Hello, I'm Roger Safian. Today is Thursday, April 12, and you're listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

I'll just start off the podcast by saying I'll talk all about the Apple, the Mac Flashback malware at the end of the podcast because it's probably gonna be the most time-consuming part of the podcast this week because a lot of information about that. So let's just get on to the other things. Patch Tuesday for Microsoft was just this recent Tuesday so you should see updates to Microsoft on your system. They took a longer than I expected to install so you might want to leave a little extra time for these updates to install. and if you haven't done it yet you know do it right away because as we've discussed before as soon as updates are available, the window starts close and I think the bad guys try to take advantage of an unpatched systems as quickly as they can. And updates are available for other products as well, seems like just about everything had something this week: there's a new version of Google Chrome and it again fixes some security vulnerabilities out there. So Chrome should update itself but if it hasn't updated recently again go and update yourself automatically. There's new versions of Reader and Acrobat so those again should update themselves especially if you're using the most current version; if you're not, you definitely want to manually go and update yourself. You can go to the Adobe website and get that taken care of. Then something we don't talk about very often, there's an update for Samba and this is a pretty big update so if you are running Samba on your Linux machine then you definitely want to get this update because it's remote execution and it allows root access. So that's about as bad as it possibly get. Now for the Samba update their is a workaround: you could use hosts.allow in order to limit your exposure to this. I don't personally think that's acceptable, I mean it'll work sort of short-term but IP addresses get spoofed and things like that, maybe it's not an ideal thing. but the reason I bring it up is if your Linux machine is in such a state such that you can't just apply this patch and possibly reboot and do other things to it without causing problems to the work that you’re already doing, then you can do this fix where you could modify hosts.allow such that you would limit the number of host that could connect to your machine until you’re able to apply the patch.

Then I wanted to follow-up with the story we talked about a couple weeks ago. This was about the credit card thefts from Global Payments that million and a half credit cards exposed, you might remember that story. Basically what they're saying is now that they're aware of the problem and are starting to deal with it, what they have to deal with is a sort of the backlash, the consumer backlash. And in a little way I’m glad that somebody is thinking about that. Because the consumers end up all the time—you get this letter that essentially says “Hey mea culpa, we've made a mistake,” sometimes they'll do a credit monitoring service
for you, sometimes they won't. But your left kind of in this state like is something that happened in my identity? You're apprehensive and there's trust that's lost there. And I'm glad that somebody is looking into those types of issues as well.

And I also want to talk—this is the last story before we talk about the Apple stuff—the FBI released a report about smart meter hacks. And smart meters are for a variety of things: in my suburb I know that the people don't have to go up to read the meters anymore, at least for some of our meters they can just drive down the street and pick up all the meter’s information right there. And you know that's kind of nice. some of the other things that smart meters will allow, like the electrical smart meters, will allow you to put current back into the system—in other words, if you've got solar panels or something on your roof you could, essentially the meter will run backwards so that you can make money off solar panels on your roof. Anyway it turns out—and we would talk about this before—but it turns out that there's a variety of attacks against the smart meters and some of them are pretty simple. In fact some of them are so simple I was surprised that they were put out in this report. I mean I don’t necessarily believe that security through obscurity works but again some of these things are so simple it seems that just about anybody could go and take advantage of this here, so I was a little surprised that the FBI did it. I'll put a link to the article, Krebs put this up on his website earlier this week so I'll put a link to it, you can read it. I thought was pretty interesting.

Alright, let's talk about Flashback. There’s a ton of information out about this here and some of it's good, some of it's bad. What I would say is right now the important things that I think to know is there is a patch available for this here but the patch is only available for Snow Leopard and Lion. If you're running Leopard or anything prior to that—so that's 10.5.whatever—you're not gonna get a patch. So the only real solution that you have here is to disable Java or uninstall Java. I think it's probably more practical to disable Java, you can do that via the utilities screen, there's a Java preferences there, you can disable it there. If you are running an old version of the Mac OS, 10.5. Whatever, this might be a good time to update the machine. It's not terribly expensive to update the operating system, I think they want to charge you 30 bucks. Even if you solve this problem—you know, you disable Java—there are so many other security updates that you're missing, you're just asking for it. And really take this as a wake-up call if you’re Macintosh user. the “I'm a PC,” “I'm a Mac” sort of commercials that ran a couple years ago where Apple made it seem like malware was just some PC problem and you'd never have to worry about it? Well those were just commercials on television and guess what? Commercials on television aren't always telling you the truth and malware is a serious problem in the Apple community, and it's really important that you take it seriously. So if you don't have antiviral software on your Macintosh right now, now's a good time to go get some. if you're kind of taking a few more risks—you don't install your updates for example when you should—now's the time you want to change that behavior because this Flashback thing is just going to be the start. I suspect that were going to see the Apples are really
going to be attacked a lot and I think the reason that that's gonna happened is because Apple has set up a model that in some respects makes it very easy for the bad guys to take advantage of these situations. For example Apple’s not patching their old machines and that means the bad guys know that everybody who’s got an old Macintosh, they're vulnerable to this here unless they've taken steps to secure themselves and that's not a good thing. I really would like to see Apple address this problem. Security updates should not be cut off for an operating system that's only a few years old. If you think about it, a lot of updates still come out for Windows XP and that's a long time so I would like to see that done. Anyway, there are some removal tools, I’ll post a link in the show notes to some of the removal tools that are out there, maybe just one or two, but if you search around you can find removal tools. There are instructions online, for example CNET had a pretty good set of instructions on how to remove these things manually. there is a tool that's available I saw on Ars Technica where it'll tell you if you show the signs of infection, but it looks like that tools not working all the time, hopefully it will be updated as well. Looks like the tool's not working all the time and it's because the software is being updated on regular basis so that's problematic as well.

There’s another story I found was pretty interesting, kind of a reality check, and the people are saying this, people are saying that, but here's what the true story is, so I thought that was pretty useful. And the last thing that I want to say about this here is Apple has said that they are going to release a detection and removal tool for the Mac. now again it's probably just gonna be for Snow Leopard and Lion, so if you're running an old version of the Mac this isn't gonna help you at all, but at least it'd be doing something about it. Now they did not give a date about when this tool or this update would be available. It's not available yet, I hope it's available soon. Again this virus is pretty widespread and if Apple can do something to get this fixed themselves I think that's gonna be the ideal situation. As soon as I hear something about that I'll be sure to talk about it. Probably you know it's gonna take a little while, though if I had a bet, I would say that we probably won’t see something till next month. But I really hope that Apple surprises me and that next week we can have a conversation about how the tools available.

Anyway, thanks for listening. If you have any comments or suggestions, please feel free to send them to r-safian@northwestern.edu, and as always you'll find additional security information as well as the notes that contain the links for today’s podcast at our website www.it.northwestern.edu/security/.