September 2012

Information Security

Better Implementation of Controls for Mobile Devices Should Be Encouraged

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-757, a report to congressional committees

Why GAO Did This Study

Millions of Americans currently use mobile devices—e.g., cellphones, smartphones, and tablet computers—on a daily basis to communicate, obtain Internet-based information, and share their own information, photographs, and videos. Given the extent of consumer reliance on mobile interactions, it is increasingly important that these devices be secured from expanding threats to the confidentiality, integrity, and availability of the information they maintain and share.

Accordingly, GAO was asked to determine (1) what common security threats and vulnerabilities affect mobile devices, (2) what security features and practices have been identified to mitigate the risks associated with these vulnerabilities, and (3) the extent to which government and private entities have been addressing the security vulnerabilities of mobile devices. To do so, GAO analyzed publically available mobile security reports, surveys related to consumer cybersecurity practices, as well as statutes, regulations, and agency policies; GAO also interviewed representatives from federal agencies and private companies with responsibilities in telecommunications and cybersecurity.

What GAO Recommends

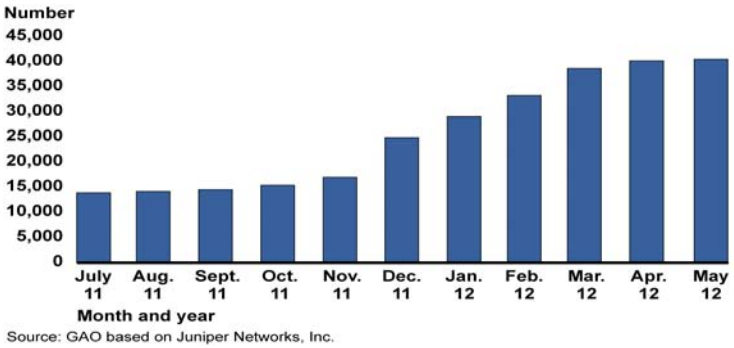
GAO recommends that FCC encourage the private sector to implement a broad, industry-defined baseline of mobile security safeguards. GAO also recommends that DHS and NIST take steps to better measure progress in raising national cybersecurity awareness. The FCC, DHS, and NIST generally concurred with GAO's recommendations.

View GAO-12-757. For more information, contact Gregory C. Wilshusen at 202-512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

Threats to the security of mobile devices and the information they store and process have been increasing significantly. For example, the number of variants of malicious software, known as "malware," aimed at mobile devices has reportedly risen from about 14,000 to 40,000 or about 185 percent in less than a year (see figure). Cyber criminals may use a variety of attack methods, including intercepting data as they are transmitted to and from mobile devices and inserting malicious code into software applications to gain access to users' sensitive information. These threats and attacks are facilitated by vulnerabilities in the design and configuration of mobile devices, as well as the ways consumers use them. Common vulnerabilities include a failure to enable password protection and operating systems that are not kept up to date with the latest security patches.

Figure: Number of Malware Variants Identified Globally between July 2011 and May 2012



Source: GAO based on Juniper Networks, Inc.

Mobile device manufacturers and wireless carriers can implement technical features, such as enabling passwords and encryption to limit or prevent attacks. In addition, consumers can adopt key practices, such as setting passwords and limiting the use of public wireless connections for sensitive transactions, which can significantly mitigate the risk that their devices will be compromised.

Federal agencies and private companies have promoted secure technologies and practices through standards and public private partnerships. Despite these efforts, safeguards have not been consistently implemented. Although the Federal Communications Commission (FCC) has facilitated public-private coordination to address specific challenges such as cellphone theft, it has not yet taken similar steps to encourage device manufacturers and wireless carriers to implement a more complete industry baseline of mobile security safeguards. In addition, many consumers still do not know how to protect themselves from mobile security vulnerabilities, raising questions about the effectiveness of public awareness efforts. The Department of Homeland Security (DHS) and National Institute of Standards and Technology (NIST) have not yet developed performance measures or a baseline understanding of the current state of national cybersecurity awareness that would help them determine whether public awareness efforts are achieving stated goals and objectives.