New NIST resources help organizations protect systems from mobile threats

September 15 2016

Credit: Unsplash/CC0 Public Domain

IT security departments have used guidance from NIST and other sources to help them defend the vulnerable connections between mobile devices and enterprise computer systems from malware, viruses and

other types of attacks. Recently, organizations from both the public and private sectors have requested more specific information on threats and ways to mitigate them.
The draft Mobile Threat Catalogue (MTC) and the accompanying draft Assessing Threats to Mobile Devices & Infrastructure (NIST Interagency Report 8144) seek to answer those requests.

"Often IT shops or security managers will address or secure the apps on a phone and protect the operating system from potential threats," NIST cybersecurity engineer Joshua Franklin said. "But there is a much wider range of threats that need to be addressed. For example, enterprise security teams often don't focus on the cellular radios in smartphones, which, if not secured, can allow someone to eavesdrop on your CEO's calls."

The catalogue lists mobile threats in numerous areas, including authentication, supply chains, physical access, payment, ecosystem and network protocols, technologies and infrastructure. It also covers mobile security concerns involving the Global Positioning System, WiFi, Bluetooth and mobile payments, as well as commonly known, broadly understood mobile device-related security threats such as mobile malware.

The MTC categorizes the known threats and provides available information about each threat, including countermeasures to reduce the impact of a particular threat when available. The catalogue supports development and implementation of mobile security capabilities, best practices and security solutions to protect the IT systems in organizations.

Assessing Threats to Mobile Technologies & Infrastructure provides background on the threats associated with mobile devices listed in the catalogue and provides context around the MTC. The report also calls

for a new perspective on mobile security—expanding the view to include the entire mobile security ecosystem, including threats that occur through cellular networks, cloud infrastructure and app stores.

The catalogue was created in part in response from earlier work at NIST's National Cybersecurity Center of Excellence (NCCoE), draft NIST SP 1800-4 Mobile Device Security: Cloud and Hybrid Builds . Authors also used data from responses to a 2015 Request for Information on Mobile Threats and Defenses and interviews with security experts from major corporations. NIST worked with the Department of Homeland Security Science & Technology Directorate on the Mobile Threat Catalogue and NISTIR 8144, which will be used to inform the Study on Mobile Device Security, due to Congress in December 2016, as a part of Title IV, Section 401 of the Cybersecurity Act of 2015 (Division N of the Consolidated Appropriations Act, 2016). The MTC also will help guide future research projects by the NCCoE.

More information: To strengthen the catalogue, the authors request practitioners and experts in the field to review the catalogue and provide feedback and additional information. Please send comments on both projects to Nistir8144@nist.gov

Provided by National Institute of Standards and Technology