Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 4 pp. 610-615, 2023

https://doi.org/10.5762/KAIS.2023.24.4.610
ISSN 1975-4701 / eISSN 2288-4688

APT(Advanced Persistent Threat) 공격 시나리오 검증 시스템 연구

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

A Study on the APT Attack Scenario Verification System

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

요 약 APT(Advanced Persistent Threat)는 대상시스템을 사전에 조사한 후에 악성코드에 감염시키다. 이러한 APT 공격 대상은 스마트빌딩, 스마트팩토리 등과 같은 디지털화된 공간과 결합이 되면서 점차 다양한 공격으로 변화하고 있다. 스마트빌딩, 스마트팩토리에서 APT 공격에 접점으로서 IoT센서, 보안용 CCTV, 공급망에 대상으로 APT 공격이 발생하고 있다. 이는 기존의 거주지, 산업공간이 4차산업기술과 융합이 되면서 통신연결, IoT센서를 통한 자동화를 통한 데이터 수집이 되면서 APT 공격 대상도 확대되고 있다. 본 연구에서는 IoT센서 무선취약점 APT 공격 시나리오, CCTV 계정 취약점 APT 공격 시나리오, 공급망 네트워크 취약점 APT에 대해 MITRE ATT&CK 프레임워크 절차에 따라 개발하였다. 제안하는 APT 시나리오 검증 시스템을 통해서 3개 APT를 특정 시스템을 대상으로 실험을 수행하였으며 3개 APT 공격에 대해서는 해당 시스템에 전체 공격 성공율은 86.9%로 취약한 것으로 분석되었다. 본 연구를 통해 다양한 APT 공격의 시나리오를 개발하고 검증하는데 활용이 가능하다.

Abstract APT (Advanced Persistent Threat) pre-investigates the target system and infects it with malicious code. These APT targets are gradually changing into various attacks as they are combined with digitized spaces, such as smart buildings and smart factories. In smart buildings and factories, attacks on IoT sensors, security CCTV, and supply chains are being hit as contact points for APT attacks. This combines existing residential areas and industrial spaces with the fourth industrial technology to collect data automatically through communication connections and IoT sensors. The target of APT attacks is expanding. In this study, the IoT sensor wireless vulnerability APT attack scenario, CCTV account vulnerability APT attack scenario, and supply chain network vulnerability APT was developed according to MITREATT&CK framework procedures. Using the proposed APT scenario verification system, three APTs were examined on specific systems, and the overall success rate for the three APT attacks was 86.9%, which was analyzed as vulnerable. These results can be used to develop and verify scenarios for various APT attacks.

Keywords : APT(Advanced Persistent Threat), APT Attack Scenario, APT Attack Scenario Verification System, MITRE ATT&CK Framework, Vulnerability Discovery

*Corresponding Author : Yong-Joon Lee(Far East University)
email: bigman2u@naver.com
Received March 16, 2023 Revised April 4, 2023
Accepted April 7, 2023 Published April 30, 2023

1. 서론

APT(Advanced Persistent Threat)는 대상시스템을 사전에 조사한 후에 악성코드에 감염시키다. APT의 특징은 지속성과 지능성인데 장시간 스파이처럼 은닉하여 피해 시스템에 잠복하여 정보를 빼내는 특징을 가지고 있다. 잠복하는 기간은 수일에서 수년까지 공격이 지속되기도 한다[1].

스마트홈, 스마트빌딩, 스마트팩토리에서 APT 공격에 접점으로서 IoT센서, 보안용 CCTV, 공급망에 대상으로 APT 공격이 발생한다. 이는 기존의 거주지, 산업공간이 4차산업기술과 융합이 되면서 통신연결, IoT센서를 통한 자동화된 데이터 수집이 되면서 APT 공격 도 확대되고 있다[2].

2022년 국내외 IoT 11,700대가 악성코드 Mozi 봇넷에 감염되어 가상화폐 채굴용 악성코드 유포 등에 악용이 되었다. IoT 장비로는 유무선공유기, CCTV, 영상녹화장비 등이 있어 IoT 취약점을 통한 APT 공격 가능성은 지속적으로 증가하는 추세이다.

2021년 CCTV 해킹을 통해 아파트에 영상파일을 다크웹에 판매하는 사례가 발생했다. 이는 보안용 CCTV 계정 취약점을 이용하여 동영상 정보를 취득하는 방식으로 APT 공격의 대상이 되고 있다. CCTV 취약점을 통해 스마트홈에 잠입하는 APT공격에 경로가 될 수 있는 것이다.

APT 대표적인 방법으로는 2020년 솔라윈즈 기업의 모니터링 솔루션 업데이트에 악성코드가 배포한 공급망 공격이다. 정상 SW 배포하는 과정에서 배포 서버의 취약점을 이용하여 사용자에게 배포될 소프트웨어를 변조하여 악성코드를 삽입하여 유포하는 방법이 발생했다. 공급망에 대한 APT공격은 공급망 전체에 영향을 주게 되는데 표적이된 SW를 사용하는 기업과 이용자가 악성코드에 감염되어 대규모 피해를 발생시킨다.

이와 같이, 스마트홈, 스마트빌딩, 스마트팩토리에서 APT 공격의 접점으로서 IoT센서, 보안용 CCTV, 공급망에 대상으로 APT 공격이 발생은 증가하고 있다. 따라서 새로운 스마트 환경에 대한 APT 공격의 가능성을 사전에 검토할 수 있는 APT 공격 사나리오에 대한 연구가 필요하다.

본 연구에서는 IoT센서 무선취약점 APT 공격 시나리오, CCTV 계정 취약점 APT 공격 시나리오, 공급망 네트워크 취약점 APT에 대해 MITRE ATT&CK 프레임워크 절차에 따라 설계하고 APT 시나리오 검증 시스템을 통해 실험으로 APT 공격에 대한 검증 결과를 제시한다.

2. 관련 연구

기존에 해외에서 발생한 IoT센서, CCTV, 공급망에 대한 APT 공격 사례를 조사하고 이를 통해 공격 시나리오를 설계하여 시험 환경에서 검증하기 위한 기초 자료를 분석하였다.

2.1 IoT센서 무선 취약점을 이용한 APT 공격

2017년 미국 카지노에서 IoT기기를 활용하는 수조 관리용 PC 통해 고객정보를 유출하는 해킹 사례가 발생했다. 수조의 청정도와 물고기 상태를 감시하는 IoT센서와 관리용 PC 상호간 무선 Wi-Fi 취약점을 스캔하고 내부망에 침투하여 카지노 고객 DB서버에서 고객정보 1GB를 해외 유출하는 APT공격이 발생했다[3].

APT 공격 프로세스는 Fig. 1과 같다. ① 수조관리용 IoT센서와 무선 공유기의 WPA2 Wi-Fi 통신 프로토콜의 취약점 발견, ② 공유기의 네트워크에 침입하여 내부 네트워크를 스캔, ③ 관리용 PC에 접속하여 고객DB서버에 접속, ④ 고객DB서버에 있는 고객정보 1GB를 해외로 유출의 절차를 따른다.

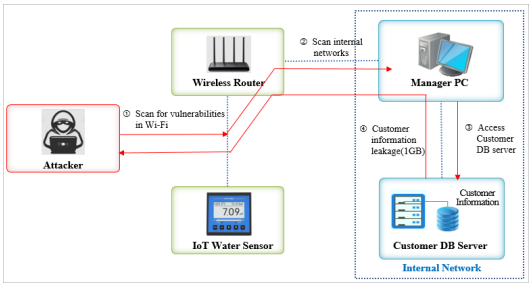

Fig. 1. APT attack procedure using IoT sensor wireless vulnerability

2.2 CCTV 계정 취약점을 이용한 APT 공격

2013년 미국연방거래위원회(FTC, Federal Trade Commission)는 보안용 CCTV제품의 계정정보 노출에 대한 취약점을 이용하여 내부망으로 침투하였다. 추가적으로 CCTV 동영상 서버에 접속하여 동영상을 인터넷상에 무단으로 게시하는 APT 공격이 발생하였다[4].

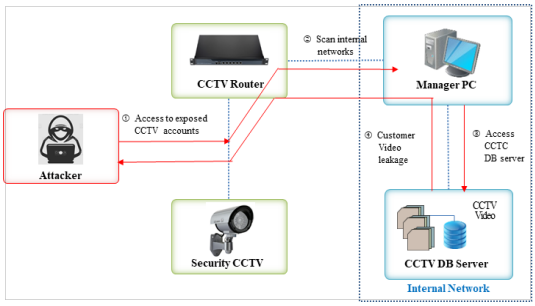

Fig. 2. APT attack procedure using IoT sensor wireless vulnerability

APT 공격 프로세스는 Fig. 2와 같다. ① 쇼단에서 검색을 통해 노출된 CCTV 계정 정보 확보 및 접속, ② CCTV 통신망을 통해 내부 네트워크를 스캔, ③ CCTV 관리자PC에 접속하여 CCTV DB서버에 접속, ④ CCTV DB서버에 있는 동영상을 인터넷에 노출하는 절차를 따른다.

2.3 공급망 네트워크 취약점을 통한 APT 공격

2019년에 발생한 스랭그리캣(Thrangrycat) 하드웨어 기반의 공급망 공격은 펌웨어 파일에 보안 기능을 담당하는 트러스트 앵커(Trust Anchor Module)의 논리적 결함을 이용해 권한 상승을 유발하여 원격 제어를 통해 해킹한 사례가 있다[5].

APT 공격 프로세스는 Fig. 3과 같다. ① 공급망 관리용 PC 취약점을 통한 계정획득, ② 공급망 관리용 PC를 통해 악성코드가 은닉된 SW를 공급망 서버에 업데이트, ③ 공급망 내부 사용자 PC 자동화된 업데이트로 악성코드 감염, ④ 사용자 PC에 기밀자료를 공격자에게 전송하는 공격 절차를 따른다.

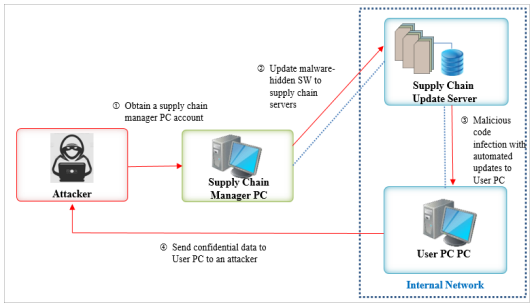

Fig. 3. APT attack procedure using IoT sensor wireless vulnerability

3. APT 공격 시나리오 설계

APT 공격에 대한 사례를 분석하여 IoT 센서 무선 취약점 APT 공격 시나리오, CCTV 계정 취약점 APT공격 시나리오, 공급망 네트워크 취약점 APT 공격 시나리오를 MITRE ATT&CK 프레임워크 절차에 따라서 설계하였다[6].

3.1 IoT센서 무선 취약점 APT 공격 시나리오 개발

IoT 센서 무선 취약점을 이용한 APT 공격 시나리오 개발을 MITRE ATT&CK 프레임워크에 절차에 기반하여 시나리오를 구성하였다[7]. Fig. 4에서 보듯이 MITRE ATT&CK에 따른 공격절차는 다음과 같다. ① 무선 Wi-Fi 취약점 스캔(T1590_Gather Victim Network Information), ② 내부 네트워크 스캔(T1040_Network Sniffing), ③ 공격결과 전송, ④ 계정공격(T1212_Exploitation for Credential Access), ⑤ 보안이 취약한 계정 공격(T1552_Unsecured Credentials), ⑥ 계정획득(T1078_Valid Accounts), ⑦ DB 정보유출 공격(T1570_Lateral Tool Transfer), ⑧ 정보유출 추가공격(T1041_Exfiltration Over C2 Channel), ⑨ 고객정보 획득(T1020_Automated Exfiltration)에 따른 시나리오를 개발하였다[8].

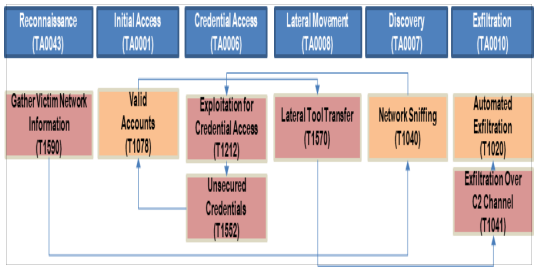

Fig. 4. IoT Sensor Wireless Vulnerability APT Attack Scenario

3.2 CCTV 계정 취약점 APT 공격 시나리오 개발

CCTV 계정 취약점을 이용한 APT 공격 시나리오 개발을 MITRE ATT&CK 프레임워크에 절차에 기반하여 시나리오를 구성하였다.

Fig. 5에서 보듯이 MITRE ATT&CK에 따른 공격절차는 다음과 같다. ① CCTV 계정 취득 공격(T1078_Valid Accounts / T1087_Account Discovery), ② 계정획득(T1078_Valid Accounts), ③ 펌웨어 업데이트

공격(T1053_Scheduled Task/Job) ④ 공격결과 전송, ⑤ 고객영상 유출 공격(T1213_Data from Information Repositories), ⑥ 영상유출 추가공격(T1005_Data from Local System), ⑦ 고객영상 획득(T1020Automated Exfiltration)에 따른 시나리오를 개발하였다[9].

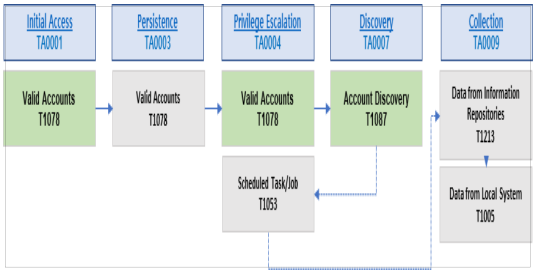

Fig. 5. CCTV Account Vulnerability APT Attack Scenario

3.3 공급망 네트워크 취약점 APT 공격 시나리오 개발

공급망 네트워크 취약점을 이용한 APT 공격 시나리오 개발을 MITRE ATT&CK 프레임워크에 절차에 기반하여 시나리오를 구성하였다. Fig. 6에서 보듯이 MITRE ATT&CK에 따른 공격절차는 다음과 같다. ① 공급망 업데이트를 통한 악성코드가 은닉된 SW 전송(T1195_Supply Chain Compromise) ② 공격결과 전송, ③ 악성코드가 은닉된 SW 저장, ④ 펌웨어 업데이트 공격(T1053_Acquire Infrastructure), ⑤ 악성코드가 은닉된 SW 저장(T1574_Hijack Execution Flow), ⑥ 공격결과 전송, ⑦ 관리자 권한상승 명령(T1068_Exploitation for Privilege Escalation / T1071_Application Layer Protocol), ⑧ 관리자 권한 상승(T1211_Exploitation for Defense Evasion), ⑨ 공격결과 전송에 따른 시나리오를 개발하였다[10].

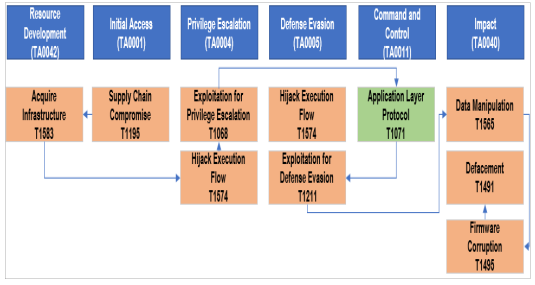

Fig. 6. Supply Chain Network Vulnerability APT Attack Scenario

4. APT 공격 시나리오 검증 시스템

제안하는 APT 공격 시나리오 검증 시스템은 사용자가 정의한 공격 시나리오를 MITRE ATT&CK 프레임워크에 절차에 따라서 점검대상 시스템에 공격을 실행하도록 구성하였다.

4.1 APT 공격 시나리오 검증 시스템 구성

Fig. 7과 같이 APT 공격 시나리오 검증 시스템은 외부에 공격자 에이전트와 공격도구가 구축되어 있다. 내부에는 피해 시스템을 구성되어 있으며 공격시나리오 절차를 통제하기 위한 정책 및 관리자 기능으로 구성하였다 APT 공격 시나리오 검증 시스템은 내부에 F/W, IDS, IPS 등의 기본적인 정보보안제품 기능이 동작하도록 설정되어 있다.

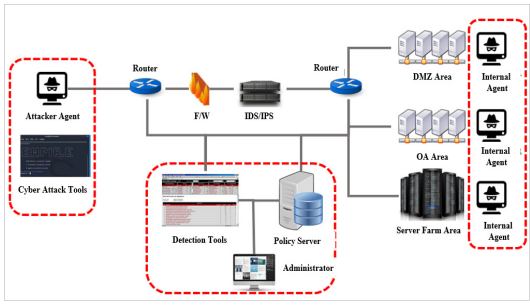

Fig. 7. APT Attack Scenario Verification System

4.2 APT 공격 시나리오 검증 시험

APT 공격 시나리오 검증 시스템은 3개 APT 시나리오를 대상으로 실험 환경에서 APT 공격이 탐지 가능한지 여부를 실험하였다.

Fig. 8. Process for APT Attack Scenario Verification Test

Fig. 8에서 보듯이, 3개 APT 시나리오를 수행하는 과정을 나타낸 것이다. APT 공격의 절차 수행 과정, APT 공격 성공여부, 수행시간, APT 공격이 실패한 경우 탐지한 내역이 표시하게 된다.

Fig. 9. APT Attack Scenario Verification Detailed Results

Fig. 9에서 보듯이 APT 공격 시나리오 검증 결과를 상세하게 조회하면 MITRE ATT&CK 프레임워크에 따른 TID 공격코드에 따른 절차와 공격 성공 여부를 확인할 수 있다. 공격에 사용된 방식과 공격에 대한 이력이 상세히 조회된다.

Table 1. Result of APT Attack Scenario Verification

	Attack Scenario	MITRE ATT&CK TID	Successful Attack	Detection	Attack Success Rate
1	IoT Sensor Wireless Vulnerability APT	T1590	Y		75%
		T1040	Y		
		T1212	Y		
		T1552	N	Crypt	
		T1078	Y		
		T1570	N	F/W	
		T1041	Y		
		T1020	Y		
2	CCTV Account Vulnerability APT	T1078	Y		85.7%
		T1087	Y		
		T1078	Y		
		T1053	Y		
		T1213	N	IDS	
		T1005	Y		
		T1020	Y		
3	Supply Chain Network Vulnerability APT	T1195	Y		100%
		T1053	Y		
		T1574	Y		
		T1068	Y		
		T1071	Y		
		T1211	Y		
Total results					86.9%

Table 1은 APT 공격 시나리오를 특정 시스템을 대상으로 검증 결과를 보여준다.

IoT센서 무선 취약점 APT 공격 시나리오는 8개 TID 공격을 수행하였으며 6개 공격이 성공하여 성공률은 75%를 보여 주었다. 성공 실패 2건은 보안이 취약한 계정 공격(T1552_Unsecured Credentials)은 계정정보가 암호화되어 있어 실패하였으며 DB 정보유출 공격(T1570_Lateral Tool Transfer)은 F/W에서 개인정보 패턴을 탐지하여 차단함으로서 실패하였다.

CCTV 계정 취약점 APT 공격 시나리오는 7개 TID를 공격하여 5개가 성공하여 71.4%를 보여주었다. 고객영상 유출 공격(T1213_Data from Information Repositories)은 IDS에서 영상정보에 비정상 접근에 대해 차단하여 실패하였다.

공급망 네트워크 취약점 APT 공격 시나리오는 6개 TID 공격이 모두 성공하여 100%를 보여주었다. APT 공격 시나리오 검증을 통해 공급망 네트워크 취약점 APT 공격이 가장 위험하다는 것을 실험에서 보여주었다.

본 실험에서 3개 APT 공격에 대해서는 해당 시스템에 전체 공격성공율은 86.9%로 취약한 것으로 분석되었다.

5. 결론

APT(Advanced Persistent Threat)는 대상시스템을 사전에 조사한 후에 악성코드에 감염시키다. 그리고 내부망으로 접속할 수 있는 백도어를 설치하여 내부망에 접속할 수 있도록 권한을 획득한다. 목표 설정 및 사전조사, 악성코드 감염 , 내부망 스캔 및 백도어 설치, 권한탈취, 내부망 장악, APT 보안사고 발생으로 이어진다. 이러한 APT공격 최근에 스마트빌딩, 스마트팩토리 등과 같은 디지털화된 공간과 결합이 되면서 점차 다양한 공격으로 변화하고 있다.

스마트빌딩, 스마트팩토리에서 APT 공격에 대한 접점으로서 IoT센서, 보안용 CCTV, 공급망을 대상으로 APT 공격이 증가하고 있다. 기존의 산업공간이 4차산업 기술과 융합이 되면서 통신연결, IoT센서를 통한 자동화된 정보기술이 발전하면서 APT 공격 대상도 확대되고 있다.

본 연구에서는 IoT센서 무선취약점 APT 공격 시나리오, CCTV 계정 취약점 APT 공격 시나리오, 공급망 네트워크 취약점 APT에 대해 MITRE ATT&CK 프레임워크 절차에 따라 개발하였다.

제안하는 APT 시나리오 검증 시스템을 통해서 3개 APT를 특정 시스템을 대상으로 실험을 수행하였으며 3개 APT 공격에 대해서는 실험을 통해 전체 공격성공율은 86.9%로 취약한 것으로 분석되었다. 본 연구를 통해서 다양한 APT 공격의 시나리오를 개발하고 검증하는데 활용할 수 있을 것으로 예상된다.

References

[1] Meicong Li et al., "The study of APT attack stage model," 2016 IEEE/ACIS 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.
DOI: https://doi.org/10.1109/iwcmc.2018.8450512

[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, 2019.
DOI: https://doi.org/10.1109/sp.2019.00026

[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.
DOI: https://doi.org/10.1109/rew53955.2021.00071

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

[8] M. J. Kim, S. H. Park and Se. W. 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] S. Y. Cho, Y. W. Park and K. S. 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] S. Y. Cho, Y. W. Park, K. H. 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