Journal of Korea Multimedia Society Vol. 19, No. 1, January 2016(pp. 51-59)
http://dx.doi.org/10.9717/kmms.2016.19.1.051

물리보안 관제시스템의 보안위협 사례를 통한 취약점 분석 및 대응방안 연구

고윤성[†], 박광혁[††], 김창수[†††]

Problem Analysis and Countermeasures Research through Security Threat Cases of Physical Security Control Systems

Yun Seong Ko[†], Kwang Hyuk Park[††], Chang Soo Kim[†††]

ABSTRACT

Physical security protecting people from physical threats, such as a person or vehicle, has received a great attention. However, it has many risks of hacking and other security threats because it is highly dependent on automated management systems. In addition, a representative system of physical security, a CCTV control system has a high risk of hacking, such as video interceptions or video modulation. So physical security needs urgent security measures in accordance with these threats. In this paper, we examine the case of security threats that have occurred in the past, prevent those from threatening the physical security, and analyze the security problem with the threats. Then we study the countermeasures to prevent these security threats based on the problems found in each case. Finally we study for the method to apply these countermeasures.

Key words: Physical Security, CCTV, Backdoor, IP Exposure.

1. 서 론

최근 세계적으로 IT 산업과 IT 보안시장의 규모가 지속적으로 성장하고 있다. 국내 시장도 세계 시장에 비해 규모는 적지만 꾸준히 증가하고 있는 실정이고, 특히 주요 시설이나 재산 등을 보호하는 물리보안 관제 기술의 성장이 크게 이루어지고 있다. 물리보안 관제란 물리적 위협 수단인 사람, 물품, 차량 등으로부터 재산이나 인명 등을 지키지 위하여 CCTV나 보안 시스템 등의 물리적 수단에 의해 이루어지는 보안관리이다. 물리보안관리 업무의 주체는 사람이며, 물리적 보안 시스템이 사람을 보조하여 관리 업무를 보다 효율적으로 할 수 있도록 돕는다. 민간 경비업무나 CCTV를 활용한 교통관제, 범죄예방 등이 물리보안 관제의 대표적인 방법이다[1].

하지만 이런 물리보안 관제 시스템에도 치명적인 약점이 있는데, 그것은 온라인으로 인터넷에 연결되어 있다는 것이다. 과거에는 폐쇄되어있는 내부망 내에서 물리보안 관제를 하는 경우가 대부분이었지만, 인터넷이 발달한 요즘에는 물리보안 관제시스템의 대부분이 인터넷과 연결되어 있어 서버와의 데이터를 주고받는 등의 작업을 하기 때문에 통신 과정에서

※ Corresponding Author : Chang Soo Kim, Address: (608-737) Ungbi Bldg., Yongso-Ro 45, Nam-Gu, Busan, Korea, TEL : +82-51-629-6245, FAX : +82-51-629-6230, E-mail : cskim@pknu.ac.kr
Receipt date : Oct. 12, 2015, Revision date : Nov. 18, 2015
Approval date : Nov. 23, 2015

[†] Dept. of IT Convergence and Application Engineering, Pukyong National University
E-mail : kysung1234@naver.com
[††] Interdisciplinary Program of Information Systems, Pukyong National University
E-mail : rhkdgur@hanmail.net
[†††] Dept. of IT Convergence and Application Engineering, Pukyong National University

Table 1. Physical security application system and major equipment

Security System	Major Function	Major Equipment
CCTV System	- Real-time monitoring - Video recording, image recognition and alarm - Video transmission	- Cameras, Lenses, PTZ - DVR, Motion Detector - Image recognition S/W - Cable, IP network
Access Control System	- Personnel and vehicles access control - Import goods search/control -	- Aware devices(smart cards, biometrics, RFID) - X-ray finder, metal detector
Intrusion Alarm System	- Unauthorized intrusion alarm, notification and response - Unmanned security services - Local systems	- Sensors, alarms - Control S/W

데이터 위·변조 등의 해킹 위협에 직면할 수 있다.

본 연구에서는 물리보안 관제에 대한 보안 취약성을 연구하고 대응방안을 제시한다. 세부적으로는 물리보안 관제 시스템의 구축현황 및 보안위협 사례를 조사하고, 그에 따른 보안 취약성을 분석한다. 분석된 자료를 토대로 물리보안 관제의 보안 취약성에 대한 대응방안을 제시하고, 마지막으로 연구된 대응방안을 적용시킬 수 있는 방법에 대해서도 연구한다.

2. 관련연구

2.1 물리보안(Physical Security)

물리보안은 물리적으로 정보, 인명, 시설 등을 보호하는 것을 의미한다. 이는 인가자/비인가자의 출입관리, 천재지변으로부터의 시설 보호, 방범 관리 등의 모든 물리적인 위협으로부터 인명이나 재산 등을 보호하는 것이다[2].

국내에는 2012년 물리보안 기업의 총 매출이 4,662,041백만원에서 연 평균 22.1%씩 꾸준히 증가하여 2017년에는 12,673,886백만원에 달할 것으로 전망된다. 물리보안 제품은 2012년 3,191,294백만원에서 연평균 25.4%씩 성장하여 2017년에는 9,912,960백만원에 이를 것으로 전망되며, 물리보안 서비스는 2012년 1,470,747백만원에서 연평균 13.4%씩 성장하여 2017년에는 2,760,926백만원에 이를 것으로 전망된다[3].

3. 물리보안 관제시스템의 보안위협 사례

3.1 2014년 러시아 Insecam의 CCTV 해킹

2014년 러시아의 한 해커가 IP가 노출된 CCTV 73,000여 개를 해킹하여 'Insecam.org' 사이트에 실시간 생중계하여 큰 논란거리가 되었다. 해킹당한 CCTV의 화면들은 국가별로 나누어 사이트에 생중계되었고, 이로 인해 수많은 사람들의 사생활이 침해되었다. 해킹 방법은 인터넷에 노출되어 있는 수많은 IP주소를 수집하여 그 중에 CCTV로 사용되는 IP를 찾고, 아이디·패스워드가 없거나 'admin-1234', 'admin-admin'등과 같은 기본으로 주어진 아이디·패스워드를 가지고 있는 CCTV에 접속하여 권한을 얻은 후 CCTV 화면을 획득하는 방법을 사용하였다. Fig. 1은 해당 Insecam.org 사이트의 화면이다. 좌측 메뉴에는 국가별 CCTV 영상을 구분하고 각 국가별로 해킹당한 CCTV의 개수를 확인할 수 있고, 국가의 이름을 선택하면 중앙에서 사이트 접속자가 선택한 국가의 노출된 CCTV 화면을 볼 수 있게 구성되어있다. 국내 CCTV도 8,000여 개가 생중계되고 있어 큰

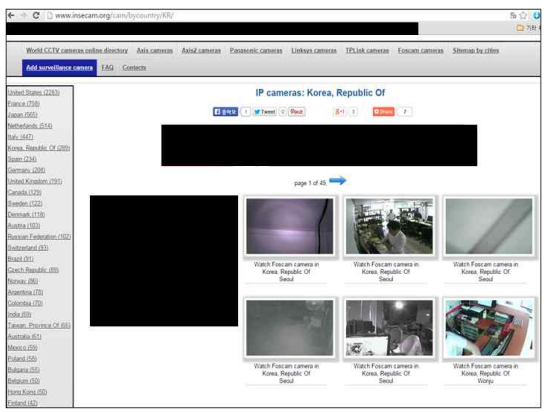

Fig. 1. Insecam.org Web site.

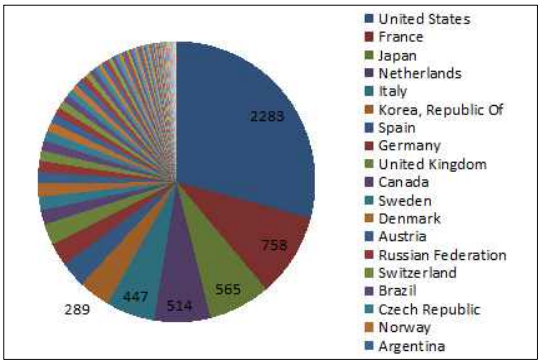

Fig. 2. Country classification of the device disclosed in Insecam.org.

파장을 일으켰다[14].

현재 2015년 8월에 Insecam.org 사이트에서 확보하여 공개하는 CCTV 디바이스의 수는 예전보다는 줄어들었지만 여전히 많은 7,832개의 장치들이 보안의 허술함으로 인해 공개되고 있다. Fig. 2에서 볼 수 있듯이 미국의 장치 수가 가장 많고, 그 다음 프랑스, 일본, 네덜란드, 이탈리아, 한국, 스페인, 독일의 순이고 이 외에도 수많은 국가들의 장비가 공개되었다.

비록 이 Insecam.org 사이트의 해킹 사례가 CCTV의 보안 설정 및 사용자들의 보안의식 강화를 알리기 위해 행해진 것이라 하더라도, 이토록 쉽게 공공 인터넷망에서 IP주소를 획득할 수 있다는 점과 기본 아이디·패스워드를 바꾸지 않거나 설정 자체를 하지 않는 등 사용자들의 보안에 대한 부주의를 이용한 사이버 공격이 계속 이루어진다면 작게는 개인 사생활 침해나 가정용 시스템의 해킹부터 시작해 크게는 국가 주요 기관의 중요한 시스템 해킹까지 이루어질 수 있어서 큰 문제가 되고 있다.

3.2 중국산 CCTV에 백도어 장착

중국 유명 CCTV 제조사 TP-Link와 D-Link에서 국내에 판매중인 일부 IP-CCTV 카메라에서 녹화된 영상 정보를 외부로 유출시킬 수 있는 백도어가 심어져 있는 사실이 발견되었다. NSHC 레드얼럿 연구팀과 카이스트 시스템보안 연구실이 공동으로 분석한 결과, 해당 제조사들이 자사가 개발한 IP-CCTV의 모든 권한을 가질 수 있는 백도어를 심어놓고, 중국 내에 위치한 제조사의 클라우드 서버를 통해서만 백도어를 접근할 수 있게 했다는 사실이 드러났다. 이 연구팀은 “해당 기기 매뉴얼에도 나오지 않은 접근 방법을 악용할 경우 사생활 침해는 물론 회사나 국가 기반 시설의 정보 유출이나 산업스파이 활동으로까지 이어질 수 있다”고 밝혔다[5].

이 백도어는 암호화를 적용한 고도의 은닉 기법을 사용하여 숨겨져 있었다. 마음만 먹으면 해당 IP-CCTV 제조사에서 카메라를 마음대로 조종하거나 영상 정보를 위·변조, 유출 등이 가능하였다. 만약 해당 IP-CCTV에 대해 관리자 권한을 획득한 공격자가 임의의 악성코드를 설치해 영상 정보를 탈취하는 것은 물론, 이 카메라가 기업이나 국가 주요 시설에 네트워크로 연결되어 있을 경우에는 내부 네트워크로 접속하여 국가의 주요 기밀을 훔칠 수 있다는 취약점이 있다.

또한 분석결과 CCTV의 관리자 페이지도 매우 허술하게 관리되고 있는 사실이 밝혀졌다. 설정 변경 및 영상을 모니터링하기 위한 관리자 페이지에 접근하기 위해 필요한 아이디·패스워드가 클라우드 시스템에 암호화되지 않은 평문으로 저장되어 있었다. 이를 통해 악의적인 공격자가 마음만 먹으면 쉽게 아이디·패스워드를 탈취할 수 있고, 해당 아이디·패스워드로 CCTV에 접근하여 영상 전송 및 각종 설정을 변경하거나 영상 데이터를 위·변조 하는 등의 피해가 발생할 수 있다.

3.3 미국 중앙교통 통제시스템 해킹

2009년 미국에서는 해커가 중앙교통 통제시스템을 해킹해 “앞쪽에 공룡이 있으니 주의하세요”라는 메시지를 교통 표지판에 남긴 사례가 있었다. 쉽게 보면 이는 단지 교통 표지판의 글자를 다른 글자로 바꾼 가벼운 장난으로 취급할 수도 있지만, 만일 앞의 도로가 공사 중인 상황이었거나 앞에서 발생한 사고를 알리는 표지판이 해킹당한다면 더욱 큰 피해와 혼란을 야기할 수 있었을 것이다. 또한 유사한 해킹방법을 사용하여 교통 표지판의 사용을 불가하게 만든다던지 교통 표지판과 연결된 교통통제센터에 대한 해킹공격이 이루어져 일대 교통이 마비가 된다면 피해가 더욱 커졌을 것이다. 국가 운영 시스템을 전적으로 신뢰하고 있었던 국민들에게 불신을 주어 혼란을 야기한 점도 하나의 피해라 볼 수 있다[15].

4. 물리보안 관제시스템의 보안 문제점 분석

4.1 IP기반 CCTV의 IP노출에 따른 보안 취약성

많은 IP기반 CCTV들의 사용자는 제조사에서 출시될 때 기본적으로 가지고 있는 아이디·패스워드를 변경하지 않고 그대로 사용하는 경우가 많다. 제조사에서 제공하는 초기 아이디·비밀번호는 대부분 인터넷에 공개되어 있기 때문에 검색만으로 쉽게 얻을 수 있으며, 그 패턴 역시 admin, 1111, 1234, 1234567890 등으로 뻔하고 단순한 패턴을 사용하고 있기 때문에 접속 권한 획득이 아주 쉽다. Table 2는 제조사 및 모델별 초기 아이디와 비밀번호를 표로 작성한 것이다.

이런 현상에 더불어 IoT(Internet of Things; 사물인터넷)장비 검색 엔진인 'Shodan'을 사용하면 키워드 검색만으로 다양한 CCTV의 IP주소를 얻을 수 있으며, 그에 따른 부가적인 정보 또한 쉽게 얻을 수 있다. Table 3은 Shodan에서 얻을 수 있는 IP주소에 대한 정보이다.

Table 3을 보면 IP주소부터 시작하여 포트번호, 도메인·호스트 이름, ISP, 위치정보 및 여러 가지 다른 데이터 등 수많은 중요한 데이터들을 Shodan 검색엔진에서 얻을 수 있다. 이는 즉 IP노출로 인해 이러한 부가적인 정보까지 손쉽게 얻을 수 있다는 것이므로 IP노출에 대한 피해가 더욱 커질 수 있다.

이렇게 IP노출로 인해 CCTV의 취약점이 발견되면 이를 악용하여 CCTV가 설치되어있는 장소에 물리적인 범죄를 실행하기 전에 미리 주변 동향을 살피거나 침입 전 카메라의 각도를 돌려놓아 범죄의 흔적을 남기지 않게 만들 수도 있고, 범죄 이후 흔적을 지우기 위해 카메라에 접근하여 데이터를 삭제하는 것 또한 가능하다.

Table 2. The manufacturer or model-specific initial username and password

Manufacturer or Model name	Username	Password
FOSCAM	admin	-
TP-LINK	admin	admin
HIKvision	admin	12345
EGPIS EHR-F400	admin	1111
EGPIS	admin	123456
Tibet DVR PHR-04	admin	000000
VSTARCAM-100H	-	888888
Cowon	-	cowon
LG HD network cam	admin	admin
⋮	⋮	⋮

Table 3. The information about IP address that can be obtained through the Shodan

Attributes	Description
domains	Domain name
hostnames	Host name
ip	IP address(numerical)
data	Various information about the IP address
port	Port number
isp	Internet Service Providers
asn	Autonomous System Numbers
ip_str	IP address(character)
org	Organization
os	Operating System
timestamp	Timestamp
location	Location information

4.2 IP기반 CCTV 카메라의 히든 백도어 위협

IP기반 CCTV 카메라는 기본적으로 오픈 인터넷 망에 연결된다는 특성이 있는데, 이를 통해 IP기반 CCTV에 백도어를 설치하여 영상을 빼돌릴 수 있다는 취약점이 있다. 이 백도어는 보통 제조사만이 모든 권한을 가지고 있어 제조사의 클라우드 서버에서만 접근이 가능하도록 만들어져있다. 이러한 백도어가 악의적으로 사용된다면 가정 내에 사생활 침해는 물론이고 나아가서 국가적으로도 큰 손해를 불러올 수 있다. 실례로 최근 미국과 유럽 등에서는 이러한 CCTV의 백도어를 막기 위해 특정 국가의 IT기기 수입을 전면 금지하는 경우도 있다. 특히 대기업이나 국가기반으로 사용되는 CCTV나 IT기기들은 백도어로 인해 공격당할 시에 더욱 큰 피해를 유발할 수 있기 때문에 이런 규제가 더욱 엄격하게 적용되고 있는 추세이다[5].

이러한 백도어 공격은 더욱 나아가 내부망 시스템을 대상으로 2차적인 공격까지 할 수 있다. 최근 대부분의 CCTV나 IP카메라들은 원격에서 해당 카메라의 영상을 확인하고 제어할 수 있는 기능을 가지고

있다. 이를 통해 인증된 사용자들은 언제 어디서든 해당 카메라의 영상을 확인하고 제어할 수 있다. 또한 최근의 일부 제조사들은 클라우스 서비스를 활용하여 CCTV 서비스를 제공하고 있다. 이를 통해 허가된 사용자는 제조사에서 제공하는 클라우드 서비스를 사용할 수 있으며, 내부 사설망에 설치된 CCTV의 경우에도 클라우드 서비스를 통하여 접근할 수 있다. 문제는 공격자가 해당 CCTV와 클라우드 시스템의 VPN(Virtual Private Network) 통신을 통하여 사설망 통제 시스템과 보안 프로그램을 우회하여 내부 망에 접근할 수 있고, 이를 통해 내부 망에 설치되어있는 CCTV에 대한 2차적인 공격을 가할 수 있다.

4.3 미국 항공관제 컴퓨터의 보안 취약성

미국 연방항공청(FAA)에서 항공관제에 사용되는 컴퓨터가 해킹 공격에 취약하다고 미 회계감사원(GAO)에서 지적했다. GAO는 FAA에서 항공관제 컴퓨터에 대해 사용권한 통제를 강화해야 하고, 전산망에 대한 공격을 막기 위하여 방화벽을 더욱 견고하게 만들어야 한다고 지적했다. 현재 항공 관제소에서 통제하는 항공기가 약 2,850대에 이르기 때문에 만약 항공관제 컴퓨터가 해커의 공격을 받아 통제 불능이 된다면 그 피해는 엄청날 것이다[6].

또한 현재 항공기들은 HF(High Frequencies)나 VHF(Very High Frequencies)등의 전파를 이용해 지상과 음성 위주로 통신을 주고받지만, 미국의 차세대 항공관제 시스템은 웹 기반의 WiFi로 통신하도록 변경된다. 따라서 관제시설과 항공기간의 WiFi 통신망이라는 해커들이 뚫고 들어갈 틈이 생겨버린 것이다. 특히 최신 항공기의 경우 조종기와 기체가 기계적으로 연결되어있지 않고 컴퓨터를 통하여 자동으로 조종하는 시스템이기 때문에 해커들이 항공기를 해킹하여 마음대로 조종하거나 또는 테러를 가하는 등의 심각한 보안 위협을 가할 수 있다.

5. 보안 문제점에 대한 대응방안

5.1 IP노출 문제점에 대한 대응방안

5.1.1 노출 IP 검색시스템 개발

IP기반 CCTV의 취약점을 개선하기 위해 넘어야 할 큰 과제중 하나는 IP주소 노출에 대한 위험을 최소화하는 것이다. 이를 위해서는 기본적으로 노출된

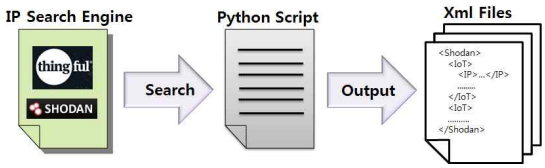

Fig. 3. IP Exposure Notification System Configuration.

IP주소를 검색할 수 있는 시스템에 대한 연구가 필요하다. 본 연구에서는 사물인터넷 검색엔진 Shodan을 사용해 IP주소 및 기타 정보들을 검색하여 출력하는 IP노출 알림 시스템을 개발하였다. 먼저 IP주소가 노출된 CCTV들을 검색하기 위한 핵심 키워드에 대해 연구하고, Shodan API를 통해 해당 키워드에 대한 IP주소 및 기타 정보들을 수집하여 결과 값을 XML 파일 형태로 출력한다. Fig. 4는 해당 시스템의 구성도이다.

해당 시스템을 통해 IP 주소를 검색하기 위해서는 먼저 Shodan 페이지에 접속하여 데이터를 획득할 수 있는 권한을 얻어야 한다. Shodan 페이지에서 데이터를 얻을 수 있는 방법은 총 두 가지가 있는데, 첫 번째는 웹 페이지를 통해서 얻는 것이고, 두 번째는 Shodan API 키를 사용하여 얻는 것이다. 웹 페이지를 통해서 얻는 정보들은 대부분 단편적인 정보밖에 없어서 해당 IP 주소에 대한 다양한 정보를 얻어야 하는 본 시스템에서는 사용하기에 부적절하다. 하지만 Shodan API 키를 통해 얻을 수 있는 정보들은 웹 페이지를 사용하여 얻을 수 있는 정보에 더하여 위치 정보나 포트 번호, 그 밖에 유용한 정보들을 얻을 수 있기 때문에 사용하기가 적절하다. 또한 노출

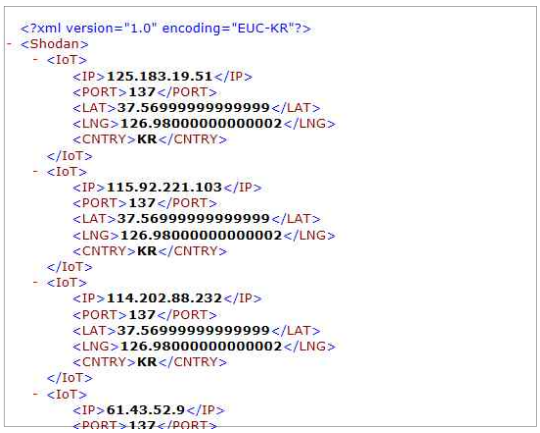

Fig. 4. The XML file of Experiment Result.

IP 검색 시스템을 통한 자동화 소프트웨어를 제작하기 위해서도 Shodan API 키를 사용하여 데이터를 얻는 편이 편리하다.

Shodan API를 통해 데이터를 수집한 후 Python Language를 사용하여 자동화된 시스템을 개발한다. 먼저 Python에서 Shodan API를 사용하기 위해 API 라이센스를 구입하고, 그에 따른 API 키를 입력한다. 그 후 결과 값으로 출력될 XML 파일 형식을 지정하고 IP 검색엔진에 입력될 쿼리를 문자열 형태의 입력값으로 받아 쿼리를 실행하고, 결과 값을 배열형 변수에 입력시킨다. 해당 쿼리를 통해 데이터를 수집하였으면 그 데이터들을 XML 파일 안에 입력하고 최종 결과물을 출력한다. Fig. 5는 해당 시스템의 실행결과 XML 파일이다. 노출된 IP 주소와 포트번호, 위·경도, 국가 값을 입력하여 XML 파일 형태로 출력하였다.

5.1.2 IP노출 위험도 산정 시스템 개발

IP노출 방지 방안 중 하나는 IP노출 위험도를 산정하여 해당 IP주소가 공격에 얼마나 취약한 지를 알려주는 것이다. 먼저 IP노출 위험도를 산정하기 위해서는 IP노출 인자 값이 필요하다. 이 인자 값은 해당 IP기반 CCTV 장비가 얼마나 보안에 취약한 지를 분류하는 기준으로, Table 4는 제안하는 인자들의 종류이다.

이러한 인자 값들을 사용하여 IP 노출에 대한 위험도를 단계별로 매긴다. 산정 기준에 대해 안전하다고 판단되면 노출안전 점수를 높이고, 그렇지 않다면 노출안전 점수를 낮춘다. 예를 들어 '인증되지 않은 IP 주소를 차단하는가?'의 인자 값의 점수 산정기준 중 '인증되지 않은 IP주소 전부 차단' 기준을 만족한다면 안전하다 판단하여 점수를 높이고, '모든 IP주소 허용' 기준을 만족한다면 위험하다 판단하여 점수를 낮춘다. 최종적으로 위 인자들의 점수를 단계적으로 산정하여 점수가 높을수록 안전하다고 판단하고, 낮을수록 위험하다고 판단하여 그에 따른 등급을 매긴다.

이렇게 IP노출 위험도를 산정하여 위의 노출IP 검색 시스템과 결합한다면 노출된 IP주소 중 공격에 취약한 IP주소를 선별하여 확인할 수 있고, 해당 시스템의 관리자에게 위험성을 알리는 등의 조치를 취할 수 있다. 이를 통해 IP 노출에 대한 위험성을 미리 차단하는 결과를 가져올 수 있다.

5.2 IP기반 CCTV 카메라의 백도어 취약점 개선방안

CCTV 카메라의 히든 백도어를 통한 취약점을 개선하기 위해서는 미국이나 해외 국가들이 행했던 방법처럼 어느 특정 국가의 IT 기기를 전면 수입 금지하거나 해당 CCTV 제품을 수입 금지하는 방법이 있다. 또한 백도어를 불법으로 설치한 회사가 클라우드 서비스를 통해 CCTV 영상 데이터를 불법으로 취득하는 것을 막기 위해 클라우드 서비스에 대한 특정 IP를 차단하는 방법도 사용할 수 있고, 사내 와이파이 및 블루투스 등 통신 기기에 대한 사용을 불허하도록 할 수도 있다. 제품을 수입할 때 백도어를 탐지·확인하기 어려운 경우에는 위와 같은 방법으로 2차 피해를 예방할 수 있다.

서비스적인 측면으로 볼 때 백도어의 이러한 취약점을 개선하기 위해서는 백도어 예방 전담팀을 구성하여 관련 보안 취약점에 대한 대응 및 기술 지원을

Table 4. Factor values of IP exposure calculating system

인자 값	점수 산정 기준
It should block unauthorized IP addresses?	- Blocking all unauthorized IP address : Safety - Some block unauthorized IP address : Average - Allow all IP address : Risks
ID/Password difficult to obtain?	- Secure password in accordance with the regulations : Safety - Short or simple password : Average - default passwords such as 'admin - 1234', and no passwords : Risks
It use a security program?	- Use security program : Safety - Not use security program : Risks
The importance of a system that uses the IP address	- Personal/Household CCTV : Normal - Commercial/Kensington CCTV : Important - National agencies CCTV : Very important

제공해야 한다. IPS(Intrusion Prevention System), IDS(Intrusion Detection System), F/W 정책 설정 지원, 자동화된 점검 도구를 사용하여 해당 위협에 대한 보안 점검 지원, 기타 CCTV나 IP 카메라에 대한 보안 점검 지원, 데모 시연 및 보안교육 등을 전담팀에서 지원하여 백도어로 인한 피해를 줄여야 한다.

5.3 물리보안 관제 보안관련 법안 및 관리지침 작성

대부분의 물리보안 관제시스템의 IP주소 노출 등의 원인은 사용자의 부주의나 관리 소홀로 인한 인적 취약성 때문인 경우가 많다. 이러한 위험을 방지하기 위해서는 물리보안 관제의 보안 관련 법안과 관리지침을 더욱 강화하여 작성해야 할 필요성이 있다. 물리보안의 중요성이 더욱 커지고 물리보안 장비들의 숫자나 시장에서 갖는 규모가 더욱 증가하고 있기 때문에 CCTV 등과 같은 기기를 통틀어서 적용하는 범용적 법안을 제정해야 한다. 또한 사용자들의 인적 소홀로 인한 관리적 소홀함을 경계하기 위해서 관련 관리지침도 작성하여야 한다.

5.3.1 법안 제안

- IP기반 물리보안 장비의 기본 접속 패스워드 변경

IP주소 기반의 물리보안 관련 장비들이 해킹당하여 위협에 노출되는 대부분의 이유는 접근 권한 등의 설정을 하지 않거나 제조사로부터 초기에 제공되는 'admin-1234'와 같은 기본 아이디·패스워드를 변경하지 않고 사용하는 데 있다. 이러한 기본 접속권한은 이미 인터넷 망에 널리 퍼져있을 뿐만 아니라 간단한 해킹 툴만으로도 쉽게 뚫리기 때문에 보안상의 큰 위협으로 다가온다. 이러한 보안 위협을 방지하기 위해 IP기반 물리보안 장비를 사용할 때에는 항상 아이디·패스워드를 변경하고 사용하도록 법안을 제정해야 한다. 예를 들어 CCTV 등의 물리보안 장비를 개발할 때 초기에 비밀번호를 변경하지 않고서는 사용을 할 수 없게 시스템을 개발하거나, 패스워드를 변경하지 않을 시에는 주기적으로 패스워드를 변경하라는 경고 문구를 표출하는 등의 방법이 있다. 그러기 위해서는 물리보안 장비를 개발하는 개발사에 대한 법 제정과 사용하는 사용자에 대한 제정이 동시에 이루어져야 한다. 개발사는 초기에 시스템의 접근권한을 설정하도록 해야 할 것이고, 사용자에게도 사용자의 부주의로 인해 접근권한을 변경하지 않아 생기는 모든 피해에 대해서 사용자의 책임을 묻는 등의 법안을 제정해야 한다.

- 물리보안 장비의 보안 프로그램 설치 의무화

물리보안 장비들의 보안 위험성을 줄이기 위해서는 보안 프로그램 설치가 반드시 필요하다. 비록 물리보안 장비에 대해 따로 접근 권한을 설정했다 하더라도 해킹 방법에 따라 뚫릴 수도 있는 것이 패스워드이기에, 이를 막기 위해서는 물리보안 장비들에 최적화된 보안 프로그램을 장비에 도입해야 한다. 현재는 이러한 부분에 대해서는 연구 자체가 부족한 실정이기에 더욱 문제가 심각하다. 보안 프로그램에 대한 법안은 두 가지 방향으로 제시될 수 있다. 첫 번째는 물리보안 장비 제조업체에서 보안업체와 협력하여 시스템 개발 시에 보안 프로그램을 포함하여 개발하도록 법안을 제정하는 것이고, 두 번째는 물리보안 장비를 사용하는 사용자들이 직접 보안 프로그램을 설치하도록 의무화하는 것이다. 전자는 어떤 물리보안 장비에도 보안 프로그램이 장착되어 나오기 때문에 안전하고 신뢰성이 있지만, 물리보안 장비의 자체 가격이 비싸진다는 점과 수많은 물리보안 장비에 적용하기에 어렵다는 단점이 있다. 후자는 가격도 비싸지지 않고 적용하기에도 무리가 없지만, 단점은 사용자가 보안 프로그램을 설치를 하지 않을 수도 있고, 사용자 입장에서 보안 프로그램의 설치가 번거로워서 설치를 피할 수도 있다는 점이다. 가장 좋은 방법은 두 가지를 혼합해서 제조사와 사용자가 같이 보안 프로그램을 설치하도록 유도하는 것이다.

5.3.2 관리지침 작성

해킹들 중 대다수는 해당 시스템의 관리자나 사용자의 관리 소홀로 일어나는 경우가 많다. 이러한 인적 취약성에 대응하기 위해서는 관리지침이 필요하다. 물리보안 장비들의 종류도 많고 점점 그 수가 늘어가기 때문에 CCTV같은 특정한 장비 대상이 아닌 범용적으로 사용 가능한 관리지침이 필요하다. 예를 들어 해당 시스템의 패스워드를 외부에 노출하거나 텍스트 파일 등에 적어두지 않기, 패스워드를 주기적으로 변경하기, 보안 프로그램 업데이트 주기적으로 실행하기 등의 관리지침을 작성하면 보안에 관심이 없는 일반 사용자들에게 나타나는 인적 취약성을 사전에 예방할 수 있다.

6. 결 론

물리 보안에 대한 비중이 점점 커짐에 따라 시장 가치와 물리보안 관련 기술이 점점 증가하고 있다. 그에 따라 물리보안에 대한 보안위협 또한 증가하고 있지만 아직 뚜렷한 보안대책이 마련되지는 않고 있다. 이에 본 논문에서는 물리보안 관제에 대한 보안 위협 사례를 조사하여 그에 따른 보안 취약성을 분석하였다. 분석된 취약성을 토대로 대응방안을 제시하고 나아갈 방향 또한 제시하였다.

본 연구를 토대로 우리는 물리보안 관제시스템이 해커들의 간단한 공격에도 뚫릴 만큼 보안에 취약하다는 것과 지속적으로 높아져가는 관심 속에서도 물리보안 관제시스템의 보안 위협에 대한 대응책이 미비하다는 결론을 얻을 수 있었다. 이러한 IP주소 노출이나 패스워드 미변경, 백도어 공격이나 관제시스템 해킹 등의 공격을 미리 파악하고 대응방안에서 제시하였던 노출 IP 검색 시스템과 IP노출 위험도, 백도어 대응 방안 등을 토대로 대응책을 짠다면 더욱 안전한 물리보안 환경을 만들 수 있을 것이라 생각한다.

향후 우리는 본 연구에서 제시했던 노출 IP 검색 시스템과 IP 노출 위험도를 결합하여 최종적인 물리보안 관제 통합 시스템 구축에 관하여 연구할 것이다. 통합 시스템에서는 위치정보를 기반으로 각각의 노출된 IP주소에 노출 위험도를 결합하여 해당 IP주소를 가진 시스템이 얼마나 위험한 지를 쉽게 알 수 있고, 그 것을 지도를 포함한 웹 어플리케이션으로 개발하여 한 눈에 해당 장비에 대한 위험도를 알아보기 쉽게 만들 수 있다. 또한 본 연구를 통해 물리보안 관제시스템의 취약점 및 대응방안을 제시하여 후에 이 주제에 대해 더욱 발전된 대응방안을 찾을 수 있을 것이라 생각한다.

REFERENCE

[1] D.H. Kim, S.W. Yoon, and Y.P. Lee, “Security for IoT Services,“ *Journal of Korea Communications Society (Information and Communication)*, Vol. 30, No. 8, pp. 53-59, 2013.

[2] Physical Security in Wikipedia, https://ko.wikipedia.org/wiki/%EB%AC%BC%EB%A6% AC%EB%B3%B4%EC%95%88(accessed Aug. 25. 2015).

[3] KISA, *Survey for Information Security Industry in Korea : Year 2013*, KISIA & KDCA, 2013.

[4] T.W. Seo, S.R. Lee, B.C. Bae, E.J. Yoon, and C.S. Kim, “An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control,” *Journal of Korea Multimedia Society,* Vol. 15, No. 1, pp. 93-1 00, 2012.

[5] KAIST, *Security Threat Report of Foreign-made CCTV, IP-Camera*, SysSec lab, 2015.

[6] GAO, *Information Security - FAA Needs to Address Weaknesses in Air Traffic Control Systems*, 2015.

[7] Y.W. Joo and S.J. Lee, *Intelligent CCTV Trends and Performance Improvement*, 2013.

[8] S.H. Park, *Intelligent CCTV System Technology Issues and Industry Trends*, 2013.

[9] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, “Evaluation of the Ability of the Shodan Search Engine to Identify Internet-facing Industrial Control Devices,” *International Journal of Critical Infrastructure Protection*, Vol. 7, No. 2, pp. 114-123, 2014.

[10] H.J. Shin and Y.K. Jeong, “Device Alive Check Algorithm Using TCP Session under CCTV Network based on NAT,” *Journal of Korea Multimedia Society,* Vol. 18, No. 5, pp. 631-640, 2015.

[11] S.J. Park and J.H. Park, “Current Status and Analysis of Domestic Security Monitoring Systems,” *Korea Institute of Electronic Communication Science,* Vol. 9, No. 2, pp. 261-266, 2014.

[12] Y.J. Kim, S.Y. Lee, H.Y. Kwon, and J.I. Lim, “A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services,” *Korea Institute of Information Security & Cryptography,* Vol. 19, No. 1, pp. 103-111, 2009.

[13] R.A. Rouse, *Is Someone Watching You Through Your Webcam?*, 2012.

[14] C. Rodriguez, *The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security*, 2012.
[15] KISA, *Survey for Global Information Security Industry : Year 2013*, 2013.

고 윤 성

2014년 부경대 컴퓨터멀티미디어 공학부 학사
2014년~현재 부경대학교 IT융합응용공학과 석사과정
관심분야 : 사물인터넷, 물리보안, GIS, 임베디드 시스템

박 광 혁

2014년 홍익대학교 도시공학과 학사 졸업
2015년~현재 부경대학교 정보시스템협동과정 석사과정
관심분야 : 사물인터넷, 물리보안, GIS, 임베디드 시스템

김 창 수

1991년 중앙대학교 컴퓨터공학과 박사
2012년~현재 부산 IoT 도시협회 부회장
2013년~2014년 U. of Colorado Denver 방문교수
2015년~현재 한국멀티미디어학회 부회장
1992년~현재 부경대학교 IT융합응용공학과 교수
관심분야 : 방재IT, UIS/GIS, 운영체제, 시멘틱 웹, 재난관리, 공간검색, 도시방재 등