THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET September 28, 2016 | TTR not mapped yet | Mark Sableman

The serious security vulnerabilities of mobile devices

If you have wondered about security threats to your mobile device, a recent report of the National Institute of Standards and Technology may answer some of your questions – and increase your fears.

The report, "Assessing Threats to Mobile Device & Infrastructure," explains all the elements and systems of mobile devices, and assesses and catalogs security vulnerabilities.

The bottom line message: There are lots of security threats to mobile devices. And the report's cataloging of them is only the first step. NIST's National Cybersecurity Center of Excellence will be constructing a series of mobile security projects to address the threats, focusing first on threats that currently lack mitigation capabilities.

The report describes a consumer's cozy mobile device as a complex stack of hardware, firmware, operating system, application and device layers, communicating with the outside world through eight different methods, each of them often involving thousands of channels and multiple technologies.

Mobile devices are created through supply chains involving multiple vendors, especially in the case of Android devices. Moreover, the device acts within an ecosystem populated with communications networks, public and private app stores, vendor infrastructure, and enterprise systems.

The report essentially states that almost every one of these aspects of mobile devices is a potential point of security vulnerability.

A few highlights:

- Each of the eight different wired and non-wired device communication mechanisms (e.g., cellular, Wi-Fi, Bluetooth, GPS, etc.) "expose the device to a distinct set of threats."
- New SIM technology (the eSIM) will give users more flexibility in choosing or switching among networks, and at the same time they will "introduce a new set of threats."
- Supply chain threats are particularly troublesome and difficult to mitigate because of the continuing development process, particularly if the device firmware contains vulnerabilities.
- Even seemingly benign parts of the device, like the power port, constitute security threats, because of the dual use of those parts for both power and data.

These security vulnerabilities shouldn't just worry consumers: It's safe to say that every type of business is staffed – and led – by people who use mobile devices to communicate about the business, share business and financial data, and work with outside vendors or customers. In those instances, it's not just credit card data or family photos that are at risk to hackers – key business information or propriety products or services could be accessed at any time. Effective corporate cybersecurity response plans address mobile device security at all levels of employee use.

If you are interested in mobile device security, the report, particularly with its explanation of the systems and elements within mobile devices, is a great starting point. If you want to sleep well at night and not worry about your mobile device, read a novel instead.

“Each of these wireless and wired device communication mechanisms exposes a mobile device to a distinct set of threats and must be secured or the overall security of the device may be compromised.” Source: NIST, “Assessing Threats to Mobile Device & Infrastructure”

Mark Sableman is a partner in Thompson Coburn’s Intellectual Property and Privacy/Data Use and Security groups.

authorsTest

mark

Mark Sableman