HP FORTIFY MOBILE APPLICATION SECURITY SOLUTIONS

Mobile Security for Android and iOS Applications

Data sheet

HP is transforming the enterprise security landscape with its Security Intelligence and Risk Management (SIRM) Platform. The SIRM Platform uniquely leverages advanced threat research with powerful correlation of security events and vulnerabilities. By delivering unparalleled visibility across security assets in context of business critical processes and applications we help our customers manage their risk and maximize their security investments.

The Mobile Security Problem

Mobile computing is a fact of life in the modern enterprise. With the rapid and everyday adoption of mobile devices, enterprise applications have been extended beyond the confines of the corporate network. Today, employees are using their company-issued smart phones and tablets for both business and personal reasons: to browse the Internet, make online purchases, play games, and conduct critical business transactions anytime, anywhere – wherever they are. That's a lot of mobile, representing a large potential attack surface.

The large attack surface and the proliferation of mobile devices have created a significant security challenge for companies and IT professionals. How do you ensure that your organization's mobile presence is always safe and secure?

Securing the complete mobile stack

HP Fortify Mobile Application Security solutions provide the most comprehensive, automated and advanced mobile security protection for the enterprise. Whether your application is developed in-house, procured from third-party sources or running in production, we ensure that every single line of code is written securely for Apple iOS or Android devices.

HP Fortify secures the whole mobile stack, from the client device to the network communications to the backend server.

Device-based attacks
Attacks against the device are the most tangible, impactful and obvious to the average person. Anyone who has ever misplaced or lost their smart phone or tablet understands the fear and danger: your personal information could be accessed or stolen off the device because of unencrypted credentials, insecure storage, or cached data.

However, a more dangerous scenario occurs when employees download unknown applications from iTunes or the Android App Store. These applications could install malware on the company-issued smart device. This could lead to information leakage or complete compromise of the device, allowing attackers to install

Figure 1:
Securing the client, the server and the network communications.

malicious certificates, reconfigure proxy settings or allow man-in-the-middle (MiTM) visibility into every user transaction.

Network-based attacks
Due to the mobility of smart phones and tablets, employees are freely accessing their devices in very public and insecure places. When data is transmitted over a WiFi network, malicious attackers can easily steal the potentially sensitive information right out of the air. This happens because very few applications properly secure their sensitive data by managing TLS/SSL certificates or employing encryption technologies.

Unfortunately, even if applications are claiming to use encryption technology, they are only encrypting the initial user login. After successful login, the application will then switch to using cleartext data.

Server-based attacks
The mobile device is useless unless it's communicating with something on the backend. Usually, this backend is comprised of web components and services that the client device interacts with via standard HTTP. As a result, common web vulnerabilities like authentication, SQL injection, cross-site scripting, and cross-site request forgery still apply.

The Mobile Security Solution

Mobile Product Support
- Test the security of all mobile applications—whether it's built for the client device, the backend server or the network
- Pinpoint with line-of-code precision the root cause of vulnerabilities for any application built for Apple iOS and Google Android
- Prioritize all mobile application vulnerabilities by severity and criticality, with detailed fix recommendation, for ease of remediation

Mobile Assessment Services
- Assess security throughout the entire mobile stack —at the client, server and network layers
- Prove mobile security compliance for PCI, SOX, HIPAA and other government and industry regulations and standards with third-party, independent validation
- Leverage single assessment for a one-time project or an annual subscription for unlimited, continuous assessments

HP Fortify Mobile Application Security solutions provide the following benefits:
- Secure all mobile applications from attacks—whether you're developing mobile applications for your customers to access or deploying third-party applications on corporate mobile devices for employees
- Save time and money by removing security vulnerabilities at the source--in the software on the mobile device or server
- Increase development productivity by enabling security to be built into mobile applications, rather than added on after it an application is deployed

About HP Fortify Mobile Application Security Solutions

HP Fortify Mobile Application Security Solutions are part of the HP Fortify Software Security Center suite, a comprehensive solution for automating and managing an application security program in the enterprise. HP Fortify Software Security Center proactively eliminates the immediate risk in legacy applications, as well as the systemic risk in application development processes. HP Fortify Mobile Application Security solutions are available for use on-premise or on-demand, and with managed services.

About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats. Find out more at www.hpenterprisesecurity.com.

ESP-SDS003-020812-02, Created February 2012