

Are Your Devices Secure?

Mobile devices pose significant security risks for today's organizations. Don't believe me? In the past six months alone, I have exploited and extracted data from iPhones and iPads a few hundred times.

As a security professional, it's my job to know – not guess – the exact risks that devices pose to an organization's network. I'm in a constant race to help others understand mobile device security risks before it's too late. In my experience, the easiest way to demonstrate risk is to show just how easy it is to actually exploit and extract data from devices with others looking over my shoulder.

Hackers Target Mobile Devices

It's no surprise that mobile devices are an attractive target for hackers. They are powerful little computers that encourage users to store important data and information locally and on apps. Unfortunately, many users make the mistake of thinking that their devices are secure simply because they don't have wires coming out of them.

Knowing the risks that mobile devices pose, it's hard not to become the *no* man. I know first-hand how tempting it is to say *no* to users requesting access to corporate email and file shares on a growing number of diverse devices. There's simply too much risk. What makes it even harder is saying *no* without being able to demonstrate how devices can expose users and organizations to risk of data theft and corruption, which certainly doesn't help one's reputation.

And let's face it, reputation counts. I love the IT Crowd as much as the next guy, but I want to be seen as a

business enabler. I have spent a lot of time proving to business executives that baking security into initiatives early can lead to a smoother project. Not security for the sake of it, but security that helps ensure the system is more stable and reliant. I don't want to ruin the result of the hard work to understand the critical goals of the business groups just to turn around and say *no* to every mobile request that comes in.

Criteria for Testing Mobile Devices

I've gotten smart about mobile device security and I've established criteria by which the security of any mobile device can be physically tested. This isn't a paper exercise, but an actual attempt to break into devices and extract data.

The fun part is performing tests in front of device owners. Nothing says permission to exploit like having them click on the link!

The criteria can be boiled down to two categories:

- How easily is the business able to control the device and the data on it?
- How easily is an attacker able to control the device and the data on it?

Business control is fairly straight forward. If an organization can't remotely configure, update or wipe the device, then it is in trouble.

Join

PenTest Mag team!



PenTest Magazine is looking for regular contributors. If you want to be a part of the first magazine devoted to penetration testing, now's your chance to join us. We especially need:

- news contributors – send in a piece of news of an interest for a pentester and make your own comment on it.
- “point of view” section writers – short articles (800 words tops) with you discussing an issue you think should be discussed.
- “vulnerability check” writers – what a pentester can use in his work.
- reviewers – found an interesting tool? Review it for us.
- betatesters – read an article before it's published in the magazine and share your opinion on it with us.

Regular contributors are given free subscription to the magazine and – if they represent companies – free advertising in the mag. And, of course, an earned mention in the magazine.

Worth it? Ask for details:

maciej.kozuszek@software.com.pl

Attacker control, however, is a bigger worry. If an organization can't leverage the commercial-grade equivalent of the exploits and techniques used by attackers, they are only measuring how to manage the device. It's like ranking missile defense systems by how easy each is to launch without ever testing the capability the system has to actually prevent an attack from being successful. Simply put – if a device is easier for an attacker to control than it is for IT operations to control, the risk obviously isn't worth it.

Simplifying Risk with a Pen Testing Solution

Professional pen testing products make performing pen tests and understanding risk simple. Pen test solutions allow organizations to run pen tests against servers, web applications, end users (via email), the new WiFi network they just added to the conference room, or my personal favorite, the multi-vector attacker where they bounce from one vector to another.

It's absolutely critical to perform pen testing against your organization's mobile devices. Pen testing produces real world metrics on how devices stack up against security criteria, which every business unit can understand. Knowing this, organizations can make informed decisions to determine if mobile device security risks are acceptable to the business.

The beauty of a well thought out mobile penetration testing plan is that every time you exploit someone's phone and show the data that can be exposed, they thank you. For me, I just look them in the eye and tell them not to thank me – it's my job.

ALEX HORAN

Alex Horan is a product manager at Core Security (<http://www.coresecurity.com/>), a security test and measurement company that helps more than 1,300 enterprises and government organizations worldwide address and manage critical online threats throughout the entire IT infrastructure. Alex can be reached at ahoran@coresecurity.com.