Mobile Device Security Threats, Risks, and Actions to Take
Transcript

Part 1: Why Mobile Devices Are Becoming More Vulnerable

Julia Allen: Welcome to CERT's podcast series, Security For Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org. Shownotes for today's conversation are available at the podcast website. My name is Julia Allen. I'm a senior researcher at CERT, working on operational resilience and software assurance. Today I'm pleased to welcome Jonathan Frederick. Jonathan is a member of CERT's Workforce Development team, and today he and I will be discussing the increasing security threats to mobile devices -- something we haven't talked about before on the podcast series -- and some ways to combat these. So welcome Jonathan, really glad to have you with us today.

Jonathan Frederick: Thank you. I'm glad to be here.

Julia Allen: So we're hearing lots about mobile devices, all types, all persuasions, they're becoming more ubiquitous, cell phones, smart phones, PDAs, tablet PCs, Bluetooth, all of it is kind of flying fast and furious in terms of network connectivity. So why are these now increasing their profile on the radar screen when it comes to being more vulnerable to attack?

Jonathan Frederick: Well, the same thing that's making them this popular, where everybody wants to have one, is also making them more vulnerable to attacks. So these are the new capabilities, specifically things that come out with the new smart phones: the ability to send text messages, also to send multimedia messages, connect them to wireless LANs in order to pull down content from the internet, and also the GPS capabilities that are built into these new devices. We can also connect them physically to our personal computers in order to transfer files onto them or to manage these devices. Now the problem with this is that we're lacking the firewalls and intrusion detection systems, and also usually virus protection that we have on our personal computers. So these are a lot more open to vulnerabilities than personal computers in our homes.

Julia Allen: So do you think it would be fair to say that when it was just phone to phone, mobile phone to mobile phone, and we were just using the carrier-provided networks, it was a little bit safer? But now that they're all becoming so internet-connected without the commensurate protections, that that's really a part of what's happening?

Jonathan Frederick: Absolutely. There was some vulnerabilities with just the simple voice communications years ago but not to the degree that we have today. Maybe a phone that was on an analog voice network could be spoofed, but it's not nearly as critical as the financial transactions that could be compromised with today's smart phones.

Julia Allen: Okay, because I know you said, as we were preparing for this podcast, you were talking about the fact that these devices are holding more data, right?

Jonathan Frederick: Right, absolutely. They're holding a lot more data. And the older phones are typically again, you just have your logs, your contacts, and maybe some text messages. And that data can actually be compromised and maybe used as a blackmail against an individual, or it's definitely a privacy concern. But the newer smart phones can hold corporate data, financial data, secret keys that are used for VPN into corporate networks, and also other authentication like stored credentials. So all that data is a lot more critical, especially when you start to look at an enterprise perspective.

Julia Allen: Okay, and what about the fact that they're kind of like also our personal locater devices, right, because we carry them with us all the time?

Jonathan Frederick: Absolutely. There's GPS built into pretty much every device out there right now. And this is a feature that the mobile carriers -- Verizon, AT&T, Cingular -- really like, because they can sell additional services. So a lot of these GPS-enabled devices can link back to Verizon's website and parents can maybe track their children, and you pay an extra ten dollars a month for that feature. So there was a big push for GPS to be embedded into all new devices so that somebody can make a profit off of these.

Julia Allen: And I found thinking about this a little bit more, the fact that there are all these unsecured wireless LANs that are out there, and as we are walking through these various areas, we can -- isn't it correct that we can be unintentionally connected to them?

Julia Allen: Especially the iPhone; it has the most vulnerable aspect of this. And what happens is, once an iPhone is connected to an unsecured wireless LAN, if it goes out in the public somewhere and finds that wireless LAN name out there again, and that's unsecured, it's not even going to ask the device owner for permission to connect. So it will automatically connect to this and this can be malicious LANs, so that somebody can be out there actually pulling down the packet captures as information is transmitted from the iPhones.

And this is especially a concern because whenever you go out and buy a new Linksys, or a new Cisco wireless router, they're all named the same thing by default. So if you take one of these items home and connect to it, it's going to have the same name as someone that purchased one right out of the box.

Julia Allen: And what about users? Are you finding in your research and in your interactions with the community, that users of these devices are aware of some of these emerging threats, or do we have a big awareness hurdle to cross?

Jonathan Frederick: We definitely have a big hurdle to cross here. And I think that we've all experienced maybe malware or possibly a credit card number being stolen from a PC transaction, or we certainly know someone that has. But we haven't really experienced the problems that can be associated with mobile device security.

There was a study done, late in 2009 by Trend Micro and they found that 77 percent of users were actually not enabling any security features because we don't see it as a threat. And that definitely also comes into play because we're not -- we don't want to be inconvenienced. So the amount of time it takes to submit a password into our mobile device in order to get into it, nobody wants to take that additional time out of their day and have it more secure for that reason.

Julia Allen: Well that makes sense. I know I don't like to be inconvenienced, and here we are in the business. And we're probably -- some of us aren't doing what we're supposed to do with respect to our mobile devices, right?

Jonathan Frederick: Right, definitely.

Part 2: Growing Threats to Devices and Back-End Systems

Julia Allen: So okay, so I'm getting the feeling that we've got this bow wave that's starting in terms of both the ubiquity, the connectivity, the emerging threats, the fact that we have more data. So are we kind of at a tipping point in terms of what may have delayed attacks up to this point, and they're starting to come on the horizon? And are there some trends that will cause the attack profiles to have an uptick?

Jonathan Frederick: Yes. So the fact that smart phones have only recently -- and when I say recently, maybe two or three years -- become as popular as they are definitely has delayed a lot of attacks. There are a lot more attacks that can be associated directly with smart phones instead of just your common voice phones.

In the beginning of 2009, there was only 16 percent of the market that had smart phones, and now in the beginning of 2010, there's been 23. And I honestly think that within two or three years, we're going to see that number a lot more close to maybe 50 percent. Because the device carriers, Verizon, AT&T, Cingular, aren't really selling those old voice-only phones anymore. And again, that's because they want to make money. So if they sell -- if the only phones that they have for sale are smart phones, then they can maybe convince someone to purchase a data plan or purchase a multimedia messaging plan.

Julia Allen: Well that makes sense too. I can see that, as we evolve to smarter devices, obviously there's opportunity and there's risk. What about for the criminal element? They've probably been watching what's happening here. But what might make mobile device attacks more profitable for the criminal element?

Jonathan Frederick: Well that's the main key here, is that the criminals need to actually have some kind of financial gain here before they want to begin to attack devices. So in the PC realm, we've been doing this for years. They send you a piece of spyware that says, “Send us your credit card.” Or a phishing attack, where they might be able to pull down credentials to get into a bank and set themselves up as a bill to be paid. And now we're heading into that direction for smart phones as well. There was a study done by Data Innovation Corp, and it showed that 70 percent of smart phone users were actually checking balances on their smart phones. Now that may sound high, but that's definitely not nearly as scary as the 40 percent that were found to be transferring funds, and the 29 percent that were actually paying bills from their smart phones.

This information is definitely key to a criminal because they'll be able to maybe perform a man-in-the- middle attack and send those funds in a different direction, maybe to their own accounts. There's also been applications that have just been recently, like within the last six months, developed for transactions. PayPal has come out with an application for iPhones where you bump two iPhones together and it actually performs a financial transaction. And we have the capability to swipe credit cards in a little sugar-cube sized device that connects to our phones and then be able to record the magnetic strip and send it off somewhere.

Julia Allen: That's really scary, isn't it? We're starting to use these devices for all aspects of our life with, I suspect, not much realization of these types of risks, right?

Jonathan Frederick: Right, absolutely.

Julia Allen: What about some of the, like what some of the vendors are doing in terms of the custom implementations of operating systems? I suspect the diversity, or the heterogeneity of mobile device operating systems, has helped but are you seeing a shift there?

Jonathan Frederick: Yes, absolutely. There was a study done by the Nielson Company and they found that 91 percent of smart phones were either using BlackBerry, Apple's iPhone, Mobile -- Windows Mobile, and also the new Android. And the concern here is, from a financial perspective for a criminal, they want to get the most bang for their buck. So they want to develop applications, malicious applications, spyware, that's destined for a larger user base than say, maybe, just one single device that's using its own custom implementation of a Linux operating system.

Julia Allen: Right, so they basically have a larger attack base, right?

Jonathan Frederick: Right, absolutely. So as we move closer to that, as the iPhone takes over the world pretty much, those are going to be where the attacks come from the most. Those are what's going to be profitable for a criminal to actually develop the malware for.

Julia Allen: Okay, you mentioned malware and spyware, and we all know that apps on things like the iPhone are becoming more and more popular. People download them without even thinking about it. What about apps and malware? What are you seeing in terms of connections there?

Jonathan Frederick: Well there's been some documented instances where there's been malware inside of an application. It can be maybe repackaged or bundled with legitimate applications.

There was a case about three or four months ago, where there was a Windows Mobile application that could be downloaded, and to the common person, it was just a 3D shooter game. But on the back side, while this person was playing this game, it was actually dialing, autodialing premium rate numbers and charging that customer a lot more money through the mobile carrier.

Julia Allen: Well you started to mention some of the unique security threats, things that are above and beyond what we would typically see for a normal PC or a laptop or other type of normal computing device. But are there some other unique security threats that mobile device owners should be paying attention to?

Jonathan Frederick: Sure. So the greatest threat is definitely your malicious applications and that's your adware and spyware. They could steal information off the devices and send it out to maybe a command and control center. They can also perform a denial of service. And historically, the malware that has been out in the field on mobile devices, that's definitely been the most common.

So not nearly as big a concern as actually stealing information off because you're only usually affecting one user and one mobile device, whereas denial of service on an entire corporate network would definitely affect a lot more financial information and things like that.

Julia Allen: So you're saying, as users put more -- if they're using their mobile device for connecting to their home organization's network and downloading business information, clearly some of the malware that can have access to that information, that becomes a much bigger issue, right?

Jonathan Frederick: Yes, definitely. These devices, once the malware gets into them, they can also run commands. So that example that I provided earlier with the 3D shooter game, a criminal could actually set up a 1-900 service and then have this malware give it a call continuously and be charging the customer a lot of money for that service.

Julia Allen: And what about intercepting voice and data transmissions? Again, this notion of our mobile device as a personal locator that we use for everything that we're doing. Are you seeing instances where that's starting to happen?

Jonathan Frederick: Yes, definitely. If you go to Google and actually search for mobile device tracking, or something very similar to that, you'll come up with at least a dozen different companies that will sell just about anybody with a sufficient amount of money the software required to actually perform this. So if you are able to get someone's device, temporarily install the software, which may or may not take a considerable amount of time, and then get that device back in the hands of the user prior to, before they actually know that it was taken in the first place, you then have the capability to retrieve text messages, review the logs. And you could even go as far, with some of the software, as turning on the microphone and sitting there and listening to the conversations that were going on while that device was in the possession of their owner.

Julia Allen: Wow. One of the things that I found, that I hadn't even considered when you and I were talking earlier, is the notion of some of the back-end systems that are used by the mobile service, or telecommunications service providers, to service all of these different devices. So what things should we be concerned about there with respect to the back-end systems?

Jonathan Frederick: Well the back- end systems are probably the most overlooked. We don't typically -- we see our device, we know to keep it locked up, or to keep it on our person at all times. But we're not thinking about that back- end system that's holding possibly the same information as the devices themselves. So a good example of this was actually the Paris Hilton T-Mobile Sidekick incident that happened and was in the media a couple of years ago. And a lot of people instantly thought, “Wow, somebody hacked into the Sidekick and what's going on here? Is mine vulnerable?”

But in reality what happened was an attacker actually compromised the T-Mobile servers themselves and then was able to pull down the same contacts and other information that they would have been able to get if they physically had access to that device. There's also a lot of BlackBerry server vulnerabilities. So it's not just the public that needs to be concerned; it's corporations and enterprises as well. There's been 13 BlackBerry enterprise server vulnerabilities in the CERT database since 2005.

And just last year there was one where if a specially crafted PDF was sent to the BlackBerry server from a device, someone could then execute code on, without any restriction on, those BlackBerry servers. And that's kind of the keys to the kingdom. From there you can get into other servers and steal corporate information.

Part 3: Mitigate Mobile Device Security Risks

Julia Allen: Well we've certainly spent a good part of time so far talking about the emerging threats, the ubiquity of the devices, the things that, the approaches that could be used to attack phones and steal data that's stored on phones. So why don't we turn our attention to how do we get our heads around this and take action to try to mitigate some of these risks? Do you have some particular recommendations on what actions organizations can take to start to get this a little bit more under control?

Jonathan Frederick: Absolutely. So the first step is actually performing a risk analysis and determining what are the risks of our organization. Or you could think about it from a public standpoint or a personal level, and say, “What information am I willing to put onto my devices?” From there you perform device selection, and BlackBerry, historically, has been known as the most secure device for anyone, both personal and corporate-size customers. And this is mostly because the BlackBerry devices themselves actually encrypt the data. So if you were to lose that BlackBerry device, you wouldn't be able to have someone go out and access the memory and pull down the information later on. But also BlackBerry's accredited so of course the government and large enterprises really appreciate that as well.

Another thing that you can do to mitigate these is again perform your risk analysis but then figure out what features do you actually need. And a good example of this is the Air Force who has disabled the multimedia text messaging capabilities of their BlackBerrys. They've also limited the BlackBerrys from installing any additional applications, which would keep you from pulling down new malware. And the Bluetooth is disabled with the exception of their common access card readers, which allows them to have multifactor authentication into the BlackBerry devices --

Julia Allen: Excuse me, you make an interesting point here, which you were probably about to elaborate before I cut you off. But this notion of a corporate or an organizational or, in this case, a government device that's used to conduct government business versus a personal device.

What are you seeing? Because we're all so used to using our devices pretty much for any aspect of our lives. But are you seeing some of the actions and risk mitigations be around controlling device use and therefore having more control over device configuration?

Jonathan Frederick: We’ll Take the government for example, because they're the biggest. But they typically are not going to allow a user or an employee to bring their personal device and attach it to their corporate network. So in their case, they actually give devices out to the critical personnel that are going to need them. And this is extremely beneficial because you can perform configuration management. You can certify and accredit the actual devices and hardware and maybe the network that that information is going on.

Whereas, the other hand is allowing your customers or your employees to bring their devices and attach it to your network. And that's when you start to lose that control. But it may be necessary in some cases, because the US tax laws are going to require that a business device, something owned by the business, is only used for business purposes, and that can be challenging. That can definitely be difficult to monitor and maybe even a privacy concern -- telling your employees that, “Here's a device and you have to carry two now, one for business, and one for personal, and it can only be used for business purposes.”

Julia Allen: Do you think on that, if a business leader wants to adopt that particular strategy or evaluate if that's going to work in their organization, do you think it ties to mission? What I mean by that is, if the organization has critical data that needs to be accessed by mobile devices, that the mission can actually help drive, and maybe that's part of the risk analysis that the mission can help drive the determination about do we go separate, or do we allow personal devices? Are you finding that that's a consideration?

Jonathan Frederick: Yes, definitely. So if you have no need for your users or your employees to have that information while out on the road, then they shouldn't maybe have a device in the first place. You've got to take steps back and start from the beginning and say, “Does our mission actually require that?” And sometimes it may, and sometimes it may not.

Julia Allen: And what about the tradeoff between data on a mobile device versus data on a PC? Are you finding cases where organizations have opted to keep, because the PC environment is more secure, they've opted to keep information constrained to only being accessed via PC versus accessed by a mobile device?

Jonathan Frederick: Yes. So typically our PCs, we have policies in place, we've been dealing with them for years and setting up the restrictions and antivirus and everything else. And it might be better just to tell your employees, "Okay, instead of actually transferring information that you're going to need to access later onto your mobile device, well go ahead and use a net book." The boot up times of the more recent operating systems can be just as quick now as maybe a mobile device. And also then you really lock down the devices from ever actually pulling this information in and then exposing that risk later on out in the public somewhere.

Julia Allen: Excellent. Well I think those are all great recommendations. So Jonathan, I know we've only touched the tip of the iceberg here but do you have some sources and places where you would recommend our listeners take a look to learn more about this?

Jonathan Frederick: Sure. So whether you are government or maybe even a personal user, a really good place to start is the National Institute of Science and Technology's special publication 800-124, and that's your guidelines on cell phone and PDA security. And they're going to cover a lot of the same things that I just did. It may be a couple of years out of date and might not go into the applications and maybe malware as much.

But in addition to that, you could browse more recent incidents and also go directly to your device's vendor. So if you have an iPhone, go out to Apple and see what they're saying. If you have a BlackBerry, there's tons of white papers comparing BlackBerrys and iPhones and mobile devices.

If you are a corporation and you run something such as BlackBerry exchange server, which a lot of places do, you can go out to the DISA STIGS website and that's iase.disa.mil. And you can actually pull down a security checklist of what the DOD sees as a best practice for securing your BlackBerry enterprise servers. On top of that you can also pull down a policy file which could then be imported directly into your servers and you don't even have to go through the 100-some manual checks that set up the security there.

Julia Allen: Excellent. Well I can't thank you enough, Jonathan, for your time, and your expertise, and shedding a light on this growing issue, and providing such strong recommendations for our listeners to consider. So thanks very much for your time today.

Jonathan Frederick: Thank you as well.