	×	△	×	△	○	△	△
	전산실 이중장치	△	○	×	×	○	×	○
	CCTV감시체계	△	○	×	×	○	×	△
기술적	디폴트계정 제거	△	×	×	×	×	○	△
	외부 접근 차단	○	△	△	△	△	○	×
	제어망내 접근통제	×	×	×	×	×	×	×
	계정보안	△	△	×	×	×	×	×
	장비이중화 구성	×	×	×	△	○	×	○
	타기관과의未연계	○	×	×	×	×	○	○

〔범례〕 ○ : 적용 △ : 일부 적용 × : 미적용



〔그림 3〕 교통신호제어시스템 구성과 보안취약점

공에 대한 위협요소를 최소화하기 위해 별도의 망을 구성하여 업무망 또는 외부망과 분리한다. 하지만 제어시스템에 대한 내부 직원의 시스템 관리, 외부 기관으로의 교통정보 제공 등을 위해 네트워크 구성 상 연결되어 있음을 알 수 있다. 따라서, 교통신호제어시스템 네트워크 구성 점검을 통하여 제어시스템 네트워크를 통해 발생 가능한 보안위협을 구분해 보았다. 〔그림 3〕은 교통신호제어시스템 운영을 위한 네트워크 구성도이며, 외부기관과의 연계망, 제어망, 업무망, 인터넷망 등을 나타내고 있다.

① 무선랜 취약점 : 일반적으로는 제어시스템 운영망과 업무망은 분리되어 있지만, 원격 접속 관리를 위해 업무망에서 VPN을 통해 제어시스템을 접속하도록 구성되어 있다. 이때 업무망에서 사용하는 외부 인터넷 접속 가능 무선AP의 취약점을 통해 침투하고VPN을 통해 제어시스템까지 접속이 가능하다. 이 때 무선랜의 취약한 암호화 방식 사용으로 인해 외부 비인가자의 무선랜 접속이 가능하다. 무선랜 접속 후 파일서버 등의 공유정보를 확인하여 제어시스템의 정보를 얻고 이를 통해 제어망에 접근하여 제어망의 주요 시스템에 대한 권한 획득이 가능하다.

② 모니터링 및 관리를 위한 업무망 연결 : 제어시스템에 대한 모니터링 및 관리를 위해 업무망과 연결되어 있는 구간으로 VPN 또는 방화벽을 통해 통제 적용하고 있다. 그러나, 업무망에 연결되어 있는 파일서버나 PC 공유폴더 내에 저장되어있는 시스템관련 중요정보 등이 미암호화 상태로 노출되어 있으므로 제어망으로의 접속 후 이 정보를 통해 제어시스템 권한 획득이 가능하다.

③ BIS(버스정보시스템) 등의 외부 제공 서비스 : BIS 등의 시스템은 제어시스템으로 분류되어 있지 않아 기반시설 대상은 아니므로 취약점 점검을 수행하지

않는다. 하지만, 외부 서비스 제공을 위해 공인 IP로 설정 운영되고 있으므로 외부에서의 직접 접근이 가능하며 별도의 통제장치 없이 제어망과 연결되어 있는 경우가 있다. 따라서, BIS 네트워크 영역을통한 침투 가능성이 존재하므로 이러한 외부 서비스를 제공하는 시스템에 대해서도 취약점 점검을 수행하고 취약점에 대한 보안 조치가 필요하다.

④ 운영 콘솔 내의 중요 정보의 노출 : 운영 콘솔의 경우 각 운영프로그램의 설정정보에 주요 시스템 접속 정보가 평문으로 저장되어 있어 비인가자가 정보를 획득했을 경우 해당 시스템 관리 권한 획득이 가능하다. 또한 윈도우 보안 패치나 바이러스 백신 업데이트가 미흡할 경우 해당 취약점을 통해 해당 PC의 관리자 권한을 획득할 수 있다.

⑤ 웹서버 취약점 : 교통정보 대외 서비스를 위한 웹서버를 운영하고 있으며, 제어망 또는 업무망과 방화벽 등의 보안시스템을 통해 통제 적용하고 있다. 웹서버의 취약점으로 인해 외부 비인가자가 침투하여 웹서버 관리 권한을 획득할 수 있으며, 이후 DMZ에서 제어망으로의 접근이 가능하다. 제어망 내의 DB 권한을 획득하고, 교통신호 제어프로그램 관리 권한을 획득하여 교통신호제어시스템 통제가 가능하다.

이와 같은 취약점분석 결과에 대한 원인을 분석해 보면 교통신호제어시설의 기반시설 지정은 2012년에 처음으로 지정되었다. 따라서, 그 이전까지는 정보보호에 대한 전반적인 점검 및 대응 조치가 체계적으로 이뤄지기가 어려웠다고 볼 수 있다. 제어시설 기준은 미비하여 기관별 기반시설 범위가 다르고 표준화된 정책/지침 가이드를 제시할 수 없었고, 정보보호 담당자는 운영이 주업무여서 기술적인 취약점 조치 등은 유지보수 업체에 의존할 수 밖에 없으므로 기관 내의 자체 정보보호 전문가는 부족한 실정이다. 또한, 제어망은 폐쇄망이며 제어시스템의 특수성으로 안전하다는 인식이 일반적이었으나 실제로는 다양한 서비스망과 연결되어 있고, 서버 및 운영 콘솔 등은 윈도우즈를 사용하고 있어 일반 시스템의 보안취약점 특성도 그대로 포함하고 있음을 알 수 있다. 따라서, 이러한 근본적인 원인을 해결하기 위해 제도적, 관리적, 물리적, 기술적 분야별로 대응방안을 수립하고자 한다.

V. 교통신호분야 기반시설 보안취약점 대응방안

5.1 제도적 개선 방안

교통신호 제어시설을 관리하고 있는 7개 기관의 기반시설 대상 범위를 보면 시스템 용어가 통일되지 않거나 기반시설 범위 또한 다름을 알 수 있다. 이러한 이유로 공통적인 정책 및 지침 등의 가이드 제시가 어렵다. 또한, 시스템 변경 시에 필요한 구축 가이드도 마련되어 있지 않아 시스템 변경 및 구축 시에 보안 기준을 적용하지 못하고 있다. 따라서, 기반시설 관리 영역 범위로 설정하기 위한 기준을 수립하고, 동일 시설 및 동일 용도의 자산에 대해서 용어를 표준화해야 한다. 그리고, 시설 변경 발생 시 적용할 구축 및 통제 구현 표준가이드를 제시하여 최초 시스템 도입 또는 변경 시 보안 기준을 적용하여 보안취약점을 사전에 제거하는 절차를 수립하여야 한다. 그리고, 정보보호 활동을 강화하기 위한 성과관리 제도가 필요하며 취약점 분석평가 결과 및 취약점 이행 조치율 등의 KPI 관리를 통해 관리 수준을 높이고, 이에 대한 결과를 각 기관장들의 경영성과 평가에 반영하여 보안의 중요성을 강조함으로써 보안담당자의 책임감을 높일 수 있도록 해야 한다. 또한, 제어시스템을 운영하는 각 기관에는 제어시스템에 대한 정보보호 전문가가 부족하여 적극적인 조치 및 이행 확인이 제대로 이루어지지 않고 있으므로 제어시설별 중앙부처 및 지자체의 협조 및 지원을 통해 정보보호 실무자들에 대한 보안관리 능력을 향상시킬 수 있도록 정기적인 기술 및 정보교류를 실시하고, 신규 취약점 및 기술적 조치방법 등에 대한 기술교육을 의무화해야 한다.

5.2 관리·물리적 개선 방안

교통신호제어시설 취약점 분석평가 결과에 따라 관리·물리 분야의 공통적인 주요 취약점을 확인할 수 있었고, 각 취약점에 대한 보안방안을 정리하면 〔표 10〕과 같다. 7개 교통신호제어시스템 관리 기관은 각 시의 정보통신 보안업무규정을 준용하되 교통신호제어 분야 특성에 맞는 관리적, 물리적, 기술적 부문에 대한 보안 업무 지침을 수립하고, 이에 대한 평가 항목을 마련해야 한다. 또한, 시스템 유지보수 및 운영을 외부업체에 위탁운영하고 있기 때문에 유지보수업체의 업무수행에 대한 보안요구사항을 정의하고, 정기적인 실태 관리를 수행해야 한다. 보안업무를 수행하는 정보보호담당자는 전문적인 보안교육을 받지 못했을 뿐 아니라 제어시스템 운영이 주업무이고 보안업무는 부가적인 업무이기 때문에 제어시설 정보보호 담당자 역량 강화를 위한 교육과정의 개발이 필요하며 이는 관리기관의 역할이 아닌 중앙부처 및 지자체 등의 상

〔표 10〕 관리·물리적 보안 방안

구분		보안 방안
관리적	정보보호 정책	- 교통신호제어시스템 특성을 반영한 정책/지침/절차 수립 - 유지보수 업무수행에 대한 보안요구사항 및 실태관리
	정보보호 조직	- 제어시설 보안 전담 인력 확충
	교육 및 훈련	- 정보보호책임자/실무자, 제어시설 운영자 의무 교육 실시 - 외부 용역 직원 대상 정보보호 교육 실시
물리적	접근통제	- 출입통제시스템을 통한 비인가자 출입 통제
	감시통제	- CCTV 설치 및 출입자대장 관리
	환경통제	- 전산실과 업무공간의 물리적 분리

위기관에서 지원해줘야 한다. 이러한 교육을 실시하여 정보보호 수준 제고 및 보안 성숙도를 높일 수 있다. 교통신호제어시스템을 관리하는 교통정보센터는 각 시의 경찰청 내에 위치하거나 독립 센터로 운영되는데 독립 센터는 경찰청 내부 시설에 비해 물리적으로 취약하다. 따라서 CCTV 설치 및 외부 출입자 관리 등을 통하여 접근통제 및 감시통제를 강화하여야 한다.

5.3 기술적 개선 방안

서버, 네트워크, 보안시스템의 기술적 취약점에 대한 보안방안은 〔표 11〕과 같이 정리할 수 있다. 이러한 기술적 취약점은 주기적인 점검 및 보안조치를 통해 개선해야 하며, 실제 취약점 조치는 외부 운영업체에 의존하여 이루어지고 있기 때문에 관리기관 담당자는 관련 기술지침을 명확히 제시하고, 보안 조치 등의 운영 결과에 대한 지속적인 관리가 필요하다. 또한, 〔그림 3〕과 같이 교통신호제어시스템 네트워크 구성상 발생 가능한 보안위협은 무선랜 취약점, 업무망 연결 취약점, 외부 제공 서비스 취약점, 운영 콘솔 취약점, 웹서버 취약점의 5가지로 정리할 수 있으며, 이에 대한 대응방안은 다음과 같다.

5.3.1 무선랜 취약점 대응방안

무선AP 등의 무선 접속은 제어망 내에서는 사용하지는 않지만, 제어망과 연결되어 있는 업무망 또는 원격 관제를 위한 외부 네트워크 망에서는 사용하고 있다. 하지만, 취약한 암호화 방식(WEP)을 사용하거나

〔표 11〕 기술적 보안 방안

구분	보안 방안
계정관리	- 제어시스템 운영관리 계정 공유 금지 및 개별 발급 관리
패치관리	- 패치 등의 보안조치 수행 시 사전 검증을 통한 신뢰성 확보 후 적용
접근통제	- 제어시스템 운영자 권한 분리 - 보안USB, USB 포트락 등의 이동식 저장매체 제어
보안관리	- 발생된 취약점 즉각 조치 및 주기적인 점검을 통한 안전성 확보

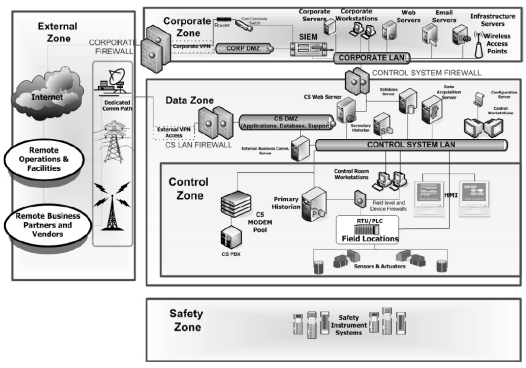
인증 없이 접속이 가능하도록 설정되어 있어서 외부 비인가자가 무선AP를 통해 업무망으로 쉽게 접속이 가능하고 시스템 또는 네트워크 구성 상의 취약점을 이용하여 제어망까지 침투가 가능한 상황이다. 따라서, 무선랜 보안을 위해서는 반드시 필요한 경우가 아니라면 무선AP를 제거해야 하나 부득이 사용하여야 할 경우에는 보안을 강화하여야 한다.

WEP방식은 64비트나 128비트 암호화키를 생성해 보안을 유지한다. 하지만 이 키는 일정한 값을 유지하기 때문에 이를 이용한 취약점이 노출될 수 있다. 이를 보완하기 위해 AES(Advanced Encryption Standard) 암호화 기술로 보안을 강화한 WPA-PSK 이상의 강한 암호화 방식을 적용해야 한다. 이 방식은 서로 다른 코드 또는 키를 사용하여 각 정보 패킷을 암호화하는 방식으로 키가 지속적으로 생성되고 변경되기 때문에 WEP 암호화에 비해 우수한 보안기술이라 할 수 있다. 이와 같이 무선랜에 기본적으로 탑재된 보안기술로도 보안대응이 가능하지만 갈수록 진화하는 무선해킹 공격에 대응하기 위해서는 WIPS와 같은 무선보안솔루션 도입이 필요하다. WIPS는 무선침입방지시스템으로서 무선AP의 범위 내에서 불법 AP나 사용자 단말기를 이용한 침입시도, 애드혹(Ad-Hoc) 연결, AP의 MAC 변조, 서비스 거부(DoS) 공격 등을 막을 수 있다.

5.3.2 업무망 연결 취약점 대응방안

교통신호제어시스템은 업무망 및 인터넷과 차단되도록 구축되어야 하나 모니터링 및 관리를 위해 업무망과 연결되어 안정적인 데이터 전송과 외부로부터의 침입방지를 위해 VPN 또는 방화벽을 통해 통제하고 있다〔11〕. 이러한 환경에서의 보안위협을 해소하기 위한 구성을 다음과 같이 제시하고자 한다.

제어시스템은 외부 인터넷망, 업무망, 타 시스템 등



〔그림 4〕 제어시스템의 심층방어 구조

과 연결되어 있어 다양한 보안 이슈를 가지고 있다. 이러한 다양한 보안 이슈들은 한가지의 방법만으로 해결하기는 어렵기 때문에 〔그림 4〕의 미국 국토안보부(Department of Homeland Security) CSSP (Control Systems Security Program)에서 권고되는 구조와 같은 심층 방어 기법에 기반한 네트워크 보안 전략이 필요하다[12]. 이러한 제어시스템 심층방어구조는 인터넷망(External Zone), 업무망(Corporate Zone), DMZ(Data Zone), 제어망(Control Zone), 안전망(Safety Zone)의 5가지 Zone으로 구성하고 각 Zone간에 방화벽, 침입탐지/방지시스템과 같은 보안 시스템을 통해 접근통제 및 트래픽 모니터링을 수행한다. 하지만 이러한 구성 환경에서는 두 가지의 단점을 가지고 있다. 첫째, 만약 데이터서버가 업무망에 존재한다면 방화벽은 데이터서버와 제어망의 제어 장치들 간의 통신을 허용해야만 하고, 이로 인해 업무망의 호스트로부터 생성된 악의적인 패킷이 제어망의 제어시스템에 전송될 수 있다. 둘째, 제어망에 영향을 줄 수 있는 도용 패킷이 프로토콜에 은닉될 수 있다. 따라서, 업무망과 제어망 사이의 이중 방화벽 구성을 권고한다. 첫 번째 방화벽은 제어망 또는 공유 데이터 저장 서버로 유입되는 임의의 패킷을 차단하고, 두 번째 방화벽은 침해된 서버로부터 원치 않는 트래픽이 제어망으로 유입되는 것을 방지할 수 있고, 제어망의 트래픽이 공유 서버에 영향을 주는 것을 방지할 수 있다.

5.3.3 외부 제공 서비스 취약점 대응방안

교통신호제어시스템을 관리하는 교통정보센터에서는 일부 BIS(버스정보시스템)와 같은 외부에 서비스를 제공하는 서버와 네트워크 상으로 연결되어 있고, 방화벽 정책을 통해 접근 통제를 수행하고 있다. 하지만 BIS 등의 시스템은 기반시설 대상에 포함되어 있지 않아 취약점 점검 및 조치가 이뤄지지 않고 있고, 주요 시스템에 대한 접속정보가 평문으로 저장되어 있어 방화벽 우회 등의 방법으로 제어시스템에 접근이 가능하다. 그러므로, 외부 서비스 제공 서버의 경우 기반시설 점검 기준으로 취약점 점검 및 조치를 수행하여 제어망에 대한 침투를 미연에 방지하여야 한다. 또한, 화이트리스트 기반의 보안기술을 적용하여 타 시스템간 허용된 프로토콜 및 프로그램을 사용하도록 하고, 이러한 통신 환경에 대한 주기적인 모니터링을 수행한다.

기존의 방화벽 등은 제어시스템의 독자적인 프로토콜(MODBUS, ICCP, DNP3P 등) 및 공격 패턴의 특성을 반영하지 않기 때문에 특화된 공격 트래픽 탐지 및 방지에 한계점이 존재한다. 또한, 제어시스템은 쉽게 구조를 변경하거나 장비를 교체하기 어렵다는 특징을 가지고 있기 때문에 이상증후 탐지(anomaly-based detection)를 기반으로 한 침입탐지시스템과 같은 솔루션이 필요하다[13]. 침입 탐지 및 방지 시스템 적용 시에는 제어시스템과 사내 시스템의 사용 프로토콜이 다르기 때문에 두 시스템 모두를 모니터링 할 수 있고, 침입 탐지 시그니처를 구분하여 적용할 수 있어야 한다. 또한, 제어시스템의 가동 중단 및 부하를 일으키지 않는 방법으로 공격 트래픽을 탐지하고, 탐지결과를 신속하게 분석 및 대응할 수 있는 보안관제 체계 구축이 필요하다.

5.3.4 운영 콘솔 취약점 대응방안

제어망에는 제어시스템을 운영하기 위한 운영 콘솔, DB서버 등이 있다. 기본적으로 제어망 내부에서 사용하는 PC 및 서버는 취약점 점검을 통해 취약점을 확인하고 조치하여 안전한 환경에서 운영하도록 해야 한다. 그리고, 운영상 필요한 내부 중요정보에 대한 유출 방지를 위해 일부 파일에 대한 암호화 적용 또는 DRM 등과 같은 솔루션을 통하여 통제를 수행하며 USB를 통한 악성코드 유입방지를 위해 보안USB 사용을 의무화해야 한다.

5.3.5 웹서버 취약점 대응방안

웹서버는 대외 서비스를 위해 DMZ 구간에 구성되

며 방화벽을 통해 인터넷망과 업무망에 연결되어 있다. 웹서버의 취약점을 통해 웹관리자 권한 획득, 웹서버 권한 획득이 가능하고, 이를 통해 제어시스템까지 침투가 가능하므로 웹서버 자체의 취약점을 제거해야 한다. 또한, 웹서버의 정보 연동을 위해 웹DB와 제어DB가 웹서버와 연동되어 있으므로 중요 DB 정보의 유출 방지를 위해 웹 구간과 제어시스템 구간의 완전한 분리 구성이 필요하다.

VI. 결론

교통, 철도, 전력 등의 주요 기반시설은 사이버 공격 등으로 인해 가동이 중단될 경우 사회·경제적 손실뿐 아니라 국민 생활에 심각한 불편을 초래하게 된다. 특히, 농협 금융사고, 방송사 해킹사고 등으로 기반시설에 대한 취약점이 드러남으로써 교통신호제어시스템의 경우에도 사이버 침해 위험성이 더욱 커지고 있고, 과거와 달리 최근의 제어시스템 환경은 개방형으로 바뀌면서 다양한 외부 서비스 및 관리를 위해 외부망과 연결되는 접점이 존재하고 있어 이에 대한 보안 위협이 커지고 있는 상황이다.

본 연구에서는 주요정보통신기반시설로 지정된 시설 중 교통신호제어시스템 7개 기관에 대한 취약점 분석·평가 결과를 비교·분석하여 교통신호 분야 기반시설의 공통적인 보안 취약점 및 개선사항을 알아보았고, 교통신호제어시스템을 포함하는 지능형교통시스템의 구성 및 특징을 알아본 후 보안취약점을 분석하여 교통신호분야 기반시설에 대한 관리적·물리적·기술적 개선방안을 제시하였다. 교통신호제어시스템은 일반적인 기반시설에 대한 점검기준과 다른 교통신호제어시스템에 특화된 점검 기준 마련이 필요하며, 보안담당자의 잦은 보직 변경으로 인한 보안관리 업무의 연속성 문제 및 외주업체를 통한 운영업무 수행으로 인한 인적 보안이 필수적이다. 하지만, 기반시설을 관리하는 기관에서 자체적으로 보안대책을 수립하는데는 어려움이 있기 때문에 정보보호 관리 기관의 제도적인 지원 및 정보보호 활동 강화를 위한 교육, 정보제공 등의 지속적인 관심 및 지원 체계가 필요하다. 교통신호제어시스템 보안담당자들은 제어시스템의 특수성 및 중요성을 인지하고 정보보호 활동 강화에 많은 관심을 가져야 할 것이다.

참고문헌

〔1〕 ICS-CERT MONITOR, Octorber/November/ December 2012.

〔2〕 행정안전부, 2012 국가정보화백서, 2012년 8월.

〔3〕 김완집, 김휘강, 이경호, 염흥열, “도시 기반시설 SCADA 망의 위험분석 및 모니터링 모델 연구,” 정보보호학회논문지, 21(6), pp. 67-81, 2011년 12월.

〔4〕 윤정한, 김우년, 서정택, “제어시스템 네트워크 보안기술 동향,” 정보보호학회지, 22(5), pp. 22-27, 2012년 8월.

〔5〕 이재호, 이영수, “철도관제시스템의 정보보안에 대한 고찰,” 정보보호학회지, 22(5), pp. 35-39, 2012년 8월.

〔6〕 문영준, 박순용, “지능형교통시스템(ITS)의 이해와 동향,” 전기의 세계, 2006년.

〔7〕 NIST, “Guide to Industrial Control System (ICS) Security,” Special publician 800-32, Oct. 2008.

〔8〕 김영진, 이정현, 임종인, “SCADA 시스템의 안전성 확보방안에 관한 연구,” 정보보호학회논문지, 19(6), pp. 145-152, 2009년 12월.

〔9〕 US. Department of Transportation, “Intelligent Transportation Systems - Information Security Analysis,” Nov. 1997.

〔10〕 강동주, 김휘강, “스마트그리드에서의 CPS (cyber-physical system) 시뮬레이션 구현을 위한 제반 연구이슈 및 방법론 검토,” 정보보호학회지, 22(5), pp. 62-72, 2012년 8월.

〔11〕 박준영, 김휘강, “Smart Grid를 위한 필드형 가상사설망(VPN) 게이트웨이의 구현,” 정보보호학회논문지, 21(4), pp. 125-136, 2011년 8월.

〔12〕 U.S. Department of Homeland Security, “Recommended Practice : Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies,” Oct. 2009.

〔13〕 고폴린, 최화재, 김세령, 권혁민, 김휘강, “트래픽 자기 유사성(Self-similarity)에 기반한 SCADA 시스템 환경에서의 침입탐지방법론,” 정보보호학회논문지, 22(2), pp. 267-281, 2012년 4월.

〈저자소개〉

조 평 현 (Pyoung Hyun Jo), 정회원
1996년 2월: 전남대학교 컴퓨터공학과 졸업
1996년 2월~2000년 2월: ㈜에스원
2000년 3월~현재: ㈜시큐아이
2009년 8월: 고려대학교 정보보호대학원 석사 수료
〈관심분야〉 정보보호관리체계, 개인정보보호, 네트워크 보안

임 종 인 (Jong In Lim), 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
現 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

김 휘 강 (Huy Kang Kim), 종신회원
1998년 2월: KAIST 산업경영학 학사
2000년 2월: KAIST 산업공학과 석사
2004년 5월~2010년 2월: NC소프트 정보보안실장, Technical Director
2010년 3월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직, 침입탐지시스템, 봇넷탐지