Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 5 pp. 579-584, 2023

https://doi.org/10.5762/KAIS.2023.24.5.579
ISSN 1975-4701 / eISSN 2288-4688

거주시설 단지망에 대한 사이버 공격포인트 연구

장석우[1], 이용준[2*]
[1]안양대학교 소프트웨어학과, [2]극동대학교 해킹보안학과

A Study on Cyber Attack Points for Residential Facilities

Seok-Woo Jang[1], Yong-Joon Lee[2*]
[1]Department of Software, Anyang University
[2]Department of Hacking Security, Far East University

요 약 최근 거주시설을 대상으로 폐쇄 네트워크에 사이버공격이 지속적으로 발생하고 있다. 이에 본 연구에서는 거주시설의 단지망에 침투하기 위해 공격포인트로 주로 사용되고 있는 IoT 기기, 스마트 기기를 통한 사이버공격 사례와 최근의 ICT 취약점에 대해 분석하였다. 주거시설에 대상 사이버 공격포인트로는 IoT 권한정보 획득을 통한 시스템 장악, 공개된 FTP 서버 계정 탈취, 아파트 관리용 홈페이지의 취약점을 이용하는 사이버 공격포인트에 대해 사례를 조사하였다. 본 연구에서는 주거시설 사이버 공격포인트에 대한 실증적 실험을 위해 IoT 권한정보 취득을 통한 시스템 장악, 내부 FTP 계정 탈취를 통한 정보유출, 세션관리 부재를 이용한 권한 획득에 대해 실증 시험과 보안대책을 제시하였다. 본 실험에서 IoT 권한정보 취득을 통한 시스템 장악, 공개된 FTP 계정 탈취를 통한 정보 유출, 세션 관리 부재를 통한 권한 획득에 대한 3개 거주시설 단지망에 대한 향후 사이버공격 탐지 및 보안이 가능할 것으로 기대된다.

Abstract Recently, cyberattacks on closed residential facility networks have continued to occur. In this study, cases of cyberattacks through IoT devices and smart home appliances used in home networks that penetrate a residential facility's short network were analyzed along with recent ICT vulnerabilities. We analyzed recently occurring cyberattack points for residential facilities that use system control through IoT authority information acquisition, public FTP server account theft, and session management vulnerabilities on apartment management webpages. For an experiment on cyberattack points in three residential facilities, this study presented attack-point tests, detection methods, and security measures for system control to prevent IoT authorization information acquisition, information leakage through internal FTP account theft, and acquisition of authority through session management.

Keywords : Residential Facilities, Apartment Complex Network, Cyber Attack Points, Check for Vulnerabilities, IoT Device

1. 서론

정보통신의 기술의 발전과 함께 IoT의 기술은 지속적인 발전을 거듭하고 있다. IoT의 발전은 주거시설에도 디지털화로 변화하고 있다. 주거시설 내부에 조명, 가스, 난방, 도어 기기 등 다양한 IoT 기기는 무선으로 연결되어 내•외부에서 IoT 기기를 제어할 수 있는 환경이 구축되었다[1].

최근 주거시설 단지망의 설비 자동제어시스템 서버가 해킹되는 사례가 발생했다. 조사결과 해당 시스템은 원격제어 프로그램이 설치되었고 해외 40개 국가를 대상으로 인터넷 서버를 공격하는 경유지로 활용된 것으로 조사되었다. 주거시설 내의 스마트 기기가 인터넷으로 연결된 Home IoT 시대에 보안취약점은 주거시설 단지망

*Corresponding Author : Yong-Joon Lee(Far East University)
email: bigman2u@naver.com
Received April 3, 2023 Revised April 25, 2023
Accepted May 12, 2023 Published May 31, 2023

의 시스템 해킹 아니라 거주민의 개인정보 유출 등 심각한 피해를 발생시킬 수 있다[2].

본 연구에서는 거주시설의 단지망에 침투하기 위해 홈네트워크에서 사용하고 있는 IoT 기기, 스마트 가전을 통한 사이버공격 사례와 이와 관련된 ICT 취약점에 대해 조사분석하였다[3].

본 연구에서는 세부 연구에서는 주거시설 사이버 공격 포인트에 대한 실험을 위해 IoT 권한정보 취득을 통한 시스템 장악, 내부 FTP 계정 탈취를 통한 정보 유출, 세션 관리 부재를 통한 권한 획득에 대한 공격유형에 공격 포인트 시험과 보안대책을 제시하고자 한다.

2. 관련 연구

거주시설 폐쇄 네트워크인 단지망에 대한 사이버공격이 지속적으로 발생하고 있다. 본 연구에서는 거주시설의 단지망에 침투하기 위해 홈네트워크에서 사용하고 있는 IoT 기기, 스마트 가전 등을 통한 사이버공격 사례와 최근의 ICT 취약점에 대해 분석하였다[4].

2.1 거주시설 ICT기기에 대한 취약점

거주시설에 단지망에 ICT기기를 이용한 사이버 공격 포인드가 주로 발생하고 있는데 다음은 주로 발생하는 월패드, 지능형 CCTV, 무선AP, AI 스피커에서 발생한 취약점은 다음과 같다[6].

- 월패드(CVE-2019-19163) : COMMAX WallPad (CDP-1020MB) 펌웨어의 취약점으로 인해 이전 버전의 MySQL을 사용하기 때문에 인증되지 않은 인접 공격자가 임의코드가 실행되는 취약점
- 지능형 CCTV(CVE-2019-25062) : Sricam IP CCTV 카메라에서 취약점이 발견되어 치명적으로 분류되었으며 구성요소 장치 뷰어의 일부 알 수 없는 처리에 영향을 주어 메모리 손상이 가능한 취약점
- 무선 AP(CVE-2021-33843) : Fresenius Kabi Agilia SP MC WiFi vD25 및 이전 버전에는 인증 없이 액세스할 수 있는 기본 구성 페이지가 있어서 공격자는 이 기능을 사용하여 네트워크 설정과 같은 노출된 구성 값을 변경할 수 있는 취약점
- AI 스피커(CVE-2019-5271) : Huawei 스마트 스피커 Myna에 정보유출 취약성으로 스피커가 일부 데이터를 처리에 오류가 발생

2.2 거주시설 단지망에 발생한 국내외 사이버공격 사례

거주시설의 단지망을 대상하는 국내외 사이버공격 사례가 다양하게 발생하고 있으며 월패드, 주거시설 IoT 봇넷, 스마트 TV 악성코드 유포 등이 발생하고 있으며 해당 사례는 다음과 같다[5].

- 월패드 해킹 : 2021년 국내 거주시설 내부 영상 17만건 공개된 사건이 발생했으며 웹셀을 통해서 중앙관리 서버를 통해 주거단지 게이트웨이, 댁내 월패드가 해킹된 사건 사례
- 주거시설 IoT 봇넷 : 2022년 국내외 IoT 장비 1만 1700여대가 악성코드 Mozi 봇넷에 감염되어 국내 주거시설 단지망에 해킹과 접속을 하였으며 가상화폐 채굴용 악성코드 경유지로 악용되었는데 감염된 IoT 장비는 무선 공유기, CCTV, 영상녹화장비, PC 광고 모니터 등에 발생한 사건 사례
- 스마트 TV 악성코드 : 2016년 LG Android TV는 Cyber.Police(FLocker) 랜섬웨어와 2018년 ADB.Miner 웜은 해커를 위한 암호화폐 채굴을 목표로 Android 기반 스마트 TV를 표적으로 하이재킹을 시도하는 악성코드 유포 사례

3. 주거시설 사이버 공격포인트 분석

주거시설에 대한 사이버 공격포인트에 대해 IoT 권한정보 획득을 통한 시스템 장악 , 공개된 FTP 서버 계정 탈취, 아파트 관리 페이지의 세션관리 취약점을 이용하는 사이버 공격포인트에 대해 분석하였다[7].

3.1 IoT 권한정보 취득을 위한 공격포인트

관리자 프로그램의 초기 계정이 취약하거나 통신구간 암호화가 안된 인증정보를 획득하는 공격포인트를 통해 거주시설의 내부 서버에 접속하여 서버기능을 장악하는 공격이 가능하다[8].

Fig. 1과 같이, 공격포인트는 ① 초기 인증정보 설정을 통한 획득으로 IoT 초기 인증정보가 동일하거나 인증정보 변경을 하지 않는 경우 공격자는 Default 인증정보로 접근할 수 있는 취약점이 발생한다. ② IoT 통신구간 암호화 취약정보를 활용하는 것으로 인증정보, 암호키와 같이 IoT 통신구간 암호화가 미적용되는 경우 인증정보가 평문으로 노출되어, 스니핑 및 패킷 위·변조의 취

약점에 노출 될 수 있다. 또한 SSL/TLS 사용시 신뢰할 수 없는 기관에서 발급한 인증서의 사용, 만료 또는 해지 등 취약한 인증서를 사용하는 경우 비인가 사용자가 중간자 공격이 가능한 취약점이 발생한다.

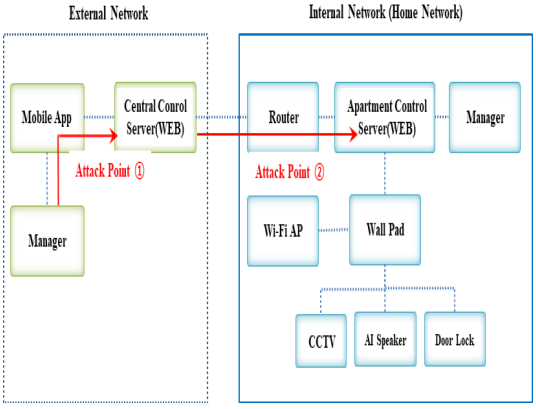

Fig. 1. Attack Point for Control of IoT through The Acquisition Information

3.2 오픈된 FTP 계정 탈취 공격포인트

내부 주거시설 단지망의 서버에 오픈된 FTP 서비스를 통해 계정을 탈취하여 내부 서버 시스템 침입이 가능하다[9].

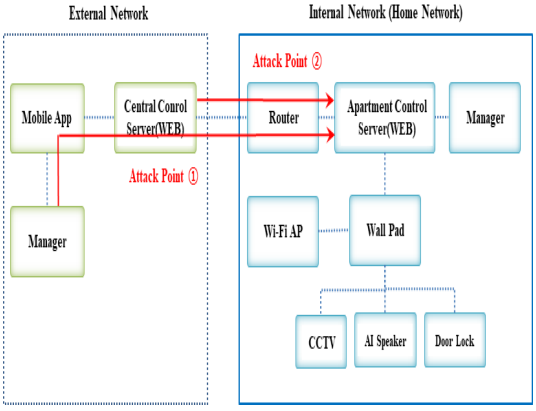

Fig. 2. Attack Point for Information Leakage through FTP Account Theft

Fig. 2와 같이, 공격포인트는 ① 외부로 공개된 FTP 서버를 통한 것으로 운영체제 또는 소프트웨어에 기본적으로 설치되는 불필요한 서비스가 활성화되어 있는 경우 외부 공격자의 침입이 가능하다. ② 추가적으로 주거시설 단지내에 통신구간 암호화 취약 정보를 활용하는 것으로 인증정보, 암호키와 같이 통신구간 암호화가 미적용되는 경우 인증정보가 평문으로 노출되어, 스니핑 및 패킷 위·변조의 위험에 노출 될 수 있다.

3.3 세션정보 획득 공격포인트

관리자 사이트의 세션 관리 부재를 이용해 중요 페이지에 접근하여 내부 정보 유출이 가능하다[10].

Fig. 3과 같이, 공격포인트는 ① 주거시설에 대한 관리, 영상 노출 페이지의 접근 통제을 통한 것으로 관리 페이지와 같이 중요 페이지 접근 시 인가된 권한을 검증하는 기능이 부재한 경우 공격자가 중요페이지에 직접 접근하여 기기 정보 열람 또는 제어하는 취약점이 존재한다. ② 세션 관리 결함을 활용하는 공격포인트는 세션의 관리 기능의 결함이 존재하는 경우 공격자가 세션 하이재킹 등의 공격에 의해 관리자 계정 탈취하는 취약점이 발생할 수 있다.

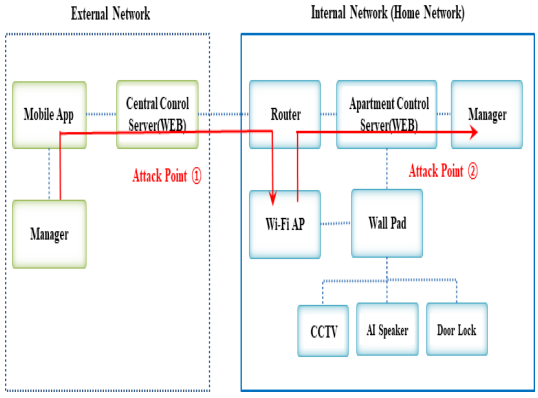

Fig. 3. Attack Point for Acquire Session Information

4. 주거시설 사이버 공격포인트 시험

본 연구에서는 주거시설 사이버 공격포인트에 대한 실험을 위해 IoT 권한정보 취득을 통한 시스템 장악, 내부 FTP 계정 탈취를 통한 정보 유출, 세션 관리 부재를 통한 권한 획득에 대한 공격유형에 공격포인트 시험과 보안대책을 제시하였다.

4.1 IoT 권한정보 취득을 통한 시스템 장악

Fig. 4와 같이, 초기 인증정보 설정을 통한 획득 점검을 위해 기기 뒷면 초기 인증정보 기재 확인, 기기 초기 인증시 관리자 계정 인증정보를 강제로 변경하는 절차가 있는지 확인하였다. IoT 기기 제품 정보에 인증정보(예

admin / amin)가 노출되어 있는 경우 보안인증이 취약하며 초기에 IoT 관련 인증정보로 인증된 이후에 강제적 기능으로 인증정보를 변경하지 않고 기존의 계정정보를 사용할 수 있다면 계정정보에 대한 권한획득이 가능하다.

Fig. 4. Check for Initial IoT Authentication Information Vulnerability

Fig. 5와 같이 중요정보 통신구간 암호화 취약 정보를 점검하는 방법으로는 Wireshark를 통해 패킷을 분석하여 암호화와 인증에 대한 트래픽 확인이 가능하다. 인증정보가 보안이 안전하지 않는 MD5 해쉬를 사용하는 취약점, 암호화가 되지 않는 Base64 인코딩으로 하는 취약점, 통신구간에 암호화가 되지 않아 인증정보가 노출되는 취약점 등을 통해 거주시설 단지망으로 진입이 가능하다.

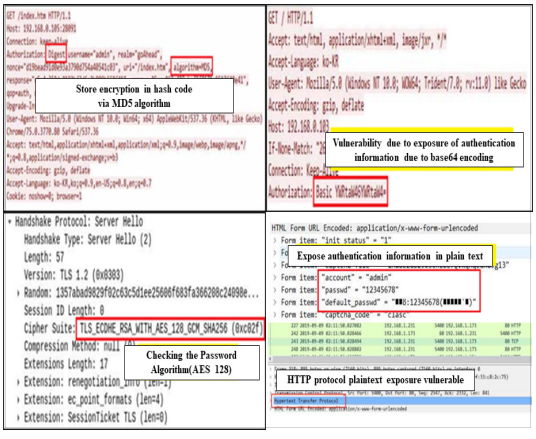

Fig. 5. Check for Cross-Communication Encryption Vulnerabilities

4.2 내부 FTP 계정 탈취를 통한 정보 유출

내부 아파트 단지망의 서버에 공개된 FTP 서비스를 통해서 내부 서버 시스템에 대한 진입이 가능하다. Fig. 6과 같이, Nmap을 통해 분석하면 호스트, TCP서비스, UDP서비스 스캔이 가능하다. 또한 불필요한 FTP 서비스가 공개된 경우 거주지 단지망으로 침투가할 수 있다.

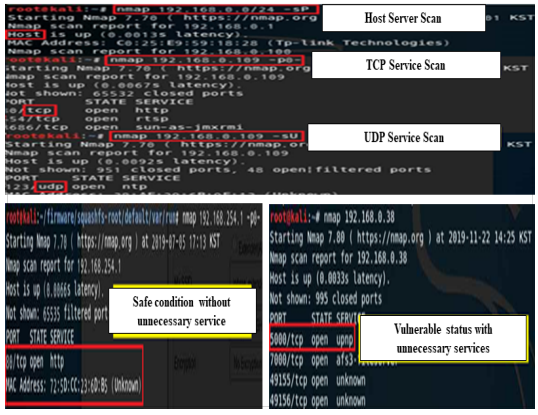

Fig. 6. Check for Open FTP Service Vulnerabilities

4.3 세션 관리 부재를 통한 권한 획득

거주시설 관리용 웹사이트에 관리, 영상 노출 페이지의 접근 통제 점검하여 영상이 포함된 페이지 또는 관리자 페이지에서 개발자 옵션(F12)을 통해 소스코드 확인, URL 추출 후 새 탭에서 해당 URL 접속할 수 있다. Fig. 7과 같이, 거주시설 웹사이트에서 영상 관련 페이지, 관리자 페이지에 대해 접속을 요청한 경우, 리다이렉트하여 인증을 재요청하는 경우는 안전하지만 인증에 대한 추가 확인이 없는 취약점이 분석이 되었다.

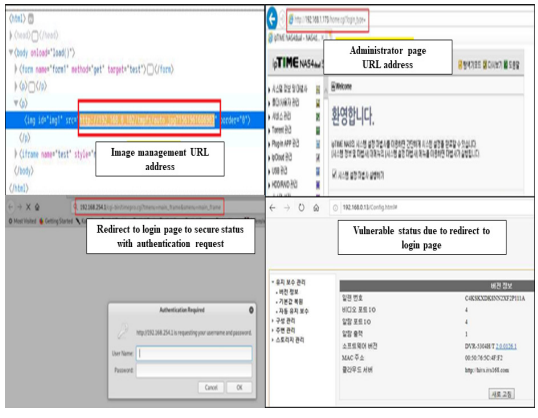

Fig. 7. Check for Session Information Vulnerabilities

4.4 거주시설 사이버 공격포인트 시험결과

Table 1은 거주시설 사이버 공격포인트에 대한 시험 결과를 보여준다.

Table 1. Cyber Attack Point Test Results for Residential Facilities

	Attack Type	Attack Point	Inspection Method	Protective Measures
1	Acquisition of IoT Authority Information	Initial Authentication Information	Person Inpection	Change Initial Account
		Encryption Vulnerable Information	Wireshark	Secure Cryptographic Algorithms
2	Internal FTP Accout Hijacking	Expose FTP Servie	Mmap	Eliminate Unnecessary Service
		Encryption Vulnerable Information	Wireshark	Secure Cryptographic Algorithms
3	Session Authorization Attack	Exposed Website Authentication Page	OWASP ZAP	Reconnect Authentication
		Session Management Vulnerability	OWASP ZAP	Secure Session Management

IoT 권한정보 취득을 통한 시스템 장악의 공격포인트로 초기 인증정보 확인하고 Default 계정으로 접속이 가능하다. 해당 취약점은 IoT 기기 인증정보를 육안으로 확인해서 접속할 수 있었다. 취약점 보안대책은 초기 비밀번호를 강제적으로 변경하는 절차가 있어야 한다. IoT 통신구간에서 암호화 취약점을 이용하는 경우에는 Wireshark를 통해 통신구간의 계정 정보가 노출될 수 있다. 보안대책으로 보안에 대한 안전이 확인된 암호 알고리즘을 채택해야 한다.

공개된 FTP 계정 탈취를 통한 정보 유출의 경우는 불필요하게 공개된 FTP 서버를 통해 공격이 가능한데 Mmap 스캔을 통해 불필요한 서비스에 대한 IP, Port를 확인하여 공격정보로 활용할 수 있다. 보안대책으로 거주시설 단지망에 사용하지 않는 FTP, Mail 등 서비스는 기능을 사용하지 않아야 한다. 서버의 통신구간의 암호화에 취약점이 있는 경우 Wireshark를 통해 통신구간에서 계정정보가 노출를 확인하고 사용할 수 있다.

세션 관리 부재를 통한 권한 획득의 공격은 단지망 웹사이트 관리자 페이지의 노출 페이지를 검색하는 방식으로 OWASP ZAP(Zed Attack Proxy) 웹취약점 점검 도구를 통해 확인이 가능했으며 보안대책은 인증 페이지에 대해서는 재인증을 요청하는 기능이 있어야 한다. 세션에 대한 하이제킹 공격이 OWASP ZAP으로 가능하며 보안대책은 강화된 세션관리 설정이 필요하다.

본 실험에서 3개 거주시설 단지망에 대한 공격포인트에 대한 침입 결과와 보안대책을 제시하였다.

5. 결론

거주시설 폐쇄 네트워크인 단지망에 대한 사이버공격이 지속적으로 발생하고 있어 본 연구에서는 거주시설의 단지망에 침투하기 위해 홈네트워크에 대해 조사하였다. 사이버공격의 경로로 주로 사용되는 IoT 기기, 스마트 가전에 대한 국내외 공격사례를 조사하였다.

주거시설에 대한 사이버 공격포인트에 대해 IoT 권한정보 획득을 통한 시스템 장악, 공개된 FTP 서버 계정 탈취, 아파트 관리 홈페이지의 세션관리 취약점을 이용하는 사이버 공격포인트에 대해 분석하였다.

주거시설에 단지망의 사이버 공격포인트에 대한 해킹 실험을 위해 IoT 권한정보 취득을 통한 시스템 장악, 내부 FTP 계정 탈취를 통한 정보유출, 세션관리 부재를 통한 권한 획득에 대한 공격유형에 공격포인트 실증시험과 보안대책을 제시하였다.

본 실험에서 IoT 권한정보 취득을 통한 시스템 장악, 공개된 FTP 계정 탈취를 통한 정보 유출, 세션 관리 부재를 통한 권한 획득에 대한 3개 거주시설 단지망 환경을 구성하였다. 거주시설 단지망에 대한 취약점 확인을 위해 취약점 분석가, Wireshark, Mmap, OWASP ZAP 점검도구로 분석하였으며 계정관리 개선, 강화된 암호화, 불필요한 서비스 제거 등의 보안대책을 제시하였다. 향후 거주시설에 대한 스마트 TV, 도어락 등에 대해서도 추가적 연구가 필요하다.

References

[1] Meicong Li et al., "The study of APT attack stage model," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), June 2016, Available: https://ieeexplore.ieee.org/document/7550947 DOI: https://doi.org/10.1109/ICIS.2016.7550947

[2] M. Husak and J. Kaspar, “towards Predicting Cyber Attacks Using Information Exchange and Data Mining,” in 2018 14th International Wireless Communications

Mobile Computing Conference(IWCMC), 2018.

[3] S. M. Milajerdi, R. Gjomemo, B. Eshete, R. Sekar and V. N. Venkatakrishnan, "HOLMES:Real-time APT detection through correlation of suspicious information flows," 2019 IEEE Symposium on Security and Privacy,pp.1137-1152,May 2019.

[4] Argyrios Alexopoulos and Nicholas J. Daras, "Mathematical Study of Advanced Persistent Threat (APT) Hunting Techniques," Journal of Computations 2020. DOI: https://doi.org/10.47260/jcomod/1021

[5] Josyula Rao, Yan Chen, R. Sekar, Venkat Venkatakrishnan, "Mitigating advanced and persistent threat(APT) damage by reasoning with provenance in large enterprise network (MARPLE) Program," AFRL-RY-WP-TR-2019-0285, International Business Machines Corporation, Jan. 2020.

[6] S. Park, J. Jung and S. Lee, "Multi-perspective APT Attack Risk Assessment Framework using Risk-Aware Problem Domain Ontology," 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), pp. 400-405, 2021.

[7] MITRE, ATT&CK, https://attack.mitre.org/, accessed on Mar. 2022

[8] MinJu Kim, Sihn-Hye Park and Seok-Won Lee, "A Security Requirements Recommendation Framework Based on APT Attack Cases, " Journal of KIISE, Vol.48, No.9, pp.1014-1026, 2021.9. DOI: https://doi.org/10.5626/JOK.2021.48.9.1014

[9] Sungyoung Cho, Yongwoo Park and Kyeongsik Lee, "Implementation of an APT Attack Detection System through ATT&CK-Based Attack Chain Reconstruction," Journal of The Korea Institute of Information Security & Cryptology Vol.32, No.3, Jun. 2022. DOI: https://doi.org/10.13089/JKIISC.2022.32.3.527

[10] Sungyoung Cho, Yongwoo Park, Kunho Lee et al, "An APT Attack Scoring Method Using MITRE ATT&CK," Journal of The Korea Institute of Information Security & Cryptology Vol.32, No.4, Aug. 2022. DOI: https://doi.org/10.13089/JKIISC.2022.32.4.673

장 석 우(Seok-Woo Jang) [종신회원]

- 1995년 2월 : 숭실대학교 전자계산학과 (공학사)
- 1997년 2월 : 숭실대학교 일반대학원 컴퓨터학과 (공학석사)
- 2000년 8월 : 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
- 2009년 3월 ~ 현재 : 안양대학교 소프트웨어학과 교수

〈관심분야〉
로봇비전, 증강현실, HCI, 비디오 색인 및 검색 등

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구위원
- 2016년 4월 ~ 2020년 3월 : 국방보안연구소 연구관
- 2021년 4월 ~ 현재 : 극동대학교 해킹보안학과 교수

〈관심분야〉
해킹보안, 국방보안, 인공지능보안