CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Mobile Device Security: Threats, Risks, and Actions to Take

Key Message: Internet-connected mobile devices are becoming increasingly attractive targets.

Executive Summary

"Today's advanced mobile devices are well integrated with the Internet and have far more functionality than mobile phones of the past. They are increasingly used in the same way as personal computers (PCs), potentially making them susceptible to similar threats affecting PCs connected to the Internet. Since mobile devices can contain vast amounts of sensitive and personal information, they are attractive targets that provide unique opportunities for criminals intent on exploiting them. Both individuals and society as a whole can suffer serious consequences if these devices are compromised." [1]

In this podcast, Jonathan Frederick, a member of CERT's Workforce Development team discusses the increasing threats to mobile devices and some ways to mitigate their impact.

PART 1: WHY MOBILE DEVICES ARE BECOMING MORE VULNERABLE

More Attractive Targets

The features that are making devices such as smart phones more popular are also making them more attractive as targets, including the ability to

- send and receive text and multi-media messages
- connect to the internet via wireless networksthe ongoing operations of a government
- be located using the device's GPS (global positioning system) capabilities
- connect to a personal computer to transfer files and manage the mobile device
- conduct financial transactions be located using the device's GPS (global positioning system) capabilitiesthe ability of critical infrastructures to continue to function

More Vulnerable

Mobile devices typically lack the security software that resides on personal computers such as firewalls, intrusions detection systems, and virus protection. This makes them more vulnerable to attack.

Today's smart phones are capable of storing sensitive information such as corporate and financial data, keys for VPN (virtual private network) access, and other authentication credentials.

Mobile carriers like to take advantage of device GPS capabilities to sell additional services such as child location trackers for parents, so GPS is built into most new devices.

Once an iPhone is connected to an unsecured wireless LAN (local area network), it will automatically connect to any network with the same name without asking the device owner's permission to connect. These LANs can be controlled by attackers. This is of concern as all new Linksys and Cisco wireless routers are named the same by default.

Users Generally Unaware

Most users have not experienced security issues with their mobile devices that match their experiences with personal computers.

A 2009 Trend Micro survey reports that 77 percent of users do not enable any security features on their mobile devices. Users do not want to be inconvenienced.

PART 2: GROWING THREATS TO DEVICES AND BACK-END SYSTEMS

Trends To Pay Attention To

In early 2009, 16 percent of the market had smart phones; in early 2010, this has increased to 23 percent. This number may be close to 50 percent within 2 to 3 years.

As smart phone use increases, device carriers (Verizon, AT&T, Cingular) will likely stop selling voice-only phones, since smart phones come with additional services such as data plans and multimedia messaging plans and carriers are in the business of selling services.

Increasing Criminal Interest

According to a Data Innovation Corporation survey , 70 percent of smart phone users are checking bank account balances using their smart phone. Forty percent are transferring funds and 29 percent are paying bills.

Attackers can launch man-in-the-middle attacks to redirect funds accessed by mobile devices.

New Applications

PayPal provides an application where a financial transaction is performed by bumping two iPhones together. In addition, credit cards can be swiped by using a small sugar-cube-sized device that connects to a smart phone and reads the magnetic strip data.

Criminals Target Most Commonly Used Operating Systems

According to a Nielson Company survey, 91 percent of smart phones use one of the following operating systems: Blackberry, Apple iPhone, Windows Mobile, or Android.

Criminals will target one or more of these operating systems when developing malicious applications and spyware, so they can attack the largest number of mobile devices.

Apps and Malware

The community is developing new applications every day for all of our mobile devices. Users often download these without ever thinking about security. Intruders can develop malware that is bundled with legitimate applications.

One specific case involved a Windows Mobile 3D shooter application that autodialed premium rate phone numbers, charging these to the smart phone owner without their knowledge.

Security Threats Migrating to Mobile Devices

As mobile devices become more internet-connected, they will experience more of the following threats:

- malicious applications containing malware and spyware. Such malware can steal information resident on the mobile device. It can also use the mobile device as a point of connection to launch denial-of-service attacks on an entire corporate network.
- commands and dialing services that the user does not intend (at great cost)
- voice and data transmissions, text messages, and call logs being intercepted (violations of privacy)
- the mobile device GPS locator being used to track an individual’s physical location (stalking)

Risks to Back-End Systems that Are Used by Mobile Devices

Back-end systems, used by mobile device service providers, typically store and process much of the same information as the device itself.

Attackers can compromise a back-end server and gain access to all of the information that is on user mobile devices that connect to that server. This happened to Paris Hilton in 2005, when the T-mobile server that stored her contact information was compromised, resulting in her information being posted on the internet.

Blackberry servers are known to have a number of vulnerabilities, which, if exploited, could greatly compromise a corporation's servers and networks, and allow unauthorized access to corporate information.

PART 3: MITIGATE MOBILE DEVICE SECURITY RISKS

Actions to Take

The first step is to perform a risk analysis, to determine what information should or should not be stored on mobile devices.

When performing device selection, make sure device security is high on the list of selection criteria. For example, Blackberry encrypts all data on mobile devices so if you lose it, your data is not easily accessed.

Determine what device features are essential versus nice to have. For example, the U.S. Air Force has disabled multimedia text messaging for their organizational Blackberrys. They also restrict users from installing applications and have disabled most Bluetooth features.

Organization- versus Personally-Owned Devices

Most organizations do not permit users to connect their personal mobile devices to the organization's network

Organization-owned devices that are provided to users to conduct business are carefully configured. They can also be certified and accredited.

Given that almost everyone owns some type of mobile device, it can be challenging to determine when personal devices can and cannot be used to conduct business. Alternatively, some users may be required to carry two devices: one for business and one for their personal use. If there is critical data that needs to be protected while being accessed by mobile devices, this requirement can help inform the risk analysis to determine if a business-controlled and -owned device is needed.

Data on a PC versus Data on a Mobile Device

Desktop and laptop computing devices typically are subject to policies and procedures, and contain security software. So they tend to be more secure than mobile devices. As a result, some organizations are providing guidelines that require data to be accessed using a netbook, and not by a mobile device such as a smart phone.

Resources

[1] US-CERT Technical Information Paper TIP-10-105-01 " Cyber Threats to Mobile Devices," April 15, 2010.

U. S. National Institute of Standards and Technology SP 800-124 Guidelines on Cell Phone and PDA Security , October 2008

U.S. Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) Security Technical Implementation Guides (STIGS) and Supporting Documents

EDUCAUSE “ Ten Steps to Secure Your Mobile Devices ”

Vendor web sites including Apple (for iPhone) and Blackberry