This point-of-view paper discusses application security and enterprise vulnerability and outlines best practices to ensure security in mobile application development.

**Introduction**

Any computing device containing sensitive information that also has access to the internet is vulnerable to security attacks — especially smartphones and mobile devices. A report by Symantec ranks mobility as the “leading IT risk among organizations — more than any other initiative, including virtualization, Web 2.0 and even public cloud computing.”

However, mobility is imperative in today’s rapidly changing market, providing many advantages for businesses, customers and employees. It’s no wonder organizations continue to spend millions to ensure, safeguard and secure mobile environments. How can you increase security for mobile devices, despite the varied threats that can strike at any time? More specifically, how can you ensure security across every aspect of mobility operations — network, data, applications and devices?

Companies need to set up standard secure practices as they develop an application, keeping in mind the following concerns:

- **Data**: How does the application fetch and display data?
- **Network**: How does the application access networks?
- **Device**: How vulnerable is the device to loss or theft?
- **Application**: How securely and effectively is the application coded?

To truly secure mobile solutions, companies need to answer these questions, so they can effectively provide proactive and continuous monitoring. They can also reuse the security frameworks and practices they establish — improving maintenance at a greatly reduced cost.
Written by:
Shailesh Wankhade

Shailesh is a Practice Manager with the Enterprise Mobility group at Dell Services. He has more than a decade of experience in business-engineering mobility and embedded solutions for enterprises.

Table of contents

The mobile ecosystem and inherent threats .............................................. 3
Secure application development practices ........................................... 4
  Designing the application ................................................................. 4
  Developing the application ............................................................. 5
  Testing the application ................................................................. 5
  Deploying and maintaining the application ..................................... 5
Conclusion .......................................................................................... 6
While a consumer is only concerned with the security of the mobile device, operating system (OS) and applications, enterprises have much more complex issues to manage — such as physical security, data storage, authentication and safe browsing practices. In the enterprise mobile ecosystem, there are multiple factors involved including:

- Mobile devices with varying degrees of resolution
- Five or more mobile operating systems, with different versions
- One or more platforms
- Applications growing in number and variety

What makes mobile devices vulnerable to security threats? The diversity and complexity of devices, hardware, operating systems and platforms can make it challenging to create a system to secure all of the configurations.

Mobile browser security is also limited compared to desktops browsers. For example, due to the smaller screen size, mobile devices rarely show the entire URL — leaving a user more vulnerable to accessing spoofed websites that can gather personal information. Phishing and other security threats like these are increasingly prevalent in today's mobile economy.

Applications, another area of concern, utilize common data source on most devices — making it easier for malicious applications to access data. Industry standards (including authentication) are often lacking or nonexistent for mobile security, and user awareness is extremely low.

The main threats for enterprises — including loss and theft, malware, spam, phishing and man-in-the-middle attacks — impact the entire mobile ecosystem. With secure practices applied across the mobile operating chain, enterprises can create a safe mobile environment.

Open Web Application Security Project’s (OWASP) top 10 security threats of 2013:

- Injection
- Broken authentication and session management
- Cross-site scripting (XSS)
- Insecure direct object references
- Security misconfiguration
- Sensitive data exposure
- Missing function-level access control
- Cross-site request forgery (CSRF)
- Using components with known vulnerabilities
- Unvalidated redirects and forwards

Security threats impacting mobile operations
Applications are considered the key driver for the increased use of smartphones and mobile devices — and should be top priority for organizations looking to improve mobile security.

Application security varies based on the needs and goals of the application. For example, a consumer application that searches store locations captures limited to no user information and has minimal security risks. A mobile banking application, on the other hand, carries sensitive information and will need to be highly secured. It is important to understand the varied threats and potential vulnerabilities of a mobile application to help calculate risk and potential security impact.

The challenge when creating an application is there is no standard checklist for securing all mobile applications. Security and support practices vary from platform to platform; developers must be well versed in mobile operating systems and application development platforms. Security processes should be adopted and maintained, starting from the requirement analysis phase and continuing into development.

Creating strong policies to ensure application security during the entire development lifecycle — design, development, testing and deployment — will go a long way in safeguarding the application. This will also help reduce effort and costs, using different techniques such as denial of service, elevation privilege and information disclosure.

During the requirement analysis phase, it is very important to understand and document the scope thoroughly to capture the following:

- Use case and user types
- Process
- Number of operating systems that need to be supported
- Organization’s security policy
- Development approach — cross platform/hybrid/web
- Back-end systems/process that will be exposed
- Critical data

Designing the application

Based on the findings of the requirements analysis phase, an architect should work on an application risk profile, as part of the overall architecture — evaluating any complications and restrictions involving security and compliance.

With real-estate restrictions and keypad limitations, it is important to find the right balance between the information that can be displayed and the number of interactions needed to access data. For example, when using a mobile banking application, it can be difficult to enter an alpha-numeric account password because most mobile keypads have limited functionality compared to a full-size keyboard. This limitation

**Best practices**

**Securing the application layer**

**Ensure:**
- Secure sockets layer (SSL)/transport layer security (TLS) validation
- Local session timeouts
- Application settings are protected
- User privacy is protected
- Secure deletion

**Utilize:**
- Enterprise applications crash logs for debugging
- Geolocation (use very carefully)
- Third-party libraries testing
- Secure data storage
- Two-factor authentication

**Avoid:**
- Storing sensitive data
- Caching application data
- Using query string for sensitive data
- Using tokens instead of account numbers
- Caching user names (use sparingly)

**Securing the network layer**

- Pin down certificates
- Validate inputs
- Check session settings
- Configure SSL
- Pen test web services
- Protect internal resources
is also opening opportunities for the development of new authentication methods such as biometric scans, near field communication (NFC) devices and face recognition.

The user interface is a critical aspect of mobile applications. It needs to be simple and intuitive, while taking into account user behavior to identify any security risks or vulnerabilities.

Devices with enhanced and innovative features have improved the mobile ecosystem considerably over the years. To keep up with constantly evolving technology, developers should strive to provide rich user interfaces over low bandwidth while supporting large data sets and native runtime features — such as camera, global positioning system (GPS) and graphics. Basics, such as the central processing unit (CPU), memory, storage capacity and battery life, should be given equal consideration when designing next-generation devices.

**Developing the application**

Every mobile application platform has different characteristics, security features, capabilities and weaknesses. The impact and security implications of these differences vary with the application development approach (native/cross platform/hybrid/web) and platform support. Developers should understand these inherent platform characteristics when developing applications.

<table>
<thead>
<tr>
<th>Mobile operating system</th>
<th>Apple iOS</th>
<th>Google Android</th>
<th>RIM Blackberry</th>
<th>Microsoft Windows Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access control options</strong></td>
<td>PIN, passcode</td>
<td>PIN, passcode, swipe, face unlock</td>
<td>PIN, smartcard</td>
<td>PIN, passcode, smartcard</td>
</tr>
<tr>
<td><strong>PIN/passcode length, complexity, retry policies</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>File system encryption</strong></td>
<td>iPhone 3GS and up, iPad</td>
<td>Selected tablets (Android 3.0 and up), selected phones (Android 4 and up)</td>
<td>All Blackberry</td>
<td>Windows Mobile 6.5, Windows 8</td>
</tr>
<tr>
<td><strong>SD card encryption</strong></td>
<td>No SD card slot</td>
<td>OEM proprietary</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Remote wipe</strong></td>
<td>Removes encryption keys</td>
<td>Resets to factory default</td>
<td>Removes encryption keys, optionally scrubs memory</td>
<td>Varies by OEM/OS version</td>
</tr>
<tr>
<td><strong>Over-the-air encryption</strong></td>
<td>TLS, WAP2, L2TP, IPsec VPN</td>
<td>TLS, WAP2, L2TP, IPsec VPN</td>
<td>Advance encryption standard/ Triple data encryption secure transport, TLS, WPA2, (IPsec, VTP)</td>
<td>TLS, WPA2</td>
</tr>
<tr>
<td><strong>Security patch flow</strong></td>
<td>Apple to carrier</td>
<td>Google to OEM to carrier</td>
<td>RIM to carrier</td>
<td>Microsoft to OEM to carrier</td>
</tr>
<tr>
<td><strong>App store governance</strong></td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

**Testing the application**

Continuous testing is crucial to mobile application development and security. Testing processes may vary based on the application. It is also extremely important to utilize aspects defined during the design phase — such as use case and threat model. These document risk scenarios and test cases, including source code reviews. Some important application testing features include:

- User interface (UI)/User experience (UX)
- Functional testing
- Vulnerability/penetration testing

**Deploying and maintaining the application**

After testing, enterprises need to deploy the application to devices — based on application and user type. The development and security teams need to work together during the deployment phase to ensure application security through maintenance and support.

Once the application is deployed, maintaining and supporting the application becomes crucial — especially for high-threat applications. For these applications, continuous vulnerability/penetration testing is not only advisable but is necessary to ensure application security. As part of their application management program, enterprises need proactive, secure and strong update processes.

---

**Acronym key**

Security threats are everywhere — from poor application coding and weak data encryption to unsecure web gateways or a lost handset. Even as enterprises try to safeguard mobility, the mobile threat landscape can look like a veritable battlefield with malware, spam, phishing and other attacks around every corner. However, mobility can be safeguarded by the enterprise by using and ensuring security practices at every front and potential line of attack.

Organizations can apply security practices to devices, data, networks and applications in the following ways:

- PIN/password protection and mobile device management (MDM) solutions
- Secure networking practices and web gateways
- Firewall/intrusion prevention systems
- Identity management
- Data virtualization
- Application containerization and sandboxing

Companies should also adhere to security standards when building applications by completing security checkpoints throughout the system development lifecycle. When following these security practices, enterprises can be reassured they have a strong, proactive security framework that can be reused to improve ongoing maintenance and reduce costs.

For more information on enterprise mobility, write to: enterprise_mobility_appsboro@dell.com.
For more information about any of our service offerings, please visit Dell.com/services or contact your Dell representative.

References
1 2012 State of Mobility Survey

Open Web Application Security Project (OWASP) is an open-source web application security project. It is also an emerging standards authority, with the publication of its first standard in December 2008 — the OWASP Application Security Verification Standard (ASVS). The OWASP Top 10 for 2013 is based on eight datasets from seven firms that specialize in application security, including four consulting companies and three tool/software-as-a-service vendors (one static, one dynamic and one with both). This data spans over 500,000 vulnerabilities across hundreds of organizations and thousands of applications. The top 10 items are selected and prioritized according to the data, in combination with consensus estimates of exploitability, detectability and impact estimates.

3 http://searchconsumerization.techtarget.com/tip/Comparing-mobile-operating-systems-manageability-and-security