Analysis against Security Issues of Voice over 5G

Hyungjin CHO†, Member, Seongmin PARK†, Youngkwon PARK†, Bomin CHOI†, Dowon KIM†, and Kangbin YIM††, Nonmembers

SUMMARY In Feb 2021, As the competition for commercialization of 5G mobile communication has been increasing, 5G SA Network and Vo5G are expected to be commercialized soon. 5G mobile communication aims to provide 20 Gbps transmission speed which is 20 times faster than 4G mobile communication, connection of at least 1 million devices per 1 km², and 1 ms transmission delay which is 10 times shorter than 4G. To meet this, various technological developments were required, and various technologies such as Massive MIMO (Multiple-Input and Multiple-Output), mmWave, and small cell network were developed and applied in the area of 5G access network. However, in the core network area, the components constituting the LTE (Long Term Evolution) core network are utilized as they are in the NSA (Non-Standalone) architecture, and only the changes in the SA (Standalone) architecture have occurred. Also, in the network area for providing the voice service, the IMS (IP Multimedia Subsystem) infrastructure is still used in the SA architecture. Here, the issue is that while 5G mobile communication is evolving openly to provide various services, security elements are vulnerable to various cyber-attacks because they maintain the same form as before. Therefore, in this paper, we will look at what the network standard for 5G voice service provision consists of, and what are the vulnerable problems in terms of security. And we suggest possible attack scenario using security issue. We also want to consider whether these problems can actually occur and what is the countermeasure.

key words: 5G voice communication, voice over 5G, mobile network, IMS, SIP, 5G security

1. Introduction

In Feb 2021, As the competition for commercialization of 5G mobile communication has been increasing, 5G SA Network and Vo5G are expected to be commercialized soon. 5G mobile communication aims to provide 20 Gbps transmission speed which is 20 times faster than 4G mobile communication, connection of at least 1 million devices per 1 km², and 1 ms transmission delay which is 10 times shorter than 4G. To meet this, various technological developments were required, and various technologies such as Massive MIMO (Multiple-Input and Multiple-Output), mmWave, and small cell network were developed and applied in the area of 5G access network.

Meanwhile, the voice service of the conventional mobile communication network was provided using circuit switch-based network (2G and 3G), and the packet switch-based network at the time was used for data communication purposes and from the 4th generation mobile communication, it began to provide voice services with packet switch-based network by supporting the ALL-IP structure of the mobile communication network. The 4th generation mobile communication voice service based on VoIP (Voice over IP) is called VoLTE (Voice over LTE) and currently provides stable voice service in 4th generation mobile communication.

As the competition for commercialization of 5G mobile communication has been increasing, voice services in 5G mobile communication are expected to be commercialized soon. Voice service in 5th generation mobile communication is called Vo5G (Voice over 5G), and it uses VoIP related technologies such as VoLTE. VoIP is widely used through online voice chat, internet phone, and mobile communication voice services. Research on related vulnerabilities has been actively conducted since long time ago and security measures have been developed.

VoIP is also used in 5G mobile communication, and 3GPP (Third Generation Partnership Project) has defined security measures for mobile communication networks and voice services. However, despite the definition of security measures in the standard, there may be still vulnerabilities caused by implementation errors, and occurred by the non-forced security items in the standard and the resulting loose security level. In this paper, we examine the security vulnerability of SIP (Session Initiation Protocol)/RTP (Real-Time Transport Protocol) according to the application of mobile voice service in traditional VoIP and security vulnerability according to non-forced security items in the standard from three perspectives. First, SIP protocol, which is a representative session control protocol of VoIP, allows easy manipulation of headers based on text. Second, the traffic of the RTP protocol, which is a data transmission protocol of VoIP, is easy to be reproduced. Third, in the 3GPP standard, LTE or 5G voice communication is defined to be encrypted through IPSec (IP Security), but it is defined as a non-forced item and can be selectively operated as required by the manufacturer or carrier. Therefore, we want to check whether there are any vulnerabilities that can occur based on these weaknesses, and to find out the countermeasures [16].

In this regard, Chapter 2 in this paper examines the...
standards and status related to 5G mobile communication. Chapter 3 identifies problems related to 5G voice service and presents test methods. Chapter 4 tries to derive problems based on the test results. Chapter 5 proposes countermeasures to problems. The final Chapter 6 makes a conclusion.

2. Mobile Communication Network Standards and Status

2.1 5G Mobile Communication Network Status

5G mobile communication network is a next generation mobile communication technology led by 3GPP standardization group. Currently, technology competition for 5G commercialization is actively taking place worldwide, and 5G mobile communication service to public is in progress, starting with commercialization services in China, Korea, the United States, and Japan in 2019 [1]. Starting from the NSA structure, the 5G mobile communication network is currently commercializing the SA structure (see Fig. 1). When it is commercialized, the 5G voice communication might be serviced by 5GC (5G Core) which is the SA core network and is called Vo5G [5] (see Fig. 2).

2.2 3GPP IMS Security Standard

In 3GPP, IMS security standards specify security-related matters in TS 33.210, TS 33.328, and TS 33.203 standard documents. In 3GPP, the IPSec-based security mechanism is applied all control plane IP communication to the external network through the Security Gateway (SEG). IPSec has so many options, therefore it is difficult to provide full interoperability, and the options of IPSec has reduced in 3GPP. Communication with the different network domain is performed through SEG, and the Za interface, which is an external network connection section, must be implemented with IPSec, and is optional in the Zb interface which is an internal network connection section. In the Zb interface, authentication must always be provided, but encryption is optional (see Fig. 3). In addition to Z-interface, the Gm interface is defined as interface of UE and P-CSCF of IMS. In case of the Gm interface, use of IPSec is not depends on network domain but local policy of the P-CSCF.

The 3GPP IMS security architecture is specified in TS 33.203. In the IMS security architecture, four entities (UE, P-CSCF, I-CSCF, and S-CSCF) interact and aim for subscriber authentication and integrity protection. Confidentiality protection does not apply to IMS [2], [3].

2.3 SIP/RTP Protocol

The SIP protocol is defined in IETF (Internet Engineering Task Force) RFC (Request for Comments) 3261 [6] and is an application layer signaling protocol. The 3GPP standard has been adopted in the IMS (IP Multimedia Subsystem) architecture since November 2000 and is still in use. The RTP protocol is a protocol for end-to-end, real-time transmission of streaming media and is defined in IETF RFC 3550 [7], and is used for the purpose of voice data transmission with SIP protocol in mobile communication networks.

The SIP protocol is a text-based message, and the SIP message format consists of Starting Line, Header Field, Separator, and Message Body. For basic SIP session connection, when the caller sends an Invitation message, the Callee responds with 100 Trying, 180 Ringing, and 200 OK messages. When the caller sends an ACK message, a session is established and voice data is exchanged. When the call ends, the callee sends a BYE message, and the caller responds with a 200 OK message [6] (see Fig. 4). Voice data is transmitted through RTP which is for real-time delivery and multitasking [7].
3. Problems and Test Methods

3.1 Related Work

Several related studies have been conducted about VoIP and SIP attacks and countermeasures[11], [12]. For example, there are billing bypass [8], man-in-the-middle attack [9], and authentication neutralization [10]. If 5G mobile communication using SIP/RTP protocol was not considered, these attacks could also be a potential threat to Vo5G.

According to the VoLTE attack paper published in CCS’15 ACM, attacks such as DoS (Denial of Service), overcharge, free video calls, and sender forgery are possible through the VoLTE hidden channel [13].

Recently, a study on the secret key generation method to protect the 5G wireless network section from man-in-the-middle attacks was conducted [15].

In other related studies, we analyzed the NAS protocol related to Voice over 5G eavesdropping attack in IoT environment and proposed a dedicated IDS to respond to eavesdropping attack [18].

In 5G mobile communication, voice calls are supported in the form of Vo5G. If Vo5G is implemented without complementing VoLTE-related attacks, these attacks can be a potential threat in Vo5G.

3.2 Problems of 5G Voice Communication (The Proposed Approach)

This section shows the problem of IMS, a network that provides 5G voice communication. The problems of the IMS standard can be divided into three categories.

3.2.1 Easy Manipulation of Text-Based SIP Protocol Headers

The SIP packet has a header name and a header value in text format, so a malicious attacker can easily change the text if desired. In particular, the Initial Register message for registering a user device on the IMS server is delivered before the encryption setting even if it uses IPSec encryption, so it can be easily obtained through a packet dump on the device. Among them, an attacker can manipulate several header values to change the information of the user who delivers the message. The headers of Contact, To, From, and Authorization can be changed to the subject’s IMSI or URI, and the

| Table 1 | Headers that require manipulation for malicious use of the register message. |
|---------|----------------------------------------------------------------------------|
| Header Requiring Change | Register User Information Changes |
| Via | Change IP address |
| Contact | Change UE URI |
| To | Change UE URI |
| From | Change UE URI |
| Cseq | Change to higher value |
| Expires | Change to 3600 or 0 |
| Authorization | IMSI or UE Calling Number |

Expire value can be changed to set up or cancel the registration (see Table 1).

Subscribe messages used to provide real-time PTT (Push to Talk) services, such as RCS (Rich Communication Services) services, can also be used maliciously. Like the Register, the Subscribe message requires the manipulation of several header values to change user information (see Table 2).

3.2.2 Easy Reproduction of RTP Traffic

RTP traffic is exposed through sniffing when SRTP (Secure Real-time Transport Protocol) is not used. The exposed RTP traffic can be reproduced through Wireshark. When going to the RTP, RTP Streams menu on the Telephony tab, information about RTP packets is summarized and displayed. If you request Analyze by selecting the desired source and destination, you can show the Stream Analysis result between specific peers and request Play Streams. Wireshark can output audio for PCMU (Pulse Code Modulation Mu-Law)/PCMA (Pulse Code Modulation A-Law) codec and for AMR (Adaptive Multi-Rate) or AMR-WB (Adaptive Multi-Rate Wideband) codec, a separate program is required together with file dump. File dumps can be created using tshark -nr rtp.pcap -R rtp -T fields -e rtp.payload, and audio playback can be played through AMRPlayer [14].

| Table 2 | Headers needed to change user information in subscribe message. |
|---------|----------------------------------------------------------------|
| Header Requiring Change | Subscribe User Information Changes |
| Request URI | Change IP address |
| Via | Change IP address |
| Contact | Change UE URI |
| To | Change UE URI |
| From | Change UE URI |
| Cseq | Change to higher value |
| P-Preferred-Identity | IMSI or UE Calling Number |

3.2.3 Non-Mandatory for IPSec Encryption

As described above, the interface for using IPSec SAs (Security Associations) is divided into Gm interface and Z-interface. The Za interface is used for different network domain entities, therefore the use of IPSec is mandatory in the Za interface. The Zb interface is used for same network domain entities, therefore the use of IPSec is optional in the Zb interface. In 3GPP, the use of IPSec on Za is defined as mandatory, while reducing the range of options related to
IPSec configuration to ensure compatibility. In this case, the operation mode is divided into transport and tunnel mode. In the case of using the tunneling mode, the entire original IP packet can be encrypted to maintain the confidentiality of the origin and destination. However, IPs of two IPSec VPN (Virtual Private Network) Nodes are exposed through the new IP header. In the transmission mode, only data is encrypted, and confidentiality of the traffic flow is not provided (see Table 3).

In the Zb interface, the process for using IPSec in a 5G voice service terminal is as follows. First, in order to use IPSec, the device inserts the Security-Client header with the Require header and sends it to the first Register message. The Require header is a request for the use of IPSec encryption, and the Security-Client header contains configuration requests for setting various IPSec encryption (see Table 4).

However, in the Gm interface, whether UE and P-CSCF is in the same network domain or not, the use of IPSec is depends on local policy of the P-CSCF. Therefore, if the IMS uses IPSec on Gm interface as optional, even if an UE located in different network domain is registered to IMS without using IPSec at the device, communication is performed in decrypted text if authentication is made [4].

3.3 Test Method (Implementation)

The IMS network that provides 5G voice communication supports IPSec and uses the IPSec mechanism for user registration of the device. If IPSec is not used, it can be very vulnerable to threats such as Rogue base stations, and it is possible to manipulate the outgoing number by capturing SIP messages that communicate in plain text. 5G Android devices released so far have been developed to use IPSec, and if you dump the packet of the device, you can see that in addition to the first Register message and 401 Unauthorized message. And next messages are encrypted using IPSec ESP (Encapsulating Security Payload). However, there is a hidden menu for developers on the device to disable IPSec SAs and communicate without that. We tested using the representative 5G device, Galaxy S10, and the test devices used are as follows (see Table 5).

3.3.1 IPSec Disable

When accessing the hidden menu of the test device, there is a ‘VoLTE Settings’ menu, and there are context menus that can change the IMS service settings of the device. Among them, if you access the ‘VoLTE Profile’ by entering the ‘IMS Profile’ setting, there is SIP menu with CSCF (Call Session Control Function) settings. In the SIP menu, there are submenus for setting the SIP port, IP version, etc. Among them, you can see that the option, Enable IPSec is checked. If you disable this option and reboot the device, the setting is completed.

3.3.2 Packet Sniffing

When the IPSec disabling process of the device is finished, procedure for sniffing the terminal packet should be performed. Packets can be sniffed with tcpdump from the device and must be rooted in advance. The rooting process using Odin is divided into 4 steps. The first step is to prepare for rooting. Download and install and run the Magisk Manager app on the device. The second is the Un-LOCK stage for rooting. Download and install and run the Magisk Manager app on the device. The second is the Un-LOCK stage of the bootloader, which unlocks OEM (Original Equipment Manufacturing) lock in the developer options of the device. The third step is to install custom recovery. Flashing the device through Odin program and installing custom recovery. Last step is acquiring root authority. After factory reset in recovery mode, the root authority is acquired using the Magisk patch created using the Magisk Manager app. Linux OS and open sources such as tcpdump were installed on the rooted device as follows (see Table 6).

3.3.3 Packet Analysis

Dumped packets from the device can be analyzed by moving to PC. Wireshark is used, and the header value inside the SIP packet can be checked through SIP filtering. We conducted this process using two Operators’ USIM (Universal

### Table 3

| Requirements                  | Setting value  |
|-------------------------------|----------------|
| Protocol (prot)               | Use EPS only   |
| Operation mode (mod)          | Always use Tunnel Mode |
| Integrity Algorithm           | HMAC-SHA-1     |
| Encryption Algorithm          | 3DES           |

### Table 4

| Requirements                  | Setting value                                           |
|-------------------------------|---------------------------------------------------------|
| Protocol (prot)               | EPS                                                      |
| Operation mode (mod)          | Transport                                                |
| spi-c, port-c                 | Client Index & Port Number                               |
| spi-s, port-s                 | Server Index & Port Number                               |
| Integrity Algorithm           | HMAC-MD5-96 or HMAC-SHA-1-96                             |
| Encryption Algorithm          | AES-CBC or AES-GCM                                       |

### Table 5

| Test device          | Galaxy S10 (SM-G977N) |
|----------------------|------------------------|
| Android OS version   | 9 (Pie)                |
| Kernel version       | 4.14.85                |

### Table 6

| Installed Components | Components Details |
|----------------------|--------------------|
| Linux OS             | Distributor ID: Ubuntu |
|                      | Description: Ubuntu 16.04 LTS |
|                      | Release: 16.04 |
|                      | Codename: xenial |
| tcpdump              | 4.7.4               |
| libpcap              | 1.7.4               |
| OpenSSL              | 1.0.2g              |
Subscriber Identify Module(s) and compared the differences.

4. Test Results and Problem Identification

4.1 Test Result

Packets can be captured by using tcpdump in the environment where the device is rooted. When the captured packets are checked with Wireshark, SIP messages and RTP traffic in plain text can be viewed.

As a result of testing the USIMs of the two operators, IPSec is disabled when using the first Operator(A)'s USIM, and it is decrypted. However, when using the USIM of the other Operator(B), IPSec is not disabled, and voice communication is performed with encryption even though we set off for the IPSec configuration on the testing devices. It is estimated that the registered user from Operator receive that Configuration Values for Registration before SIP Registration. And then, it is estimated to ignore values set on the device and force IPSec Enabling based on Provisioning values.

Comparing the packets for the two Operators’ USIMs, you can see that the Initial Register message is different. In the case of Operator A (see Fig. 5), there is no Require, Supported and Security-Client header in the Initial Register message, and if you send a SIP message, you can see that it is sent in plain text. However, in the case of Operator B (see Fig. 6), you can clearly see that Require, Supported and Security-Client headers were added to the Initial Register message and transmitted. Which means, when using B Operator’s USIM, it can be assumed that security settings for use in 5G voice communication are obtained from the network, not from the device. A packet captured in the test using Operator A’s USIM can be altered using open source such as HxD. In addition, by using an open source such as sendip, it is possible to generate a threat such as forgery of the originating number by sending an altered packet (see Table 7).

4.2 Attack Scenario

In the attack scenario using IPSec disabling, a SIP message manipulation attack based on Man in the Middle is possible. Typical attacks include Denial of Service, Message Manipulation [17], and Charging Avoidance [18]. If IPSec is disabled, it can be exposed to man-in-the-middle attacks. For Example, the phone call charge avoidance scenario will be described by manipulating the eavesdropping and SIP message. the sequence diagram of the phone call charge avoidance scenario using IPsec off vulnerabilities (see Fig. 7). The precondition of the attacker(C) is the configuration of the vulnerable UE environment with the IPsec option off and the UE network traffic snipping environment. If snipping is done in the RAN section, plaintext must be acquired through tcpdump from the UE or AS security neutralization must be performed using NAS null-ciphering vulnerabilities [18]. If the victim UE(A) with the IPsec option off sends the SIP register message to IMS, the attacker(C) will snip this message and saves various information on the victim UE(A). If the victim UE(A) finishes registration, it will not use IPsec, and if the attacker(C) can neutralize AS security, the attacker(C) can disguise as the victim UE(A) and send

| Table 7 | Characteristics of 5G voice communication on tested operators. |
|---------|---------------------------------------------------------------|
| Type    | Operator A | Operator B |
| Network Protocol | IPv6 | IPv6 |
| Transport protocol | UDP | UDP |
| Use of IPSec | V | V |
| Integrity Algorithm | AES-CBC | AES-CBC |
| Encryption Algorithm | HMAC-SHA-1-96 | HMAC-SHA-1-96 |
| IPSec disable by UE | V | X |
| 5G Service Type | NSA | NSA |

Fig. 5 SIP decryption testing on IPSec disabled device with operator A’s USIM.

Fig. 6 SIP decryption testing on IPSec disabled device with operator B’s USIM.

Fig. 7 Charging avoidance attack scenario using IPSec disabling.
a message to IMS. Accordingly, if the attacker(C) changes the originating number of his/her SIP invite message into the number of the victim UE(A) and transmits it as illustrated in Fig. 7, a phone call will be established with the information of the victim UE(A), but the attacker(C) will make the phone call. As a result, the victim UE(A) cannot make a phone call while the attacker(C) is talking on the phone, and the charge for the attacker(C)’s phone call will be charged to the victim UE(A).

5. Countermeasures

5.1 Countermeasures at Security Appliance Level

You can think of introducing physical system such as IPS (Intrusion Prevention System) at the security device level. Packets flowing into the core network are monitored using a dedicated IPS capable to detect voice communication protocol such as SIP or RTP, and then detected and blocked in the case of an attacking or manipulated packet. Depending on the policy, it may be possible to alert the operator after detection without blocking it immediately to secure the availability of the voice service. However, in this case, the cost of investing in security equipment will be considerable and the efficiency of the investment must be considered.

5.2 Countermeasures at IMS Server Level

Among the IMS servers, CSCF or SBC (Session Border Controller) might be able to play a role of SEG. When manipulating SIP packets by disabling IPSec, CSCF or SBC can be supplemented to go through the verification procedure on the mismatch between the IP of the terminal and the manipulated field value, and the manipulated packet would be able to be blocked. In this case, there is no need to invest in additional security equipment, but performance degradation in CSCF or SBC can be expected.

5.3 Countermeasures at IPSec Configuration Level

There may be a way to prevent 5G users from essentially disabling IPSec. That is, when a terminal accesses a 5G network, it receives information such as IPSec settings from a separate server and communicates without depending on the IPSec setting values set in the terminal. This method must satisfy two conditions; Development of server to send IPSec configuration information and IPSec configuration control through USIM. If the operator is equipped with DM (Device Management) system, it will be very effective method against the investment to block IPSec disabling in advance. However, if you need to build new server, you will need to consider the operator’s point of view.

5.4 Countermeasures at 3GPP Standard Level

In 3GPP, the application of IPSec on Gm interface depends on local policy of the P-CSCF. However, it is necessary to review at the 3GPP standard level for the change to compulsory by making the IPSec on Gm interface mandatory. However, it is considered that the 3GPP standard revision is very time consuming and requires lots of efforts and there must be a reason to define the IPSec on Gm interface as optional. Therefore, it can be expected that it will be difficult to respond at the 3GPP standard level.

6. Concluding Remarks and Future Work

Through this study, we can see that there is security problems with voice communication in 5G networks, and it is very easy to access the problem with a device. First, security problems for 5G voice communication can be divided into three categories, easy operation, easy RTP traffic reproduction, and non-force of IPSec encryption due to text-type SIP protocol header. This paper focused on two problems, and further research seems to be needed for the other. Besides, the procedure for 5G voice communication security test can be divided into three steps. The first is the process of disabling the IPSec of the device, and it was easy to enter through the hidden menu. The second is to make it sniffable by rooting the device. The third step is to analyze the actual 5G voice packet by sniffing it. Here, it is necessary to take further action to analyze the third voice packet analysis process by dividing it into SIP, RTP protocols and reproducing threats such as bugging or tampering. However, since 5G mobile communication network is a private communication network, it is obviously illegal to threaten or bug on the network. Therefore, it is desirable to proceed it by using test network. In the future, operators will build 5G SA environment that has never existed before, and provide customers with new and convenient services that utilize its advantages. However, before launching a service, it is also necessary to think about what security threats exist in new services and countermeasures. So we trying to installation 5G stand-alone testbed for security analysis. And We Will be Coworking MNO Company for their 5G infrastructure security assessment.

Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2019-0-00793, Intelligent 5G Core Network Abnormal Attack Detection & Countermeasure Technology Development).

References

[1] CTIA, https://www.citia.org/national-spectrum-strategy, accessed Feb. 10 2021.
[2] 3GPP TS 23.228, IP Multimedia Subsystem (IMS) stage 2, 2011.
[3] 3GPP TS 33.203, Access security for IP-based services, 2011.
[4] 3GPP TS 33.210, Network Domain Security (NDS); IP network layer security, 2011.
[5] Huawei, Vo5G Technical White Paper, 2018.
[6] IETF, RFC 3261, SIP: Session Initiation Protocol.
[7] IETF, RFC 3550, RTP: A transport protocol for real-time applications.
[8] R. Zhang, X. Wang, X. Yang, and X. Jiang, “Billing attacks on SIP-based VoIP systems,” WOOT, vol.7, pp.1–8, 2007.
[9] R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang, “On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers,” Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, pp.61–69, ACM, 2009.
[10] J. Beekman and C. Thompson, Breaking Cell Phone Authentication: Vulnerabilities in AKA, IMS, and Android, WOOT, 2013.
[11] R. Ferdous, SIP Malformed Message detection, SIP LEX, University of Trento, Italy, Jan. 2012.
[12] D. Seo, H. Lee, and E. Nuwere, “SIPAD: SIP/VoIP Anomaly Detection using a Stateful Rule Tree,” Computer Communications, vol.36, no.5, pp.562–574, 2013.
[13] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, “Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations,” CCS’15 ACM, Denver, pp.328–339, 2015.
[14] CloudShark, https://www.cloudshark.org/captures/71c1b394bbbf, accessed 12 June 2020.
[15] Q. Wang, M. Kang, G. Wu, Y. Ren, and C. Su, “A Practical Secret Key Generation Scheme Based on Wireless Channel Characteristics for 5G Networks,” IEICE Trans. Inf. & Syst., vol.E103-D, no.2, pp.230–238, Feb. 2020.
[16] S. Park, H. Cho, Y. Park, B. Choi, D. Kim, and K. Yim, “Security problems of 5G voice communication,” WISA 2020 (Jeju), pp.317–329, 2020.
[17] M.M. Naem, I. Hassain, and M.M.S. Missen, “A survey on registration hijacking attack consequences and protection for session initiation protocol (SIP),” Computer Networks, vol.175, April 2020.
[18] S. Kwon, S. Park, H. Cho, Y. Park, D. Kim, and K. Yim, “Towards 5G-based IoT security analysis against Vo5G eavesdropping,” Computing, vol.103, no.3, pp.425–447, Jan. 2021.

Hyungjin Cho received the B.S. and M.S. degrees in Computer Communications and Security from Chungnam National University in 2011 and 2013, respectively. During 2012–2019, he stayed in KISC (KRCERT/CC). He is now with AI Security Technology Division, Korea Internet & Security Agency. His current research interests include 5G network security, Malware Analysis, Cyber Threat Intelligence, Cyber Security, Artificial Intelligence, Software Vulnerability, Forensics, etc.

Seongmin Park received the B.S. and M.S. degrees from Sogang University in 2009 and 2015, respectively. During 2009–2013, he stayed in LGUplus Co. He is now with AI Security Technology Division, Korea Internet & Security Agency. His current research interests include 5G network security, 5G Standards Analysis, Cyber Threat Intelligence, Cyber Security, etc.

Youngkwon Park received B.S. degrees in information Security from hoso University, received M.S. degrees in information Security from Graduate school of International Affairs & Information Security of Dongguk University in 2013 and 2017, respectively. During 2013–2018, he stayed in Personal Data Protection Center. He is now with the Korea Internet Security Center, Korea Internet & Security Agency. His current research interests include 5G network security, Spam, Cyber Security, etc.

Bomin Choi received the B.S. and M.S. degrees in Computer Engineering from Gachon University in 2012 and 2014, respectively. During 2014–2019, She stayed in Information Security R&D Technology Sharing Center. She is now with the KISC (KRCERT/CC), Korea Internet & Security Agency. Her current research interests include 5G network security, Cyber Threat Intelligence, Artificial Intelligence and etc.

Dowon Kim received B.S. degree in Computer Science from Gyeongsang National University in 2005 and M.S. degree in Computer & Information Communication from Korea University in 2010. he worked at KRNIC during 2005–2014 and KISC (KRCERT/CC) during 2014–2019, Korea Internet & Security Agency. He is now in AI Security Technology Division, Korea Internet & Security Agency. He currently oversees research and development of 5G security technology, vulnerability analysis, and AI based security control technology as head of the infrastructure security technology team.

Kangbin Yim received the B.S., M.S., and Ph.D. degrees from the Department of Electronics Engineering, Ajou University, South Korea, in 1992, 1994, and 2001, respectively. He is currently a Full Professor with the Department of Information Security Engineering, Soonchunhyang University. His research interests include vulnerability assessment, malware analysis, leakage prevention, secure architecture, especially on mobile network, industrial control systems, and vehicular platforms.