THERE'S AN APP FOR THAT, BUT IS IT SECURE?

IT leaders rethink application security as they race to embrace.

EXECUTIVE SUMMARY

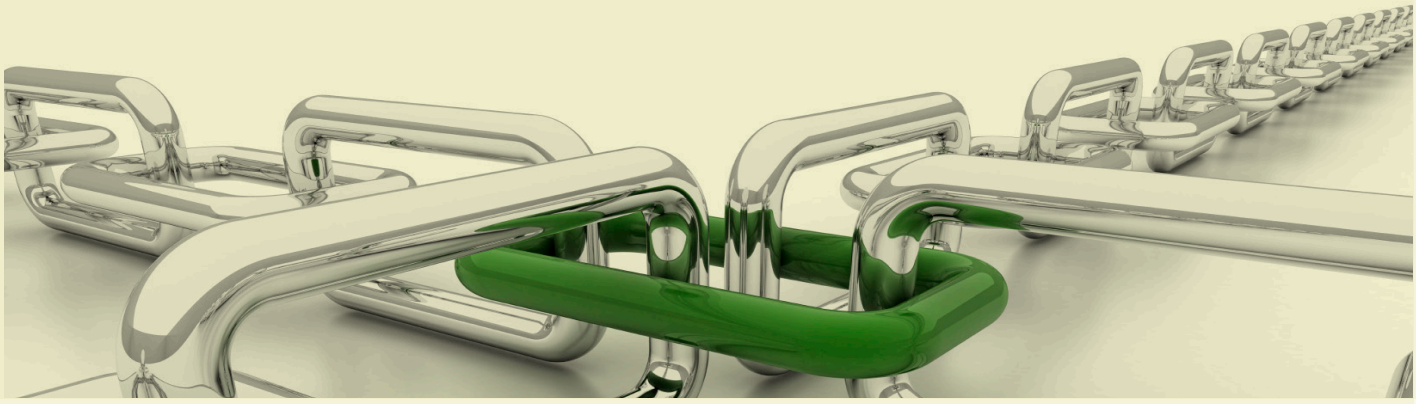
Companies can't move fast enough to meet customer and employee demand for mobile services. But security has eroded over the past decade as companies strive to create applications for multiple platforms by farming design and development out to subcontractors. This trend has strained the processes and governance put in place to ensure application security. It takes proven best practices to mitigate risk and embrace mobility without trepidation.

MOBILITY IS TRANSFORMING BUSINESS. This is evidenced by its rampant adoption. In fact, International Data Corp. last year estimated that all smartphones—consumer and business—would amount to 472 million shipments in 2011, with expectation that annual shipments will nearly double to 982 million by the end of 2015.

Driven by employee and customer demand and the fear of falling behind competitors, companies rush to develop mobile apps for traditional productivity tasks, such as email and sales forecasting, and customer-facing activities such as online banking, online purchases, and order tracking. These new applications rely largely on providing end-users and customers with unprecedented access to corporate networks, data stores and legacy applications.

In their effort to deliver, many companies are kick-starting internal development of mobile applications or outsourcing to relatively new development partners. The diversity of platforms often means organizations contract different boutique development shops to create versions of the same application for different devices. Distribution may even depend on third-party app stores.

This all comes at a time when data security breaches—whether for profit, mischief, or political causes—are on the rise. Corporate security and



technology chiefs are clearly aware of growing threats as they deploy mobile apps. "The enthusiastic adoption of personal-liable smartphones for work is forcing organizations to develop expanded mobility strategies focused less on providing devices and more on managing security and access to devices, applications and data," says Gina Luk, senior analyst of mobile workforce strategies with Strategy Analytics and co-author of a recent forecast report on business smartphone use.

Still, there's a gap between awareness and action. The 2012 Global State of Information Security Survey, conducted by PwC, *CIO Magazine* and *CSO Magazine*, polled more than 9,600 c-level executives and IT chiefs and found fewer than half implement safeguards to protect the enterprise from security hazards that mobile devices and social media can introduce. Just 43 percent have a security strategy for employee use of personal devices, and only 37 percent have a security strategy for mobile devices.

CSO publisher Bob Bragdon says the survey suggests the rush to embrace mobility and consumerization is "exposing the business to risks that it may not be wise to accept." Nonetheless, technology races ahead, and companies struggle to keep up.

IMPACT OF MOBILE ON APPLICATION SECURITY PRACTICES

Software development resources are one area where the struggle is quite evident. This is not unprecedented, of course; there's a similar paradigm shift with the demand for Web applications requiring organizations to incorporate new skill sets and techniques into traditional software development lifecycle (SDLC) processes.

Development for enterprise mobile apps has many similarities with traditional client/server applications and newer Web applications, says Jacob West, director of software security research at HP. "Most of the work that an enterprise mobile app does, most of the data it stores, most of the data or intellectual property it protects, is all still on a server somewhere," he says.

But there are key differences. Organizations are not simply creating mobile Web sites, but rather building mobile applications. And those native mobile applications run on platforms—leaving many organizations supporting multiple platforms.

Wendy Nather, research director in the enterprise security practice of market research firm 451 Research, says developers "are used to writing for a Web app that runs on a server behind a firewall and the end-client is very thin. They are not used to thinking in terms of actual code executing on the mobile device, where there is a thicker client and it's in a hostile environment."

For many, that hostile environment includes third-party distribution channels. Researchers at Pennsylvania State University's Networking and Security Research Center have been analyzing 1,100 freely downloadable Android apps and have reached some disturbing conclusions: "Smartphone applications are frequently incompletely vetted, poorly isolated, and installed by users without restraint … Unfortunately, the limitations of application markets make them a poor agent for certifying that applications are secure."

ANATOMY OF THE MOBILE APP—IDENTIFYING SECURITY GAPS

When it come to mobile applications, it's important to consider various aspects of their lifecycle to identify potential vulnerability points. Yet the haste to mobilize applications seems to have prompted organizations to short-circuit lessons learned over the past decade regarding building security into their lifecycles.

DESIGN AND DEVELOPMENT

Businesses are scrambling to find developers with scarce mobile app skills. As a result, many businesses farm out app development to marketing firms with little if any appreciation for enterprise security. But whether organizations contract development to third parties or rely on newly hired or newly trained internal staff, the core knowledge on how to write mobile applications securely is often lacking.

Even companies with well-established SDLC processes with internal development teams or long-established external partners are turning to less established system integrators with expertise in new mobile skills but lacking the security acumen businesses expect, says West. "Now they often have three different systems integrators building three one-off applications for different platforms, with none of the existing corporate governance and process." And this results in insecure apps.

IMPLEMENTATION

In many ways, development for mobile apps is no different than developing for Web and traditional client/server applications. But mobile devices often contain personal information, may incorporate powerful tracking capabilities and, in the case of business users, provide access to sensitive enterprise applications.

Another factor complicating security is that many businesses are now pushing applications out to customers and consumers with little appreciation for security. It was recently disclosed, for example, that Apple's App Store is littered with apps that gain unauthorized access to iPhone address books. Third-party services such as Twitter and Facebook have routinely utilized this access to upload contact information to their databases, albeit with disclosure policies that may or may not be readily apparent to users. Google and other companies have circumvented privacy settings of Safari users on iPhones and other Apple computers.

A common error is when developers write code that stores passwords and other sensitive data—from proprietary corporate information to consumer credit card accounts—unencrypted on devices. Another key issue is transporting sensitive data without encryption.

Various problems have been revealed related to the way mobile apps communicate with the underlying OS and potentially with other apps running on the same platform. "There are some pretty complex permissioning and communications schemes that have been set up for how applications can shuffle data between themselves and the OS and between multiple apps," West says. These schemes represent a vital security feature, but are often misunderstood by developers and lead to enterprise security risks.

MORE THAN ONE BAD APPLE

Apple's App Store is littered with apps that gain unauthorized access to iPhone address books. Third-party services such as Twitter and Facebook have routinely utilized this access to upload contact information to their databases.

MAINTENANCE AND SUPPORT

Further complicating the situation for enterprise IT is that mobile apps rely on third parties: handset manufacturers and network service providers on one hand, and third-party distribution by app stores and marketplaces on the other. So, if a customer cries foul over a breach, there is no clean way to assess liability.

Patches and updates can also introduce risk as developers may struggle to keep apps on different platforms in sync in the face of OS revisions and changing requirements of app stores. Those code changes can "break" security during the revision cycle. With the quickly changing nature of mobile development and reliance in many cases on third parties, just keeping track of apps can be a challenge, let alone keeping up with changes in security requirements and policies.

FOSTERING BEST PRACTICES FOR MOBILE APPS

In a recent report, the Aberdeen Group observed, "Application security-related incidents have a high probability of occurrence, a high frequency of occurrence, and a high financial impact per occurrence." The report asserts that even "lagging performers" experience a positive return on their investments in application security, while top performers "experienced fewer actual data loss or data exposure incidents, as well as fewer audit deficiencies, related to application security."

Aberdeen's study found respondents are currently most concerned about security risks of legacy applications with Web-based front ends, .NET-based and Java-based Web applications, and Web 2.0 applications. But the firm expects enterprise mobile applications to "jump to the top of the list in the near future."

The problem with mobile apps is that it's not so simple to apply the skills and tools of existing software development application security to a new area. "What I think we are missing so far is a secure software development lifecycle that is customized for mobile applications," says Nather.

In the meantime, organizations must apply existing tools and best practices to new ways of developing and outsourcing applications. This means adapting internal software initiatives, internal governance policies, and training to specifically encompass mobile development and mobile security. When dealing with outside developers, organizations must specify the security performance and features that are required and demand source code and a functioning runtime against which they can verify and test application security.

The emphasis on testing code is growing. The Aberdeen report indicates between 40 percent and 50 percent of survey respondents currently use static source code analysis or dynamic source code analysis, and many others plan to use these tools within 12 months or are currently evaluating them.

Static and dynamic analysis are two methods for locating and ranking hidden, exploitable vulnerabilities inside software, whether an application is in development or already in production.

Static analysis, also known as static application security testing (SAST), pinpoints the root cause of vulnerabilities with line-of-code detail to help identify critical issues during development when they are easiest and least expensive to fix. Dynamic analysis, also known as dynamic application security testing (DAST), detects vulnerabilities in running Web applications and Web services by simulating comprehensive attack scenarios.

Used independently, the static and dynamic approaches each have strengths, but also weaknesses. With DAST, knowledge of potential attack pathways is sometimes incomplete, and tools can only detect the symptoms of vulnerability, not the underlying cause within the code. SAST is extremely proficient at finding potential vulnerabilities in source code, but does not produce concrete test cases to demonstrate the exploitability of the vulnerabilities it exposes.

Combining these methods in a hybrid code analysis tool would seem an ideal solution, but until recently such an approach was limited by the inability to correlate results until after testing was complete. More recently, though, introduction of real-time testing in a hybrid approach has dramatically improved analysis results by observing applications in real time at code level while they are being attacked, and by applying this information to DAST and SAST analysis while testing is underway.

ANALYZE THIS

BETWEEN 40 PERCENT AND 50 PERCENT of survey respondents currently use static source code analysis or dynamic source code analysis. **MANY OTHERS** plan to use these tools within 12 months or are currently evaluating them.

IRRESISTIBLE FORCES

The movement to mobile is an irresistible force, yet it opens up known and unknown challenges to application security. With hackers and criminals using increasingly sophisticated means to breach enterprise security, the stakes have never been higher and corporations need the tools to make sure they're not introducing unnecessary risk though mobile applications.

Whether development is in-house or farmed out, businesses need established guidelines for secure coding and processes for validating compliance. Automating source code analysis can identify exploitable vulnerabilities in less time and with less effort regardless of how or where application software originates—so companies can embrace mobility with peace of mind.

Bottom line: Mobile application security requires rethinking of traditional approaches so good software development processes are not overridden in the race to value. Information technology and security leaders must assess their application security and plug all the holes opened by mobility, or risk the consequences.

SYNDICATED CONTENT

DANIEL MIESSLER • PRINCIPAL SECURITY CONSULTANT, HP

THE (IN)SECURITY OF MOBILE DEVICES: ANATOMY OF A NEW TYPE OF RISK

IT WASN'T LONG AGO that being on the cutting edge of business equated to having a website. Soon after, it wasn't enough to simply have an Internet presence; you had to be interactive and engaging (see Web 2.0). But now there's a new standard. In order to truly compete in the second decade of the 21st century, you need to be in the mobile space.

That means you either have an iPhone and/or Android application or you're likely losing business to competitors who do.

MOBILE BY THE NUMBERS

How big is mobile? It's big. A study by Arc Worldwide recently showed that half of Americans already use a mobile device to shop, and according to Smart Insights, mobile device use tripled for the third year in a row in 2010. They estimate that global mobile data traffic will increase 26 percent by 2015 and that there will be nearly one mobile device per capita by that same year. Most estimates identify that year as the point at which mobile Internet use will overtake traditional use.

If you think about it, the numbers aren't that surprising. Until now we have only been able to use the Internet while at home or at work -- and that's for the relatively low percentage of people who had Internet access in those places. Nowadays, access is being brought to more and more people, but without the restriction of location. Give everyone a mobile device and suddenly people can casually browse, make purchases or conduct business wherever they are. That's a lot of mobile, and if you're in the security game, that's a lot of attack surface.

WHAT'S SO DIFFERENT ABOUT IT?

Many point out that we've had the Internet and a global website infrastructure of clients and servers for quite a while now and that we should be ready for mobile. After all, it's just the Web on a different type of device, right? Shouldn't it be the same? As it turns out -- no. The world making the transition to mobile Internet use presents a number of unique and interesting challenges:

Physical access. It's a lot easier to secure a computing device when it never leaves the home or workplace. It's something else altogether when that device fits in a shirt

pocket, where it can be lost or stolen very easily. Physical access is the first and arguably the most critical level of security, and having it under constant threat means additional controls must be put in place.

Wireless opportunity. Another luxury that we have had with home and work computers is that they tend to be plugged in, so that people watching the airwaves can't pull data from nearby. Even if wireless is used in a house, the range is short enough so that an attacker would have to be near your home to take advantage. With mobile the threat is different: Attackers can simply go to where many people are, and they'll find plenty of mobile users to attack.

Location fixation. So many of the applications that are popular on mobile platforms hinge on being location-aware. This is great for the user -- and great for an attacker. Securing that sensitive location information is paramount.

MOBILE ATTACK SURFACES

When it comes to actually attacking and defending within the mobile landscape, there are three primary components to consider:

- Attacks against the device.
- Attacks against network traffic.
- Attacks against the server.

DEVICE-BASED ATTACKS

Attacks against the device are probably the most intuitive to people. One avenue is much like the stolen laptop scenario whereby a piece of hardware is stolen so that an attacker can attempt to connect to the system and pull data off of it. Common vulnerabilities here include unencrypted credentials and cached sensitive data that can be pulled off by an attacker.

Another type of threat against the device itself includes the installation of malware on the system that can lead to information leakage and even complete compromise. Attackers commonly install malicious certificates, reconfigure proxy settings and perform other modifications that allow man-in-the-middle (MiTM) visibility into user transactions.

CLICK HERE FOR THE COMPLETE ARTICLE

SYNDICATED CONTENT | HP SERVICE BRIEF

HP MOBILE APPLICATION SECURITY ASSESSMENT

LET HP BE YOUR EXTENDED TEAM of Mobile application security experts. Whether you need us to identify and prioritize your vulnerabilities or help you make the business case for a Mobile application security program, we can perform Mobile application security tests as a single assessment, a series of assessments, or as part of a regular scheduled service.

ASSESSMENT OVERVIEW

By leveraging the HP Security Services team, your security professionals and developers can focus on fixing the security vulnerabilities in your Mobile applications while you eliminate the time and expense associated with installation, hardware, and software maintenance. HP Mobile Security Assessments are designed to pinpoint and prioritize risks that threaten the integrity of the confidential data you store and process.

HP Mobile Security experts work closely with you to develop a custom assessment program and to conduct a comprehensive assessment of your Mobile applications using an established and proven methodology combining our market-leading software with our comprehensive, world-renowned expertise. We will assess your Mobile applications, analyze and validate the results, and then prioritize the vulnerabilities.

CLICK HERE FOR THE COMPLETE ASSESSMENT

SYNDICATED CONTENT | WHITE PAPER

REAL-TIME HYBRID ANALYSIS: FIND MORE, FIX FASTER

A VULNERABILITY GLUT

The exponential growth of software applications and their ubiquitous accessibility make security a daunting endeavor for even the best funded and staffed IT organizations. As high-profile security breaches involving Sony, Citigroup, and legions of others demonstrate, exploitable vulnerabilities in software introduce substantial risk. While the sheer number of applications continues to soar, so does the prevalence of vulnerabilities and the severe repercussions caused by insecure software. Compounding the problem is the complexity of modern software, which increasingly targets versatile, "always-on" scenarios including Web 2.0, mobile, and the cloud.

Against this backdrop, software security practitioners and developers, facing business mandates for efficiency and profitability, are often compelled to secure applications more rapidly while using fewer resources. Making the task yet more difficult is the labor-intensive nature of software security assurance processes. To successfully distinguish critical vulnerabilities that must truly be addressed from those that involve little to no risk can require substantial effort, far beyond the capacity of most IT organizations. Understandably, solutions that can automate the most arduous software security tasks have generated great interest in recent years. Among available candidates, hybrid technology has been perhaps the most compelling.

THE FOUNDATIONS OF HYBRID ANALYSIS: DYNAMIC AND STATIC TESTING

The most effective automated vulnerability detection techniques available today are Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST). DAST works by attacking the application under test using techniques akin to those a hacker might employ. It tries many attack scenarios and monitors the application's response in order to diagnose vulnerabilities. SAST (also known as source code or binary analysis) finds security vulnerabilities by examining software without executing it.

Pros and cons of DAST and SAST: DAST and SAST each possess unique strengths. DAST is ideal for conducting an end-to-end system test. In just minutes, it can attempt thousands of attacks against an application, whether staged or in production. It automatically discovers application entry points (also known as the attack surface) and delivers attack payloads from an extensive knowledgebase. SAST is comprehensive in nature (it simulates all possible outcomes and inspects every line of code) and can identify more types of vulnerabilities than any other analysis method. Additionally, SAST provides full root-cause analysis, which pinpoints the location of vulnerabilities with line-of-code precision.

However, each method also has its weaknesses. DAST must explore the attack surface to launch a successful attack, but its knowledge of potential attack pathways is sometimes incomplete, inhibiting its ability to fully test an application. Additionally, DAST is able to detect only the symptoms of a vulnerability, not its underlying cause within the code. DAST also cannot observe an application's internal behavior. For example, if a DAST tool launched a successful SQL injection attack that destroyed a database, the only symptom DAST might detect would be the appearance in HTTP of a "404 – Page Not Found" error message, with no insight into the error's cause. In this scenario, and others like it, DAST might register the attack as meaningless or even unsuccessful, and hence the underlying vulnerability would slip through undiagnosed. And while SAST offers greater coverage and is extremely proficient at finding potential vulnerabilities in source code, it does not produce concrete test cases to demonstrate the exploitability of the vulnerabilities it finds.

CLICK HERE FOR THE COMPLETE ARTICLE

SYNDICATED CONTENT | ABERDEEN GROUP ANALYST INSIGHT

SECURING YOUR APPLICATIONS: GET STARTED NOW

If your organization hasn't gotten started yet in the area of application security—in spite of the dynamic nature of the application security threat ladscape, the size and diversity of your application software portfolio, and the significant financial impact of the average application security-related incident—do it because of the positive impact on your bottom line. This article reviews several practucal steps you can take to get started now.

BUSINESS CONTEXT: THE BIGGEST NO-BRAINER IN SECURITY?

New headlines provide ongoing evidence that IT Security teams are losing the battle against attackers, reinforcing the need to address the security of enterprise applications. In the recent CitiGroup breach, for example, more than 200,000 cardholders had their names, email addresses, account numbers and transaction histories exposed as a result of a well-known application security vulnerability. As reported in the *New York Times*:

> *The data thieves were able to penetrate the bank's defenses by first logging on to the site reserved for its credit card customers. Once inside, they leapfrogged between the accounts of different Citi customers by inserting various account numbers into a string of text located in the browser's address bar. The hackers' code systems automatically repeated this exercise tens of thousands of times—allowing them to capture the confidential private data.*

In the language of the application security community, this is referred to as a direct object reference, which occurs when attackers are able to manipulate direct references to an internal implementation object (e.g., a file, directory or database key) to access unauthorized data. It's actually on the Top 10 list of web application security threats identified by the Open Web Application Security Project (OWASP)

But this article is not about fear-mongering or sensationalizating the latest headlines to gain your focus on securing your applications. It is about your organization's bottom line.

TOP 10 WEB APPLICATION SECURITY VULNERABILITIES

- **INJECTIONS**
- **CROSS-SITE SCRIPTING**
- **AUTHENTICATION AND SESSION MANAGEMENT**
- **DIRECT OBJECT REFERENCES**
- **CROSS-SITE REQUEST FORGERY**
- **SECURITY MISCONFIGURATION**
- **INSECURE CRYPTOGRAPHIC STORAGE**
- **FAILURE TO RESTRICT URL ACCESS**
- **INSUFFICIENT TRANSPORT LAYER PROTECTION**
- **UNVALIDATED REDIRECTS AND FORWARDS**

SOURCE: Open Web Application Security Project, 2010

CLICK HERE FOR THE COMPLETE ARTICLE