U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

June 9, 2017

TO: Members, Subcommittee on Communications and Technology

FROM: Committee Majority Staff

RE: Hearing entitled “Promoting Security in Wireless Technology”

I. INTRODUCTION

The Subcommittee on Communications and Technology will hold a hearing on Tuesday, June 13, 2017, at 10:00 a.m. in 2322 Rayburn House Office Building. The hearing is entitled “Promoting Security in Wireless Technology.”

II. WITNESSES

- Bill Wright, Director, Government Affairs & Senior Policy Counsel, Symantec;
- Amit Yoran, Chairman and CEO, Tenable Network Security;
- Dr. Charles Clancy, Director and Professor, Hume Center for National Security and Technology, Virginia Tech
- Kiersten E. Todt, Former Executive Director, Commission on Enhancing National Cybersecurity; Managing Partner, Liberty Group Ventures, LLC; Resident Scholar, University of Pittsburgh Institute for Cyber Law, Policy, and Security

III. BACKGROUND

The United States’ economy continues to embrace and rely on mobile connectivity. Seventy-seven percent of adults in the U.S. own a smartphone, and 51percent own a tablet.[1] Further, the amount of time Americans spend on mobile devices continues to increase, with the average adult spending five hours a day on mobile devices. This trend is supported by almost 380 million wireless connections in the U.S. alone.[2] Those connections produce terabytes of data that travel over wireless networks.

As this technology has evolved, so have the cyber threats to devices and networks. Cyber criminals utilize a number of strategies to launch attacks on wireless technologies such as exploiting vulnerabilities to gain unauthorized access to wireless networks and targeting mobile devices through malware and phishing attacks. From 2013 to 2015, new mobile vulnerabilities

[1] Joe Ross, “The Future of Cybersecurity is Mobile” Huffington Post, Apr. 26, 2017, available at http://www.huffingtonpost.com/entry/the-future-of-cybersecurity-is-mobile_us_59010075e4b06feec8ac930f
[2] “Wireless Industry Summary Report, Year-End 2015 Results” CTIA, Jan. 2016, available at https://www.ctia.org/industry-data/ctia-annual-wireless-industry-survey

increased about 214 percent,[3] the number of malicious mobile applications grew 105percent,[4] and from 2015 to 2016, mobile malware attacks increased by more than 300 percent.[5]

Network operators, as well as manufacturers and service providers continue, to invest in a variety of defense mechanisms to protect their networks and products. These include the use of encryption, authentication standards, data monitoring, app screening, and the use of and anti-spamming and anti-virus software.

This hearing will examine a variety of cybersecurity issues and challenges that face the mobile industry, as well as potential solutions.

A. Mobile Threats

As the use of mobile devices continues to grow, so has the amount of sensitive information stored on these devices. Americans regularly use their mobile devices to access financial and health records, sensitive work information, and personal contacts, photos, and conversations. This trend has created a valuable target for cyber criminals who execute a number of strategies to gain unauthorized access to this data.

1. Phishing

Phishing is the attempt to obtain sensitive user information such as login credentials by disguising as a trustworthy source. The most common phishing technique is "spear phishing" in which attackers collect information about the target that allows them to tailor the disguise of a phishing email or message, increasing their probability of success. While this technique is not unique to mobile technology, more than half of all emails opened occurs on mobile phones or tablets.[6] Phishing can also occur through malicious apps – a nefarious application disguised as a legitimate application – or malicious behavior within apps – when an attacker modifies the content that an application is showing.

2. Ransomware

Mobile ransomware is a type of malicious software that prevents access to the user's data or threatens to publish or delete it until a ransom is paid. Criminals remotely access a victim's device and lock the user's data using encryption, offering to unlock it in exchange for payment.

[3] "Internet Security Threat Report 2016" Symantec Corporation, p. 9 Apr. 2016, available at https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[4] "Internet Security Threat Report 2017" Symantec Corporation, p. 68 Apr. 2017, available at https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[5] "Mobile Malware Evolution", Kaspersky Lab, p. 11 Feb. 28, 2017, available at https://press.kaspersky.com/files/2016/02/Mobile_virusology_2015_FINAL_eng_1902206-2.pdf
[6] "Quarterly Email Benchmark Report" Experian, p. 11 June 2016, available at http://www.experian.com/assets/marketing-services/p/ems-q2-2016-email-benchmark-report.pdf

Ransomware malware can be spread through malicious e-mail attachments and links, compromised applications, and infected websites.

3. Malware

Mobile malware is malicious software aimed at mobile devices that compromises the security of the device, allowing adversaries to access personal information or alter the device's functionality. Malware can infect a device when a user downloads a malicious application, clicks on a compromised link, or even when the user simply visits an infected site.

B. Threats to Wireless Networks

Mobile devices transmit millions of terabytes of data each year using numerous air interfaces, including 3G, 4G, and Wi-Fi. Each interface offers different cybersecurity defenses, creating a number of unique security vulnerabilities and attack methods.

1. Packet Sniffing

Information sent over a network is carried by packets. Packet sniffers intercept network traffic, capture packets, and decode the packet data. While packet sniffing is often used by network technicians to diagnose network problems, the technique can also be used by hackers to obtain data including financial information and passwords.

2. Rogue Access Points

A rogue access point is an access point that has been added to a network without authorization. The access point can then be used to flood the network with data, creating a denial of service, or to capture data traveling over the network.

3. Jamming

Jamming is the use of a device to block or interfere with wireless communications. This is often accomplished by overwhelming wireless frequencies with illegitimate traffic, thereby preventing legitimate traffic from reaching its destination.

4. WEP/WPA/WPA2 Attacks

WEP, WPA, and WPA2 are acronyms that refer to wireless encryption protocols that are used to protect the information sent over Wi-Fi. Adversaries attempt to discover and exploit security flaws in the encryption algorithms, allowing them to decrypt data or launch an attack.

C. Threat Defense

Network operators, as well as manufacturers and service providers, are engaged in ongoing efforts to protect networks and devices from attacks. They continue to invest in a variety of defense mechanisms to enhance the security of their products and services. The use of standards-based encryption has increasingly become a part of cybersecurity strategies in both the public and private sectors. Encryption scrambles the information sent over the network so that it is unreadable to unauthorized users. To limit access to networks, operators often utilize authentication standards, which verify a user's identity before permitting access. Additional common practices include data monitoring, application screening, and the use of anti-spamming and anti-virus software.

Effectively defending networks and devices requires continuous investment and innovation. The public and private sectors have worked together to identify threat trends, develop best practices, and provide resources for consumers and businesses. For example, CTIA's Cybersecurity Working Group (CSWG) brings together members of the mobile ecosystem to engage with government entities including the National Institute for Standards and Technology (NIST), the Department of Homeland Security (DHS), the Federal Communications Commission (FCC), and others. In addition, standards-setting organizations such as 3GPP, IETF, and IEEE are continually working to develop standards and policies that enable organizations to defend their products and services more effectively.

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Lauren McCarty of the Committee staff at (202) 225-2927.