Testimony of Dr. Charles Clancy

Professor of Electrical and Computer Engineering, Virginia Tech

before the House Energy and Commerce Committee, Subcommittee on Communications and Technology, Hearing on Promoting Security in Wireless Technologies

June 13, 2017

Introduction

Chairman Blackburn, Ranking Member Doyle, and Subcommittee Members:

My name is Charles Clancy and I am a professor of electrical and computer engineering at Virginia Tech, where I direct the Hume Center for National Security and Technology. In these roles, I lead major university programs in cybersecurity and telecommunications. I am an internationally-recognized expert in wireless security and have held leadership roles within international standards and technology organizations including the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE). From 2015-2016 I led the successful negotiations between the Pentagon and wireless industry on security requirements for spectrum sharing in the Navy's 3.5 GHz radar band, and from 2008-2012 I led the development of security requirements for military deployment of WiMAX, LTE, and cognitive radio technologies. I am co-author to over 200 peer-reviewed academic publications, to include five books on digital communications; am co-inventor to over 20 patents; and am co-founder of four venture-back startup companies all focused in the wireless and security sectors. Prior to joining Virginia Tech in 2010, I served as research leader for emerging mobile technologies at the National Security Agency.

Background

While viewed as a luxury a few decades ago, access to wireless communications is a critical component of our society. Over the past decade, smartphones have further entrenched our reliance on wireless communications and the need for ubiquitous mobile broadband. The next decade brings the so-called Internet of Things, or IoT, which connects to the cloud everything from home appliances to industrial infrastructure. The cellular industry's next generation of technology, 5G, is being designed to specifically address these needs. Gartner projects[1] that by 2020, there will be over 20 billion IoT devices connected to the Internet representing a $3 billion market. Achieving and sustaining this exponential market growth requires that the wireless technologies underpinning the IoT are secure.

[1] http://www.gartner.com/newsroom/id/3165317

Along the way, military and public safety communities have begun embracing commercial wireless technologies as components to their mission-critical communications systems. Examples include FirstNet's use of commercial LTE for public safety users, Wireless Priority System (WPS) for national security and emergency response users, and US military use of WiFi and private LTE networks both domestically and overseas. These critical missions all demand more from a security and resilience perspective than traditional personal and commercial use of these technologies. Additionally efforts to share spectrum between legacy military systems and commercial wireless broadband operators adds an additional wrinkle to understanding security. Unlocking the value of shared spectrum and achieving the economies of scale by leveraging commercial infrastructure are only feasible if these heightened security requirements can be achieved without major changes to the underlying technologies.

Security of Wireless Infrastructure

In order to securely and reliably deliver media and services to wireless devices, we must rely on the underlying security of the infrastructure itself. To better explore this topic, we can break things down into systems operating over licensed spectrum, like cell phones, and those operating over unlicensed spectrum, like WiFi.

Cellular systems have the advantage of being centrally managed which helps ensure that security safeguards are implemented. While industry continues to advance and innovate security safeguards, that security may be undermined by the need to continue supporting backward-compatible legacy technologies. Our new 4G-LTE systems are secure, but the 2G networks are vulnerable to a wide range of attacks that can compromise subscribers' security and privacy. Recently-publicized attacks against the SS7 protocol and unlawful use of IMSI catchers – also known as Stingrays – are examples of risks in legacy 2G systems.

Meanwhile as we look forward from 4G to 5G, a range of new technologies are under development that offer the opportunity to close current cybersecurity gaps while potentially opening up new ones in ways we cannot yet anticipate. Examples include software-defined networking, cloud-based radio access networks, and edge computing – all of which are fueling IoT applications.

Unlicensed technologies have their own challenges. WiFi's adoption in the early 2000s was nearly undermined by sweeping security vulnerabilities. While residential WiFi networks are generally now operating with adequate levels of security, public hotspots and paid WiFi in hotels and airplanes remain vulnerable to attacks that have been well known for nearly two decades. Meanwhile many of the shorter-range wireless protocols used in home and building automation systems are proprietary and lack needed rigorous security analyses.

Lastly, emerging shared bands that involve a coordinated mixture of licensed and unlicensed access will have a blended set of security requirements and security threats. The spectrum sensors and coordination databases represent new attack surfaces and if exploited could disrupt spectrum availability and compromise the privacy of sensitive incumbent activity. In the 3.5 GHz band, rigorous security protections have been developed, but the threat and risk varies from band to band depending on the criticality and sensitivity of incumbent activity.

Security of Wireless Ecosystems

Riding on top of this wireless infrastructure is a complex, interlinked ecosystems of device manufacturers, software and app developers, cloud infrastructure providers, and platforms for media and services. Key cyber threats include exploiting thousands of devices to use them as part of massive Internet attacks, such as the Mirai botnet attack against the Dyn Internet infrastructure company in October 2016; mobile and IoT ransomware, such as the Android ransomware that affected LG smart TVs in January; privacy compromising attacks that steal financial or other personal data, such as the growth of robocalls and SMS phishing attacks; or cyber attacks against safety-critical systems that could lead to loss of life or property, such as the Jeep telematics hack demonstrated in 2015.

The biggest challenge in securing these ecosystems is their complexity and heterogeneity. Over the past decade, this rich tapestry of companies has fueled unprecedented levels of mobile technology innovation, but the consequence is that no one entity controls enough of the ecosystem to unilaterally guarantee the needed security. Another side effect is that regulatory authority is distributed across the Department of Homeland Security, Federal Communications Commission, Federal Trade Commission, and various other sector-specific regulators. Without a single “belly button”, top-down approaches to achieving objective levels of security are infeasible.

Consequently it is imperative that we develop mechanisms to foster continued collaboration. In the policy and regulatory arena, the NIST Cybersecurity Framework and the Cybersecurity Information Sharing Act (CISA) are both examples of activities that achieved broad support from both government and industry. Similarly, cyber workforce initiatives from CyberCorps to the National Initiative for Cybersecurity Education (NICE) have had a transformative effect on understanding what skills are needed for these 21st century jobs and incentivizing our nation’s education system to implement the needed education and training programs.

Conclusions

Looking forward, I encourage this subcommittee to consider the following.

First, it is imperative that the federal government continue to act as a convener, bringing together this complex cast of characters and help set priorities for cyber defense based on its unique knowledge of the threat. Industry needs consensus issues that they can solve based on a shared understanding of threats to our critical networks and privacy of our citizens.

Second, IoT and 5G wireless represent major shifts in the nature of telecommunications and the Internet. Both industry and the federal government need to significantly increase research funding in these areas so we can work to build security in from the start as these standards are being defined, rather than through after-the-fact solutions applied with duct tape and bubble gum. As an example, last year the National Science Foundation worked with Intel Labs to jointly fund a grant program in IoT security with a total budget of $6M. While this is an excellent example of co-investment, orders of magnitude more resources need to be brought to bear if we hope to get out in front of this problem.

Third, despite many great programs to help bolster the cyber workforce, the nation currently has over a million total jobs in cybersecurity, of which 31% are currently vacant[2]. In the area of cybersecurity for wireless and telecommunications systems the gap is even wider – most universities are shifting curriculum away from large-scale telecom infrastructure toward how to write an app. As a result the number of graduating students with the needed mixture of skills as a ratio of the need is declining. Programs are needed to incentivize universities to build programs to support cybersecurity for telecommunications, and more broadly critical infrastructure.

Thank you for the opportunity to address the subcommittee today and I look forward to questions.

[2] http://cyberseek.org/heatmap.html