Enterprise Security

Attacking the Problems of Application and Mobile Security
Contents

3 Introduction: Securing the Mobile Enterprise

5 Understanding the Source Devices

6 Networks

Servers

9 Orasi and Micro Focus: Application and Mobile Security Solutions

10 About Orasi Software, Inc.

7 Application and Mobile Security

Application Security Testing

Secure Application Development

Conclusion
Introduction: Securing the Mobile Enterprise

The mobile enterprise has created vast opportunities—and serious new challenges.

IT is increasingly consumerized. “Bring Your Own Device” (BYOD) is the new byword of today’s on-the-move workforce. Hackers, whether seeking profit or Intellectual Property (IP) and often working behind the protection of Nation States, continue to penetrate personal computers and organizational IT environments and have added mobile devices to their targets.

Mobile phones, mobile applications, and the network infrastructure are particularly vulnerable to attack and intrusion—and can all too often be the weak link in an otherwise secure enterprise infrastructure. Smartphones and mobile apps are being adopted at a phenomenal rate worldwide, with business users driving uptake in many markets. The burgeoning mobile Internet presents a tempting target for hackers and cybercriminals.

So it is not surprising that for many enterprises, perhaps the most pressing security concern is the need to protect mobile phones, applications, networks, and sensitive information in the ongoing age of mobility.

In this Orasi white paper, we examine the current threats and realities affecting mobile enterprise security, and evaluate Best Practices in the areas of mobile testing and security. The authors recommend a comprehensive approach to enterprise security, one that addresses the device, network, servers, and the full secure development lifecycle (SDL) of mobile applications. We also offer a brief summary of Orasi mobile security, offered in partnership with enterprise security solutions from Micro Focus.

Trends in Enterprise Security

As businesses adapt to the new anywhere/anytime realities of the always-on environment that comes with mobility, they are presented with real opportunities...and significant new challenges.

Companies can leverage mobility to expand their market reach, to accelerate innovation, and to forge closer and more rewarding relationships with customers and partners. Mobile storefronts make products and solutions available worldwide at the touch of a keystroke. Mobility also allows a workforce to respond more quickly and productively. Business software is more accessible, and even legacy and in-house applications can be made available via the web, across the cloud, and on mobile devices.

However, enterprise mobility also poses real challenges and difficulties. While websites and e-commerce were once sufficient, today’s on-the-move stakeholders expect interactive and engaging mobile experiences that are accessible via smartphones, tablets, and other devices. Without a mobile presence, organizations lose standing and business to more nimble competitors.

As enterprise mobility grows, so does the realization of the serious threats this still-emerging technology can pose to an organization’s infrastructure, applications, and information. Because software is now extended far beyond the traditional IT perimeter defenses, those applications and a vast store of highly-sensitive enterprise information are often left surprisingly vulnerable to loss, fraud, and cyber-crime.
Threats of many kinds—from hackers and organized crime cartels to competitors and hostile governments—work constantly to exploit vulnerabilities in enterprise software. Those attackers might seek to steal customer identities, account information, or corporate intellectual property. Others might work to disrupt normal business operations, inflict damage to a brand image, or put employees or the general public at risk.

Research from leading security and technology organizations confirm the ongoing threats.

- In almost all of the compiled material referencing mobile computing (also referred to as mobile systems), an exponential increase in threats is being predicted. This trend follows the relevant market trends of mobile devices, consumerization of IT, BYOD and mobile user empowerment. (ENISA – ENISA Threat Landscape: Responding to the Evolving Threat Environment)

- Mobile applications are different, but the same. In addition to the broader information leakage problems presented by changing use cases and platforms, mobile applications are designed to leak data. (Micro Focus - 2011 Top Cyber Security Risks report)

- The beginning of 2012 was marked by a qualitative change in the botnet ecosystem. Botmasters, who had begun to feel overcrowded in the Windows world, actively targeted the mobile and Mac OS segments. Unfortunately, few users realize that their smartphones are fully-functional computers which contain valuable data that may be of interest to cybercriminals. (Kaspersky Lab - IT Threat Evolution: Q1 2012)

- Cross-site scripting has been one of the most persistent exploits of the Internet. This attack works on any web browsing technology, including mobile devices. The attack is extremely popular and can pose a significant security risk. (IBM - IBM X-Force 2012 Mid-year Trend and Risk Report)

...and the problem will only grow.
“By the end of 2012, the number of mobile-connected devices will exceed the number of people on earth, and by 2016 there will be 1.4 mobile devices per capita. There will be over 10 billion mobile-connected devices in 2016, including machine-to-machine (M2M) modules-exceeding the world’s population at that time (7.3 billion).” (Cisco Visual Networking Index: Global Mobile Data Traffic Forecast)

With the explosive growth of mobile devices and applications, the need to secure them is critical. BYOD often means one device shared between corporate and personal use and needs. They are designed to be out-of-the-box capable of connecting to many sites and services. It takes an active effort on the part of the user to disable these unneeded connections.

It is not only the people within your organization, over whom you can attempt to exert some level of control, who must be considered, but threats can also come from anyone these people interact with through social media or other applications using their mobile device. Screen size of mobile devices further increases exposure and risk. The smaller screen size makes it difficult even for trained users to recognize a fake or counterfeit website.

Understanding the Source

The inherent openness of mobility creates a number of security risks. Mobile software vulnerabilities can vary greatly depending on the vector, or source, of the threat. A robust, enterprise-class security program should evaluate and protect against risks that originate from any quarter. Threats against enterprise applications originate from one of three principal sources: devices, servers, and networks.

Devices

Device-oriented attacks often begin when a tablet, smartphone, or other on-the-move asset is lost or stolen. Bad actors may then exploit cached data or unencrypted credentials to connect to an enterprise system to remove or damage sensitive information. Attackers may work to install malware on a system, reconfigure proxy settings, or compromise certificates to allow what is called man-in-the-middle intrusions into mobile transactions. Mobile applications that reside on phones and PDAs may also be vulnerable to the exploitation of text messages, email, and other user inputs.

Mobile applications increase the attack surface for any organization, and BYOD policies accentuate those vulnerabilities. When users access social media via their mobile devices, they may expose enterprise environments to new and dangerous threats.
**Networks**

Modern enterprises depend heavily on communications networks, but that same network infrastructure can be one of the most common and dangerous sources of security risk to mobile applications. An on-the-go workforce is particularly vulnerable in public places, where easily-available hacking tools allow bad actors to pull information directly from unsecured WiFi signals. Other network-based vulnerabilities include poorly secured TLS/SSL certificates, networks that encrypt only at login and then switch to cleartext, and code that transparently reveals network communication protocols.

**Servers**

Servers are the crucial touchpoints between mobile devices and an enterprise, and those web-based assets can be vulnerable to a wide range of attacks. Mobile applications typically interact with back-end web sites, and many of those sites use web services that can be exploited by SQL injection, cross-site scripting, and other well-known attack strategies.

Because most IT units focus on the security issues relating to devices, applications, and end user behavior, threats to servers may be overlooked. In addition to testing devices and mobile software, a reliable security program will also assess the web infrastructure that hosts the application on the server side.

Given the dynamics and sophistication of the mobile device-oriented threat landscape and extended attack surfaces, organizations are advised to employ robust security protections, including both manual and automated code reviews, dynamic testing techniques, comprehensive testing of all devices under real-world operating conditions, and implementing network and perimeter controls to counter the mobile threats.

**Application and Mobile Security**

In partnership with Micro Focus, Orasi recommends a proactive, holistic approach to application and mobile security in the enterprise environment. This approach is based on the principle of securing applications during the development stage, when it is more effective and less costly to do so. The best of today’s security programs offer a comprehensive and disciplined framework designed to eliminate vulnerability and risk in the software organizations use to communicate and work—whether those applications are deployed in traditional enterprise networks, the cloud, or across mobile technologies.

Thus, the goals of any reliable application security effort should be to identify and remove risks in existing applications, but also to apply secure software development practices. These objectives are met through two primary techniques: testing and development.
Application Security Testing

Application testing is a crucial element in any enterprise security regimen, and a workable testing program should be calibrated to quickly and economically identify exploitable vulnerabilities. Testing should provide an accurate view of threats regardless of the source of an application—whether it was developed in-house, purchased off-the-shelf, or provided by third-party vendors.

There are three basic types of application testing:

- **Static Analysis**: Also known as Static Application Security Testing (SAST). Designed to detect a very broad range of potential vulnerabilities and is ideally suited for detecting security threats during application development. Also identifies vulnerabilities at a line-of-code level of detail, providing very precise information on potential threats to mission-critical software, greatly easing remediation efforts and speeding resolution of the security issue.

- **Dynamic Analysis**: Also called Dynamic Application Security Testing (DAST). Simulates various attack scenarios to detect vulnerabilities in deployed Web-oriented applications and services. By validating whether a specific vulnerability is indeed exploitable, dynamic analysis allows organizations to recognize and remediate the most serious security threats.

- **Hybrid Analysis**: Developed by Micro Focus and recommended by Orasi, real-time hybrid analysis combines robust vulnerability verification with broad application coverage and code-level insight into current and potential threats. This hybrid approach can greatly improve the scope and accuracy of static and dynamic testing techniques. Hybrid analysis generates highly relevant results—including the exact cause and precise source code location of each threat—thus giving organizations the insights needed to recognize and counter their most significant security threats.

Secure Application Development

To ensure optimum effectiveness, the software testing techniques described previously should be applied as part of a broader program designed to eliminate software risk across the enterprise.

A secure development lifecycle must encompass internal and external third-party vendor development teams, and should address the security of software applications that are currently deployed, in development, or being planned. A systematic approach allows organizations to find and fix current threats, while ensuring that security is a fundamental element in all future application deployments.

There are five basic elements in a reliable lifecycle approach to software security.

**Threat Intelligence**

Because cybercriminals work constantly to find and exploit new software vulnerabilities, organizations must create and maintain a constant, in-depth, proactive approach to application security. Good threat intelligence leverages up-to-date information on current and emerging security issues and risks, as well as ongoing research into vulnerability levels and remediation priorities.
An Application & Mobile Security Checklist

As noted, the testing of mobile software applications is a crucial aspect of any reliable enterprise security program. Micro Focus and Orasi recommend that organizations consider the following checklist to ensure mobile applications are fully tested.

- Bad actors will probe and attack software when it is deployed and running, so to ensure optimum protection, mobile applications should be tested dynamically in full and operating configurations.
- Since most mobile applications are multi-tiered, complete tests should incorporate all three tiers of the mobile stack – client, network, and server components.
- For best results, perform both dynamic and static tests of mobile applications.
- Both automated and manual testing offer specific advantages, and in many cases manual testing should be used to supplement automated testing for dynamic and static tests.

Remediation Management

Once a threat has been identified and understood, the lifecycle approach calls for a rapid response to triage, repair, validate, monitor, and manage each specific vulnerability. Those efforts should be pursued by a coordinated team of software security and development specialists, working in a collaborative environment and leveraging advanced techniques. Today's most effective remediation programs employ automated detection processes, audit toolsets, bug tracking systems, quality assurance tools, integrated development environments, and other technologies to address threats more quickly and at a lower cost.

Proactive Management

An ongoing, forward-looking software security management approach allows organizations to embed security into all application-related activities, processes, and output. A holistic management program provides a centralized place for tools and templates, and allows the automation and orchestration of security efforts. When considering a proactive security management effort, organizations should carefully evaluate appropriate policies and best practices, and then apply those guidelines across the entire application lifecycle.

A Comprehensive Approach

Of course, mobile security testing is just one key element in any successful enterprise strategy. A more comprehensive approach will also address quality assurance (QA), performance validation, application security, business service automation and management, and demand and portfolio management. Key test and quality components may include mobility testing, functional and performance tests, test automation, load testing, application security, and specific QA software technologies.
Orasi and Micro Focus: Application and Mobile Security Solutions

Orasi is an Atlanta-based software reseller and professional services company focused on enterprise software quality testing and management. Orasi is a Micro Focus Platinum Partner and authorized Support partner.

Orasi partners with Micro Focus to provide solutions for the entire application and security lifecycle. Those solutions are designed to mitigate risk, strengthen compliance, and defend against advanced and emerging threats. The Micro Focus Security Intelligence Platform uniquely delivers the robust correlation, application protection, and network defense needed to protect today’s mobile IT infrastructure.

Micro Focus Enterprise Security delivers comprehensive security solutions in the areas of:

- **Application Security** – enables developers, QA teams, and security experts to find and fix vulnerabilities throughout the application development lifecycle. Micro Focus Fortify software delivers advanced and proactive security testing to protect mission-critical enterprise software.

- **Enterprise Security** – allows organizations of all sizes to achieve comprehensive security management, compliance, control, and risk mitigation. The Micro Focus ArcSight security monitoring and detection suite helps organizations understand who is on their network, what information they are seeing, and which actions they are taking with that information.

- **Network Security** – protects physical, virtual, and cloud infrastructures from network-based threats and intrusions. The Micro Focus TippingPoint adaptive network defense solution leverages deep research and intrusion prevention techniques to automatically block attacks.

Conclusion

Application and mobile security presents both promise and problems for today’s enterprise.

Mobile technologies can open amazing opportunities to extend market reach, drive productivity and innovation, and build closer relationships with customers, suppliers, and partners. Mobility is no longer a luxury: for many organizations it is a competitive requirement.

But mobility can be a challenge. On-the-go employees are bringing their own devices to the workplace, and expect anywhere/anytime access to corporate systems and data. Customers and consumers now demand a responsive and interactive mobile experience.

Smartphones, mobile apps, and mobile networks are highly vulnerable to cyber-attacks. In fact, current research indicates that mobile infrastructure is the fastest-growing source of fraud and intrusion.
That is why forward-looking organizations are making application and mobile security a key priority. As discussed here, a robust mobile security program must address devices, networks and servers, and the complete lifecycle of applications and mobile assets. By applying Best Practice testing and security management, organizations can protect their operations, their sensitive information, and their stakeholders.

Orasi and Micro Focus are uniquely positioned to assist organizations in assessing their application and mobile security posture, and in deploying a robust and cost-effective testing and security program.

About Orasi Software, Inc.

Orasi is an award-winning software reseller and provider of software training, support and professional services. To help companies focus on a complete software quality lifecycle, Orasi offers market-leading consulting services and solutions to support automated testing, application performance management/intelligence, mobile technologies, DevOps pipeline efficiency, and operational excellence. Orasi continues to expand its offerings across the entire software delivery spectrum, from data analytics to continuous delivery and open source tooling. Orasi maintains strategic partnerships with Micro Focus (formerly HPE), Chef, Delphix, SAP, XebiaLabs, and others. For more information, please visit www.orasi.com.