Black Hat 2011: Android attacks and smartphone privacy leaks

Interviewer: We're here with Neil Daswani. He's Chief Technology Officer at Dasient. You actually have a talk here at Black Hat, on some of your team's vulnerability research, as well as some malware analysis. Let's start with the Android attack that you're going to be talking about. How serious is this? Give us a few details of what you guys came across.

Neil Daswani: So, I'll be giving a talk on Thursday. And I'll be covering some of the findings from our team. We have been spending a little bit more time looking at Android security. There are two key contributions that we will be talking about. The first is that if you look at most mobile malware, they've been spreading as Trojans: programs that do one thing but claim to do something else. And, if you look at malware distribution on the web, a lot of malware gets spread by drive-by downloads.

So one question that we wanted to answer is "Is it possible to spread malware on Android via the drive-by vector?" And so one thing that the team has done is put together a prototype drive-by for Android. We'll be talking about that, and how that works.

The second major contribution that we put forth in our work is that we analyzed behaviorally 10,000 Android applications, and identified that some of them were conducting privacy violations, some of them were incurring some negative performance, and some of them of course had interesting security implications. So, we'll be covering both the prototype drive-by, as well as the data that we learned from analyzing the 10,000 Android applications.

Interviewer: Let's talk a little bit more about the prototype drive-by. It takes advantage of two vulnerabilities, right? One in WebKit and the other in Skype. I thought that Android has some security features built in--Sandboxing being one--to kind of prevent these kinds of attacks. What's going on here?

Neil Daswani: Sure. So, Android has had quite a bit of work put into its security. That said, the operating system is a piece of software just like any other, and software has vulnerabilities. So in the prototype, what we have strived to look at it is that there's been a lot of different component vulnerabilities--in WebKit, in Skype, and in a number of other packages.

The question we wanted to answer is "Is it possible to glue together these vulnerabilities to create a drive-by, much in the same way that malware distributors do on the web?" We found that that indeed was the case. And in this particular prototype we used an issue vulnerability against WebKit as well as one against Skype to steal the user's IM conversations off the device.

But one thing that I should note is that when you have vulnerabilities in software like WebKit, it's possible not just to steal the user's Skype/IM conversations, but to conduct other kinds of attacks using vulnerabilities against other client-side software, as well as against the operating system itself--to take root access, and pretty much own the device.

Interviewer: Wow. Is this something that has already been patched, or is this still in the wild, still available?

Neil Daswani: These two vulnerabilities that were used in this particular prototype drive-by are both known vulnerabilities. That said, they are patched on some systems but not others. One of the things that we've been seeing in the Android and mobile device world is that patching currently takes longer than patching does on desktop/PC platforms. So, ten to twelve years ago, the world worked and moved towards getting on a weekly patch schedule, for instance, for Windows. And because of the complexity of carriers' networks, operators, and all the different devices, the world is still getting there. But that said, the good news is that carriers have the opportunity to help create such a patch cycle and keep it organized.

Interviewer: In terms of the iPhone, is the iPhone susceptible to drive-by attacks as well?

Neil Daswani: The iPhone has had a drive-by attack published about it. There's for instance a site called jailbreakme, and if you go to the Jailbreak Me site on your iPhone, then supposedly you can get your iPhone jailbroken just by loading the webpage there at that site. So, drive-bys seem to be possible on iOS as well. IOS is a complex piece of software, just like many others. I think that thus far we haven't seen as many drive-by attacks on these mobile platforms, but there's nothing to indicate that they won't be soon to come, because of the fact that the devices are getting used more and more so for mobile commerce and mobile banking, and we'll have to work together to keep the world a

safer place.

Interviewer: You mentioned patching, and how it's a little more complicated for mobile platforms, especially I suppose Android, right, because there's so many different devices out there, and then you've got the carrier issue. Is that really what complicates it?

Neil Daswani: That is one for the things that complicates it. If you look at the Android world, there are a lot of different carriers, there are a lot of different devices. Even though the OS is the same, there are many different versions of the OS. So that makes uniform patching harder.

At the same time, if you look at the Apple platform, Apple has a lot more central control. So they are able to do updates and patches in a more uniform way. It currently requires some level of user permission. Each of the platforms has their own trade-off. If you look at the Android platform, just about anybody can write an application. You don't have to go through a very complex vetting process. Some may hope that will lead to more innovation and more applications.

At the same time, it also means that keeping the environment locked down and keeping security in good shape will probably take a little bit more work in the Android world. Of course, in the iOS world, there's more centralization. What that may mean is that there may be fewer applications that come out due to the vetting process. But I think it will remain to be seen. We'll have to see where things go.

Interviewer: Let's move on. This actually brings us to your analysis of all of these applications, 10,000 Android applications. And you found some interesting things, some privacy issues.

Neil Daswani: We certainly did. We conducted a behavioral analysis of these 10,000 Android applications and found a couple of things relating to privacy that I think are definitely worth mentioning. Out of the 10,000 applications that we had analyzed, about 8% of them, or just 840 of them, were sending the user's IMEI number off to a remote server. The user's IMEI number is an ID that is tied to their device, and basically it can tell the remote server things like how long that user has been using the phone over time. It can also be used for other reasons. In addition to the IMEI number leaking in some of the cases, the IMSI number was also

leaked in some amount of the cases.

About 60 applications leaked their IMSI number. And both the IMEI and the IMSI number could be used to clone the phone and/or the SIM card that's being used. The reason that's not good of course is that an attacker could potentially clone a SIM card and charge calls to that user.

Now, I think that one of the things I should mention is that all these applications of course do ask for permission from the user to access these numbers. There are also permissions that get asked for, to connect to other servers on the internet. But users very often don't think . . .

Interviewer: They have no idea what these numbers are.

Neil Daswani: . . . about the implications, that's right. They just say "Yes, yes, yes." I think that while there is a good permissions model in place, we'll probably have to work together as a community to make sure that the permissions model used continues to get refined and so that there are third parties that help assess what all these applications are doing.

Interviewer: Are some of these applications, are the developers building these features in maliciously, or is this a case where some of them are just poorly coding? What's going on there?

Neil Daswani: In most of these cases the application developers themselves probably are not malicious. They just want to get their applications built, they want to get them out there, and they often may not be thinking through all the different privacy implications of what's taking place. So, for instance, if they need a user ID to identify a user, there are many other options besides using an IMEI number or an IMSI number. They could connect to a server and choose an ID at random. They could use the user's email address. That would have the advantage, that as the user switches devices, that user ID would stay with them even as they go across devices. I think that over time application developers will become more sophisticated about how they're coding and building their applications, to not only provide better functionality but also to maintain more privacy and maintain more security.

Interviewer: Most of our viewers are enterprises. They're CISO's--security officers at large, mid-size, even small enterprises. How much should they

be paying attention to what's going on in the mobile space, especially with the different applications? We hear so much about vulnerabilities, we hear the issue of mobile malware coming. Not a whole lot of it yet, but how closely should people that are in charge of some of these areas in the enterprise pay attention?

Neil Daswani: I think that chief security officers and IT administrators should absolutely be paying attention to some of these things going on in the mobile world. For instance, in the Thursday presentation we're going to be talking about privacy leaks, there's also other data that could also leak off the device. If you look at what's been taking place in the mobile malware space, if we look at the first 6 months of 2011 there has been more mobile malware released than in the several years prior to that. It's going to continue to grow.

Chief security officers and IT administrators will need to make sure that they put countermeasures in place to protect their corporate data, so that even if mobile malware does come down to a device--like a Droid drain, which attempts to take root access on the device, and sends sensitive information about the device off to a bot master--the chief security officers, the IT administration can protect confidentiality and the integrity of their corporate data, even in the midst of all these threats. It's going to be really important for them to pay attention.

Interviewer: One last question. It seems like security vendors and a lot for the security software can't really run effectively on mobile platforms, due to some of the restrictions that both Google and Apple put on the devices. I've heard some people call for them to open up a little bit more. Is that really needed in order for security software to run effectively on these devices?

Neil Daswani: I think the topic of how to protect all these devices from traditional virus threats is going to be really important to address. If you look at the operating systems, if you look at the Android OS, it is very open in many ways. If you look at iOS, they do provide access to a certain level of things. But I think that also, before we get into the mechanisms, we need to think about the general model. If you think about traditional antivirus for PCs, some antivirus packages have a reputation for slowing down your PC, and they can become resource intensive.

Now, if you look at the resources available on a mobile device--

in terms of the lower amount of CPU available, the less network bandwidth available--in order for them to provide protections we're going to have to think pretty hard about how to make sure that antivirus protections can come to mobile phones, but without all the issues from before with regards to performance as well as detection capability.

We've seen that more and more traditional antivirus software on PCs has been leveraging cloud-based scanning, so that the resources of the server can be leveraged in order to help it do a scan efficiently. And that's for a machine that has a good amount of capability. If we look at mobile devices, I think it's going to be even more important to take advantage of cloud-based scanning techniques so that we can continue to keep the devices safe, but not incur any performance penalties on them.

Interviewer: Well, Neil thanks very much. Appreciate it.

Neil Daswani: You're very welcome.