이동통신망의 보안 및 취약점에 대한 기술동향

Edward Kwao, 김태훈*•, 방인규•
한밭대학교 지능미디어공학과, *한밭대학교 컴퓨터공학과
30215294@edu.hanbat.ac.kr, thkim@hanbat.ac.kr, ikbang@hanbat.ac.kr

Technical Trend of Security and Vulnerability Issues in Cellular Networks

Edward Kwao, Taehoon Kim*•, Inkyu Bang•
Department of Intelligence Media Engineering, Hanbat National University
*Department of Computer Engineering, Hanbat National University

Abstract

In this paper, we summarize the recent vulnerabilities discovered in the Third Generation Partnership Project (3GPP) security protocol specifications and network providers' implementation flaws that significantly undermine the security and privacy of the ever-increasing number of mobile subscribers. We further provide noteworthy insights into security concerns for the next-generation mobile networks.

Ⅰ. Introduction

The mobile communication standards have gone through magnificent security evolution since the inception of the first analog technology, 1G that was popularly known to be vulnerable to cloning attacks. Despite the security facelift through 2G, 3G, and 4G, cellular networks are still susceptible to several classes of different attacks. Even the latest and supposedly secure and refined mobile standard, 5G is no exception to these security and privacy threats [1-5]. In this paper, we provide an insightful summary of the recent security and privacy issues in mobile networks and shed light on inheritable issues by the next-generation mobile networks.

Ⅱ. Recent Security and Vulnerability Issues in Cellular Networks

By exploiting missing integrity protection of LTE user data and the ability to acquire plaintext information up to the packet-data convergence protocol (PDCP), the authors in [1] presented an attack where a passive sniffer decodes downlink control information (DCI) that provides unencrypted information up to the PDCP layer. From this, the attacker learns and distinguishes requests made to different websites. They finally introduced an LTE user data manipulation attack concept where a malicious relay is deployed between a victim's UE and a commercial network to manipulate the encrypted payload of victim's data and redirects the victim's DNS requests to a malicious website by modifying the destination IP address.

Based on core network capabilities (e.g., attach requests) and radio access capabilities (e.g., UE capabilities information) obtained from UEs by mobile operators prior to radio resource control (RRC) security setup, the authors in [2] introduced a mobile mapping attack where devices are identified in a network based on baseband vendor, model, cellular or cellular IoT and manufacturer. They also set up a malicious relay that can modify, deactivate, or downgrade some UE capabilities such as data rate and battery life span through a bidding down attack and battery draining attack.

Eavesdropping of encrypted LTE calls was studied in [3]. The authors discovered that the same data radio bearer (DRB) ID is reused and thus it results in the same encryption keystream during two successive calls in the same radio connection. They implemented an attack where a target call was made to the victim's UE and recorded using signaling collection and analysis tool (SCAT). A downlink sniffer was configured to note the end of the target call and before the 10 seconds RRC inactivity time set by providers was due, a subsequent keystream learning call was made to the same victim to amass all information crucial to decrypting the target call.

Although 5G conceals the subscriber permanent identifier (SUPI) by encrypting it with the operator's public key, the authors in [4] found a vulnerability in the authentication and key agreement (AKA) procedure that makes it possible to capture encrypted subscription concealed identifiers (SUCIs) and link user identities between sessions.

• Corresponding Authors: Taehoon Kim (thkim@hanbat.ac.kr), Inkyu Bang (ikbang@hanbat.ac.kr)

The authors in [5] implemented passive sniffers that exploit the time of arrival of uplink and downlink messages and timing advance command information to facilitate a surreptitiously precise tracking of mobile users' location. Although they also involved active attacks, they achieved the surreptitious nature of their attack by employing an adaptive overshadowing technique that modified some exchanges in the RRC connection procedure without using increased signal strength.

In summary, Figure 1 shows vulnerable aspects of the protocol stacks against these recent attacks in mobile networks where the attacker exploits software-defined radios (SDR) to operate malicious UE and or malicious networks for the purpose of launching the attacks. Note that the implementations of discussed attacks require a different set of skills and knowledge of cellular networks including specifications.

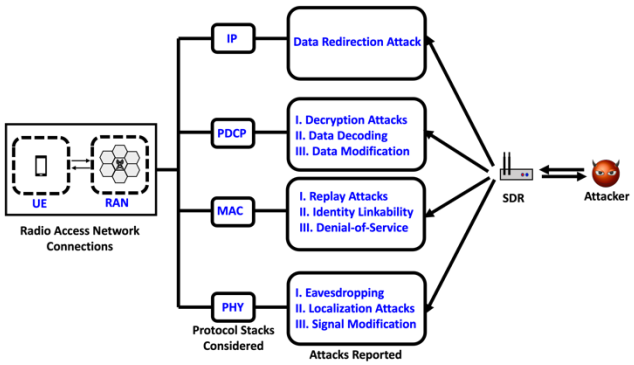

Figure 1. Summary of attacks against radio access network connections based on protocol stacks exploited

Ⅲ. Future Attacks in 5G and Beyond Networks

In this section, we briefly discuss possible threats in 5G and next-generation cellular networks. In the future, a malicious user can alter radio resources assignment information sent to legitimate users by employing the stealth adaptive overshadowing technique [5]. This is possible since random access response (RAR) contains UE temporary identifiers and uplink grant, sent unencrypted over air. Timing advance information can also be acquired by malicious users to cause synchronization failure problems. In addition, a user in a mobile network can be exposed to serious threats in the event where its RRC security context is removed or circumvented by an attacker posing as a legitimate eNodeB.

IV. Conclusion

We have reported the recent security issues in cellular networks focusing on specification and implementation flaws. In addition, we have provided the possibility of new threats in 5G and beyond mobile networks. In the future, we will investigate the possibility of timing advance information and RRC security circumvention to be exploited to implement synchronization failure and denial of service threats.

References

[1] D. Rupprecht, et al. "Breaking LTE on layer two," in the Proceedings of 2019 IEEE Symposium on Security and Privacy, 2019.

[2] A. Shaik, et al. "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in the Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2019.

[3] Rupprecht, David, et al. "Call me maybe: Eavesdropping encrypted LTE calls With ReVoLTE," in the Proceedings of 29th USENIX Security Symposium, 2020.

[4] Chlosta, Merlin, et al. "5G SUCI-catchers: Still catching them all?," In the Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2021.

[5] Kotuliak, Martin, et al. "LTRACK: Stealthy tracking of mobile phones in LTE," in the Proceedings of 31st USENIX Security Symposium, 2022.