Public Safety and Homeland Security Bureau Chief
DAVID TURETSKY
PREPARED REMARKS
FOR
MOBILECON 2012 EVENT
ON
THE SECURITY OF ADVANCED MOBILE COMMUNICATIONS DEVICES: THE VIEW FROM THE FCC

SAN DIEGO, CA
OCTOBER 9, 2012

Preamble

Thank you for inviting me to be here with you today.

You are participating in a dynamic industry that is helping to change the way we live and work. Anyone who heard this morning's keynote presentations cannot doubt this.

The innovation unleashed by the deployment of faster broadband networks is empowering more consumers and businesses than ever before to connect to the content they choose, anywhere at anytime. We now use wireless devices to conduct commercial transactions; to connect to, transmit, or store confidential financial and medical data; to entertain ourselves and, of course, to communicate, whether by voice, text, email or otherwise. New businesses depending on these networks and devices are creating exciting products and capabilities, empowering consumers to make more choices about how they live their lives.

With this expanding freedom also comes the responsibility to face up to some not-so-pleasant realities. There are people who find in these developments opportunities of a much different and sinister character. That brings me to my purpose today, to discuss some of the Commission's ongoing work related to security, particularly cybersecurity, in connection with smart devices.

It is particularly fitting that we speak about mobile security today, because the President has declared October, "National Cybersecurity Awareness Month."

Let me be among the first to wish each of you "Happy National Cybersecurity Awareness Month" – and let's reflect upon and renew our resolve and strengthen our collective efforts to stem growing cybersecurity threats – especially those emerging threats aimed at mobile platforms.

You'll find cybersecurity highlighted through much of the month on the web sites of CTIA, the Federal Communications Commission, and the Department of Homeland Security, among others. Let me also invite you to attend and spread the word that, as part of Cybersecurity Awareness Month, the Commission will host a “Mobile Security Showcase” in its Technology Experience Center at the Commission on October 17, the date the Commission holds its Open Meeting this month.

Today, I’ll discuss the growing mobile security threat to our nation, where we see the biggest challenges, and how we are embracing the challenges with our industry partners. I will also touch on our outlook on the future, as we, both public and private industry, aggressively pursue measures to address mobile security vulnerabilities.

The Growing Mobile Security Threat

The FCC is keenly aware that the transition from limited-use cell phones to smart mobile devices is moving with blazing speed. Not only is the FCC moving to make more spectrum available, but as FCC Chairman Genachowski recently noted, 2 million iPads were sold in a weekend; and more recently, in the first three days the new Apple iPhone 5 model was available last month, 5 million were sold. And, of course, consumer ownership of Android smartphones in the U.S. far exceeds that of Apple smartphones.

These are only some among many amazing stories about consumers’ appetite for technology products that utilize the faster mobile broadband networks that carriers are deploying more widely. These faster connections are spurring the development of a broad and innovative ecosystem of exciting products and capabilities that are helping our entire economy to grow.

The Government Accountability Office (GAO), in a new, September 2012 report on mobile device security, cited a recent analysis finding that mobile devices are the fastest growing consumer technology, with worldwide sales still increasing rapidly, from 300 million in 2010 to an estimated 650 million in 2012. And in the U.S., where nearly 9 out of 10 adults own cell phones, about half of those devices, or about 107 million, are considered smartphones.

These smart mobile devices are providing impressive productivity benefits to consumers and a wide variety of organizations, and I think we are just scratching the surface of what is possible. But if not properly protected, these devices pose a variety of security risks because they are attractive targets for those who would steal critical and sensitive information, and money, or try to bring down the people, entities, and operations that depend on these devices.

Thus, it is hardly surprising or shocking to those of you here that the GAO also reports that threats to the security of mobile devices and the information they store and process are increasing significantly. A huge jump in the number of cyber attacks and malicious apps aimed at mobile devices has followed the pattern of growth in consumer usage. More and more consumers are installing all kinds of apps on their smart devices.

Indeed, it is now estimated that about six out of every ten cybersecurity breaches are associated with a mobile phone. And if the frequency of these attacks isn't disturbing enough, cyber threats to smart devices have grown in size and sophistication.

We will all feel the impact if we continue down the path that we're on. As I noted earlier, smart devices are delivering more and more benefits to people and enterprises every day. Because attacks on these devices can be so devastating both to consumers and businesses, there is a compelling need to secure these devices.

Many of these threats are similar to those that have long plagued traditional computing devices connected to the Internet. In a moment, I'll say some more about the lessons learned from the FCC in fighting those other cybersecurity threats, shoulder-to-shoulder with an array of stakeholders, for fighting mobile security threats.

The Problem

The entire ecosystem that supports smart mobile devices and their applications, including the consumers and businesses that buy these products, have an important role to play in improving mobile security. The GAO's new report on mobile device security acknowledged the extensive efforts undertaken within both the private and public sectors, but called for more to be done. Specifically, the GAO recommended that the FCC continue to work with wireless carriers and device manufacturers on implementing cybersecurity best practices, and monitor progress towards achievement of milestones. I was interested to hear CTIA's CEO Steve Largent report in his remarks this morning that there was 70 percent support for industry/government collaboration on standards in a recent survey of company CIOs and IT managers.

Consumers are one of the most important audiences to reach with information and tools to enhance mobile cybersecurity. Even when their mobile devices and apps have been attacked, many consumers are unaware of the risks and fail to take action to mitigate them. With too few consumers taking precautions to protect their devices, this means that smart devices represent a "weak link," which can be easily exploited for profit. And as they download more apps, particularly from outside, well-established apps stores, more malware will arrive.

Consumers can benefit from additional education about even basic tools to protect their information, including about locating, locking and remotely wiping smartphones and tablets that are lost or stolen. In April, 2012, FCC Chairman Genachowski, with the support and participation of CTIA and Major City Police Chiefs, announced new initiatives by wireless carriers to work cooperatively on specific initiatives to advance these goals.

For example, as part of the "Locate, Lock and Wipe" initiative, smartphone makers will be able to alert users on new smartphones of available locking and secured access capabilities via passwords, by April 2013. Additionally, wireless providers participating in this voluntary initiative will embark on an education campaign to inform consumers about applications that can lock, locate and erase data from smartphones. You can also find a consumer fact sheet on the FCC web site about Stolen and Lost Wireless Devices and how to protect the data on your phone.

I'm pleased that these efforts are progressing apace.

Notwithstanding that good news, the situation is dynamic and very serious. More and more exploitable vulnerabilities are being discovered every day, even though in many cases, solutions are available that could address the problems.

For example, best practices, such as those addressing device passwords and detecting the presence of device malware, exist for wireless service providers and device manufacturers, and can be used to mitigate many of the common mobile device vulnerabilities identified by the GAO; however, the extent to which the best practices are being followed is not known. To reduce those vulnerabilities, a greater and more concerted effort is required.

To address the situation, we will continue to work closely with industry stakeholders over the next several months.

I believe that success at combating these evolving and ubiquitous mobile device threats will require, in part, a sustained, collaborative public-private partnership, if there are to be long term solutions.

This is not a new idea. The FCC, together with our industry partners, has successfully helped to formulate cybersecurity best practices and recommendations that could help to address some of the most pressing cybersecurity threats to non-mobile computing devices. The challenge is to leverage this knowledge and experience to address the threats to smart device security in a similar manner.

The Model: The Multi-Stakeholder Approach

Let me tell you more about what we did in applying the multi-stakeholder participation approach to other cyber-related challenges, and why we have good reason to believe it can work again when applied to smart devices.

We followed this collaborative approach with great success recently in our work with the FCC's Communications Security, Reliability and Interoperability Council, or CSRIC. CSRIC, and its predecessor organizations, have been working for over a decade on cybersecurity issues with success. In fact, a predecessor organization was one of the first federal entities to develop cybersecurity best practices.

Made up of industry leaders, academics, engineers, and federal partners, CSRIC made well-heralded recommendations in the spring of 2012 to help address critical private-sector Internet security vulnerabilities, including, among other key achievements, an anti-bot code of conduct for ISPs. That has now been subscribed to by ISPs representing 90 percent of broadband subscriptions. This is a voluntary solution gaining wide adherence developed through a multi-stakeholder process. That makes this botnet work a particularly important model because of the scope of the commitments to adhere to it.

In 2011, a prior CSRIC generated some other best practices that were relevant, such as providing recommendations on default settings that reduce vulnerability, fraud detection systems that detect caller anomalies, third-party security patch processes that are effective, and strong passwords, among other topics.

FCC Initiatives

Now, I want to mention a newer initiative to address mobile wireless security vulnerabilities that was undertaken by the FCC and follows this multi-stakeholder approach.

In addition to our own staff's stepped-up efforts over the past 1 ½ years to study smart device security problems, in the spring of this year, the FCC formed and chartered the Technology Advisory Council (the "TAC"). The TAC is a Federal Advisory Committee that was formed to advise us on the most pressing technology issues. The TAC includes top experts from industry who understand the key smart device security problems facing consumers and enterprises.

While the TAC will announce its mobile security recommendations to the FCC in December, its preliminary work, made known last month, suggests that it may recommend a number of targeted, voluntary mitigation measures that should be taken. These include seeking collaborative ways to partner with industry to:

- limit the exposure of older, less secure cellular technologies;
- reduce malware attacks or threats against network and vital services, including bots;
- reduce exposure from unsecure Wi-Fi access, particularly improving encryption in Wi-Fi links;
- reduce the incidence of mobile apps that contain malicious code; and
- limit end users' exposure to mobile malware and device theft or loss.

Although the TAC recognizes there are no "silver bullet" solutions to comprehensively address the wireless security threats, they believe taking the steps above are key to quickly responding to the rapidly growing exploitation of known wireless security vulnerabilities and will result in a significant reduction in the wireless security risks to mobile users. So, stay tuned for the TAC's release in December of recommendations on mobile security.

We look forward very much to the TAC's final recommendations.

Closing

There are many issues that we could talk about when it comes to mobile security. We might or might not agree on which ones deserve the greatest attention and in what order.

Meanwhile, the risks of cyber vulnerabilities to smart devices loom ever larger.

Each of these issues will have to be addressed and, given the trends, with a sense of urgency and purpose. But these issues can only be successfully attacked in an environment filled with so many different types of stakeholders if everyone agrees to step forward and participate in finding the right solutions. I am confident that, together, we can make a real difference in increasing the security of smart devices, while making full use of the tremendous new opportunities that smart devices have allowed us to enjoy.

We will continue to work with you to implement cybersecurity best practices for mobile security.