ITL BULLETIN FOR JANUARY 2018

GUIDANCE FOR IMPROVING LTE-BASED MOBILE COMMUNICATIONS SECURITY

Jeff Cichonski, Joshua Franklin, Michael Bartock, Larry Feldman,[1] and Greg Witte,[1] Editors
Applied Cybersecurity Division and Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

The odds are high that those reading this bulletin have used a cellular communications device recently. The use of cellular mobile networks has significantly changed the way people and devices communicate. Expanding far beyond yesterday's voice calls, cellular devices store and process personal information, act as the primary portal to the Internet for a large segment of the population, and provide enterprise connectivity. People increasingly rely on cellular devices for applications that require stringent security and safety. Such devices include public safety Long Term Evolution (LTE) devices, medical devices, and devices used in communication networks that guide autonomous vehicles.

Cellular infrastructure has transitioned from the early days of mobile telephone service to older second generation (2G) and third generation (3G) cellular technologies. Many Mobile Network Operators (MNOs) have adopted LTE technology as an ongoing way to increase the capacity and speed of wireless data networks. LTE's fourth generation (4G) technology is now the dominant air interface technology across the United States and around the globe.

To support the growing need for security and privacy protection related to these LTE networks, NIST's Information Technology Laboratory created Special Publication (SP) 800-187, Guide to LTE Security. In this article, we provide an overview of how LTE technology is deployed, the LTE security architecture and threats to LTE networks, and mitigations to many of the described threats.

Overview of LTE Technology

A cellular network is a wireless communication system consisting of interconnected and distributed radio equipment, each supporting a geographic area, called a cell. A cellular site is often owned and operated by a wireless telecommunications company, Internet service provider, or possibly a government entity. Wireless telecommunications companies, which provide service to end users, may own the cellular site or pay for access to the cellular infrastructure. MNOs distribute cellular radio

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.

equipment throughout a large geographic region and connect them back to a core network they typically own and operate. In areas receiving poor cellular service, such as inside a building, MNOs may provide a signal booster or a small-scale base station directly to the end user to operate.

Before LTE, cellular systems were modeled after the traditional wireline telephony system, in which a dedicated circuit was provided to a user making a telephone call. In comparison to the circuit-switched cellular networks of the past, LTE networks use packet switching, like computer networks on the Internet. An LTE network provides consistent Internet Protocol (IP) connectivity between an end user's mobile device and IP services on the data network, while maintaining connectivity when the user moves in and out of range of individual radio towers.

So, what is LTE? It is a mobile broadband communication standard defined by the 3rd Generation Partnership Project (3GPP), a worldwide standards-development organization. LTE networks are deployed across the globe, and installations continue to increase as the demand for high-speed mobile networks is constantly rising. According to 3GPP,[2] LTE systems need to meet several high-level goals, including:

- Provide increased data speeds with decreased latency;
- Build upon the security foundations of previous cellular systems;
- Support interoperability between current and next-generation cellular systems and other data networks;
- Improve system performance while maintaining current quality of service; and
- Maintain interoperability with legacy systems.

NIST SP 800-187 provides details of the various standards, protocols, and interfaces of LTE technology and architecture, with helpful diagrams to illustrate the concepts.

LTE Security Architecture and Threats to LTE Networks

NIST SP 800-187 distills various 3GPP standards into a central knowledge base for end users to easily reference.

The guidance outlines several categories of threats to LTE networks, including references to LTE threat research conducted by the Security Working Group of 3GPP's Service and System Aspects Technical Specification Group (3GPP SA3). These threats are important to understand because they are not just theoretical notions – while many threats listed have been identified via academic research, others are based upon documented real-world attacks that have occurred in deployed cellular systems.

[2] 3rd Generation Partnership Project, *Service requirements for the Evolved Packet System (EPS)*, 3GPP TS 22.278 V13.2, 2014. http://www.3gpp.org/DynaReport/22278.htm

Organizations can use the higher-level threat categories presented in the guidance as a starting point for their own detailed threat models.

Some of these threats impact the availability and resiliency of networks, while most of the threats affect only a limited portion of the network. Other types of threats impact user-data integrity and confidentiality. Unfortunately, because low-cost LTE hardware and software is increasingly available, hackers can more easily implement many of the threats described in NIST SP 800-187, including:

- General cybersecurity threats, such as malware attacks on specific network components;
- Rogue base stations;
- Air interface eavesdropping;
- Attacks via compromised femtocells;
- Radio jamming attacks;
- Backhaul and core eavesdropping;
- Physical attacks on network infrastructure;
- Attacks against keys used to protect different layers of LTE communication; and
- Stealing services, such as the theft of a removable universal integrated circuit card (UICC) from one mobile device and its placement into another, with the goal of stealing service.

Mitigations

NIST SP 800-187 identifies mitigations to many of the threats described. Each mitigation addresses at least one threat listed in the guidance, and the higher-level mitigation descriptions may be helpful for organizations looking to address threats identified during threat-modeling exercises.

Many of the mitigations are intended to be implemented by MNOs, mobile operating system developers, and hardware manufacturers rather than by end users. MNOs can work to implement many of the mitigation techniques described in the guidance, while understanding that challenges may exist when hardware, firmware, and software do not support these countermeasures. Because both threats and mitigation go beyond organizational and network boundaries, it is important that the broader community works together to continue to research, develop, and implement security features in commercial cellular equipment.

Individuals and organizations that are concerned about adequately mitigating the threats described in NIST SP 800-187 may need to discuss these security protections with their service providers. Many of the listed mitigations may simply be accomplished by modifying certain configurations of already implemented features – an option that may be feasible in the near term. Other mitigations may require software updates to mobile operating systems and/or baseband processors or modifications to 3GPP standards. Such mitigations would take much more time to implement.

Conclusion

When compared to previous evolutions of cellular networks, the security capabilities provided by LTE are noticeably more robust. The addition of mutual authentication (between the cellular network and the device) and the application of publicly reviewed cryptographic algorithms using sufficiently large key sizes are positive steps forward in improving the security of cellular networks, and we all benefit from industry's work in this area. The enhanced key separation introduced into the LTE cryptographic key hierarchy and the mandatory integrity protection also help to raise the bar.

Yet, LTE systems are rarely deployed in a stand-alone fashion – they coexist with previous cellular infrastructure that was already in place. Older cellular systems continue to operate throughout many different industries, and this multigenerational deployment may lead to an overall decrease in cellular security. A primary example of this situation is the requirement for the baseband firmware to remain backward-compatible in order to support legacy security configurations, enabling users to switch devices among 2G, 3G, and 4G LTE technologies.

While this publication focuses on the fundamentals of LTE and its security architecture, we considered many concepts but determined that they would be out of scope for this document. Some of these concepts are services that build on top of the LTE architecture, while others come from specific implementations and uses of an LTE network.

The authors of this publication include a list of other areas of cellular infrastructure that are highlighted for additional research or further study:

- Security analysis of IP Multimedia Subsystem (IMS);
- Security analysis of Voice over LTE (VoLTE);
- Protection against jamming attacks;
- LTE for public safety use;
- Security implications of Over-the-Air (OTA) updates;
- Multi-Operator Core Networks (MOCN); and
- Security capabilities of Network Function Virtualization (NFV).

As LTE technology continues to expand, including widespread application of 4G and emerging standardization and implementation of proposed fifth generation (5G) cellular systems, the threats and potential mitigations described in NIST SP 800-187 are important to consider. Exploring and enabling the mitigations included within this document will require a coordinated effort among mobile operating system vendors, baseband firmware developers, standards organizations, mobile-network operators, and end users. It is critical that the community continues to perform relevant research and develop solutions to evolving challenges, since LTE is the nation's dominant cellular communications technology and is likely to remain so for future generations.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov