Chapter 47
Mobile Devices: The Case for Cyber Security Hardened Systems

Maurice Dawson
University of Missouri – St. Louis, USA

Jorja Wright
Florida Institute of Technology, USA

Marwan Omar
Nawroz University, Iraq

ABSTRACT

Mobile devices are becoming a method to provide an efficient and convenient way to access, find and share information; however, the availability of this information has caused an increase in cyber attacks. Currently, cyber threats range from Trojans and viruses to botnets and toolkits. Presently, 96% of mobile devices do not have pre-installed security software while approximately 65% of the vulnerabilities are found within the application layer. This lack in security and policy driven systems is an opportunity for malicious cyber attackers to hack into the various popular devices. Traditional security software found in desktop computing platforms, such as firewalls, antivirus, and encryption, is widely used by the general public in mobile devices. Moreover, mobile devices are even more vulnerable than personal desktop computers because more people are using mobile devices to do personal tasks. This review attempts to display the importance of developing a national security policy created for mobile devices in order to protect sensitive and confidential data.

INTRODUCTION

Currently, mobile devices are the preferred device for web browsing, emailing, using social media and making purchases. Due to their size, mobile devices are easily carried in people's pockets, purses or briefcases. Unfortunately, the popularity of mobile devices is a breeding ground for cyber attackers. Operating systems on mobile devices do not contain security software to protect data. For example, traditional security software found in personal computers (PCs), such as firewalls,

DOI: 10.4018/978-1-4666-8751-6.ch047

antivirus, and encryption, is not currently available in mobile devices (Ruggiero, 2011). In addition to this, mobile phone operating systems are not frequently updated like their PC counterparts. Cyber attackers can use this gap in security to their advantage. An example of this gap in security is seen in the 2011 Valentine's Day attack. Cyber-attackers dispersed a mobile picture-sharing application that covertly sent premium-rate text messages from a user's mobile phone (Ruggiero, 2011). Thus, this example illustrates the importance of having a security policy for mobile phones.

Social Networking and Electronic Commerce (E-Commerce) Applications

Many people rely on their mobile devices to do numerous activities, like sending emails, storing contact information, passwords and other sensitive data. In addition to this, mobile devices are the device of choice when it comes to social networking; thus, mobile applications for social networking sites (Facebook, Twitter, Google+) are another loophole for cyber attackers to gain personal data from unsuspecting users (Ruggiero, 2011). Social networking sites are host to a surplus of personal data. That is why malicious applications that use social networking sites to steal data yield severe consequences. Recently, M-Commerce or "mobile e-commerce" has gained popularity in our society. Many smartphone users can now conduct monetary transactions, such as buying goods and applications (apps), redeeming coupons and tickets, banking and processing point-of-sale payments (Ruggiero, 2011). Again, all of these smartphone functions are convenient for the user but advantageous for malicious cyber attackers. Ultimately, there is a niche in technology for cyber security software that is specifically designed for the mobile operating system.

Hypothetical Consequences of Cyber Attacks on Smartphones

The consequences of a cyber attack on a smartphone can be just as detrimental, or even more detrimental than an attack on a PC. According to Patrick Traynor, a researcher and assistant professor at the Georgia Tech School of Computer Science, mobile apps rely on the browser to operate (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). As a result of this, more Web-based attacks on mobile devices will increase throughout the year. Traynor also states that IT professionals, computer scientists and engineers still need to explore the variations between mobile and traditional desktop browsers to fully understand how to prevent cyber attacks (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012).

Challenges with a Mobile Browser

One cyber security challenge for mobile devices is the screen size. For example, web address bars (which appear once the user clicks on the browser app) disappear after a few seconds on a smartphone because of the small screen size (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This is usually the first-line of defense for cyber security. Checking the Uniform Resource Locator (URL) of a website is the first way users can insure that they are at a legitimate website. Moreover, SSL certificates for a website are usually more difficult to find on a mobile phone browser (Traynor, Ahamad, Alperovitch, Conti, & Davis, 2012). This adds another gap in security for mobile devices. Furthermore, the touch-screen attribute of mobile phones can be cause for concern when dealing with cyber attackers. Traynor states that the way elements are placed on a page and users' actions are all opportunities to implant an attack. An illustration of this is seen when an attacker creates