A Look-ahead Towards 6G Security (Abstract)

Mohammed Ramadan and Shahid Raza

Cyber Security Unit, SICS, RISE - Research Institutes of Sweden, Stockholm, Sweden
mohammed ramadan@ri.se, shahid raza@ri.se

***Abstract*—6G system is in an active race to be fully deployed by 2030. 6G system is expected to provide ultra-low latency, low power consumption, ultra-high capacity, seamless coverage, high localization precision, massive MIMO (small cell and cell-free) techniques, millimeter-wave (mmWave), and terahertz (THz) bands. The high-performance specifications will enable new technologies within 6G systems. Consequently, these new technologies will significantly impact the security and privacy of the upcoming 6G system. Therefore, novel security techniques (encryption, authentication, privacy-preserving, key agreement, access control, or some fundamental changes must be considered; for instance, distributed mutual authentication protocols are highly needed for some new 6G-based technologies (e.g., HWN), whereas end-to-end security and encryption protocols are essential for some others. Thus, extensive research must be carried out to meet all system/security requirements and ensure the reliability and functionality of the upcoming 6G system.**

Keywords*—*6G Security, Privacy-preserving, Cryptography, End-to-end Security

I. Introduction

6G will provide high connectivity between people and everything. Several technologies and applications will be associated or linked to the upcoming 6G systems, such as the internet of everything (IoE), heterogeneous wireless networks (HWN), extended reality (XR), distributed ledger and blockchain (DL), brain-computer interactions (BCI), visible light communication (VLC), artificial intelligence (AI), machine learning (ML), autonomous systems, etc. These technologies will significantly impact the security and privacy of the 6G system. Therefore, providing novel, solid, secure solutions or applying fundamental changes to the existing security techniques is essential. For the current mobile security status, 4G and 5G protocols provide mutual entity authentication schemes with ley confirmation; and reduce the authentication handshaking process by using an authentication vector in the EPS-AKA protocol.

These improvements close the door to several kinds of attacks. Also, the 5G-AKA protocol supports distributed authentication mechanism (DAM) and improves the security and the functionality of the 5G system. However, some vulnerabilities still exist in 4G 5G systems or their related applications (e.g., security for IoT applications).

II. Potential 6G Security Issues

The potential security issues for 6G systems include privacy-preserving, location-based privacy, eavesdropping, traceability, extraction, replay, and DoS attacks. Also, possible security issues could be the inherited 5G security issues, as well as the incompatibility and handover process among heterogeneous nodes in the 6G system is challenging. To ensure a dynamic infrastructure using network slicing, Softwarization (SDN), and Cloudization Virtualization-NFV. This could add another level of security requirements and require more effective security solutions. Table 1 summarizes these security issues, requirements, and potential security solutions associated with 6G-based technologies.

Network slicing provides different services through different slices simultaneously. This will lead to some security risks; any security threat in the service slice will affect the security of the upper and lower slices accordingly. Consequently, we need some isolation using new distributed mutual authentication techniques. If one slice is compromised, this should not affect any other slices.

III. Potential 6G security solutions

Implementing a security model that covers all the security requirements is challenging. We can summarize some potential security solutions as follows.

- Secure algorithms against potential attacks such as replay, IMSI catcher, false base station, MITM, known key, DoS, and forward/backward secrecy.
- Providing lightweight cryptosystems for confidentiality and authentication.
- Using PKC-based techniques for more flexibility.
- Distributed security model with integrated security requirements (network slices isolation).
- End-to-end encryption.
- Authenticated encryption, Signcryption, and aggregation protocols.
- Mutual handover authentication cell structure.
- Broadcast authentication for Cell-free 6G structure.
- Key management.
- Post-quantum cryptosystems.

TABLE 1. 6G SECURITY NOTIONS

6G Technologies	Security Requirements	Security Issues	Security Solutions
Heterogeneous Wireless Networks (HWN)	• Authentication • Authorization	• Eavesdropping • Privacy-preserving	• E2E mutual authentication • Differential privacy
Distributed Intelligent Environments	• Confidentiality • Authentication	• Traceability attack • Replay attack	• Distributed authentication • Access control
Internet of Everything (IoE)	• Authentication • Authorization	• MITM attack • Privacy-preserving	• E2E encryption • Aggregate authentication
Holographic Communications Extended Reality XR, VR, AR, MR	• Confidentiality • Authentication	• Injection attack • Privacy-preserving	• E2E encryption • AKA
Brain-Computer Interactions (BCI)	• Authorization • Integrity	• Malicious attack • Poison channel attack	• Mutual Authentication • Access control
Autonomous Systems, AI, MI	• Confidentiality • Authentication	• Extraction attack • Evasion attack	• Homomorphic encryption • Access control
Visible Light Communication (VLC)	• Authentication • Integrity	• Key-leakage attack • Jamming attack	• Steganographic algorithms • AKA

IV. POTENTIAL 6G SECURITY CHALLENGES

There are still some other challenges and open issues regarding the 6G system, such as:

- Using public-key cryptosystems to encrypt the users' identifiers (IMSI, TMIS, SUPI, etc.) to resolve the issue of catching and cracking attacks.
- The ultra-low latency versus the implementation complexity of new cryptosystems.
- Location-based privacy is still an open issue, especially for the high accuracy localization of 6G systems.
- Post-quantum and multi-party communication protocols still require a lot of effort to be adopted by the 6G system.
- The evaluation of security versus performance. Then functionality versus reliability and accuracy.
- The deployment of the 6G service globally with reliable security and privacy.
- To provide a sustainable and lightweight cryptosystem system for fewer resources by significantly reducing the computational cost, communication overhead, and energy consumption. This will positively affect the sustainability pillars (environment, society, economy).
- Security against some common attacks on mobile systems is still a challenge. According to 3GPP, these attacks can be summarized as follows:
  - Replay attack during the handover process.
  - False base-station attack.
  - IMSI-cracking attack.
  - Traceability attack.
  - Linkability attack.
  - DoS attack.
  - Identifiers disclosure attack.
  - Key confirmation attack.

V. SUMMARY

6G security will be an open framework for the coming years. Several standardization organizations such as 3GPP, 5G PPP, NIST, ETSI, ITU, and IETF are responsible for finalizing and standardizing the 6G systems. 3GPP release 16 identifies some difficulties regarding implementing security techniques, which will increase the communication overhead and the processing in the user entity and the gNodeB. Security and privacy require lots of research. Some ongoing projects regarding 6G standardization, architecture, security, and privacy include HEXA-X, RISE 6G, 5GZORRO, 6G FLAGSHIP, MSIT 6G, and NEXT G ALLIANCE.

REFERENCES

[1] 3GPP TS 33.501 version 16.3.0 Release 16. "Security architecture and procedures for 5G System", August 2020. https://www.3gpp.org/release-16.

[2] Abdel Hakeem SA, Hussein HH, Kim H. "Security Requirements and Challenges of 6G Technologies and Applications". Sensors (Basel), vol. 22, no. 5, March 2022.

[3] Alwis C., Kalla A., Pham Q.-V., Kumar P., Dev K., Hwang W.-J., Liyanage M. "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies, and Future Research". IEEE Open J. Commun. Soc., vol. 2, pp. 836-886, 2021.

[4] M. A. Uusitalo et al. "6G Vision, Value, Use Cases and Technologies From European 6G Flagship Project Hexa-X". IEEE Access, vol. 9, pp. 160004-160020, 2021.

[5] Mohammed Ramadan, Yongjian Liao, Fagen Li, Shijie Zhou. "Identity-Based Signature with Server Aided Verification Scheme for 5G Mobile Systems". IEEE Access, vol. 8, pp. 51810-51820, 2020.

[6] Mohammed Ramadan, Guohong Du, Fagen Li, Chunxiang Xu. "A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems". MDPI: Symmetry 2016, vol. 8, no. 9, pp. 85-102, 2016.