Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight

"*Bolstering Data Privacy and Mobile Security: An Assessment of IMSI Catcher Threats"*

June 27, 2018

Introduction

Chairman Abraham, Ranking Member Beyer, and members of the Subcommittee, I am Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in telecommunications security.

The Role of NIST in Cybersecurity

Cybersecurity is a key priority of this Administration, for NIST, and across the Department of Commerce. With programs focused on national priorities, from advanced manufacturing and the digital economy to precision metrology, quantum science, and biosciences, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the data encryption standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop, and deploy information security standards and technology to protect the federal government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347[1]) and reaffirmed in the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. These resources are used by federal agencies and are frequently voluntarily used by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective, represent the state-of-art and have wide acceptance. NIST disseminates its resources through a variety of means that encourage the broad sharing of tools, security reference data, information security standards, guidelines, and practices, along with outreach to stakeholders, participation in government and industry events, and online mechanisms.

As the principal advisor to the White House on information and communications policy, the Commerce's National Telecommunications and Information Administration (NTIA), collaborates with NIST to ensure that the equities of innovation, economic growth, and an open Internet are factored into cybersecurity policy decisions within both domestic and international fora.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

Rogue Base Stations

Overview

As explained in NIST Special Publication 800-187, "Guide to LTE Security," which I will discuss later in more detail, rogue base stations are unlicensed cellular devices that are not owned and operated by a duly-licensed mobile network operator. These devices broadcast on spectrum licensed to legitimate mobile network operators. They are known by many names, such as *Cell-Site Simulators, Stingrays* or *International Mobile Subscriber Identity* (*IMSI) catchers*. As cell-site simulators are also an important tool for law enforcement, we note that our statement focuses on the unauthorized use of such technology by non-law enforcement actors. Rogue base stations act as a cell tower and broadcast a signal pretending to be a legitimate mobile network that may trick an individual's device into connecting to it. The necessary hardware to build a rogue base station can be inexpensively obtained using commercial off-the-shelf parts. The software required to operate a rogue base station is open source and freely available.

Rogue base stations exploit the fact that mobile devices will connect to whichever base station is broadcasting as a device's preferred carrier network and is transmitting at the highest power level. Therefore, when a rogue base station is physically near a mobile device that is transmitting at higher power levels than the legitimate antenna, the device may attempt to connect to the malicious network. Mobile devices and networks are engineered to be backwards compatible interoperating with older mobile networks, providing maximum coverage to subscribers. Rogue base station attacks can take advantage of this interoperability and exploit weaknesses in these older mobile networks. Many rogue base stations broadcast an older second generation (2G) mobile network type, also referred to as Global System for Mobile communications (GSM), that does not have the security protections needed in today's communication environment. Examples of 2G weaknesses include a lack of mutual authentication and the use of weak or broken cryptographic algorithms.

Threats

Rogue base stations can perform a passive attack known as IMSI catching. This attack sniffs cellular communication without the user's knowledge to collect mobile device identities that are sent in an unencrypted manner. I am using the term "mobile devices" here to refer to any device with a cellular connection, such as a cellphone, tablet, laptop, or mobile hotspot. In fourth generation (4G) Long-Term Evolution (LTE) networks, device identities are known as "IMSI," and correlate to a specific subscriber. This identifier can be used to indicate who owns a mobile device. When a device is physically close to a rogue base station that is masquerading as a legitimate network, the device sends a message to initiate an *attach*, or connection, to the network. This message contains the subscriber identifier IMSI and information about the device's security capabilities. It is important to understand that in 4G LTE, this message is sent unprotected, *before* security is established.

It is commonplace today for individuals to constantly wear or keep their mobile devices close by. If a rogue base station is operating near someone's home or workplace, the operator of the rogue network may be able to infer whether a specific individual is present or not. This poses a significant threat to user privacy, and potentially safety, because a malicious actor can determine if a subscriber is in a given location at a given time. Compounding this issue is the fact that

passive sniffing of IMSIs is no longer an advanced or complex attack only accessible to a small number of individuals.

A more advanced attack that can be executed using rogue base stations is a type of "man in the middle" attack, in which a malicious actor can force a user to downgrade to an older, less secure mobile network technology such as 2G or 3G. Normally, mobile networks and user devices support interworking with legacy mobile networks (2G/3G) in order to provide the highest level of connectivity to their subscribers. For example, if an area does not have 4G LTE coverage, but does have 2G or 3G coverage, a mobile device can still connect to the mobile network. This interworking with legacy networks provides a seamless connection to the user; however, it exposes that user to less robust security protections and vulnerabilities that exist in older versions of mobile networks. As a result, a malicious actor running a rogue base station would be able to trick an attached device into connecting and execute a man in the middle attack on the device.

While there are no significant, currently publicly known weaknesses in the cryptographic algorithms used to protect the confidentiality and integrity of the 3G communications, significant weaknesses are known to exist for the 2G cryptographic algorithms used to protect the confidentiality and integrity of the air interface. The air interface is the radio frequency (RF) connection between the mobile device's antenna and the base station's antenna. Examples of broken 2G cryptographic algorithms are A5/1 and A5/2. Depending on the algorithm negotiated when a device connects to a rogue base station, a cryptographically broken algorithm may be selected to protect the cellular traffic. This can lead to a loss of call and data confidentiality.

A complex "denial of service" attack can occur when a mobile device first connects to a network, a process which is known as the "attach procedure." During the attach procedure, certain messages can be sent to a device by a rogue base station before security parameters are negotiated with the bona fide network. One such unprotected message may prevent a mobile device from completing the attach procedure. In response to receiving this message, a mobile device will no longer attempt to attach to this, or other, LTE networks, essentially going into the equivalent of "airplane mode." Since this message is sent before the mobile device can authenticate the network, the mobile device is unable to distinguish the rogue base station from an authentic network. This can cause a denial of service that may persist until a hard reboot (that is, completely powering the device off and then restarting it) of the mobile device is performed. Certain mobile device cellular implementations will not automatically try to reconnect if such a message is received.

NIST activities related to Rogue Base stations

NIST began working in the cybersecurity aspects of telecommunications in 2012, focusing on 4G LTE networks used by public safety. Ultimately, these activities enabled NIST to develop *Special Publication 800-187: Guide to LTE Security*.[2] The Guide to LTE Security was released in December 2017. This publication starts with the premise that cellular technology plays an increasingly large role as the primary portal to the internet for a large segment of the nation's population. One of the main drivers making this possible is the deployment of 4G LTE cellular technologies. This publication serves as a guide to the fundamentals of how LTE networks

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

operate; it explores the LTE security architecture; and it provides an analysis of the threats posed to LTE networks and supporting mitigations. The document covers many areas of interest to the Committee, and includes a description of cell site simulators or rogue base stations as unlicensed base stations that are not owned and operated by an authentic mobile network operator. This NIST Special Publication is intended to educate federal agencies and other organizations who rely on 4G LTE networks as part of their operational environment.

Since 2012, NIST has been an active participant in the Third Generation Partnership's (3GPP's) Service and Systems Aspects (SA) Working Group 3. This working group is the standards development organization responsible for security and privacy of 3G and 4G LTE, and is currently developing 5G. Active participation with the mobile network manufacturers and carriers in developing security standards for future networks is an important way in which NIST is working to address security vulnerabilities in mobile networks today.

Security standards for 5G are, in fact, seeking to address issues surrounding rogue base stations through the introduction of optional privacy functionality. Once this functionality standard is developed for future networks, its implementation by mobile network operators will have the potential to eliminate the threat of today's passive sniffing IMSI catchers.

Concluding Observations

When compared to previous mobile networks, the security capabilities provided by 4G LTE are markedly more robust. The additions of mutual authentication between the mobile network and the mobile device, alongside the use of publicly reviewed cryptographic algorithms with sufficiently large key sizes, are positive steps forward in improving the security of mobile networks. The enhanced key separation introduced into the 4G cryptographic key hierarchy and the mandatory integrity protection also help to raise the bar. Yet 4G systems have a number of optional capabilities that mobile network operators must choose to implement. The use of the optional security settings and next generation 5G technologies will go a long way to mitigate the usage of rogue base station technology. To that extent, NIST also collaborates with our sister agency NTIA to maintain and enable U.S. 5G activities. NTIA actively identifies and studies additional spectrum bands to make available for commercial uses; supporting national and international efforts to set standards and harmonize spectrum; and helping industry to overcome obstacles in deploying the network infrastructure needed for 5G to flourish. This is essential to keeping U.S. companies at the forefront of the innovation in the wireless industry.

5G is a new and exciting technology with the ability to positively impact nearly every facet of the technology space. Much work still needs to be done to understand this technology and ensure secure deployments. NIST will continue its research and development in the security of telecommunications. We will continue to learn from our research and continue to build collaborations with industry in the publication of guidelines and best practices. NIST is also continuing to work with international standards bodies and technical committees. This is truly an exciting time in the continuing expansion of telecommunications to benefit the lives of every American.

Thank you for the opportunity to testify on NIST's work regarding telecommunications security. I will be pleased to answer any questions you may have.

Charles H. Romine

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL, one of seven research Laboratories within the National Institute of Standards and Technology (NIST), has an annual budget of $150 million, nearly 400 employees, and about 200 guest researchers from industry, universities, and foreign laboratories.

Dr. Romine oversees a research program that cultivates trust in information technology and metrology by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission, to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Within NIST's traditional role as the overseer of the National Measurement System, ITL is conducting research addressing measurement challenges in information technology as well as issues of information and software quality, integrity, and usability. ITL is also charged with leading the nation in using existing and emerging IT to help meet national priorities, including developing cybersecurity standards, guidelines, and associated methods and techniques, cloud computing, electronic voting, smart grid, homeland security applications, and health information technology.

Education:
Ph.D. in Applied Mathematics from the University of Virginia.
B.A. in Mathematics from the University of Virginia.