Understanding the Risks of Mobile Applications
Background

Modern mobile applications run on mobile devices that have the functionality of a desktop or laptop running a general purpose operating system. In this respect many of the risks are similar to those of traditional spyware, Trojan software, and insecurely designed apps. However, mobile devices are not just small computers. Mobile devices are designed around personal and communication functionality which makes the top mobile applications risks different from the top traditional computing risks.

The Mobile Stack: Risks At Every Layer

To put mobile app risk in perspective we need to look at the other sources of risks on the mobile computing platform. The following is a summary of the risks. For a more in depth look see the Veracode blog post, Identifying the Mobile Security Stack.

- **Infrastructure**: Interception of data over the air.
  - Mobile WiFi has all the same problems as laptops
  - GSM has shown some cracks. Chris Paget demo DEFCON 2010

- **Hardware**: Baseband layer attacks
  - Memory corruption defects in firmware used to root your device
  - Demonstrated at CCC/Black Hat DC 2011 by Ralf-Philipp Weinmann

- **OS**: Defects in kernel code or vendor supplied system code
  - iPhone or Android jailbrakes are usually exploiting these defects

- **Application**: Apps with vulnerabilities and malicious code have access to your data and device sensors
  - Your device isn’t rooted but all your email and pictures are stolen, your location is tracked, and your phone bill is much higher than usual.

Threat Model

The threat model is different for mobile devices. There is much more risk to private data being stolen or leaked due to the portable nature of the devices and the types of applications that are used. Here is a list of some of the significant difference from traditional computing environments:

- Mobile devices are frequently shared temporarily
- Mobile apps are highly connected to web services
- Mobile apps interact with device sensors such as microphones, cameras, and location detection.
- Mobile devices have payment capability
- Mobile devices are often consumer owned devices that can access an organization’s internal network
- Mobile devices must communicate over a wireless network
- Mobile devices have a higher likelihood of being lost or stolen
- Mobile apps are delivered from an app store
- Mobile apps are updated frequently
Many security experts are waiting for a mobile email worm attack or a mobile bot network to spring up before they agree that there are significant mobile computing risks. While these things could happen and happen soon there are other risks that have already been brought to light through real world incidents. Many of these incidents are the basis of the Top 10 Mobile App Risks which Veracode created to highlight the most serious risks from mobile applications.

The Mobile App Top 10

The Mobile Top 10 can be used to determine the coverage of a security solution which can protect against these risks. A mobile app security solution can declare its coverage of the Mobile App Top 10 so customers can understand what risks the solution mitigates. Mobile app security solutions can be used in the development of an app, as part of an app store vetting process, for acceptance testing of an app, or for security software running on a mobile device.

There are 2 main categories of mobile app risks. The category of Malicious Functionality is a list of unwanted and dangerous behaviors that are stealthily placed in a Trojan app that the user is tricked into installing. The user thinks they are installing a game or utility and instead get hidden spyware, phishing UI, or unauthorized premium dialing.

1. Malicious Functionality
   - Activity monitoring and data retrieval
   - Unauthorized dialing, SMS, and payments
   - Unauthorized network connectivity (exfiltration or command & control)
   - UI Impersonation
   - System modification (rootkit, APN proxy config)
   - Logic or Time bomb

The category of Vulnerabilities are errors in design or implementation that expose the mobile device data to interception and retrieval by attackers. Vulnerabilities can also expose the mobile device or the cloud applications used from the device to unauthorized access.

2. Vulnerabilities
   - Sensitive data leakage (inadvertent or side channel)
   - Unsafe sensitive data storage
   - Unsafe sensitive data transmission
   - Hardcoded password/keys

The Veracode Mobile App Top 10 document contains a detailed description of these risks with accompanying real world examples.
The Mobile App Delivery Mechanism

Mobile applications are installed differently than traditional software. The CD-ROM is not a supported distribution method. While on some devices you can install over USB from a laptop or desktop computer, typically apps are downloaded over the air from either a web site or an app store. App stores have the potential to screen out malicious or vulnerable apps. If an app store scans app for malicious or vulnerable code, sometimes called whitelisting, then users who get their applications from that app store will benefit from improved security.

All mobile platforms have app signing. The mobile OS will not allow apps that are not signed to execute. An exception to this is jailbroken OSes which are jailbroken by their users specifically to allow unsigned apps to run. Depending on the implementation of the signing mechanism it can be a big benefit for security. If the application is signed by the developer with a self-generated key there is little security gain, but if the application is signed by a key issued by the platform provider then there will be a security benefit based on the policies the platform provider adheres to for approving apps. Needless to say, jailbreaking removes the security benefits of the platform signing mechanism.

All mobile platforms support revocation to remove malicious apps once detected. This is a good last chance security mechanism but shouldn’t be the primary one. Unfortunately history tells us that malicious apps are typically able to compromise hundreds of thousands of users before they are detected and revoked.

The following is a chart showing the app delivery security mechanisms in place for the major platforms.

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>SIGNING</th>
<th>REVOCATION</th>
<th>SIGNING</th>
<th>SIGNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>Anonymous, self-signed</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>iOS</td>
<td>Signed by Vendor</td>
<td>Yes</td>
<td>Yes</td>
<td>Policy &amp; Quality</td>
</tr>
<tr>
<td>Blackberry</td>
<td>Signed with Vendor issued key</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Phone</td>
<td>Signed by Vendor</td>
<td>Yes</td>
<td>Yes</td>
<td>Policy, Quality &amp; Security</td>
</tr>
<tr>
<td>Symbian</td>
<td>Signed by Vendor</td>
<td>Yes</td>
<td>No</td>
<td>Quality</td>
</tr>
</tbody>
</table>

If an App store is not required is means that the user is free to choose an app store or download apps directly from the web. If the user wants to get the security benefits of an app store approval process they will need to restrict their app installation from only the platform app store.
Other Mobile Risk Lists

The mobile computing landscape is rapidly evolving and other organizations are working to enumerate and prioritize the risks. The Open Web Applications Security Project (OWASP) is well known for their OWASP Top Ten list which lists the most important web application vulnerabilities. They now have an OWASP Mobile Security Project that is working on a Mobile Top Ten.

Another team working on documenting mobile risks is ENISA, the European Network and Information Security Agency. They have published the report, “Smartphones: Information security risks, opportunities and recommendations for users.”

Solutions

Veracode provides the world’s leading application risk management platform. Veracode’s patented and proven solution leverages static binary analysis to provide unique coverage for mobile applications. Organizations can use Veracode to provide attestation of the security of mobile applications they develop, or to verify that the mobile applications they purchase and distribute are free from security issues. Mobile applications need to be tested for vulnerabilities just like any other application with access to data or access to transactions that need to be protected. Static binary analysis is an excellent technique for testing mobile apps.

Mobile applications may have several types of security risk: language inherent risk, based on common security flaws in the language; malicious data exfiltration, in which sensitive data is surreptitiously transmitted from the phone; and platform specific risk, based on specific vulnerabilities inherent in the mobile platform. Specific examples are discussed below.

Language specific flaws

Mobile applications inherit a certain amount of risk from the languages in which they are written. While some of this risk may be mitigated by the runtime environment in which the applications are deployed, there may still be threats to the confidentiality, integrity, or availability of the application and the data that it accesses from flaws of this kind. Examples of the types of language-related flaws that Veracode’s scans may detect include:

- Cryptographic flaws
- Credentials management
- Code quality
- Buffer overflows
- Numeric flaws
- Information leakage
Malicious Data Exfiltration flaws

Mobile data exfiltration is defined as the deliberate dissemination of sensitive information from a mobile handheld device to a third party via common data transmission methods. Based in Veracode’s groundbreaking work on malicious data exfiltration in conventional applications, the primary goal of the malicious data exfiltration scan is to determine if a piece of mobile binary code presents a risk via deliberate data disclosure.

- Examples of the kinds of malicious behavior that Veracode’s scans may detect include:
  - Deliberate transmission of address book data, email, phone log, or SMS
  - Surreptitious transmission of microphone, GPS, or camera data
  - Exfiltration via sockets, e-mail, HTTP, SMS, DNS, ICMP, IR

Many will think “privacy” when they see the above and clearly personal private data is a hot button topic right now for mobile devices. Corporate data is also at risk as it is often in the very same email inboxes as private data.

Conclusion

Every new information technology platform delivers new benefits and new risks. Applications running on these platforms contribute a large portion of the risk. Veracode’s Application Risk Management approach is to cover all software that puts an organization at risk no matter the source: vendor, internally developed, open source or outsourced. Mobile applications are no different. Whether you are building mobile apps or purchasing them for your workforce they should be independently analyzed for the top risks.

About Veracode

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics Veracode enables scalable, policy-driven application risk management programs that help identify and eradicate numerous vulnerabilities by leveraging best-in-class technologies from vulnerability scanning to penetration testing and static code analysis. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud. Veracode works with customers in more than 80 countries worldwide including Global 2000 brands such as Barclays PLC and Computershare as well as the California Public Employees’ Retirement System (CalPERS) and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, follow on Twitter: @Veracode or read the ZeroDay Labs blog.