Hewlett Packard Enterprise

HPE Security Fortify on Demand Mobile

End-to-end, real-world mobile application security

Insecure mobile applications represent a real security threat to enterprises and individuals. Moreover, IT teams pressured to deliver applications on time are often also tasked with the job of security; without the skills needed to complete the task. Fortunately, HPE Security Fortify on Demand offers a mobile application security testing solution delivered as a cloud-based managed service—alleviating the need to do it all in-house.

Highlights

Managed service: Cloud-based portal backed by a global 24x7 mobile application security testing team.

Comprehensive testing: Our approach includes both static and dynamic mobile security testing techniques, automated and manual.

Behavioral analysis and privacy checks: Now offered via a fully integrated dashboard and mobile application reputation database.

A three-tier approach: Assessments are performed across all three layers of the application: client, network, and server.

Supported platforms: iOS, Android, Blackberry, and Windows® Phone.

Figure 1: Comprehensive security testing across the three attack vectors: client, network, and server

Take advantage of comprehensive security testing services

The HPE Security Fortify on Demand approach to mobile security assessments is to look at the entire technology stack: client, network, and server. This holistic approach is used so that vulnerabilities found in one component (the client, for example) can be used while testing the server to paint the truest picture of mobile application security risk (similar to the methodology a hacker would employ).

Before testing begins, we start with a full installation of an application, and then perform a complete walkthrough using all the various functions available. We note where sensitive data is requested, how it moves through the application, and how it is utilized. We identify how those components work together and leverage that flow as the assessment progresses. Additionally, we insert ourselves between the mobile client and the application back end using various tools to spoof the server certificate and man-in-the-middle (MITM) Secure Sockets Layer (SSL) connection. We then begin the assessment starting with the client. Security testing is performed on test mobile devices as well as by using device emulators—depending on the application type and functionality.

See our mobile assessments (Table 1) for more information about what is offered at each service level.

Assess the mobile client

In the client of the evaluation, we test the following areas:

- **Filesystem:** p-list files, SQLite databases, geo-location data, log files, screenshots, and more. We have developed custom scripts that parse both binary and text data for a list of sensitive content types, such as usernames, passwords, and so on.
- **Memory:** Sensitive data stored in memory should be scrubbed properly, including usernames, passwords, database connection strings, and so on.

Assessment coverage
- Full installation and use
- Testing across all three vectors
- Behavioral analysis
- Thorough malware discovery

- **Run-time tampering:** We interact with methods in real time. This allows us to test and bypass security controls like SSL, jailbreak detection, and anti debugging.
- **Input validation:** Buffer overflows against text messaging, URL schemes, and Android intents.
- **Source code analysis:** Harvest URLs, format string vulnerabilities, secure coding guidelines, insecure data transmission, SQL injection, SSL issues, input validation, insecure logging, keychain use, cross-site scripting (XSS) in UIWebView, hard-coded credentials, and so on.
- **Binary analysis:** This includes sensitive data extraction, use of dangerous libraries, weak binary protections, and so on.
- **Inter-application communication:** Determine what interaction takes place between the tested application and others on the device.

Evaluate the mobile network traffic

We evaluate the network traffic sent from the mobile device to the server, covering the following key areas:

- **Transport layer security:** This includes SSL certificate management, certificate pinning, and more.
- **Data stream analysis:** Evaluate all data passing from the client to the server during normal operations, paying special attention to where sensitive data is being sent and how and where it is being stored.
- **Malware analysis:** Analyze what is being sent, to where.
- **Host communication enumeration:** All network traffic is captured and run through our toolset to find all hosts it spoke to (Android).

Analyze the Web server

The server side is examined after, and leverages everything learned from, evaluation of the client and network portions of the application. All the URLs and parameters gathered from the static, binary, and data stream analysis are now used to evaluate the back end whether it is communicating with a Web application or Web services. Testing steps include:

- **Mobile Web application vulnerability assessment:** Authentication, session management, access control, input validation, logic testing
- **Mobile SOAP1 or REST2-based Web service testing:** Finds vulnerabilities in the most common Web service-based mobile back ends
- **Static analysis of any back-end code:** Evaluates the source code of the mobile back-end system

Build security in

HPE Security Fortify on Demand enables a safer, faster go-to-market strategy for mobile application security at all points: development, procurement, and launch.

Development

Including regular security scans during development encourages secure coding, and the earlier the vulnerabilities are identified, the less costly they are to remediate. During development use a Mobile Basic scan to:

- Identify critical flaws early in the development lifecycle
- Get detailed remediation recommendations
- Prioritize and assign remediation tasks
- Pinpoint potential coding weaknesses that need focus

What we look for
Our broad range of checks look at how data is stored, accessed, and transferred. Examples include:

- Lack of proper exploit mitigations techniques (address space layout randomization (ASLR), position independent executables (PIE), stack randomization)
- Writing sensitive data to files
- Accessing or writing to public photo store
- Accessing the address book
- Accessing geo-location information
- Accessing or writing sensitive log information
- Using depreciated cryptographic libraries
- Writing sensitive data to insecure public directories
- Insecure keychain usage
- Client-side SQL injection
- Insecure HTTPs, SSL, and certificate usage

Reputation analysis of traffic endpoints.

- Identification of URLs, IP addresses, and hostnames
- Reputation on discovered endpoints

Procurement
For apps procured through a third party, we can work with your vendor to assess apps you receive are secure. Key features of our vendor management program are:

- Quick, easy, and efficient process for all involved
- Confidentiality—puts vendors at ease
- Managed by an independent, unbiased third party (HPE Security Fortify on Demand)
- Secure code introduced into your environment

Pre-production and production
Before each release, simply upload the binary of your desired application and our expert team will conduct a thorough audit of your application utilizing the Open Web Application Security Project (OWASP) Top 10 and many other checks across the client, network, and server attack layers. Utilize this deeper level test to:

- Mitigate the security of apps that handle high risk information—banking, commerce, and medical
- Observe how an application will behave in a real-world situation
- Fully test the security of a mobile application

Control potential BYOD threats to proprietary information

Introducing and using third-party applications with the advent of BYOD policies can compromise your enterprise infrastructure's security. Even mobile applications developed in-house can leak sensitive employee information and company data. By offering an easy way to analyze and whitelist or blacklist mobile applications, HPE Security Fortify on Demand gives you more control over potential threats to your proprietary information with our mobile reputation management service.

Gain insights into risky or malicious behaviors
The HPE Security Fortify Mobile Reputation Management service provides a thorough assessment of application behaviors and reputation analysis of traffic endpoints.
The service checks mobile applications for behaviors that compromise privacy, identity, and system log information. It also analyzes traffic endpoints—URLs, IP addresses, and hostnames—to determine if they are known malicious hosts or have a low reputation score.

Just point us to the (free) application in the iTunes or Google™ Play app stores, or upload the application binary.

Inform BYOD policies
Using a fully integrated mobile application reputation dashboard and database within the cloud-based portal, search for (or request) reputation analysis of Android and iOS applications.

- Gain detailed mobile security intelligence about thousands of Android and iOS applications
- Evaluate all mobile applications on enterprise-managed devices
- Keep your corporate information safe from risky mobile applications
- Enforce corporate policies regarding your employees' mobile devices
- Roll out a BYOD program that includes both preventative and corrective controls
- Unlock the full potential of your existing mobile device management (MDM) and mobile application management (MAM) solutions

Service offerings available
While we have the ability to test any mobile applications in all of the ways previously mentioned, customers often ask for only a subset of the security testing to accomplish a particular goal. We have listed a number of offerings based on those requests. All levels of application security testing include a remediation scan. Assessments can be bought singly or as a subscription, which allows for unlimited assessment of a single app over a 12-month contract period.

Use the HPE Security Fortify on Demand mobile app to review report info anytime.

OWASP mobile top 10 risks

M1—Weak server-side controls	M6—Broken cryptography
M2—Insecure data storage	M7—Client-side injection
M3—Insufficient transport layer protection	M8—Security decisions via untrusted inputs
M4—Unintended data leakage	M9—Improper session handling
M5—Poor authorization and authentication	M10—Lack of binary protections

Figure 2: OWASP Top 10, 2014

Contact
fodsales@hpe.com
+1 650 409 1611

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

Quality at scale and proven results

Leverage quality at scale

In our approach to mobile security testing, we offer an extreme focus on methodology innovation and standardization; many consultancies have good testers with solid techniques, but testing consistency can be an issue, leading to limited scalability and increased chances of false negatives. We employ a centralized methodology workflow system that walks our testers through our approved security testing steps to enable consistency.

Attain proven results

The Hewlett Packard Enterprise team has performed thousands of mobile security assessments, often achieving full compromise of both sensitive data used by the mobile application as well as the back-end server that the system runs on. This is sometimes accomplished via hard-coded information found during static analysis and other times through server-side vulnerabilities such as file inclusion vulnerabilities. In fact, in two-thirds of our tested applications, we find a critical flaw that leads either to compromise of personal data or to the underlying system.

Table 1: Service offerings matrix

MOBILE ASSESSMENTS	BASIC	STANDARD	PREMIUM
Application risk level	Low/medium	Low/medium	High
Platforms	iOS, Android, Windows, Blackberry	iOS, Android	iOS, Android, Windows, Blackberry
Client: automated binary	No	OWASP top 10	All categories
Client: manual binary	No	OWASP top 10	All categories
Client: source code	Yes	No	Yes
Network	No	OWASP top 10	All categories
Server: Web services (dynamic)	No	OWASP top 10	All categories
Server: Web services (source code)	No	No	Yes
False positive removal	Yes	Yes	Yes
Target turnaround	1–2 days	1–2 days	5–7 days

Learn more at
go.saas.hpe.com/fortifymobile

4AA4-6936ENW, November 2015, Rev. 3