Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2rCnBMg

Mobile Security Tools on A Budget

Mobile has arisen as one of the most flexible—and most prevalent—business tools available. From email to calendaring to business applications, employees are, quite literally, doing business from any device, any time of the day or night, from anywhere and everywhere on the planet. Mobile functionality has evolved from a convenience to a necessity, from a luxury to a necessary and critical component of the business environment.

As mobile has increased its business utility, it has also become one of the more challenging areas to safeguard. Not only is bring your own device (BYOD) becoming the norm in many enterprises, bringing with it an array of disparate devices into the workplace, but the increase in sophistication of both mobile devices and the applications (apps) that reside on those devices means a wider array of security and assurance challenges than has ever before been the case. Granted, it is true that both organizations and practitioners are becoming more sophisticated in their approaches to mobile and, thereby, are becoming better able to anticipate and respond to challenges in the mobile space. However, it is still very much an area of focus for organizations as it continues to represent one of the leading attack vectors and a large chunk of the overall enterprise attack surface.

Because of this, savvy practitioners are always on the hunt for tools and techniques they can apply and adapt to help them ensure that devices are protected appropriately. Fortunately, there are quite a few good tools and resources out there that are available for relatively little (or no) cost.

Note that the tools described in this article are not the only tools out there—nor is this list intended to be an exhaustive one. This article's focus is specifically on tools that are freely available—open source, community-supported editions of commercial tools, free resources, etc. These tools, indexed by category, might help solve specific security and assurance challenges relative to the mobile environment. Some of them pertain to testing scenarios on the mobile devices themselves, others relate to ensuring known-good configuration, and still others relate to leveraging older mobile devices (always easy to come by) to accomplish other security and assurance tasks.

Ed Moyle
Is director of thought leadership and research at ISACA®. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers, and senior security analyst with Trintech. Moyle is coauthor of *Cryptographic Libraries for Developers* and a frequent contributor to the information security industry as an author, public speaker and analyst.

Endnotes

1 Weidman, G.; "Using Dagah GUI," YouTube video, 30 March 2017, *https://www.youtube.com/watch?v=dqBOs4YT36M*

1 Mobile Application Testing Tools

For those organizations that have the skill set internally to perform hands-on testing, there are a number of tools that can assist in the testing of mobile devices themselves or the business applications they commonly run. Insofar as testing of applications goes, web proxying tools such as Burp Suite *(https://portswigger.net/burp/)* and Open Web Application Security Project's (OWASP) ZAP *(https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)* are excellent choices. These tools allow users to "snoop" on traffic between the mobile device (or, really, any device) and web applications with which they interact. A web testing proxy such as this intercepts messages between the mobile device and the application and allows the manipulation of various parameters (e.g., HTTP headers, response parameters) in between the mobile device and the web application. Note that these tools are useful outside of the mobile device world as well; they can be used to test any web application regardless of the platform on which it is employed. However, because mobile device use is tied so closely to the applications they run, they are addressed here.

2 Mobile Device Testing Tools

In terms of specific testing of the mobile devices themselves—including malicious applications and testing of user behavior such as responding to phishing or SMishing (phishing via short message service [SMS])—there are some fantastic options as well. The first one is the community version of Shevirah's Dagah tool *(https://www.shevirah.com/dagah/)*. Those in the penetration testing space may recall the Smartphone Pentest Framework *(www.bulbsecurity.com/products/smartphone-pentest-framework/)*, developed by Georgia Weidman in response to the Defense Advanced Research Projects Agency's (DARPA) now-defunct Fast Track grant. The community edition does have some limitations (in terms of number of targets per campaign), but it does provide the tester with the ability to target mobile devices and customize attack scenarios and delivery of those attacks to a mobile device. There are even video instructions[1] that explain common usage scenarios.

3 Mobile Forensics Tools

Of course, situations arise whereby one may need to investigate a device to determine if the device has been attacked—or to otherwise evaluate a potential incident impacting a mobile device. If one is investigating a specific device from an investigation standpoint, a fantastic resource to have in any arsenal is the Santoku Linux distribution *(https://santoku-linux.com/)*. Santoku is an entire Linux distribution dedicated specifically to mobile device forensic examination. Other testing and incident response platforms do contain mobile tools; for example, both Kali *(https://www.kali.org/)* and CAINE *(www.caine-live.net/)* contain mobile analysis tools. However, Santoku has the advantage of being entirely designed specifically from a mobile analysis perspective.

4 OS Management Tools

From a device management standpoint, there are a few options as well. Not only are there tools that are built into the ecosystems of both Android and iOS, for example, the Apple Configurator (*https://support.apple.com/apple-configurator*) and the Android Device Manager (*https://www.google.com/android/devicemanager*), but there are also tools that provide privacy tools (e.g., The Guardian Project [*https://guardianproject.info/*]) and hardened OS configurations (e.g., CopperheadOS [*https://copperhead.co/android/*]). Depending on an organization's needs and usage context, these tools could potentially have a role to play. A small/medium business (SMB), for example, might find that the Apple Configurator fits the bill for initial hardening or that Android device manager's basic device protection services, such as remote wipe in the event of a lost or stolen device, are sufficient for its needs without employing a heftier (read "more expensive") solution.

5 Repurposing Mobile Devices

One area of opportunity—particularly for an SMB or severely budget-strapped organization—is the repurposing of mobile devices to accomplish other security tasks. Anybody who works in IT will tell you that one thing they tend to have quite a bit of is old, out-of-date or otherwise unused mobile devices such as decommissioned employee smartphones. Under the right circumstances, these devices can actually still provide some value to a security team. For example, there are applications that allow an Android or Apple smartphone to operate as a remote security camera. The specific app to do this varies by platform, but almost any smartphone with a camera (even if no longer connected to the cellular network) can provide video or still image data via a WiFi connection. Is this a replacement for an "enterprise-grade" monitoring capability? Of course not. But it can provide a stopgap mechanism to ensure that locations are being appropriately monitored on a short-term basis in certain situations—for example, in the interim period between when a gap in coverage is identified and new equipment is fielded or in the case of a short-term extension in coverage.

Likewise, older (typically Android) devices can be used as remote wireless access point detection mechanisms in certain situations, for example, an organization with a large physical area to cover (e.g., numerous remote field offices or retail locations). There are literally dozens of free WiFi analyzers in the Android marketplace that will provide information about wireless networks in range. When used at a location where rogue access points are an issue and monitored remotely, these tools can alert to new, unexpected access points. Again, is this the ideal solution for all wireless intrusion prevention needs? Probably not. But can it make for a low-cost stopgap to help accomplish very targeted tasks such as rogue access point detection in the short term? Yes, it can—and under the right circumstances, that can be valuable.