Mobile Applications Security

Eugene Schultz, Ph.D., CISSP, CISM, GSLC
Chief Technology Officer
Emagined Security
EugeneSchultz@emagined.com
ISSA-Los Angeles
Los Angeles, California
January 19, 2011
The smartphone revolution

- Although there is no formal definition of “smartphone,” an informal definition is that smartphones are mobile phones that have advanced computing capabilities (often approaching those of PCs)
- The number of smartphone users around the world is unknown
- One study shows that sales of smartphones are increasing by 15 percent every year
- Trend—increasing use of smartphones intended for business for personal reasons instead
Smartphones: A target-rich environment for attackers

- Statistics from the UK Department of Trade and Industry-backed Information Security Breaches Survey show that more than half of the companies surveyed do not have any controls in place for securing company information on smart phones.
- Although more organizations have smart phone policies than two years ago, comparatively few companies have invested in technology to manage and protect these devices.
Smartphone applications: “Where the action is”

- Types of functionality include
  - Controlling or interacting with appliances that are part of the corporate network
  - Monitoring and/or remotely controlling desktop computers and/or Web servers
  - Monitoring and troubleshooting remote networks
  - Personal use
- Most are free
- Major limitation: small size of smartphone’s screen
Kinds of applications available

- Accounting
- Books
- Business
- Chat
- Cookbooks
- Educational
- Energy
- Entertainment
- Finance
- Games
- Gardening
- Health and fitness
- Lifestyle
- Music

- Navigation
- Network troubleshooting
- Photography
- Productivity
- Reference services
- Religious
- Social networking
- Sports
- Travel
- Utilities
- More…
Examples of iPhone applications

- 101 Cookbooks
- goMovies
- iPhlickr
- iPhoneDigg
- iActu
- Gas.app
- iZoho
- Google Reader
- iPhoneChat
- OneTrip Shopping List
- BumpIt
- Much more…
Security issue: “Jailbreaking” iPhones (1)

• When an iPhone is installed, it stays in a “factory state”
  ➢ Intended to be changed only as the result of Apple upgrades
• To install some applications on an iPhone, it is necessary to “jailbreak” the phone
• Jailbreaking means overwriting the phone’s firmware to
  ➢ Install application bundles
  ➢ Unlock baseband firmware that keeps the iPhone from doing things such as connecting to another service provider’s 3G network
Security issue: “Jailbreaking” iPhones (2)

- Jailbreaking may not sound like a big deal, but it:
  - Voids the iPhone service warranty
  - Produces numerous changes in the iPhone that may cause the best of iPhone forensics efforts to be thrown out in a court of law
  - Can expose the iPhone to a wider range of attacks
Vulnerabilities in smartphone applications (1)

• Because applications are intended for single-user contexts, there is little or no authentication and authorization in most smartphone applications
• Password-related vulnerabilities
  ➢ Default passwords
  ➢ If there is a password, it is likely to consist of very few characters
• Several critical security functions are almost always missing
  ➢ Data encryption
  ➢ Auditing
  ➢ Security indicators (e.g., padlocks) on Web browsers
  ➢ Security updates
Vulnerabilities in smartphone applications (2)

• Ability of applications to
  - Access any file on the smartphone
  - Do anything they want to do to the operating system with full privileges
  - Drain a smartphone’s battery, causing denial of service
• It is almost impossible to determine whether or not smartphone applications are malicious until you download them
• One recent study showed that mobile device users are even more susceptible to phishing than normal desktop computer users!
Major security controls for smartphones (1)

- Appropriate policy and standards
- Using anti-virus and anti-spyware software
- Remediation of vulnerabilities
- Strong authentication
- Encrypted network transmissions through VPNs, SSH, SFTP, and more
- Secure Wireless Application Protocol (WAP) gateways
Major security controls for smartphones (2)

- Personal firewalls
- Hard drive encryption
- Regular backups
- User security training and awareness
- More…
Major types of built-in security controls for smartphone applications

(This slide was intentionally left blank!)
The truth about security controls for smartphone applications

• Most mobile application developers do not consider security at all when they code
• Almost no information about the security of mobile applications exists
  ➢ The most widely used security model is very deficient
  ➢ Security standards? Where are they?
  ➢ Most mobile applications have not been tested for vulnerabilities
• Exception: Windows Mobile-based smartphone applications
  ➢ Digital code signing for proof of each application’s origin
  ➢ Logo certification—validation that an application meets Windows Mobile implementation guidelines
Trust and privilege levels in Windows Mobile application security

• Privileged vs. unprivileged execution mode—determines application’s access level to smartphone features and application programming interfaces (APIs)*
  ➢ Privileged trust—full access to the system and APIs
  ➢ Unprivileged trust—limited access to the system and APIs

• Untrusted applications cannot
  ➢ Be loaded on a smartphone
  ➢ Access the operating system and APIs

• The operator can select a security policy that can
  ➢ Make untrusted applications run with unprivileged access
  ➢ Require that applications be digitally signed

* - Certificates are stored in two certificate stores, one for privileged execution mode, the other for unprivileged mode
<table>
<thead>
<tr>
<th>Policy</th>
<th>Unprivileged execution mode</th>
<th>Privileged execution mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrestricted</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Standard certificate</td>
<td>None</td>
<td>Operator privileged certificate required</td>
</tr>
<tr>
<td>Restricted certificate</td>
<td>Mobile2Market unprivileged certificate required</td>
<td>Operator privileged certificate required</td>
</tr>
</tbody>
</table>
• Certificate-based code signing has proven itself to be a weak method of countering malicious code
  ➢ Is at best an *indirect* method of protecting against malicious code execution
  ➢ Forged certificates are a constant concern
  ➢ When a dialog box asking users if they want to continue executing a program, they almost always say “yes,” no matter what
  ➢ Is the method used with ActiveX controls
The bad news (2)

**Designed For Windows Mobile Logo Test**

Microsoft has discontinued the Mobile2Market Program and Designed for Windows Logo Test Program effective February 18, 2010.

If you have any questions, please go to [http://msdn.microsoft.com/en-us/windowsmobile/dd569132.aspx](http://msdn.microsoft.com/en-us/windowsmobile/dd569132.aspx) or contact Microsoft at asc@microsoft.com.
App Stores: Do they Help Security?

- All state that they screen applications, but no specifics are provided
- Informal evidence suggests that
  - The Apple iTunes App Store is more concerned about potentially offensive application content than anything else
  - The BlackBerry App World cares mostly about applications causing BlackBerrys to crash or hang
  - Symbian’s application screening consists only of virus scanning
- It is easy to bypass App Stores when downloading mobile applications
The “bottom line”

- An increasing percentage of critical business processes involves use of mobile devices
- The use of mobile applications per se is not usually a major security risk, BUT
  - If vulnerabilities in them are exploited, mobile devices, data stored on them, and networks that can be reached through them can be compromised
  - Use of many mobile applications can be a violation of an organization’s acceptable use policy
- Also consider mobile computing in regulatory compliance risk management
So where do you start re. smartphone application security? (1)

- Find out as much as you can about
  - The type and range of applications your organization’s mobile phone users are using
  - Vulnerabilities and security features in these applications
  - Applications that may have better security than currently used or candidate ones
- Start including mobile computing in the risk management process
  - Asset inventory
  - Threat and vulnerability analysis
  - Risk analysis
  - Controls selection and implementation
  - Controls evaluation
So where do you start re. smartphone application security? (2)

• Begin creating
  ➢ Policy provisions that address mobile computing operating system and application security risks
  ➢ Security standards for mobile computing operating systems and applications
  ➢ Preliminary audit procedures
Conclusion

• Achieving adequate levels of security with mobile devices and applications is a very difficult task
• A good starting point in controlling smartphone-related security risk is focusing on
 ➢ Risk assessment
 ➢ Policy and standards
• Final suggestion—also begin preparing for when your organization starts developing its own mobile applications!
Questions?

Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
+1 (650) 593-9829
eugeneschultz@emagined.com
Web: www.emagined.com
Blog: baylinks.com/blogs
Dashboard: dashboard.emagined.com

For a PDF copy of these slides send email to:
seminar@emagined.com