wiley

ALERT

NIST and NCCoE Assess Threats to Mobile Devices and Infrastructure

September 13, 2016

Today, the National Institute of Standards and Technology (NIST), together with the National Cybersecurity Center of Excellence (NCCoE), requested public comment on a draft NIST Interagency Report (NISTIR) 8144, as well as a draft Mobile Threat Catalogue. This effort aims to "support development and implementation of mobile security capabilities, best practices, and security solutions to better protect enterprise information technology." The Mobile Threat Catalogue describes, identifies, and structures the threats posed to mobile information systems. NISTIR 8144, entitled "Assessing Threats to Mobile Devices & Infrastructure," offers background information on devices and their associated infrastructure, as well as provides an overview of the Mobile Threat Catalogue and the methodology used to create it. Responses are due October 12, 2016.

NIST and NCCoE have identified and categorized potential threats and mitigations, drawing from various sources. They seek public input to validate their initial work, and to help them develop a final Mobile Threat Catalogue and NISTIR 8144 publication. These efforts are undertaken to support the Department of Homeland Security's (DHS) fulfillment of Section 401 of the Cybersecurity Information Sharing Act of 2015 (CISA), which requires it to conduct a study on threats relating to the security of the mobile devices of the federal government and submit a final report to Congress. The Mobile Threat Catalogue and NISTIR 8144 will be used to inform DHS's final report to Congress. DHS just last month received comments in response to a Request for Information on mobile security threats and defenses, and DHS is working with NIST and NCCoE to leverage those comments to further develop the Mobile Threat Catalogue and NISTIR 8144.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Madeleine M. Lottenbach
Partner
202.719.4193
mlottenbach@wiley.law

Practice Areas

Telecom, Media & Technology

NIST seeks public comment on aspects of the entire ecosystem, including:

- Mobile Applications—including software vulnerabilities and malware-based threats;
- Mobile Device Technology Stack—including potential threats to the mobile operating system, device drivers, isolated execution environments, boot firmware, baseband subsystem, and SIM card;
- Cellular—including potential risks to the air interface, small cells, messaging services, infrastructure, interoperability, and voice over LTE network (VoLTE);
- Local Area Networks and Personal Area Networks—including issues related to WiFi, Bluetooth, and near field communication;
- Authentication—including potential risks to user-to-device, user-to-remote service, or user-to-network authentication;
- Supply Chain—including concerns about device and component supply chains;
- Physical Access—including possible threats originating from outside of the device, such as device loss and malicious charging stations;
- Ecosystem—including issues related to the mobile operating system and vendor infrastructure, native public stores, private enterprise stores, and third-party stores;
- Enterprise Mobility Management (EMM)—including various issues in managing and monitoring an enterprise's device pool; and
- Mobile Payment—including mobile payment technologies, NFC-based payments, and credit card tokenization.

These are complex and rapidly-changing topics with varied technical and policy implications. NIST and NCCoE will benefit from broad input on their methodology and approach, as well as on different mobile contexts and use cases, the relative severity (or lack thereof) of risks, real-world considerations regarding exploitation, and as the utility of potential countermeasures.

As many other agencies are looking at cybersecurity and mobility, this is another area of government interest. These NIST and NCCoE efforts will be part of further discussion on security at DHS and in Congress, particularly as the Federal Government looks to procure systems, develop sound mobility management policies, and support industry efforts to advance reasonable security across the mobile ecosystem.