Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 11 pp. 148-154, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.11.148
ISSN 1975-4701 / eISSN 2288-4688

SSH 터널링을 이용한 CCTV 원격접속 보안기법

황기진[1*], 박재표[2], 양승민[3]
[1]숭실대학교 컴퓨터학과, [2]숭실대학교 정보과학대학원, [3]숭실대학교 컴퓨터학부

Security Technique using SSH Tunneling for CCTV Remote Access

GIJIN HWANG[1*], JAEPYO PARK[2], SEUNGMIN YANG[3]
[1]**Division of Computing, Soongsil University**
[2]**Graduated School of Information Sciences, Soongsil University**
[3]**Division of Computing, Soongsil University**

요 약 최근 인터넷을 통한 CCTV 영상 유출 사건으로 인해, 영상 보안 문제가 중요한 화두로 떠오르고 있다. 한국인터넷진흥원은 "CCTV 개인영상 정보보호를 위한 가이드라인"을 통해, CCTV 원격 접속 시 암호화된 프로토콜 사용을 권장하고 있지만, 아직도 다수의 제품이 이런 규칙을 지키지 않아서 해킹과 같은 보안 위협에 노출되고 있다. 본 논문에서는 이러한 보안 취약성 문제를 해결하기 위해서, SSH 터널링 기법을 사용하여 원격지에서 접속이 가능한 CCTV 시스템을 제안하고 구현하였다. 시스템은 SSH Secure Shell을 사용하여 암호화된 데이터를 전송함으로써, 보안성을 강화하였다. 또한 터널링 기법 사용하여 방화벽 내부에 존재하는 CCTV 녹화기로의 접근이 불가능 했던 문제를 해결하였다. 시스템에 대한 평가를 위해 여러 가지 CCTV 원격 접속 기법과 보안성에 대한 비교를 하였고, 시스템의 효율성에 대한 실험 결과, 전송 품질 및 시간의 큰 차이 없이 원격 접속이 가능함을 확인 할 수 있었다. 본 논문에서 제안하는 방법을 현장에 적용한다면, 해킹의 위협으로부터 안전한 시스템을 구성할 수 있을 것이다.

Abstract Video security has recently emerged as an important issue owing to CCTV video image spill accidents over the Internet. KISA recommends the use of encryption protocols for remote access through its guidelines for CCTV personal video information protection. But still, many products do not adhere to the guidelines, and those products are easily exposed to security threats, such as hacking. To solve these security vulnerabilities, this paper proposes a CCTV system that connects from remote locations, and is implemented by using secure shell (SSH) tunneling techniques. The system enhances security by transmitting encrypted data by using SSH. By using the tunneling technique, it also solves the problem of not being able to access a CCTV recorder located inside a firewall. For evaluation of the system, this paper compares various CCTV remote access schemes and security. Experimental results on the effectiveness of the system show it is possible to obtain remote access without a significant difference in transmission quality and time. Applying the method proposed in this paper, you can configure a system secure from the threats of hacking.

Keywords : CCTV(Closed Circuit Television), Remote Access, Security, SSH, Tunneling

1. 서론

최근 외국의 한 인터넷 사이트에서 CCTV 영상 유출 정보를 공개하여 전 국민적 관심을 받은 적이 있다. 다행히 해당 사이트는 차단이 되었지만, CCTV 보안 문제에 대한 경각심을 일으키기에는 충분한 사건이었다. "Table. 1" 은 인터넷 브라우저에서 CCTV 접속 링크 관련 정보를 검색할 수 있는 검색어를 카메라 제조사별로

*Corresponding Author : Gi-Jin Hwang(Soongsil Univ.)
Tel: +82-10-8791-3314 email: gjhwang@realtime.ssu.ac.kr
Received August 19, 2016 Revised (1st September 12, 2016, 2nd October 14, 2016)
Accepted November 10, 2016 Published November 30, 2016

나열한 예이다.

CCTV의 보안을 위협하는 기술은 여러 가지가 있다. 그중 해킹을 통해 사용자 ID와 암호를 취득하게 된다면, 손쉽게 CCTV를 제어할 수 있고, 영상 데이터에 대한 접근이 가능하다. 또한 데이터의 유출 및 위•변조가 가능해 진다. 따라서 해킹에 대비한 보안 요소를 강화하는 것은 중요한 이슈이다. 한국인터넷진흥원에서는 2007년도에 CCTV 개인영상 정보보호를 위한 가이드라인과 해설서를 제시하였다[1].

가이드라인에서는 개인영상정보를 외부로 전송하는 경우 보안 프로토콜을 사용하도록 명시한 점과, 권한이 없는 사용자의 접근을 통제하도록 지침하고 있지만, 우리 주변에서 설치되어 운영되고 있는 다수의 CCTV 녹화기는 암호화 되지 않은 통신방법으로 접속하거나, 시스템에서 기본적으로 제공하는 사용자 아이디와 암호를 사용하는 등 보안과 관련된 취약점이 많이 존재한다[2].

Table 1. Web Query for CCTV Related Link Search

CCTV Manufacture	Query List for CCTV Link
Web Cam	inurl:/view.shtml
	inurl:ViewerFrame?Mode=
	inurl:ViewerFrame?Mode=Refresh
Sony	/home/homeJ.html
Mobotix	/control/userimage.html
Flex Watch	/app/idxas.html

본 논문에서는 이러한 보안 취약성 문제를 해결하기 위해, SSH 터널링 기법을 사용하여 원격지에서 접속이 가능한 CCTV 시스템 구성을 제안하고 이를 구현 하였다. SSH 연결 방법을 사용하면, 암호화된 데이터 패킷을 전달 할 수 있으므로 네트워크상에서 해킹을 통한 위협으로부터 보호할 수 있다. 또한 외부 침입으로부터 시스템을 보호하기 위해 방화벽이 설치된 경우, 외부 네트워크상에서 CCTV 녹화기로의 접근이 불가능하였는데, 이를 터널링 연결을 통해 접근할 수 있도록 구성하였다.

본 논문 2장에서는 관련된 연구들을 살펴보고, 3장에서는 SSH 터널링을 이용한 원격접속 시스템의 구성과 동작 순서에 대해 기술한다. 4장에서 실험을 통해 보안성능과 서비스 품질 그리고 속도에 대한 비교 및 검증을 한 후 5장에서 결론을 맺는다.

2. 관련 연구

한국 정보통신기술 협회에서는 영상감시 시스템의 보안 요구사항을 6가지로 정의하고 있다. 첫 번째가 영상 데이터의 기밀성이다. CCTV 데이터는 기밀성이 보장되어야 하는데, 사용자 ID와 암호의 유출로 인해 손쉽게 녹화 데이터에 대한 유출이 가능하다. 두 번째는 영상 데이터의 무결성이다. 녹화 데이터가 위•변조 되면, 어떤 사건에 대한 증거로써의 효력이 상실된다. 세 번째는 영상 데이터의 현재성이다. 영상 데이터는 현재 일어나고 있는 상황임을 보장할 수 있어야 한다. 네 번째는 카메라의 침해 방지이다. 원격지에 있는 카메라에 접근하기 위해서는 인증과 침해 방지 기능이 적용되어 있어야 한다. 다섯 번째는 서비스 가용성이다. 서비스 거부 공격에 대한 탐지와 대응 기능이 필요하다. 여섯 번째는 프라이버시 보호이다. 영상에서 프라이버시를 보호하기 위해 중요한 영역을 마스킹 할 수 있어야 한다[3]. 따라서 CCTV 시스템은 위의 기준에 맞춰 설계되고 운영되어야 한다.

암호화와 관련된 연구로 영상 데이터를 전송하는 현장과 관제센터 구간의 네트워크상에 보안 채널을 구성하여, 데이터를 암호화함으로써 보안 문제를 해결 하고자 하는 연구가 있었다. 이를 구현하기 위해 TCP/IP 기반 패킷을 AES 128bit FPGA 암호화 모듈을 통해 암호화한 후 LAN을 통해 서버로 전송 하였다. 전송된 데이터는 복호화를 위한 View Server로 전달되어 암호화된 데이터 키를 통해 복호화가 이루어진다[4]. 이 연구에서는 패킷 암호화로 인해 시스템 보안성은 높아졌지만, 암•복호화를 위한 연산처리와 방화벽 통과 등과 같은 해결해야 할 문제가 남아있다.

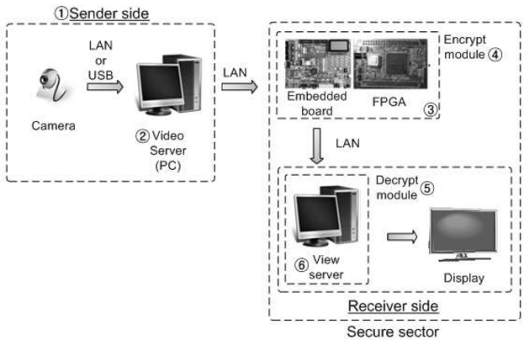

Fig. 1. Packet Encryption

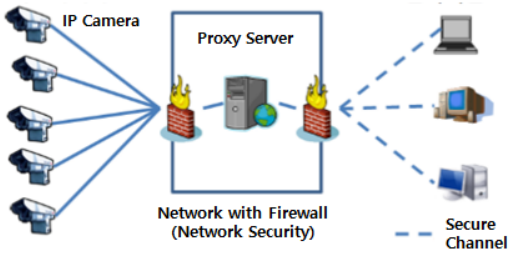

Fig. 2. Remote Access Method using Proxy Server

네트워크 카메라에서 기본적으로 제공하는 웹 서버에 의한 인증 방식은, 일반적인 웹 서버 인증방식과 동일한 방법으로, 사용자 ID와 암호의 노출로 인한 보안 문제와 연결된다. 이러한 문제를 해결하기 위해 프락시 서버를 사용하여 카메라에 접근하는 연구가 있었다. 프락시 서버는 방화벽으로 보호된 네트워크 내부에 둠으로써 외부 노출에 의한 정보 유출의 위협으로부터 보호하였고, 프락시 서버를 사용함으로써 기존에 설치된 카메라의 환경 설정 정보를 직접적으로 노출 시키지 않고 은닉할 수 있으며, 검증된 클라이언트만의 접속을 지원하며, 영상정보에 대한 등급의 설정과 등급별 클라이언트에 대한 차별화 서비스를 제공하여 보안 문제를 강화 할 수 있는 연구가 있었다[5]. 이 연구에서는 카메라로의 연결 정보에 대한 은닉과 보호가 이루어졌지만, 실제 데이터에 암호화 및 보호 방안과 카메라 주소에 대한 직접적인 연결 가능성 등은 해결해야할 문제이다.

3. 본론

3.1 시스템 구성

본 논문에서 제안한 CCTV 원격 접속 시스템은 "Fig. 3"과 같이 원격지 접속 클라이언트 "A"와 터널링 서버 "B", CCTV 녹화기 "C"로 구성된다. 클라이언트 "A"는 터널링 서버 "B"와 연결되는 응용 프로그램으로, SSH Secure Shell 을 통해 접속 한다. 터널링 서버 "B"는 클라이언트 "A"와 CCTV 녹화기 "C"사이의 터널을 생성하고 데이터를 전달하는 중계 서버 역할을 한다. "Fig. 3"은 본 논문에서 제안하는 CCTV 원격 접속 시스템의 구성도이다.

첫 번째로 보안 연결은 "A"가 "B"에게 SSH 접속을 요청하고, 상호간 사용자 인증 절차가 완료 되면, "A"와 "B"사이의 안전한 보안 연결이 수립된다. "A"와 "B"의 연결이 완료되면 "B"는 내부적으로 가지고 있는 CCTV 녹화기 "C"의 접속 정보를 "A"에게 전달한다. "A"는 "B"로부터 전달 받은 정보를 토대로 "A" 와 "C" 사이의 암호화된 터널을 생성 한다. 이렇게 터널을 통해 전달되는 데이터는 보안 암호화가 되어 있어 스니핑을 통한 패킷 분석을 할 수 없다.

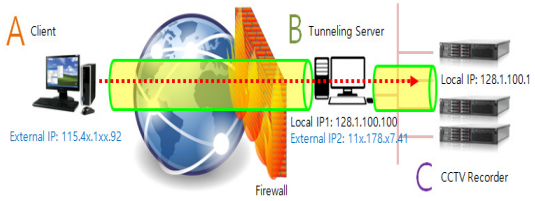

Fig. 3. CCTV Remote Access System

두 번째로 CCTV 녹화기 "C"가 방화벽 혹은 VPN (Virtual Private Network) 내부에 존재 할 경우, 외부로부터 침입에 대한 보안 효과는 높으나 외부에서는 접속이 불가능한 단점이 있다. 하지만 본 논문에서 제시한 방법을 사용한다면, 터널링 서버 "B"가 CCTV 녹화기 "C"의 데이터를 중계하여 전달해 주는 역할을 함으로 방화벽 내부로의 접속 문제를 해결할 수 있다.

3.2 접속 알고리즘

"Fig. 4"는 본 논문에서 제안한 시스템의 접속 알고리즘을 나타낸다.

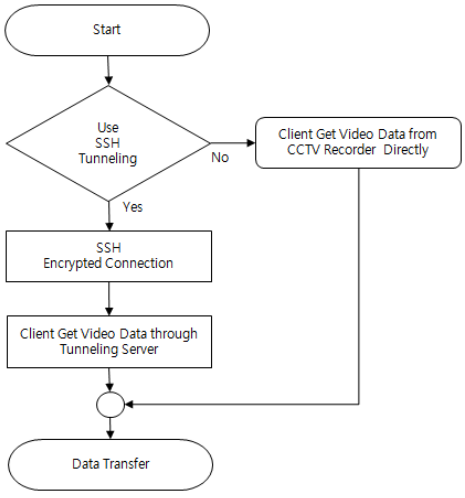

Fig. 4. Connection Algorithm

클라이언트가 실행되면 접속할 터널링 서버 주소를 입력하고 연결한다. 이 때, 터널링을 사용하여 연결 할 것인지, 아니면 CCTV 녹화기에 직접 연결 할 것인지를 선택 할 수 있다. 터널링을 사용한다면, 터널링 서버가 가지고 있는 녹화 장비에 대한 접속 정보를 이용하여 클라이언트에서 CCTV 녹화기로의 연결이 가능 하도록 터널을 생성 해 준다. 터널링 채널이 완성되면 클라이언트와 CCTV 녹화기는 상호간 암호화된 데이터 전송이 가능하다.

클라이언트 "A"가 서버 "B"에게 영상 정보를 요청하여 요청한 영상 정보를 받을 때까지의 시간을 T 라고 할 때, 터널링 기법을 사용하지 않을 경우의 시간 T_{NT} 는 수식 (1) 과 같이 연결 시간과 전송시간이 총 소요시간이 된다.

$$T_{NT} = T_{connection} + T_{Download} \quad (1)$$

$$T_{UT} = T_{connection} + T_{Encrypt} + T_{Download} + T_{Decrypt} \quad (2)$$

하지만 터널링 기법을 사용하게 되면 수식 (2)에서 보이는 것처럼 T_{UT}는 암호화(T_{Encrypt})와 복호화(T_{Decrypt}) 하는 시간이 추가적으로 필요하게 된다.

4. 실험 및 결과

4.1 실험 방법

본 논문에서 제시한 시스템의 성능을 확인하기 위해, 3가지 방법으로 실험을 하였다. 첫 번째는, 보안성 실험을 진행 하였다. 원격지에서 접속할 때, 인터넷 익스플로러를 이용할 경우와 클라이언트를 이용한 경우, 마지막으로 터널링을 사용 하였을 때 스니핑을 통한 보안성의 차이점을 확인하였다. 두 번째는, 방화벽이 설치된 환경에서의 원격 접근 여부에 대한 비교를 진행 하였다. 세 번째는, 네트워크로 접속 시 초기 영상 데이터가 전달되는 시간을 통해 암호화로 인한 전송 지연시간에 대한 비교 분석을 진행 하였다.

"Fig. 5"는 클라이언트에서 터널링을 사용하는 설정을 적용하여 CCTV 영상을 가져온 화면이다.

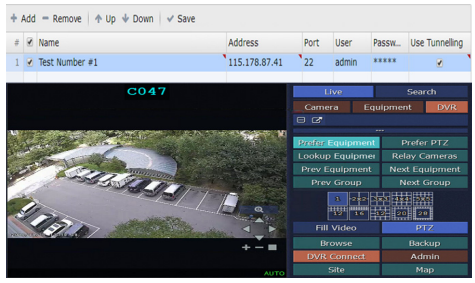

Fig. 5. Remote Access using Tunneling

4.2 실험 환경

테스트 환경은 인터넷 망에 연결된 PC에 원격 접속용 클라이언트를 설치하고, 방화벽으로 보호된 사설 네트워크 속에 터널링 서버와 CCTV 녹화기를 설치하였다. 터널링 서버에는 CCTV 녹화기에 대한 접속 정보를 기록해 두고, 외부 네트워크로의 연결은 22번 포트를 오픈하여 클라이언트에서 접속이 가능하도록 하였다. CCTV 녹화기의 사용자 아이디와 암호는 admin 으로 설정해 두었다.

4.3 패킷 보안성 검사

원격지 PC에서 웹 브라우져를 통해 HTTP 방식으로 CCTV 녹화기에 접속을 할 경우, 패킷 스니핑을 통해 보안성 여부를 확인 하였다. "Fig. 6"는 WinShark를 이용하여 전송되는 패킷의 내용을 분석한 그림이다. 현재 전달되는 패킷들 중 원격지 PC와 CCTV 녹화기 호스트 정보를 필터링하면 "Fig. 7"과 같이 사용자의 아이디와 암호가 그대로 노출되는 것을 확인할 수 있었다.

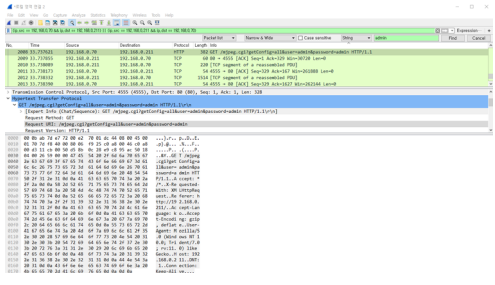

Fig. 6. Packet analysis using WinShark

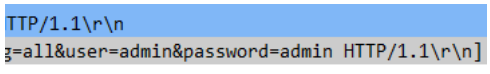

Fig. 7. Data Leakage (User ID and Password)

동일한 방법으로, SSH 접속이 이루어진 상태에서 패킷 확인을 해 보았다. "Fig. 8"과 같이 암호화 접속이 이루어진 패킷 속에서는 사용자 정보와 암호 정보를 확인할 수 없었다.

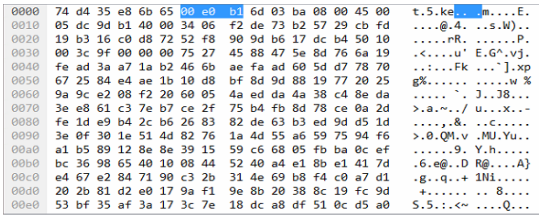

Fig. 8. Encrypted packet

4.4 방화벽 내부 시스템 접속 여부

사설 네트워크나 VPN 혹은 방화벽 내부에 있는 시스템으로의 접속은 접속에 대한 인증과 허가가 없는 경우 접근이 불가능 하였다. 제안하는 시스템은 터널링 기법을 이용하여, 사설 네트워크와 방화벽 내부에 존재하는 시스템에 대한 접근이 가능한 것을 확인 할 수 있었다.

4.5 패킷 지연시간 검사

제안하는 시스템을 사용함으로써 발생하는 접속지연 시간에 대한 비교를 진행하였다. "Fig. 9" 와 "Fig. 10"은 클라이언트가 서버에 접속하여 초기 영상을 가져오기까지의 시간을 비교한 것이다. 전체 접속시간은 네트워크의 상황에 따라 차이가 나지만, 터널링을 통한 암호화 기법을 사용할 경우가 사용하지 않을 경우 보다 평균적으로 0.7초 정도의 더 지연됨을 실험을 통해 확인 할 수 있었다.

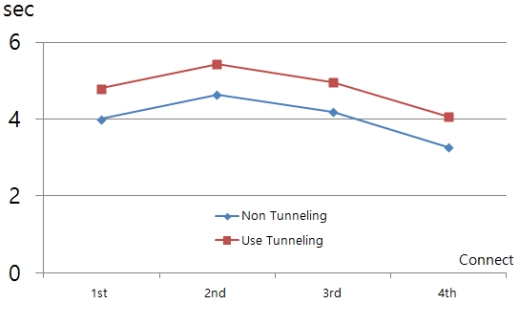

Fig. 9. Connection Delay Time

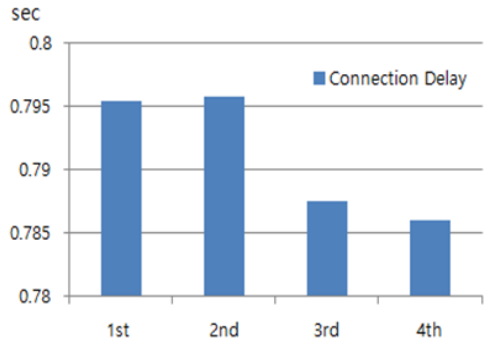

Fig. 10. Delay Time Analysis

4.6 실험 결과

"Table. 2"는 여러 가지 CCTV 원격 접속 기법과 터널링을 사용한 원격 접속 기법을 비교 분석 한 결과 이다.

Table 2. Performance Analysis

	HTTP	HTTPS	Client	Tunneling
Security	Weak	Strong	Weak	Strong
Encrypt	X	O	X	O
Extra Packet	X	O	X	O
Time Delay	X	O	X	O
Connection possibility located in Firewall	X	X	X	O

HTTP 프로토콜을 이용한 원격 접속 방법은 보안성이 결여되어 있다. 이것을 개선한 HTTPS와 같은 프로토콜이 존재하지만 방화벽 내부에 있는 시스템에 접근하기는 어렵다. 터널링을 사용하여 원격지에서 CCTV 녹화기에 접속을 할 경우, 암•복호화에 따른 전송 지연이 발생하고 패킷의 정보도 추가가 된다. 또한 내부 접속을 위한 별도의 포트 연결 정보를 보존하고 있어야 하는 작업이 있지만, 보안성 강화를 위한 필요조건으로 볼 수 있다.

Table 3. Network Environment

	Firewall	VPN	SSL VPN	SSH Tunneling
Based Configuration	H/W	H/W	H/W	S/W
Location	Server Router	Router	App Server Router	App Server
Service Cost	O	O	O	X

"Table. 3"는 네트워크 구축 환경에 따른 차이점을 터널링 기법과 비교 한 것이다. 방화벽이나, VPN, SSL-VPN은 네트워크 보호를 위한 하드웨어 기반 기술이다. 네트워크상의 라우터나 서버를 통해 서비스 할 수 있다[10]. 보안 품질이 우수하지만, 서비스 및 운영비용이 든다는 단점이 있다. 본 논문에서 제안하는 방법은 추가적인 서비스 비용 없이 보안성 강화를 할 수 있다.

5. 결론

영상 보안 시스템의 보안 성능을 높이기 위해서는 기본적으로 원격 서비스 접근 차단, 접근 가능 IP 제한, 시스템의 기본 암호 변경 등과 같은 보안 조치를 취해야 하지만, 많은 CCTV 사용자는 이러한 권고사항을 지키지 않는다. 본 논문에서는 여러 가지 해킹 위협으로부터 안전하게 영상정보를 관리할 수 있는 SSH 터널링을 이용한 CCTV 보안 관제 기법에 대해 제안하고 실험 하였다. 또한 여러 가지 CCTV 원격 접속 기법들과의 비교를 통해 장단점을 확인 해 보았다. 제안하는 시스템은 보안을 위한 암 복호화로 인한 지연시간이 발생하지만, 방화벽과 네트워크 장애물을 우회 접속하면서도 보안 우수성이 높아짐을 확인 할 수 있었다. 향후 연구 과제로 영상 채널수가 증가할수록 네트워크 지연시간이 증가하는 문제에 대한 추가적인 연구가 필요하다.

References

[1] KISA, "CCTV Personal Video Information Protection Guideline", http://www.kisa.or.kr, 2007.

[2] T.W. Seo, S.R. Lee, B.C. Bae, "An Analysis of Vulnerabilities and Performance on the CCTV Security Monitoring and Control," *Journal of Korea Multimedia Society*, vol. 15, no. 1, pp 93-100, Jan. 2012. DOI: http://dx.doi.org/10.9717/kmms.2012.15.1.093

[3] TTA, "Security Requirements of the Video Surveillance System", http://www.tta.or.kr, 2012.

[4] Y.S. Won, S. H. Yun, "CCMP Packet design for security CCTV environment," *The conference of Korea Communication Society* , Dec. 2013.

[5] K.J. Bae, K.R. Lee, K.B. Yim, "Proxy Server Providing Multi-level Privileges for Network Cameras on the Video Surveillance System," *Journal of Korea Internet Information Society*, vol. 12, no. 2, pp 123-133, Apr. 2011.

[6] Y.D. Hwang, D.K. Park, "Design and Implementation of Android-based NVR System," *The Journal of Korea Institute of Information Technology*, Apr. 2016. DOI: http://dx.doi.org/10.14801/jkiit.2016.14.4.109

[7] D.S. Kim, E. J. Yoon, "Study of Imaging Security Using Lightweight Cryptography and Data Hiding Technique on IoT," *The conference of the institute of electronics and information engineers* , pp 1791-1793, Jun. 2015.

[8] H.J. Kong, H.S.Chu, "Inter-PMIPv6-Domain Hand over Scheme Based on Tunneling," *The conference of Korea Information Society* , May 2009.

[9] Y.S. Ko, K.H. Park, C.S. Kim, "Problem Analysis and Countermeasures Research through Security Threat Cases of Physical Security Control System," *The Journal of Korea Multimedia society*, vol. 19, no. 1, January, 2016. DOI: http://dx.doi.org/10.9717/kmms.2016.19.1.051

[10] Kuwar Kuldeep V V Singh, Himanshu Gupta, "A New Approach for The Security of VPN," *Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies*, Mar. 2016.

황 기 진(Gi-Jin Hwang) **[정회원]**

- 2001년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2014년 8월 : 숭실대학교 컴퓨터학과 (박사수료)

<관심분야>
실시간 시스템, 운영체제, 영상 보안

박 재 표(Jae-Pyo Park) **[종신회원]**

- 1998년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2004년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2008년 3월 ~ 2009년 2월 : 숭실대학교 정보미디어 기술연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<관심분야>
컴퓨터 통신, 보안, 암호학, 멀티미디어 통신

양 승 민(Seung-Min Yang) **[정회원]**

- 1983년 2월 : University of South Florida. Dept of Computer Science (MS.)
- 1986년 8월 : University of South Florida. Dept of Computer Science (Ph.D.)
- 1987년 3월 ~ 1991년 2월 : Professor in the Department of Computer Science, University of Texas at Arlington.
- 1993년 3월 ~ 현재 : 숭실대학교 컴퓨터학부 교수

<관심분야>

Real Time System, System Fault Tolerance, Wireless Sensor Networks, Operating System, etc