SECURITY NOW!

Transcript of Episode #278

Tag Me! (with RFID)

Description: After catching up on the week's security news, Steve and this week's co-host Tom Merritt discuss the interesting security, privacy, management and technology issues surrounding the implantation of a remotely readable RFID (radio frequency identification) tag into one's own body for the purpose of being authenticated by devices and systems in one's own environment, such as laptop, car, garage door, house front door, etc.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-278.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-278-lq.mp3

TOM MERRITT: It's time for Security Now!, the show that helps you stay safe online, with the man who knows security better than anybody I know, Mr. GRC.com himself, Steve Gibson. Welcome to Security Now!, Steve.

Steve Gibson: Wait a minute. You're not Leo.

TOM: No, I'm Leo. A little time travel and beard growth. No, Leo's off at LeWeb in France.

Steve: LeWeb.

TOM: I am very excited to have a chance to co-host Security Now! with you here. I don't know if you know this, but SpinRite saved a hard drive for me in 1993.

Steve: I never knew that, no.

TOM: You wouldn't know unless you had some weird tracking system that...

Steve: No, no, no. Not me. I'm Mr. Privacy, so there's no tracking going on.

TOM: I had a Packard Bell 486DX that wouldn't start up. And then I booted SpinRite off a floppy, diagnosed, and was good to go from there on out.

Steve: Very cool. Still going strong, strangely enough, amazingly enough.

TOM: So there. I know you have a testimonial later in the show, but there's an extra one for you.

Steve: Well, thank you. So today we have Episode 278. And it's a topic that has sort of been on my radar for a while. And a number of technology things have sort of been happening. I wanted to talk about sort of the technology side mostly, because of course this is primarily a technology podcast, though this also has some non-technology aspects which are sort of intriguing, the idea of RFID-tagging people. So I call the show "Tag Me (With RFID)," which I thought...

TOM: So this something we're just starting to see in materials and shipping containers and clothing. We're going to be talking about doing it to ourselves?

Steve: Well, yes. And in fact, believe it or not, there are even some states that have gone so far as to put legislation on their books to prohibit employers from mandatory RFID-tagging of their employees. The FDA has approved RFID-tagging, I mean, like, subdermal, underneath your skin, so that this thing is, like, embedded in you. The FDA has approved it since, like, for the last six years, back in '04. And the technology exists. But so far, from a crypto standpoint, I'm very unimpressed.

So I thought it would be fun to sort of talk about all aspects of being tagged, what it means, like from a standpoint of tracking and health and safety. But also, primarily, what are the requirements for the technology that would, for example, have me feel - me, Steve Gibson - feel good about being tagged? And frankly, I mean, I'm not all down on it. The idea that my car would know me; that I could just have a simple button on my garage door so I don't have to have a key or a keypad; my front door could be unlocked whenever I'm in the vicinity and locked when I'm not. That my laptop would recognize me, my phone and so forth. I mean, you could imagine, if it was done right, there are some serious convenience factors associated with it. And then of course there's always the dark side, too. So I thought it would be fun talking about that this week.

TOM: And that's the important thing to get into; right? Because all technologies are tools. And there's good and bad sides. And so if you want to take advantage of the good sides, you need to know the bad sides. Am I confusing Kevin Warwick here, or is there somebody who has done this, who has RFID-chipped themselves to test this out?

Steve: There's actually a hobbyist movement. I found some content on the web, people talking about it, where one guy posted: "Hey there. Yeah, the cosmetic surgeon gave me an injection to numb the area, cut a 3mm hole in my skin, lifted it a bit using medical scissors to separate it from the underlying tissue, then gently pushed the glass tag into the hole and sealed it at least 2mm deeper into the hole by gently pushing on it with a medical instrument of some kind." He says, "The important thing is to get it between the dermis layer and the underlying tissues, and not to go deeper than just under the skin. Otherwise migration could be an issue, and you will likely have a much more difficult time removing it." Or finding it. So, I mean, you could do this at home if you were so inclined. So, yeah, I mean, it actually is happening.

TOM: It does make my skin crawl a little bit thinking about it.

Steve: I know.

TOM: You know what, I've done it to both my dogs. Both my dogs have tags.

Steve: Oh, no kidding.

TOM: In case they get lost, they can be scanned, and there's a database where you can check and find out where their address is and all of that sort of thing, in case their collar was off or anything like that.

Steve: When you say you've done it, you mean you yourself had a syringe and...

TOM: No, no, no. I should say I've had it done.

Steve: Because there are syringes you can buy that inject these things in yourself.

TOM: Yeah. Maybe I will. We'll talk about it.

Steve: And we have a little bit of updates, and of course security news. And I have an interesting testimonial about SpinRite rescuing a RAID, which is something you don't normally run into because people think, well, if you have a RAID, you don't need hard drive data recovery. Turns out not to be the case.

TOM: All right, Steve. Let's talk some security updates. What do we have in the pipe?

Steve: Well, we've had a very quiet week. I know of nothing of significance that's been updated. I did, however, want to remind people that we still have this pending local privilege escalation exploit that was a zero-day vulnerability for all versions of Windows, which the danger is that hackers are using it. It's in the wild. Microsoft learned about it without any opportunity to fix it in their last patch opportunity. And so thanks to the fact that the first of the month was a Wednesday, that means that the second Tuesday of the month, Microsoft's Patch Tuesday, is as far into the month as it can possibly be. It's not till next Tuesday, December 14, that we have the second Tuesday in December. Hopefully they'll have this thing fixed.

There was a function in the graphics library down in the kernel which had a classic buffer overrun that allows someone who calls the function to get their code to be returned to with full root-level system privileges. So what that would mean is that, if something did get onto your system - as we know, we're always telling people, do not run normally as an administrator. In the newer systems, in fact, really no one is running as administrator. You're able to elevate yourself when necessary to those privileges. But the idea being that you're relying on that boundary, being a non-privileged user, to protect you from, for example, anything that gets on your system from being able to install itself as a rootkit. So this allows for rootkit-ish style attacks by getting full kernel privileges. Hopefully this will all go away next Tuesday. And the problem is there's really no workaround for it.

TOM: That's what I was going to say. So this attack happens even if you're not running as admin.

Steve: Correct. You could be running as a non-privileged user, open a PDF, if you didn't have your Acrobat or whatever PDF reader up to speed, open a PDF that uses an exploit, whether known or not, but in any case still active, to run some software that would then get privileges which otherwise your software wouldn't have and which your system is protecting itself by restricting in order to go down and, for example, modify the boot sector and get control of the system prior to Windows booting, and then install itself as a rootkit, which there's a number of things that are doing that now. So anyway, we're holding our breath for one more week. And with any luck, next time - we're recording this next week on Wednesday after Patch Tuesday - I'll be able to say, yay, they fixed it.

TOM: I hope so. You know, I open most of my PDFs as Google Docs out of Gmail. Does that provide any extra protection against this sort of thing?

Steve: Well, in the case of PDFs it does. Google has that nice PDF viewer now. And so the idea being that you're not running the PDF interpreter on your system, you're looking at the output from it. But the other bit of news this week, or a relevant piece of news, is that the Google Chrome browser was just moved up to v8.0. It's been in the Dev channel for a while. It's now in their regular release channel. In fact, anybody who fires up their browser will probably notice that they're now at v8.0.552.215, which introduces something we've talked about as coming soon, which is now available, is Google's PDF viewer running in the Chrome browser in a sandbox.

And so the idea is - Google's been talking about doing this for some time. Their own PDF viewer, not Acrobat, not a plug-in, runs natively in the browser. The browser knows how to view PDFs. You don't have to add anything to it. And it's running with its own set of privilege restrictions. So, for example, even if you had something like this kernel flaw, nothing that was being rendered in the PDF viewer would have access to the exploit in the kernel because the browser is sandboxing the viewer itself. So that's available now. And coming soon is some similar technology for Adobe's Flash Player. That's in the Dev channel code at the moment for Google's Chrome browser. And I hope before long to be able to say that that's in the mainstream.

So but in addition to that they fixed 13 other security vulnerabilities. So yes, using Google Docs to view a PDF, or using Chrome. And Chrome is coming on strong. It's turning out to be robust from a security standpoint, and it's steadily gaining market share. I fired it up in order to take a look at this PDF viewer and see if I had the latest version. It updated itself transparently. And I was looking at it, thinking, wow, if I only had more flexible tab stuff - and NoScript. I love NoScript in Firefox.

TOM: I'm a big fan of that myself. I run it all the time. That and HTTPS Everywhere make me sleep a little better while I'm browsing for something.

Steve: Yes, there's enough of an ecosystem in Firefox that I just can't leave it yet. But if Chrome continues to move forward and add some of these things, boy, it just looks so clean. It's just, I mean, it's really nice looking.

TOM: And they're really advancing with the sandboxing. They're pushing that, not only for Chrome, but for Chrome OS, as well. I think that's a great thing.

Steve: Well, it is the sort of thing - I've railed at length on the podcast before about just sort of how crazy it is that we're running operating systems that inherently are as vulnerable as they are. That every week we're talking about one exploit or another, one vulnerability or another. People are having to patch themselves constantly to stay ahead of it. If the technology was inherently invulnerable to this, rather than being inherently vulnerable to it, we'd be in a much better situation.

TOM: It seems so simple when you put it like that.

Steve: Yeah, exactly. It'd be nice if it was. I also wanted to let our listeners know that the much-anticipated first service pack for Windows 7 is now at the release candidate level. So I expect probably within the next couple weeks I'll be able to announce that SP1 for Win7 is available. And of course that will roll up together all the security fixes, all the incremental changes which have been done to Win7. And there have been many of them since its release into a single update package, which for new installations of Windows 7 will be very nice because you'll just have all of this history homogenized into a single release.

TOM: And a lot of enterprises wait until SP1 before they make the jump. So this is highly anticipated in a lot of sectors, really.

Steve: Yes, I mean, like make the jump at all to a new OS, absolutely.

TOM: To go from, well, in some cases XP, but in some cases Vista, yeah.

Steve: Actually I'm still on XP. And that's what I preach, too, is any operating system that's brand new is inherently untrusted. Steve Ballmer may jump around onstage and proclaim that it's the securest operating system they've ever made. But as we know, security is not something that you can create by proclamation. It's something you can only test out in the real world and have its security proven over time. And of course they've never produced, Microsoft has never produced a secure operating system out of the box because they keep adding too many new things. And newness is the enemy of security.

TOM: Well, you can't create security by proclamation. Can you create privacy by proclamation? That's what the FTC wants to do.

Steve: Well, yeah, that's a good point. You can create privacy by policy. And so that's essentially what we're hoping to see. The FTC is beginning to stir, frankly. And I think this is a consequence of The New York Times. It's been doing a fantastic series of articles. I think it's under the umbrella of "What They Know" is what The New York Times calls their whole series. And just week after week after week they've been pounding on many topics of online privacy, and often about tracking.

And so what the FTC has produced is, I think it's an 80-some-page document which they have given to the browser makers, to Mozilla and to Google and to Microsoft, who all sort of accepted it cautiously, wondering what this was going to mean. What they're asking for is some sort of a mechanism, and it's still not well specified, but they look at the success of the Do Not Call registry for telephones, where people who did not want to receive telemarketing calls were able to register their phone number with the national Do Not Call registry, and telemarketers were prohibited from calling any number registered.

TOM: And that worked. I cut my calls down significantly. Now, there was an exception, if you did business with that company, so your bank or your cable provider, they could still call you. But those were the only ones I got after I signed up for Do Not Call.

Steve: Yeah, it was a great thing. So what the FTC is talking about is a Do Not Track mechanism of some sort. It's not clear whether it would be a registry. The technology of the web session is such that it probably has to be different. There is some not quite perfectly defined feature that Microsoft has announced that IE9, the next version of Internet Explorer, will have some sort of a list of sites. It's not clear whether it's opt-in or it's opt-out or exactly what it's going to be.

What would be really nice, and what the FTC has suggested, is some sort of a button on browsers that is a Do Not Track button. And so you'd press the button. And from a technology standpoint, one thing I could imagine it would do is it would add a header to all of the browser's queries. So we would change and we would enhance the HTTP protocol a bit to define a new header, essentially a Do Not Track header such that every query your browser made for pages, and all of the pages' assets, pictures and scripts and CSS files, I mean, everything, would have essentially a Do Not Track request or demand which would be essentially legally enforceable, if there was legislation to back this up, so that every query that went to a server would say, I am officially saying do not track me.

Do not do anything.

And again, this is where, okay, what is tracking? We'd have to have that clearly defined. But, I mean, I don't know anybody who wouldn't say, oh, gee, why not just have that button pressed? Keep that button pressed in, and then you're not being tracked. Now, everyone says, oh, but this would hurt online commerce, and there are sites that require tracking in order to offer their content for free. I'm really skeptical, and I've always been dubious about the amount of value which is aggregated by these guys. When you look at their databases, and you have a sense for - and this is one of the things The New York Times has been so good about elucidating is that the kind of content, the kind of personal information that is being gathered really is a little bit unnerving.

But I guess I wonder really is there an economic cost to saying I do not want to be tracked to sites. And in fact I have seen some commentary where people have said, well, you can imagine a site that would say, wait a minute, you've got your Do Not Track button enabled. But for this site we get so much revenue from our advertisers that we're only going to be able to offer you the content if you allow tracking. So it sort of could evolve into a NoScript-like technology where you do not track by default, but you could run across sites that obviously they're able to sense that you've got track blocking enabled. So they could say, hey, in the same way that sites say that you've got JavaScript enabled. And they'll say, it's like, wait a minute, you've got JavaScript enabled. In order for our site, you've got to enable that. They could say, you've got tracking blocked. If you want to use the site, we'd be happy to provide you with its features, but you're going to have to enable tracking.

TOM: I've actually run across sites that said, because I had NoScript running, you're blocking ads. But I wasn't blocking ads, I just wasn't executing the scripts. And they said you can't access our content until you stop blocking the ads. So you trust the script, if you feel like it, and then you get the content. It would just like that; right?

Steve: Yes. And if that's the way the world evolved, I think either people could say I don't care about this at all, so they would allow tracking by default, or they would say I do care about it. And then they could make an informed opt-in decision on a site-by-site basis, saying okay, fine, I'll put up with tracking in order to have access to these sites' features. So, yeah, it could work exactly like that. Which would be very cool.

TOM: Yeah, I think this would be advantageous. In many ways you might even say it could be advantageous to the businesses who are thinking, well, I need to put in a paywall, if they could say, you know what, we're going to have a better sense of who our audience really is if we say we're only going to track the people who really read this many stories or do this kind of behavior. Might be more valuable data that way.

Steve: Yeah. Well, and you sort of see things like this, too. I know for example The New York Times has content that they will offer to people who are nonregistered with them. But then there are links which have a little flag on them saying, nope, this is only available, like the full content is only available for people who register. And of course what they really want is your email address so they can send you stuff. And so it's like, okay. And so then again, you make that tradeoff. Am I willing to tolerate their spam in return for full access?

TOM: I'd rather hit a Track Me button than have to go through some long login procedure where I have to enter all that information and log in every time. That's just a pain.

Steve: Right, right. So I wanted to advise our listeners who might be using the ProFTP server. There is an open source, very nice FTP server known as ProFTPD. "D" is the server side, the daemon. There was a zero-day vulnerability in their code which hackers took advantage of because they were using their own FTP server, not surprisingly, on their website. So the zero-day vulnerability was used to gain access to their source code, and it was modified. It looks like the access was gained at the very end of November, on November 28th. And the modification of the source code wasn't discovered until December 1st. So not a big window.

But between November 28th and December 1st, anyone who downloaded this ProFTP server was downloading essentially a maliciously modified version such that a new command had been added. Someone who logged onto the server during the initial handshake and entered a new command, "HELP ACIDBITCHEZ," would have been given a root command shell into the server running this ProFTP server, which is of course not a good thing.

TOM: It's the server, not the client; right? So it's when you're operating FTP on the server side.

Steve: Correct, on the server side. And so I just wanted, if we've got listeners who are using ProFTP, if you didn't make any changes to it during that window, which I would say is most likely, you're okay and fine. They do have, of course, hashes of the valid server, so you can check yours to make sure that it's working. And they of course found the problem, fixed it, and they have not talked about what the zero-day flaw is. And it's not clear to me that it's been fixed. So there is a concern with using ProFTP. You might want to make sure that they talk about having fixed the flaw that enabled their own service to be hacked in the first place. And certainly you want to update that so that you're not vulnerable from running that service just as they were.

TOM: So you're safe to download it now?

Steve: Yes.

TOM: They fixed ProFTPD from now. Or from December 1st, I guess.

Steve: Yes, exactly. A couple security sites have sort of raised the flag that ransomware is making a comeback. We saw ransomware a couple years ago, actually it was prevalent a couple years ago, where users were getting a popup notice - typically you'd be browsing somewhere, and script would run on your browser that popped up a notice that informed you that - it looked like it was antimalware. The popup would say something like, we've just performed a quick security scan of your system and found something malicious on your computer. In order to have this removed, please click here. That would then take you somewhere else.

Then there was, for a while, there was malware even worse, which would get into your system and encrypt the contents of your file system, thus "ransomware," then saying you're not going to be able to get access to the content of your hard drive until you pay us. Now, the good news was that the technology was not very sophisticated. That is, once this was reverse engineered, it was found, for example, that the crypto key was embedded in the ransomware itself, and so it was in fact possible to get the drive decrypted without ever paying these clowns any money.

The bad news is, of course, we all know we've got the crypto technology now to do this correctly. And the ransomware that's making a comeback is now doing it correctly. It uses public key RSA 1024-bit crypto along with AES 256-bit symmetric cryptography to in fact randomly create a key which is not embedded in the ransomware. And then it will leave only a public key where the bad guys keep the private key. And so there is no way now to get your data back other than to accept, pay the ransom, essentially, which is as much as $120, to get the bad guys to give you the key required to decrypt your hard drive.

So the ransomware is being spotted, unfortunately, in PDF files. People will open a PDF, believing that it is innocent and innocuous, and find that their hard drive, after some length of time, is inaccessible. Now, we know this doesn't happen instantly. That is, in order to encrypt a file system, it's got to run through the entire system.

TOM: Yeah. Anybody who's run TrueCrypt on their drive knows it takes a while.

Steve: Precisely. I was just going to use that as an example. Perfect example. Anyone who's, like, done whole-drive encryption knows that it is not something that happens fast. So at least one security company, I think it was Kaspersky, mentioned that, if you had reason to believe that this was happening, pull the plug or hit the reset button because you would stop that process in its tracks and then be able to recover all of your drive that hadn't been encrypted.

Now, I guess I would question that. If something were loose in your system, well, the problem is you're vulnerable completely to whatever demands the bad guys make. On the other hand, if you stopped the encryption partway, you could then have huge chunks of your file system, like critical portions, like the directory system, encrypted, which would really make recovery very difficult. And it probably makes decrypting the portion that was encrypted impossible. So I guess I'd wonder whether you're not better off saying, oh, shoot, and letting it go through in order to then be able to pay up and get your whole drive decrypted. I mean, basically, you don't want this stuff on your computer at all.

TOM: Exactly. You don't want to have to face that choice. That's no choice at all.

Steve: It's really bad news.

TOM: I hate it when the bad guys follow good security practices.

Steve: Yeah, well, we've often talked on the show that security is, I mean, good crypto is available to everyone, the bad guys and the good guys. So one of my recent laments is that the FBI is talking about implementing some legislation next year where they're talking about cranking up the legislation on wiretapping so that anything encrypted on the 'Net they would have wiretapping access to. The problem, of course, is that crypto is already done. I mean, it's out there. It doesn't need to be - there's nothing left to invent. It's as good as it needs to be. And if they legislate against it, then that keeps good guys from being able to protect themselves from - just for the sake of having crypto. And the bad guys will still use it anyway.

TOM: All the good guys have broken cryptography, and all the bad guys have secure cryptography, is what it ends up with.

Steve: Exactly.

TOM: That's not a good way to go. Another reason to be shy of PDF files, that's for sure.

Steve: Yeah, yeah. As a consequence of the ongoing saga of WikiLeaks, which is bringing news every day for the last couple weeks, the Congress immediately responded with a new legislation. I love how they create these acronyms. This one is called SHIELD.

TOM: They're good at that. If they're not good at anything else, they're good at the naming.

Steve: They do have good acronyms. Securing Human Intelligence and Enforcing Lawful Dissemination, SHIELD. And essentially what this does is to amend the existing Espionage Act to include the publication of human intelligence. It was already a criminal offense to leak the information. But one of the things that has annoyed the U.S. Congress is, in the case of WikiLeaks, is it's not clear that Assange - is that his name, Assange? I think Julian.

TOM: Julian Assange, yeah.

Steve: Yeah, it's not clear that Assange has broken any current U.S. law. We know that Private First Class whatever his name was in Baghdad...

TOM: Bradley Manning, yeah, Pfc. Manning.

Steve: We know that he broke the laws by leaking this to WikiLeaks. But at the moment there's nothing illegal about WikiLeaks then publishing it. So I don't know if this is going to pass through law. It hasn't passed our own Congress, nor has Obama yet signed it into law. But the immediate reaction of Congress was to amend our Espionage Act in the U.S. to make the publication of something that was leaked against the law a criminal offense. And so I feel a little...

TOM: There's a question about whether, even if this is put in place, whether it could pass a First Amendment test.

Steve: Yes, exactly. I was going to say I feel a little queasy about this. This begins to impinge on free speech. And we know that once you get this kind of legislation, then the boundaries will be getting pushed. It's like, well, okay, what are the requirements? What constitutes information which can't be leaked and/or published? So, yeah.

TOM: The leak of the Pentagon Papers in the early '70s was allowed by the courts because of the doctrine of prior restraint. You can't stop someone from publishing. You can sue them after they've published for the consequences, in various ways - libel, slander, those sorts of things. But you can't restrain them from publishing. This seems like that would violate that doctrine of prior restraint.

Steve: Yeah, don't know. It does, though. It does seem like, had this been in place then, Ellsberg wouldn't have been able to do what he did.

TOM: Exactly.

Steve: And finally...

TOM: Speaking of prior restraint...

Steve: Speaking of prior restraint, BlackBerry and RIM is still going around in circles with India. We've talked a number of times about the problems that BlackBerry faces with the various governments which have demanded that they have access to BlackBerry's text messaging technology. Apparently the audio channel is not posing a big problem. They want email and text messages. And the problem has been that BlackBerry's technology is such that, unless the traffic is routed through them, through BlackBerry's servers, then just intercepting the traffic does not give a third party access because the cryptographic keys are contained in the endpoint phones and nowhere else.

And so in the news this week BlackBerry explained that the enterprises that were running their own BlackBerry Enterprise Servers, BES servers, those enterprises had truly unbreakable crypto, and that India or any other government would have to go to the individual companies in order to arrange some sort of access to their crypto. And I imagine that India would then threaten to block their use of cryptographic communications that they were unable to intercept. So essentially the update on that is that India is going to have to go to individual companies and see about obtaining the required credentials, I guess, for all the phones.

TOM: So what would that entail? Would they have to go into each company and say we want to put a piece of software on your BlackBerry Enterprise Server? Or would it just say we need to have your private key? How would that even work?

Steve: Apparently there is technology, which BlackBerry has talked about before, where some software would be added to the BlackBerry Enterprise Servers, essentially installing a backdoor on the servers. And that would allow, for specific users, it would essentially send traffic to the government which the government had the ability to decrypt. So it would essentially decrypt the traffic as it was passing through the enterprise server from one phone to the other, and essentially allow a wiretap where a wiretap would not otherwise be possible.

TOM: I get the feeling that this is saber-rattling on the part of India. They just want to push to see how far they can get away with stuff. Because every time the deadline gets close, and RIM says, you know what, we can't do this, they back off. They extend the deadline. They push it away. They don't want to drive companies out of India. They need that economic boost. They need that job creation. So they're going to push this as far as they can. But I get the sense that if the companies just resisted it, that there might not be any consequence.

Steve: Well, and it is also the case that the reason we're only hearing about BlackBerry at this point, I mean, there has been some concern about going after other web-based email systems like Gmail, which is now fully SSL and encrypted. But we're not hearing about other phone-based systems because none of the other ones are this secure. So, for example, Apple's iPhone doesn't offer this level of public key, endpoint-to-endpoint security which BlackBerry, I mean, that was one of the selling points that RIM has always had is that they were able to say to corporations, I mean, it's why our own President of the U.S., Barack Obama, has a RIM which has been further hardened. But they have proven security in this technology, and the other phone technologies don't.

TOM: All right. Well, we'll see. Like I say, it's fun to watch. I hope - and I don't think anything really bad is going to come out of this. But you never know. It's a lot easier to go after BlackBerry because they have the BES. It's easy for the government to see on the Internet. It's harder to see where to go after them, but it's actually easier to crack.

Steve: Yes, exactly. Well, so I wanted to update - actually, in doing the Q&A last week I ran across a number of really fun SpinRite testimonials. I always look for something new and different that I haven't talked about before. And this one was from a listener of ours, Doug White, whose subject was "SpinRite Helps the Buffalo Roam."

TOM: Oh, my.

Steve: And he said, "I got a frantic call from a friend that his NAS device," his network-attached storage device, "a Buffalo TeraStation..." Thus the roaming buffalo.

TOM: I get it.

Steve: Okay, "...was no longer appearing as a mapped drive on his network. Apparently they were doing some work in the building and had switched the breakers off and on several times over the weekend. And as the NAS was hooked to a UPS in another part of the building, they didn't hear the UPS's screams. So it appears that the NAS was cycled up and down a few times. I said, 'No worries. The TeraStation is only holding a second copy of all your files; right?' Silence. 'Right?'" He says, "I had initially set it up so that all of their important files, hundreds of gig of music tracks that he's recorded in-house for himself and for other musicians, were being copied over to the recording PC, which contained the master copy; then to the TeraStation so that there was a second backup.

"They liked the idea of the RAID 5 protection being offered by the Buffalo TeraStation so much that they decided it would be great to use the TeraStation as a central repository for all sorts of other information, such as invoices, quotes, et cetera, as well as other soundtracks that were being modified on another workstation in the building. So there was quite a bit of one-off stuff that accumulated on the TeraStation. Why not, they thought, it's got four drives in a RAID 5 configuration. What safer place to put the stuff?

"I showed up expecting a failed drive or the like, but the TeraStation's status display showed that all was well. No failed drives. I checked the workstations, and sure enough, the NAS device was not showing up on the network. I pinged its IP address, which was one of the items cycling through the NAS display, and it responded to the ping. When I tried to browse to the web-based admin interface, however, no response there, either.

"Even though it responded to pings, I wasn't entirely sure that the little Linux-based motherboard in the enclosure wasn't damaged. So I contacted Buffalo tech support. To my chagrin, they said that the device was so old" - and he says plus-six years old - "there were no enclosures to be had to attempt to swap the drives over to another enclosure. Even buying a new enclosure would not work, according to them, as the newer firmware probably wouldn't recognize the old drive's RAID encoding. I was at a loss as to where to go from there. Maybe eBay to see if I could find an old enclosure?

"Well, while I mulled over how to proceed, I figured what the heck, I'll run SpinRite on the four SATA drives while I try to locate another enclosure. Drive #1 flew through just fine, but Drive #2 of the four had some DynaStat action under SpinRite, and SpinRite had to recover some sectors. Drives 3 and 4 sailed through just fine. Curious as to whether anything had changed, I reinstalled the four drives into the NAS enclosure and fired it up. This time the NAS display indicated that it had to do some resyncing, which went on for several hours. Lo and behold, after it had resunc (!) I tried to attach to the network share and, voila, it was there. I was then able to attach to the web-based admin interface with no trouble.

"I quickly attached an external USB drive to my system and copied all the files off the shared volume." And he says, "(Well, as quickly as you can transfer 620GB across a USB device, anyway.) I'm not sure why damage to one of the drives would have prevented us from attaching to shares or logging into the web interface, but I wasn't going to look a gift horse in the mouth. I was tickled that the files were once again accessible, and you can imagine how my friends felt. I was a hero.

"I'd like to emphasize with this story that many users, technically savvy and not, assume that since their stuff is on a device that is protected against a single drive failure via

RAID 5 or the like, that all the data is safe. What many don't take into account is the what-happens-if-the-enclosure-dies scenario. So I'd like to reemphasize the 3-2-1 backup strategy that you and Leo have talked about in past shows. My friend ended up buying another newer and larger TeraStation. Fortunately the newer TeraStations have an option to synchronize files with one another. So my friend now has two NAS devices on opposite ends of the building that are syncing to one another nightly. Next up is trying to figure out how to get 600-plus gig of files offsite and backed up, either via sneakernetting a USB drive or some cloud-based backup service. Add this to the list for yet another SpinRite success story. My friend will be purchasing a copy of SpinRite for their own use from now on."

TOM: So now we have to figure out if I want to be tagged. Do I want to put a subcutaneous chip in my arm? Is it your arm? Where would you put it?

Steve: Where the hobbyists are putting it is sort of in that gap of skin between their thumb and their first finger on the backside of their hand. One of them, I did some poking around the 'Net as I was researching, like, how prevalent was this. And one of them made a comment about being careful when you put your hand into, like, tight jeans because you wouldn't want to catch the chip under your skin on, like, the pocket of your jeans. And that just sent shudders through me. It's like, oh, my goodness, no, you certainly wouldn't want that to happen.

TOM: I don't want to have to think about that.

Steve: So I think the more popular place is between your elbow and your shoulder, sort of in your upper arm. Apparently there's the question of migration, that is, a smooth capsule can tend to migrate more than one that's deliberately - there's, like, a non-migratory coating that they can receive that I think probably has, like, some fur on it, so that it sort of - it's not slippery.

TOM: A mink capsule, perhaps?

Steve: It sort of locks into your location. But I have to say, first of all, it's passive technology, so there's no batteries to replace. It's not like a pacemaker where after some length of time it needs to be taken out and opened up again. One of the concerns that exists currently is that we're still far away from standards. And I always tend to guess wrong. I went with Betamax back in the day, and of course Beta lost and VHS won. And then I also went with HD, thinking okay, well, Sony lost last time, I'm not going with...

TOM: I did the same thing.

Steve: So I've got a bunch of these red DVDs, and the blue is the one that won out.

TOM: I've got the Xbox HD DVD player attachment, as well. Be a collector's item someday.

Steve: So I'm thinking you wouldn't want to go with the Betamax of subcutaneous implants, and then have that one not win. But really, from a convenience standpoint, okay, we've talked a lot about biometrics and fingerprints. And one of the downsides is that you can't change your fingerprint. And if it really became valuable for, like, someone to desperately, like bad guys, to need your fingerprint, well, there's only one way they can get it, and that never has a happy ending.

So the idea that, okay, I've got something, you can feel it, it's there under your skin. The size of the most popular one is 2mm by 12mm. Philips makes it. It's called the Hitag. So if you just Google "Philips" with one "L," "Philips Hitag," you can find some pictures of this thing on the 'Net. It's like about the length of a - I often see it sitting next to a standard U.S. penny. And so it's about the length of the penny's diameter, and that's 12mm by 2mm. So it's a rounded-end little capsule. It uses low-frequency induction so that it's powered by the reader, which generates - it essentially magnetically couples into it. It's very much like, I'm sure people have probably seen ads now for, like, the Palm, was it the Palm Pre that doesn't need to be plugged in, you just sort of set it on its little pedestal...

TOM: Right, does an induction charge, yeah, yeah.

Steve: Right. And so these work in the same technology. They generally have a short reading range, that is, a few inches. There are some that can go feet or yards. And so that's sort of a mixed blessing. But I sort of like the idea of the convenience, if there were a standard. I mean, I don't think I would mind being tagged if the technology made sense. Mice have had a problem. Mice were tagged, and for whatever reason they tended to get some skin cancers associated with the tagging. But other medical professionals have said, well, mice get cancer. That's what mice do. And so...

TOM: That's what the smoking people said, too, but...

Steve: Exactly. And so before we went into this you'd want to make sure that it was safe, clearly safe for human implantation. There was some concern that the metal in the capsule would interact, for example, with medical scanners, like MRIs, where you would have a problem with a really strong magnetic field. But the MythBuster guys took that one on. And they were concerned that it would overheat and would burn you or something. Well, it turned out that doesn't happen. It didn't even upset the technology at all.

So my problem with current tags is that they're a little unsophisticated from a crypto standpoint. There's one guy who has a site where it's like he has had fun reverse engineering these things. And quoting from some text on his site, he said: "I can copy a proximity card at least as easily as I can take an impression of a key. This means that it's not a very good idea to reuse visitor cards without changing the ID (and that it doesn't really matter whether you get the physical card back from the guy you just fired)." Meaning that somebody who had a card could easily clone the card. There's just no difficulty in doing so. He says:

"More insidiously, it's quite practical to read someone's card without even removing it from their wallet. A bit of deliberate clumsiness, a reader up my sleeve, and I would have little trouble cloning anyone's card. I could also exploit the fact that the distance at which the cards will be powered is less than the distance at which they can be read," meaning that they can be read from a much farther distance passively than they were being powered. So he says, "If another reader is exciting the card, then my reader can read that card from the other side of a wall," for example. He says:

"This means that a sniffer concealed somewhere near a legitimate reader could intercept real transactions at a significant distance. This sort of attack is particularly good because the card repeats its ID over and over and over as long as it is in the field, so I could use signal processing...." And he goes on to talk about "...signal processing techniques to combine multiple copies of the pattern to further improve my read range."

TOM: So this is the RFID chip on a card. But essentially what you're saying is the same could be applied to an RFID chip if it's implanted; right?

Steve: Well, and that's the problem is that, for example, there is this FDA-approved chip, it's called the VeriChip, which it has just a simple 16-digit fixed ID. So there's no way that that qualifies, I mean, no listener of ours is going to accept the implantation of something that has a fixed ID, the problem being exactly that, is that everything that I just read - he's talking about access cards. But it uses exactly the same inductive technology as one of these little implantable tags. And so all it's doing is, when you ping it, essentially, it sends back the "this is who I am" response. So it's trivial to clone it. And so it just doesn't, I mean, it's got zero crypto sophistication. So what we need is we need useful cryptography in an implantable device like this.

TOM: So let's figure this out. How do we get a chip in ourselves that's secure, that nobody can scan and rewrite and steal all of our information right out of our elbow?

Steve: The secret is we need a technology which embeds, well, a secret in this chip. So we have a chip, and it needs to know something that never leaves it. So the idea being that it can be challenged by the reader, whatever entity to which it wants to authenticate, it can be challenged to prove that it has a secret without it divulging the secret. So the problem with just a simple ID of any length, even if it was more than 16 digits, is that it's unchanging. It's just not going to be different every time. So what we want to prevent is any sort of a replay attack where somebody passively listening to the chip respond is able to capture that. Or even, if there's more technology going on, if there's something fancy going on, for example, where a challenge is given and the chip responds, we want a technology such that there's no way to replay that or to gain information about the secret in the chip by eavesdropping on both sides of the conversation, the outbound to the chip and the chip's response.

So we've covered crypto topics enough here to know that there's two approaches. There's a private key approach or a public key approach. The private key approach is going to be simpler. It would involve a simple cipher like the AES cipher, for example, to drive an encryption function. So, for example, the entity to which you want to authenticate, when you approach it, it would generate - you might press a button, or you might approach it. You would respond, saying, hey, I'm here. It would respond by generating a large random number, either that or using a counter which is never going to repeat. So it's never going to issue the same value a second time, so you never need to worry about someone capturing its challenge and then seeing what the matching response is and being able to issue that. So it issues a unique challenge. And there's lots of ways to produce a cryptographically unique challenge that will never repeat. It sends that out over the air to the chip, which uses its secret key to simply encrypt that challenge and send it back.

So the idea is that - and this is the beauty of simple symmetric cryptography, is that it doesn't help an attacker to see essentially what is the plaintext going out to the chip and the ciphertext coming back. It would be a 256-bit string, for example. Or in the case of if we used AES-256, it would be a 128-bit string. But still, 128 bits is a phenomenal number of possibilities. And the challenger would never be using the same one twice. So there's just no way, even though you see these 128 bits going out, to determine what the function is inside, that is, what the secret key is which is producing a matching 128-bit reply.

Once the challenger received that reply, it would also have the secret key. It would know the secret key, and so it would similarly encrypt its challenge and verify that the result of that encryption, under the same secret key, matched the one it had, and that would prove that the secret key in the chip matched the secret key that was registered with it. So the advantage is it can be eavesdropped on. Because you're using symmetric crypto, it's relatively simple. It's a low computational cost to pull this off.

The downside of using a symmetric key is that you do have to divulge your secret to anything you want to authenticate against. And anyone who has the secret can impersonate you. So the problem with using the simplest symmetric key technology is that, if you, for example, if I wanted my garage door opener and my car and my laptop and my cell phone and all of the devices in my life to be able to authenticate me, they would have to know the secret key that I've got implanted in my body. So we want to take it probably to the next step because...

TOM: And so what you're saying is that ends up being a vulnerability, where they don't have to get the key out of your arm, they get it out of your garage door opener, or the scanner that you're passing by, or there's too many places where that key is.

Steve: Exactly. Exactly. It's not just in my arm, it's also - all of the devices that want to authenticate me would have a copy of it. And so all a bad guy would have to do is compromise one of them, get the key out of there, and then it's trivial to impersonate me by putting the same key in the same kind of device and then waving it around and getting access to something that might be substantially more useful to have access to than whatever device it was that they decrypted. I mean, you could imagine, someone who was chipped like this would probably be using it everywhere they could, just to get the maximum bang for the buck.

TOM: Yeah, what's the point of being chipped otherwise; right?

Steve: Exactly. So we take it one step further, using asymmetric key technology, which is really where I think this has to go before I'm comfortable using it. And so what that means is that, thanks to the fact that public key technology has a pair of keys which are different, and that there is no way, knowing the public key - well, I should say, I should be rigorously cryptographically correct here and say it is computationally infeasible, with everything we know, to obtain the private key from the public key. So in this scenario, my more sophisticated, more complex implant, which it might mean that it takes a little bit longer for the authentication to happen because literally I would have to hold this in the magnetic field which is powering the device long enough for it to crank through public key crypto, which is substantially more sophisticated than symmetric key crypto.

So I bring myself near the reader. I again receive a challenge. This time I use my private key to encrypt that challenge and then send it back. The beauty is that the public key can be known to everyone. In fact, we could even, for example, if a system like this became popular, you could stick it in a text record in your DNS server and say to everybody, this is Steve's public key to the chip he's got in his arm. All devices anywhere could know it. And them knowing it doesn't hurt you in any way. It just means that you get to have more use from this thing, if that's the application that you wanted to put it to.

So essentially it allows the unlocking of the challenger side such that it's possible to authenticate the ownership of the private key using the public key at any time. There's nothing that needs to be kept secret. There's a higher complexity in terms of doing the math, but still certainly not out of range of what we can embed in something like this. So it's potentially, I think, entirely feasible to come up with a workable chip which is embedded in people that would allow them to authenticate in a way that is - well, so if we step back a second and say, okay, what are the requirements that we have for this, well, we know that we want proven biological safety. We don't want this thing to get lost in our body somewhere by migrating to some other location.

TOM: Or give us the cancer.

Steve: Or we don't want it to give us the cancer, exactly. We want a single settled standard. That is, again, we don't want to choose Betamax and have the world go off in a different direction. So...

TOM: You can't get in anywhere because you picked the wrong chip.

Steve: Exactly.

TOM: Like being uninvited.

Steve: And we've talked before about having, like, a key ring of, like, dongles, where each one runs something different. Well, you wouldn't want to have to have a whole lineup of these things in your arm, of all different standards, in order to cover the different possibilities. We need it to be clone-proof, meaning that it's going to use good crypto, state-of-the-art crypto. One of the problems has been that some of these technologies, they've been proprietary. TI designed that technology that was in the Speedpass. Remember that for a while you could buy gas just by driving your car up to a pump, and it would light up? I think it might have been Mobil. I remember it was a Pegasus. I thought it was kind of a cool thing. I did sign up for and use the Speedpass for a while.

The problem was that the Texas Instruments engineers came up with their own cipher. Well, we know that's never a good idea. And it turns out it wasn't. It turned out that it was very easily crackable. It used a 40-bit cipher, which, I mean, the key length may have been enough. But why not go 128 bits? They were trying to keep the costs low. They used their own cipher. It wasn't ever vetted by the industry. Turns out it was hacked and cracked in a matter of hours. I think six hours is what it took in order for the algorithm itself to be reverse engineered from scratch. And then some people did verify that it had cracked this.

So that Speedpass was an example of an early approach that just - it wasn't standards based. It wasn't open. It was a proprietary protocol. So that's the other thing we'd want is a completely open technology so that you know what you're injecting yourself with here is, like, what the industry has agreed upon; and your laptop and your cell phone and your car and every other thing that you use is going to be able to interact with this.

And, finally, I really think it needs to be rewritable. No matter what it is you put into yourself, you'd like to be able to change it. If something happens, and you want to change your private key, even though there's no way that key can get away from you, being able to change it makes sense. If nothing else, you could just zero it in order to turn this thing off if you decided you wanted to deactivate it temporarily or maybe permanently without having it surgically removed from you.

TOM: Yeah, you want to have control over it without having to dig it out of your arm or your neck, like they do in the movies.

Steve: Exactly. And also I think it wants to be small enough that it's not going to set off security scanners every time you go through some airline TSA scan. They might be wondering what it is you've got in your right rear butt cheek.

TOM: And you don't want them to have to try to find out.

Steve: Yeah. The extensive pat down you want to avoid if possible. And finally, operating distance. I see that as the real bugaboo here because it's a tradeoff. For greater security you want shorter range. You'd like to have, for your own personal use, a few inches is probably fine. On the other hand, if your arms are loaded with bags, and you're coming in in the rain, how cool is it that your door unlocks for you, and you don't have to fumble with your keys? So again, if you were within a few feet of that, that would be nice. The problem is there isn't a hard-and-fast technology for limiting range. Range is based on signal strength. And if some bad guy wanted to ping you at a greater distance, all they'd have to use is a bigger roll of wire, more power behind it, and a greater sensitivity antenna.

TOM: So the distance is reliant on the reader, not the chip itself? To a certain extent?

Steve: Sort of both, except that you can always get greater distance by having the reader generate a stronger magnetic field and be more sensitive to the returning signal from the chip. So, yes, it's more a function of the reader, although you could deliberately design chips that had a lower range. Except, again, no matter how low you made it, you could always affect that by more juice coming from the reader. So it's just not a hard-and-fast thing. I think I'd be more inclined to have a greater reading distance than I would a short distance, just because I would want this for convenience. And it'd be nice if I could just approach the front door of the house and have it unlock, and approach my car and have it do the same thing. And frankly, I think the whole idea is kind of cool. I know it creeps some people out. The downsides are, I guess, what, being tracked, that you might be identified or pinged even when you don't want to be. Unfortunately, I can't see a means for sort of, in real-time, disabling it. It'd be nice if you could, like, click it or something.

TOM: Turn it on. Could you wrap a Faraday cage around your arm?

Steve: Ah, now, there you go. Have a big, like, copper bracelet or something you could just slip over it.

TOM: Yeah, a security sleeve that can pull down out of your shoulder.

Steve: Now, there are some companies that sell silicon wristbands that have these embedded. And as I was researching it I thought, well, I mean, it's not quite as convenient as having it in you. But you really don't need to be scanned when you're completely naked. And the rest of the time...

TOM: Unless you're going to board an airplane.

Steve: Exactly. And then I was thinking, well, okay, how about - it's such a tiny little capsule, you could also, like, drill a little 2mm hole in the sole of your shoe and slide the capsule into your shoe. So I'm just sort of thinking of alternatives to embedding it in your body that would still give you a lot of the benefit of the convenience of having something that is securely authenticatable and associated with you. On the other hand, if someone stole your shoes, then they would be you.

TOM: Well, I guess they could saw your arm off. But it's a lot more difficult to do something like that than to grab onto somebody's shoe or slip a wristband off a wrist or something. Or you could just lose it.

Steve: Yeah. And again, that's why, relative to sawing your arm off, why I'd be happy to tell my captors, here, there's the capsule there in my arm.

TOM: Here's my private key.

Steve: Just dig it out. Don't take the whole arm. You only need a little one-inch chunk.

TOM: So I agree with you. I think the fact that the problems of cryptography on this are not insurmountable. And it could be incredibly convenient for many different reasons. But you mentioned something earlier that gave me pause, which was the idea of your corporation or your place of work saying, okay, we make you carry around an ID card with an RFID chip. That's a little expensive. We'd just like everybody to have this implanted, please.

Steve: Well, yes. And so it is the case that people have been concerned about that. And as a consequence there's at least three states that have legislation on the books now that specifically prohibit employers from requiring employees to be "chipped," as the new verb has been coined. And frankly, if a standard existed, and your company was using access cards, and your chip used the same technology as the access card, then it'd be kind of cool.

TOM: That's why we need a standard; right?

Steve: That's why we need a standard. And I haven't thought through the downside. I guess I'm not living a life where I'm too concerned about the tracking aspect. For example, I would like it if, for my credit card to be used, maybe if I have to also be pinged, if I require to be physically present. That would be nice. Or again, back to the gas pump. If the gas pump had the technology, and I was chipped, then, hey, it's very easy for me to authenticate to the gas pump and not have to use a credit card.

TOM: Sit there, put in your zip code and all that crazy stuff that you have to do now. When you talk about the tracking aspect of it, though, think about it. You're totally trackable without a chip in you already. There's facial recognition software that can identify you. You're leaving fingerprints everywhere you go.

Steve: You've got a cell phone that is sending out a logged-in ping and all kinds of things, and wanting geo-tracking now.

TOM: So you can't encrypt your face. But you can encrypt a chip.

Steve: Yes.

TOM: It seems like that's actually safer than just having a face.

Steve: Well, the public key technology, if the public side were known, then you would be trackable. However, nothing prevents you from keeping that secret, too. You could still have the benefit of an asymmetric crypto and work to keep the public key secret in the same way that you would much more diligently work to keep the secret key secret. And then you may be giving off a signal, but it doesn't matter because there's no way that anyone would have of associating that with you because they wouldn't have your matching key.

TOM: Yeah. And I think some way to turn it on and off, even if it is just blocking it, makes it more viable, as well. You've almost convinced me.

Steve: We've seen the same sort of thing with passports, where passports were going to get RFID chips, and they were going to use a metal folder. And in fact I think that, what's the crazy site...

TOM: ThinkGeek?

Steve: ThinkGeek, yeah.

TOM: ThinkGeek sells the wallets, yeah.

Steve: Yes. And those block that kind of remote access. So, yeah, I mean, certainly we're a long way away from it. But I thought the fact that hobbyists are beginning to chip themselves, I mean, they're using, unfortunately, low-technology chips. This Philips chip has some sort of an encrypted challenge-and-response technology. Unfortunately, it's proprietary, and I couldn't see anywhere where they talk about the algorithm, and it wasn't very much bit length. It was a 32-bit response to, I think, two different 32-bit chunks. But again, they just didn't talk about it at all. And so for me it's got to be more than just a fixed ID that it sends out. Otherwise you really are prone to being cloned.

TOM: My friend Veronica Belmont has said she wanted to be chipped for a long time. I think you've almost convinced me to join her.

Steve: Well, I will keep us and our listeners up to date on this. If it happens, I think it'd be kind of cool. I can see some upsides.

TOM: Maybe I'll try it with the dogs first, since they're already chipped. If I could get it to where, at certain times of day, their chip allows them to just open the door automatically, and they could let themselves out, take care of their business, that in itself would be incredibly handy. And maybe that's a good test field. Pets would be a test field for this, in all seriousness, to kind of work out some of the kinks because your security level is lower there.

Steve: Well, and it's absolutely the case that there exist today silicon bracelets that carry chips in them. So if someone wanted to experiment with the convenience of using it, there are SD cards for laptops that can receive the RFID signal from a bracelet. So you could tie it to TrueCrypt so that TrueCrypt won't boot your laptop unless you're physically there. Or, that is, your bracelet is. And so there are half-steps people could take before they committed to a surgical procedure. But apparently it's just not a big deal to have it done. You just use a little outpatient plastic surgery to sort of cut a slit and slip this in, and you're done.

TOM: I just thought of one minor downside to that when you gave that example. You know, TrueCrypt has the hidden volume that you can use if they demand your password. You can give them the password for the fake volume. You couldn't do that if you were authenticating on your chip. They'd just grab you and thrust your elbow down, and you're into the real volume. You can't make use of it. But probably not a common problem. But problem enough for some people if they're worried about it.

All right, Steve. Well, I really appreciate you letting me host, while Leo is gone, with you. This is fabulous. I've learned a lot.

Steve: It's been great.

TOM: Yeah, I hope you enjoyed it, too. You can find, well, GRC.com; right? That's the place where SpinRite and ShieldsUP! and all the good products are.

Steve: Yup.

TOM: And you will be back next week. Do you know your topic, or...

Steve: Well, this not being a Q&A, we'll be doing a Q&A next week. So I did want to encourage our listeners, I imagine there'll be some interesting feedback from this topic. And so GRC.com/feedback. Please, listeners, go there, let me know what you think about this, and I think we'll have a fun episode using feedback from this rather potentially controversial topic, which Leo and I will cover next week.

TOM: All right. Thanks, everybody, for watching Security Now!. You can find us at TWiT.tv/sn. Leo will be back next week. We'll see you then.

Steve: Thanks, Tom.