Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Software Security site. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Defending Web Applications Security Essentials (DEV522)"
at http://software-security.sans.orghttp://software-security.sans.org/events/
Survey Participant Demographics  PAGE 2

Application Usage  PAGE 4

Application Development  PAGE 6

Application Management  PAGE 10
Mobile devices, particularly those owned by employees and used to access work applications, represent the latest front for attackers. Employees are downloading applications vulnerable to or infected with malware that mix with company e-mail, productivity/workforce and other business applications.

Because of this new threat, SANS conducted a survey to discover organizational awareness and the procedures around mobile application risk. (This survey follows a first survey, focused on the state of mobile device security,¹ and a second, focused on policies and practices used to secure those devices.²)

In this survey on security of mobile applications, we found that most organizations are concerned about mobile applications and the security threat they impose. The survey showed the following concerns of the organizations:

• Their biggest concern is the security of the device and how it can help protect the apps and app data available on the device.

• They most consistently rely on VPN/access controls, a tried and tested technology for company-issued mobile device access, to protect company applications from rogue bring your own device (BYOD) access.

• The largest percentage (nearly 60%) feel security checks throughout the software development lifecycle (SDLC) are important, and a smaller number is actually practicing these processes.

• Wrapping it all together under management of applications, organizations are having the most difficulty achieving the level of unified access they need to support their policies, including SDLC.

This report covers these and other trends in more detail in the following pages.

¹ www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf
² www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf
Nearly 900 people started the survey, with more than 600 answering the first 11 questions on awareness and practices. When asked if they conducted application development, 253 indicated they did and were sent to another set of questions. That suggests a strong set of developers took the survey; but the majority, being from enterprise organizations that own and manage apps, don’t develop them.

The survey was held online for six weeks during February and March 2013. Respondents came from a wide range of industries. The largest number of respondents came from highly regulated sectors such as the government sector (18%), followed closely by the financial services and “Other” categories—both of which had slightly less than 16% of the total. Government and financial services were similarly represented in our first two surveys, suggesting that mobile application security is becoming a priority or these groups. Figure 1 provides a breakdown of the survey respondents.

![Figure 1. Industries Represented](image-url)
Respondents from multinational organizations were our largest group (26%). This might indicate that these organizations are seeing and adopting more policies around their applications accessed by BYOD practices. But smaller organizations with 100–499 employees were also well represented (15%), hinting that even smaller organizations are beginning to understand the importance of mobile application security (see Figure 2).

Echoing the results from the previous two mobile surveys conducted by SANS in 2012, most of the respondents were security analysts and network administrators, lending a security-in-depth perspective to the survey. When you combine the IT manager/CIO column with the Security manager/CSO columns, you see that a large representation of senior managers (48%) also took this survey. The roles represented in survey responses are shown in Figure 3.

Interestingly, some respondents (41 staff members and 19 consultants) indicate they hold the new title of “mobility director.” The majority of respondents were staff members rather than consultants. While consultants can and do provide specialized skills and help, staff members often have a better and more long-term focus on the mobility issues an organization is experiencing. Their participation in the survey provides us with a clearer view of the needs and concerns of organizations from all perspectives. For example, developers and software engineers provide a different perspective (perhaps wanting to build in security and encryption during app development) than those holding administrative and security jobs, who see security of applications as something to handle after the fact. For example, the latter group—those who manage applications—would be more inclined to add in endpoint security, data encryption and application-wrapping security capabilities to protect against intrusion and leakage through mobile applications.
Our goal with this survey was to go beyond the extent of personal mobile device use to explore what people do on those devices. It is clear that employees in most commercial organizations use both BYOD and corporate devices to access work applications, as shown in Figure 4.

In our original survey, 37% of respondents did not allow BYOD, so this shows an increase in BYOD usage since last year. In this survey, only a small percentage checked that 100% of their users had BYOD access to work applications. The largest group (21%) actually represented the smallest number of BYOD users accessing work applications. Many respondents commented that they did not allow personal devices. Consistent with our previous two surveys, there were lower levels of BYOD usage in the government sector than in the private sector.

What Apps They’re Using

But, what are people doing with their personal devices? The answer to this question will allow us to understand the usage and, therefore, the risks organizations face and the precautions they might undertake. For example, if an organization allows remote access to its network and the connecting device is compromised, the attacker has access into the network and any unencrypted apps. The compromised device can provide remote access, becoming a pivot point from which attacks can be launched. And, the risk is greater when access is granted to business applications such as ERP and collaborative programs.

As shown in Figure 5, not surprisingly, the most common applications accessed remotely are communications and collaboration (i.e., e-mail) and general Internet access (i.e., browser, file-sharing).
Approximately 26% of the respondents say their organizations also allow access to business systems, and 33% allow access to productivity applications. From their large response to network access/VPN (44%), they are likely doing so through secured connections. This implies that these organizations either believe that the device is a safe risk for that level of data access or that they accept the related risks. These risks can be significant, given the media’s attempts to dub the past few years as the “year of mobile malware.”

Another 5% are accessing control system applications from mobile and personal devices; and another 8% are accessing field service applications, which can also be attached directly or indirectly to control systems, providing another pathway into critical control systems. Our hope is that those devices, their operators and employers are 100% aware of the risk and have layered their security or further secured the mobile applications accordingly. According to a SANS survey on SCADA security practices published in February 2013, 70% of nearly 700 respondents feel that there is a high level of cyber risk to their systems, yet lowering risk was very low on their list of priorities, and only 30% have strong security requirements for their control system procurement processes.3

What Scares Them

So, what are the biggest concerns an organization faces with regard to mobile security? Figure 6 reveals that most organizations are worried first about their data, which is, of course, accessed from the mobile app, and then about the device as a launch point for attacks.

These concerns make sense, given that these two categories cover most of the app security risk around mobile devices. It is also interesting that secured access to applications is of concern to 53% of our respondents, given that 44% of them are granting BYOD access via VPN services, as shown in the previous figure (Figure 5).

The rest of the categories checked indicate that at least 30% to 40% are also thinking about the network infrastructure, secure application components and unauthorized BYOD sprawl (managing the proliferation of devices). That number could be higher, and we suspect it will be if we conduct this survey again next year.

3 www.sans.org/reading_room/analysts_program/sans_survey_scada_2013.pdf
In addition to studying how respondents are protecting their applications being used and accessed by BYOD, this survey was also designed to find out how they manage the applications they developed themselves.

**What They’re Developing**

When asked what type of mobile applications they developed, about 2/3 of the survey base were skipped to the end because they didn’t do development. Of those 253 respondents who did answer this question, they are primarily developing web applications and updates (68%), and 32% are developing line-of-business (LOB) applications accessed by mobile/BYOD. Only 20% of those who answered this question are developing mobile apps for commercial use, with about the same amount developing their own cloud applications for mobile users, as shown in Figure 7.

With the organizations’ focus on web development capabilities, and augmented with their cloud development, it’s clear that the web-based interface will be used to replace manual processes to meet new demands to account for mobile access. And, with 32% of respondents building “internal” applications, new risks of data loss and intrusion arise. Organizations deploying their applications on mobile devices will have to develop plans to mitigate these new vectors.

![Figure 7. Mobile Applications Being Developed](image-url)
Choice of Platforms

Because of their popularity today, iOS (87%) and Android (74%) lead the pack as popular platforms organizations develop for. As shown in Figure 8, development for Windows 8 is low (30%) compared to iOS (87%) and Android (74%).

The comparatively low level of Windows development was surprising, given the release of Windows 8 tablets and mobile devices last year. Interestingly, 31% of respondents develop for the BlackBerry platform, which does not seem to have disappeared from the business landscape, despite the growth of other smart device adoption.

Their Priorities

In the survey, respondents were asked to rank their objectives, with 1 being the most important and 9 being the least important objective. It is rewarding to note that they rate the security of the data as the most important objective during development (average rating of 3.38). From the results, performance is marginally more important (3.80) than security of the application (3.86), which is promising. See Table 1 for the ranking of their priorities.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of the data</td>
<td>3.38</td>
</tr>
<tr>
<td>Performance</td>
<td>3.80</td>
</tr>
<tr>
<td>Security of the application</td>
<td>3.86</td>
</tr>
<tr>
<td>Reliability</td>
<td>4.16</td>
</tr>
<tr>
<td>Usability/user interface</td>
<td>4.59</td>
</tr>
<tr>
<td>Security of the network/enterprise</td>
<td>4.75</td>
</tr>
<tr>
<td>Rapid time to market</td>
<td>5.11</td>
</tr>
<tr>
<td>Scalability</td>
<td>5.72</td>
</tr>
<tr>
<td>Other</td>
<td>8.64</td>
</tr>
</tbody>
</table>

Table 1. Top Development Objectives
Not surprisingly, usability, scalability, reliability and performance are seen as more important than application security. This may reflect both the importance organizations place on performance of all applications and a level of management that does not yet appreciate the consequences of insecure applications.

Next, we need to look at what organizations are doing to ensure the security of their systems, data and users. Figure 9 lists several processes that organizations are implementing to different degrees.

The security practices are fairly evenly split among the various phases of the software development lifecycle (SDLC)—with a secure lifecycle being the highest chosen among them overall. No more than 50% chose any other practice; but for those developers, or the organization that supports them, they are evenly focused on dealing with security issues during coding and development.
Specifically, when asked about the use of vulnerability scans, almost 34% of the respondents either do not perform vulnerability scans of the applications at all or perform them infrequently. Continuous monitoring for possible attack vectors is a critical component of the Critical Security Controls (CSCs), particularly Critical Control 2 (inventory of authorized/unauthorized software), Critical Control 4 (continuous vulnerability assessment and remediation) and Critical Control 6 (application software security).\footnote{www.sans.org/critical-security-controls} Figure 10 shows how frequently companies conduct vulnerability scans.

The apparent lack of application-level scanning implies that the organizations are depending on source code reviews and threat assessments to protect their applications and data. We often see organizations depend on their authentication system to verify that a user actually is that user, but tools like Firesheep are able to hijack the mobile application’s session. (Firesheep was originally an attack against Facebook, but it has been improved to add support for multiple mobile applications.) Flaws found in applications after production are more expensive to repair, and if left unattended (as discovered in so many penetration tests), are even more expensive in terms of loss.
Application management is part of the SDLC. Even for organizations that don’t develop the applications being accessed by their mobile users, management of these apps is as critical as secure access and device scanning.

Of the organizations responding, more than half (55%) use internal processes to handle management and services for their applications, as shown in Figure 11.

Externally provided management, represented by use of third-party providers and public clouds, has become popular.

Most of the respondents are using multiple approaches to securing mobile applications. The most common focuses are on securing not only the devices, but also the mobile apps and content those devices use every day.

Their Practices

Figure 12 provides a list of many of the security policies and practices surrounding corporately-owned devices and how frequently they are used. We hope that these policies also address the BYOD devices.

This multilayered approach is commendable, because it builds upon the existing security controls in the non-mobile space. In fact, mobile applications often make use of existing web applications or use features, including encryption libraries, added to the existing applications for additional protection.
However, this overlap of systems and applications makes it imperative that organizations understand their existing controls and how they can be leveraged to protect the mobile users and applications. So, for example, securing the devices through use of tools such as Mobile Device Management (MDM) or enhanced NAC (Network Access Controls) organizations are also protecting against rogue applications, because both of those will check for unapproved or malicious applications based on their programmed policies. This is also a plea to MDM vendors to provide more integrated security services regarding encrypting access to business applications from MDM protected devices.

Management Difficulties

There appears to be little difference in organizations’ perceptions of how difficult these policies and practices are to implement. Most respondents consider implementation to have some moderate level of difficulty. Figure 13 shows the average difficulty ratings for each of the security policies and procedures, where 1 is “not particularly difficult,” 2 is “difficult,” and 3 is “extremely difficult.”

The higher the average score, the more difficult it is to implement the policies and procedures. Not surprisingly, protecting applications with strong authentication was comparatively easy (1.70), which is in keeping with organizational concerns (Figure 5) and controls (Figure 9).

The security industry has been using such procedures for a long time with company-issued mobile devices. On the other hand, providing an identity management framework to support remote devices (2.05) and ensuring secure development of applications (2.01), were considered more difficult. Not far behind is secure development and lifecycle practices. This applies to both development and management of applications being accessed remotely by BYOD. As stated earlier, there needs to be much more maturity in the mobile space, given the breadth and nature of threats being aimed at mobile devices.

Taken together, the results provided in Figures 12 and 13 suggest that organizations recognize and are doing the difficult work of implementing policies and practices. Moreover, they suggest that organizations should place some emphasis on developing techniques that rely on tried and true security policies to secure mobile applications. In addition, it seems clear that additional focus is required on providing adequate security review during the SDLC.
Conclusion

As organizations and their staffs continue to rush down the path of implementing and using mobile devices and applications, security needs to continue to focus on our implementations. This is becoming both easier and harder as time goes by.

The rush to implement or build mobile applications is adding to the complexity security and IT staffs have to handle. This means that responsible staff members have to be on top of the latest threats and controls available to the attackers and defenders. Proactive security during development and deployment should become a best practice.

The following suggestions can help organizations accomplish their security goals:

• Ensure and adjust policies to include the devices the organization allows to access network resources. For example, institute a policy that describes the type of mobile devices allowed to access the network.

• Evaluate the applications, data and access the mobile devices use to determine what needs can be addressed.

• Consider the inclusion of mobile app security encryption libraries during development, or apply them to third-party apps being used for larger scale corporate deployment.

• Perform security assessments of applications being built or developed. Start even before the application development begins, and continue assessing applications in production, as per the CSCs.

• Assess the mobile devices and their supporting architecture as often as possible, keeping in mind that many of the devices may be owned by employees.

• Continue to enable users with education and security updates.

These are broad-stroke mechanisms to consider for protecting the network, resources and data on endpoints from malicious hostile applications. Architectures deployed to manage this new risk need to be capable of expanding to new types of devices and applications because users will continue to make more demands in the future.
Kevin Johnson is a senior security consultant with Secure Ideas. Kevin has a long history in the IT field including system administration, network architecture and application development. He has been involved in building incident response and forensic teams, architecting security solutions for large enterprises and penetration testing everything from government agencies to Fortune 100 companies. Kevin is the author of three classes: SEC542: Web Application Penetration Testing, Ethical Hacking; SEC642: Advanced Web Application Penetration Testing and SEC571: Mobile Device Security. In addition, he is an instructor and author for the SANS Institute, a faculty member at IANS and a contributing blogger at TheMobilityHub.

James Jardine is a principal security consultant with Secure Ideas, LLC. James has over 12 years of software development experience, with over half of that focusing on application security. During his long development history, he has written both large enterprise applications, thick clients and mobile applications. He has held many roles including senior developer, software architect and application security expert. James is also involved in the open source community. He runs a number of open source projects, including WCSA (a security analyzer for web.config files) and EventValMod (a tool to modify event validation values in .Net). He is also a contributor to the Laudanum project (a collection of injectable web payloads). In addition, James is an instructor and author for the SANS Institute. He is also a contributing blogger for the Secure Ideas blog, the Jardine Software blog, and the SANS Appsec blog.

**SANS would like to thank its sponsors:**

- box
- SAP
- Veracode
# Upcoming SANS App Sec Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Copenhagen August 2020</td>
<td>Copenhagen, Denmark</td>
<td>Aug 24, 2020 - Aug 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>