Hello, I’m Roger Safian. Today is Wednesday, December 28, and you’re listening to the Information Security News podcast, brought to you by Northwestern University Information Technology.

Our first story is about Carrier IQ. We’ve covered this a few times, and there’s a couple of interesting stories that came out recently about it. One was on CNN basically talking about your cell phone being out of your control and you know the Carrier IQ problem and what sort of information may or may not be being recorded and what sort of information is being placed on the phones, and things of this nature. It’s kind of an interesting article, so I encourage you to give a read to it. More importantly though was a podcast that I found on the IEEE website where they talk about Carrier IQ, and its title is “Myth Versus Reality”. Basically what they’re saying is, “Look, this has been blown out of proportion, Carrier IQ cannot record keystrokes, so it might know that you sent an SMS for example, it might know if that SMS failed, sort of very general information, but it wouldn’t know who it sent it to and what the content was about it”. And I think what this really boils down to, and the expert they interviewed on the podcast really brought this out, part of this comes about because of the way the cell phone companies act. They put these phones in your hands, you kind of have to take it or leave it, you know, you don’t get a real chance to understand what sort of data might or might not be collected about you. You don’t get a chance to opt-out, there’s not a lot of transparency here. So hopefully what will come out of all this noise about Carrier IQ is some additional work on the part of the cell phone companies to kind of address these issues, to kind of make their customers feel a little more at ease with what they’re doing.

And then I wanted to talk also about the HP printers, and you might recall we’ve talked about these a couple times too, came out must’ve been about a month or so ago, I think the article was kind of sensationalized, “HP firmware update could possibly cause your printer to catch fire”, something like that. Well HP has got updates available. Remember, HP said at the very beginning, “Look, we don’t think you can make our printers burn”, but nonetheless they’re updating the firmware, and there’s a lot of updates available. Now I don’t believe this covers all the printers that are out there; that’s a pretty big job. And I think HP has said “we’re not going to cover some of our older machines”. I also don’t think these printers are going to update themselves. You’re going to have to go in and update your printer, if this is something that concerns you, you’re going to have to go and update your printer yourself and make sure that this firmware update gets applied. Now it might just be simpler to put your printer on a
network that’s secure and forget about this until it’s time to replace it, but you never know when something’s going to happen, so it might not be a bad idea to grab this update. I’ll make sure there’s a link to the story and to the updates on the website, and you can go there and take a look at what you need to do. I don’t have an HP printer anymore, so I can’t even try this myself, so I don’t imagine it’s going to be that difficult to do, but not having any way to test it, I can’t really tell you, but hopefully it’ll go smooth for you.

Then the last story that I want to talk about was a software bug that actually caused an airplane to dive. Now you may remember this story from a couple years ago, and basically it was a flight in Australia that kept, more than once, basically started falling out of the sky, and the pilots had to gain control and the automatic pilot was just going crazy. And they’ve essentially traced this down to a software bug, and a lot of times when people think about software bugs, you know, it’s not that drastic of a thing. Bugs happen, they put out a bug fix. Well this is obviously a much more serious case. I have to say this really concerns me, that an airplane in flight could essentially have a bug and just fall out of the sky. If things like that are out there, we are in real trouble. They need to test this software; for applications like this where there’s life and death, you really have to test, and you have to test, and you have to test some more. You have to make sure there’s no possibility something like this happens, and I hope this is a real wake-up call for that, that people are going to say, like, “Wow, we haven’t been investing enough time on the other end”. And I would encourage you, if you happen to be working in the software development industry, not necessarily a life-or-death situation there, but testing is so important, and I remember when I first got into this business a long time ago, we spent an awful lot of time testing this software. Now, it seems like, a couple of quick tests and we put it out there and hopefully everything works well, and usually it does, but sometimes it doesn’t. It’s unfortunate, but that’s just the way that it is, and I’d like to see maybe some of that change.

Anyway, have a great New Year, and 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/.

- Information Security News Podcasts Archive
- NUIIT Home