Simjacking

Description: This week we continue following the DoH story, which we begin discussing two weeks from now as a result of a rip in the space-time continuum. We also look at recent changes to Chrome 77 and the forthcoming Chrome 78, the already compromised iOS 13.0, and Mozilla Firefox's new browser VPN offering. We take a look back at last Tuesday's Patch Tuesday, take note of Chrome's Remote Desktop feature, cover another serious Exim mail server problem, handle a bit of miscellany, and examine a serious vulnerability affecting essentially ALL smartphone users known as "Simjacker."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-732.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-732-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We have a catch-up on DNS over HTTP. We talk about some great new features coming to Chrome and Firefox. Steve sings the praises of the Chrome Remote Desktop. And then hold onto your hats because there's bad news about simjacking. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 732, recorded Tuesday, September 17th, 2019: Simjacking.

It's time for Security Now!, the show where we talk about the latest in security and privacy and keeping yourself safe online with this guy right here, Steve Gibson, in the house. Hello, Steve.

Steve Gibson: Yo, Leo.

Leo: We've done a lot of Security Nows, it feels like, in the last few days.

Steve: It has. And in fact I made note of that. For this week I said we continue following the DoH story, which we begin discussing two weeks from now in the future, as a result of a rip in the space-time continuum.

Leo: Exactly.

Steve: We also look at recent changes to Chrome 77 and the forthcoming Chrome 78; the already compromised, though not yet released, iOS 13.0; Mozilla Firefox's new

browser VPN offering; and a look back at last Tuesday's Patch Tuesday. We take note of Chrome's remote desktop feature, which I just discovered, cover another serious Exim email server problem, handle a bit of miscellany, and then conclude with an examination of a serious vulnerability affecting essentially all smartphone users, known as simjacking.

Leo: Oh, man. This has been a big problem.

Steve: Yeah. It got a lot of coverage in the tech press. And I had to, like, I had no idea that a SIM could be jacked. I just figured it was a bit of - I thought it was like a bit of ROM or something. But it turns out there's a browser in your SIM. It's like, what?

Leo: What?

Steve: Yes. And so the good news is that firewalls, cellular carrier firewalls can be erected to stop this. But at the moment, there isn't any.

Leo: They're not doing it, yeah.

Steve: And it's possible for bad guys to send you an SMS message which jacks your SIM and can take over your phone. And it's like, because it's down at the SIM level, it's carrier agnostic. It's phone source agnostic. It's, if your phone has a SIM in there, and they all do, you're in trouble. I mean, but not...

Leo: Even an eSIM, even an eSIM would be vulnerable to this.

Steve: Yes. And it's going to be targeted attacks. It's not like you're going to get sprayed with it. But for people who are subject to targeting, this is a problem. So anyway, we have lots of stuff to talk about.

Leo: I can't wait, as always. Security Now!, we look forward to it every week. A reminder, Steve and I are going to be in Boston. That's why we were pre-recording our October 1st episode. On October 3rd we will be doing an event on behalf of LastPass. It's exciting. It's an event about the future of authentication. It'll be Steve. It'll be the legendary William Cheswick, Bill Cheswick, who actually created the first firewall at Bell Labs and has written a lot about security and has recently written about passwords and why they're bad. We'll also have Gerry Beuchelt, who is the CISO of LogMeIn.

It's going to be a fantastic panel event. It is absolutely free. If you're in Boston on that Thursday afternoon, October 3rd, you can go to our website, twit.to, that's the URL shortener, twit.to/unlocked. We have, I think, some room left. What's happened is that they've slowly expanded the venue. It was initially 100 people, then 200. I think we're up to 350. I think they're going to have to go to five or 600. But we're slowly expanding the venue to accommodate at the Intercontinental Hotel in Boston. If you will be in the Boston area on October 3rd, twit.to/unlocked. It's free.

It's actually for charity. Everybody who attends will get a $100 token they can donate to one of LogMeIn's three choices of charity. So that's going to be really nice,

too. You get to put your token in a charity of choice. And I can't wait to do that with you, Steve. It's going to be a lot of fun.

Steve: We'll have a ball.

Leo: Yeah. I mean, eventually we will sell out. This may be the last round of announcements. So don't delay. Let's get going, Steve. We've got a picture. We've got a picture.

Steve: I've been sitting on this one for a while. I just get a kick out of it. So this is from the iconic sci-fi movie "The Terminator" with Arnold the robot sent back in time from the future, who's at a phone booth looking up the...

Leo: You remember he was looking for Sarah Connor. He had to find her.

Steve: Exactly.

Leo: He took the phone book.

Steve: And so there's a scowl on his face down at the bottom frame because in the phone book Sarah Connor's name has been distorted with a line running through it to create a CAPTCHA.

Leo: I am a robot. I cannot read it. What have they done?

Steve: Anyway. Just a little bit of geeky security humor.

Leo: I don't think these CAPTCHAs fool anybody, especially not robots.

Steve: No. They fool us more than they fool, you know, robots.

Leo: Yes. They're hard for humans.

Steve: I'm looking at them going, I have no idea what that thing says. Just give me another one, please.

Leo: Yes.

Steve: So Chrome follows Mozilla to DoH with a bit of a twist. Google has announced that they, too, will soon be performing a trial of DNS over HTTPS, DoH, in the upcoming Chrome beta 78, which will be releasing this Thursday, September 19th. We're currently at Chrome 77. What's interesting is that, rather than having Chrome preconfigured with a

default DoH server like their own, Google will instead attempt to preserve whatever DNS the user already has chosen. And I love that idea. I think that's very clever, and that it would be really cool if they were to probe the user's currently selected DNS server to see if it was offering DoH support, test it locally, then switch to it.

But apparently that's a bit too aggressive, at least initially. So what they'll be doing is only if the user has already configured their DNS to one of six providers: CleanBrowsing, Cloudflare, DNS.SB, Google, OpenDNS, or Quad9. On the other hand, those are high-reputation, well-known services, and I imagine a lot of our listeners probably have done that.

So initially, for a small group of users running Chrome 78 beta, Google will be running an experiment that checks to see if their provider is on that short list of well-known DoH-compatible providers. And if the user's provider is, Chrome will automatically upgrade to that provider's DoH server for its DNS resolution. And if they're not already using one of those servers, nothing will change. So this will affect all platforms of Chrome other than Linux and iOS. And on Android 9 and later, if a user has already configured a DNS over TLS provider, Chrome will use that instead of the ones that are listed.

So by cleverly leaving the DNS provider as is, and only upgrading to the provider's equivalent DoH service, what I like about this is that the user experience should remain the same. For instance, any malware site protections or parental control features that are offered by the DNS provider, which presumably the user has chosen for that reason and enabled and configured, those would continue to work. If DoH fails, then Chrome will revert to the provider's regular DNS service, that is, not try to do DoH. And any of those early adopters will be able to opt out of this with a flag, chrome://flags/#dns-over-https. That'll bring you to a flag which you can turn off if you don't want it.

And on the Mozilla side - and Leo, thanks to the time machine we used last Saturday to record podcast 734, I happen to know that two weeks from now on our "Joy of Sync" podcast #734, we'll be discussing Mozilla's own move to begin experimenting with enabling DoH by default for their users. But it turns out that, as news of Mozilla's plans spread, which by the way I was unaware of two weeks from now due to a temporal paradox, Mozilla will have since received some pushback from Linux distro maintainers and some network admins.

Leo: Oh, really. Oh, why?

Steve: Yes. In an example quoted by BleepingComputer, OpenBSD developer Peter Hessler tweeted that OpenBSD has disabled DoH in their Firefox package in the current and future releases as, and this is what he said: "Sending all DNS traffic to Cloudflare by default is not a good idea." So people are objecting to Mozilla's sort of default focus on a single DoH provider.

Leo: Actually, that makes sense. If it's default, and it's defaulting to Cloudflare, that does make sense. It should, yeah.

Steve: Yes, yes.

Leo: You should have to turn it on.

Steve: And that's what is cool about what Google did, was they're trying to honor the user's existing override, if any, rather than just saying we're going to send everything to Cloudflare. Kristian Khntopp, who's a senior scalability engineer, stated that Mozilla is about to - and this is a little extreme, maybe - he says "about to break DNS" because Cloudflare will be used for DNS resolution over what was assigned by the system administrator, which of course is a concern. And he felt that this would leak the names of all the websites visited in a corporate environment to Cloudflare.

So, you know, the Internet purists are a little annoyed by this. But users are saying, hey, you know, we would prefer not to have our ISP and anybody else on the wire looking at everything, like using DNS to determine everything we're doing. And it turns out that, in the future, in two weeks from now, Leo, we note that, well, yes. But, you know, our IP address, the actual IP traffic is still somewhat of a giveaway, with the understanding that it doesn't disambiguate multiple homed sites at a given IP. But still. So anyway, some interesting movement.

And ZDNet, I picked up on a tip from them that I thought was interesting. For any of our listeners using Chrome now, who have an interest in enabling DoH today, it turns out that that's actually supported. Chrome lacks any user interface for configuring this, and you really are going to want to look at the show notes for this. It turns out that Chrome dutifully obeys launch time startup parameters, which can be added to the shortcut that you use to start Chrome.

So, for example, in Windows you would modify the startup link to add a bunch of command parameters. There's --enable-features, and then the feature is "dns-over-https<DoHTrial." That was one parameter. The next one, --force-fieldtrials, and then that one takes a "DoHTrial/Group1." And then --force-fieldtrial-params, and here's where you specify deliberately what you want to use as the DoH server. And in this case, in the example that ZDNet had, they were using 1.1.1.1 with some parameters.

So again, the show notes have the details for anyone's who's interested. And you can then go to, for example, 1.1.1.1/help, and you'll get a status screen to confirm that your browser is resolving through DNS over HTTPS. So anyway, just a cool little tip from ZDNet for our users who are really wanting to operate on the bleeding edge. Although, you know, DoH works.

In other news, there is no waiting to experience Chrome's deprecation of all obvious display of EV certs. We've talked about this coming. Basically, sadly, the death, the probable death of EV certs because really, if the browser's not giving the user any affirmative obvious indication that you are at a site who has paid extra for extended validation - as they did for a while. You got the nice big, it was like in green, Gibson Research Corporation, woohoo. And that's gone. So I have in the show notes two screenshots showing GRC.com and Wikipedia.org. GRC.com is EV. No indication. Oh, and by the way, www dot for both GRC and Wikipedia are gone. And so Chrome is back to doing that again. They decided no one cares about www, even though, okay, well, it's there in the URL.

Leo: Yeah, and there are a lot of links; right? But it still works. The links will work; right?

Steve: Yes. The links work. It just doesn't...

Leo: Doesn't show it.

Steve: I guess the argument is people don't care.

Leo: Right.

Steve: And you do see, for example, GRC.com/intro.htm where that's now - the tail is a dimmer gray, whereas GRC.com is strong. So they're sort of trying to say, you know, this is where you are. But they're just, like, for www it's like, no one cares. Okay. Anyway, so I clicked on the Show Me More to get the dropdown. And so this is now the only indication, which for all intents and purposes who even knows. You can see that I clicked on the Tell Me More for GRC. And under the certificate, which it shows as valid, it says "Issued to: Gibson Research Corporation." So that versus Wikipedia, where Wikipedia, that's not an EV cert, just says "Certificate Valid," and nothing else.

So given the fact that non-EV certs have a longer life compared to EV - I think EV's limited to two years; non-EV can be three. And if the browsers aren't showing you any benefit, it's like, that's going to be hard to justify the additional cost and the fact that you've got to do that every two years versus getting an extra year of time.

So that's in Chrome 77 now, and I think it really represents a death knell for extended validation. Which is, you know, unfortunate because you did have to jump through additional hoops, although there have been arguments that, for example, there could be a Gibson Research Corporation that was incorporated in a different state. And so that's not going to, you know, it's going to confuse people. Wait a minute. I thought I was at GRC. And now it says Gibson Research Corporation, but it's some other domain name. So I guess I can understand that.

Leo: So this is Firefox, and it does show the owner if you have an extended cert. But if you don't, like Wikipedia, it just says this website does not supply ownership information.

Steve: Ah. So Firefox is...

Leo: In Firefox, yeah.

Steve: Ah, there it is, nice big green, yup.

Leo: Right.

Steve: So it'll be interesting to see if Mozilla follows suit, you know, what their position is on this. But, yeah, it's over as far as Chrome goes. And of course Chrome is, as we know, the majority browser on the 'Net.

Leo: Right.

Steve: So lucky iOS 13. We're getting iOS 13 in two days, on Thursday, September 19th. And frankly, I'm excited for one feature in particular. I love swipey phone keyboards or tablet keyboards. I really do. But I've never been happy with any of the

third-party iOS add-on keyboards. I've tried them all - Gboard, Swype, SwiftKey, and their ilk. And I found that they all misbehave in various ways, most often by failing to deploy when they are needed. You know, you'll sometimes come to a form, and you tap in the field, and sometimes the bottom will blank out, and it's like, hello. I need a keyboard here. Nothing.

So anyway, iOS 13 finally has a swipey keyboard built-in. And I say yay because I would just love to stay with the one that will hopefully deploy when it's supposed to, unlike any of the - like all of those third-party keyboards don't.

Leo: I predict, in a future episode, you will also, whether we've done it or not, I don't know, but you will also find praise for iOS 13's privacy measures. They really now, recognizing that the biggest problem with iOS is the third-party apps, Facebook can lock everything down. But if Facebook sucks, you know, it sucks. So in fact, if you when you first...

Steve: Sucks your data.

Leo: Sucks your data. When you put iOS 13 on, all of a sudden you're going to get a cascade of warnings from Facebook saying, hey, they're looking at your location. Here's the map. You know, I think this is really good. Apple is aggressively...

Steve: That's going to force behavior on other sites, essentially.

Leo: Well, what it forced Facebook to do is already publish an article saying here's why we really should know where you are. This is - please don't. And it even says, you know, we recommend you don't - you always allow us to look at your location. We strongly recommend that. And, yeah, get ready.

Steve: And I heard Rene mention that Pokmon, like he gets a popup every week to say...

Leo: He wants - yeah.

Steve: ...oh, by the way, it's still got your location information. I think that kind of a persistent reminder is very cool.

Leo: Basically, and Steve Jobs said this years ago, he said, "Let them know. Let them know again. Make them tell you to stop letting me know because people" - and Rene's concern, which is legitimate, is that people might just go, yeah, yeah, yeah, yeah, yeah. I don't think so. I've already experienced this. I've been using the beta for some time. It is a great - I really appreciate it. And I always say do not allow unless, you know, usually if it's a mapping app I just say don't allow unless the app's open. If I've opened the app, yeah, you've got to look at where you are. There's no reason that map app needs to know where I am if it's not running.

Steve: Right.

Leo: Or Facebook or anything else. So I think it's...

Steve: Right. And especially if these things are power consumers also.

Leo: Yes.

Steve: If it's, like, draining your battery because it wants to keep, like, an eye on you, it's like, no. Go away.

Leo: No. Go away. Yeah.

Steve: So you've been using the beta. It has a swipey keyboard; right?

Leo: I actually haven't tried it. I should try it.

Steve: Oh, Leo. Okay, well, I'm dying. I got, I mean, for me it's just, like, such a convenience to have...

Leo: Oh, I far prefer swipe, yes, absolutely.

Steve: Yeah.

Leo: And of course I use, on my Android devices, I use it all the time because the default keyboard always on Android has it. I don't know...

Steve: Yeah.

Leo: Let me start typing something and see.

Steve: While I tell our users why we won't be using 13.0 for long.

Leo: Yeah.

Steve: It turns out that we will be jumping to 13.1 very soon.

Leo: On the 30th, yeah.

Steve: After the release, yes, of 13.0, since a headline-grabbing lockscreen bypass bug is already...

Leo: Oh, that's why. Oh.

Steve: ...known to exist. And it still exists in the Golden Master version of iOS 13 that has already been loaded into the many hundreds of thousands of iPhones in shipping containers out there on the high seas.

Leo: Ah. Now I understand. Ah.

Steve: Yup. iOS 13 contains a vulnerability that allows anyone to bypass the lockscreen protection to access sensitive information on that user's phone.

Leo: This has historically been a problem on Apple. For years.

Steve: Yes. Well, and you know, it's because there are just so many of those accessibility and Siri and convenience features, they just keep finding a way around. In fact, this guy, Jose Rodriguez, he found the one that was the bypass, I think it was in 12.1. So he's revealed that he discovered a lockscreen bypass bug in 13 that allowed him to access the full list of contacts on his iPhone and every piece of information saved within them. Jose discovered the newly introduced lockscreen bypass bug on his own iPhone while he was running the iOS 13 beta and reported it immediately to Apple two months ago, actually exactly two months ago, on July 17th.

However, even that was apparently too late for Apple to do anything about it. They had already got their supply chain ramped up and were stamping out iOS 13 into all the phones that they were prepping for the big release. So that bypass remains working in the Golden Master version of iOS 13, which we all get in two days, even those of us who aren't jumping on new pads or phones, and I'm not because, I mean, I did watch all of your coverage on it last Tuesday, and it's like, okay. I'm not a huge camera person. But I definitely want iOS 13.

So we'll be able to get iOS 13 in two days. The lockscreen bug is like those we've seen before, where someone having physical access to a targeted iPhone is able to trick the phone into granting them access to the full list of stored contacts, as well as detailed information for each individual contact, including names, phone numbers, emails, and so forth, using a FaceTime call. This is also similar to the same one that Jose discovered last year in iOS 12.1, just a few hours after Apple released 12.1. It allowed anyone to bypass the phone's lockscreen using the built-in voiceover feature. So this bug requires activating a FaceTime call on the target iPhone and then accessing Siri's voiceover support feature to obtain access to the contact list and all the information saved there.

However, the problem won't exist for long, as it is very much expected to be patched in 13.1, which is expected to begin trickling out to the public 11 days later, on Monday, September 30th. So if this really worries you, you could disable automatic updates until October 1st and jump right over from 12.4.1, where we are today, over to 13.1, and skip that. But I'm not worried about it. Besides, someone has to physically have your phone in order to get to your contacts.

Leo: And there's a not-insignificant amount of fiddling they have to do. So they'd have to have your phone.

Steve: Yes, that's true.

Leo: Without you looking at them for some, you know, a minute or two. Because we just ran the video. It's a lot of steps. It's not an easy - yeah.

Steve: Yeah, yeah. And Leo, in another of those bizarre time travel paradoxes, in the future, two weeks from now, during Episode 734, I have it on very good authority that I will mention that Cloudflare is launching a mobile device-oriented VPN, whereupon you inform me of the just breaking news from the past that Mozilla is also launching a privacy-focused VPN service.

Leo: Yeah.

Steve: That takes me by surprise, once again, because we've been messing around with the space-time continuum for the benefit of our faithful listeners. You know we'll do anything for our listeners.

Leo: Yes.

Steve: So due to the time warp, today, two weeks earlier than then, I am now fully up to speed...

Leo: Oh, good.

Steve: ...on Mozilla's announcement, even though I'll know nothing about it two weeks from now ago.

Leo: That's because I'm about to use the neuralyzer on Steve, and he's going to forget everything.

Steve: That's right.

Leo: Yes.

Steve: In any event, Mozilla has indeed officially launched a new privacy-focused VPN service called Firefox Private Network. It runs as a browser extension to encrypt all of a Firefox user's online activity and limiting what websites and advertisers know about Firefox users, that is, those who might have been watching. The Firefox Private Network service is currently undergoing beta testing and is available only to desktop users in the U.S. as part of Mozilla's recently reborn Firefox Test Pilot program that lets users try out new experimental features before they're officially released. The Firefox Test Pilot program we talked about a long time ago. It was initially launched by Mozilla three years ago, but was shut down at the beginning of this year.

Anyway, Mozilla has decided to bring it back in an updated and changed fashion. Marissa Wood, the vice president of product development at Mozilla, said: "The difference with the newly relaunched Test Pilot program is that these products and services may be outside the Firefox browser and will be far more polished and just a step shy of being ready for general public release." So this newly announced Firefox Private Network is part of this relaunched Test Pilot program's first new project. And as we would expect from any VPN, the Firefox Private Network masks its users' IP address from third-party trackers and protects sensitive information like the websites you visit and your financial information, when using public WiFi.

However, it's important to note, of course, that all by itself it's not offering any anti-tracking protection since these days that's primarily done from within the browser and is not dependent upon IP addresses which change as mobile users switch hotspots, cellular regions, and jump between home and office and so forth. And as you will note in the future, Leo, this is only a benefit for the browser session, not your mobile platform or your desktop in general.

Leo: Future Leo is so smart.

Steve: You were right on the ball. Just the Carnac of TWiT Network.

Leo: I foresee.

Steve: So Mozilla says its Firefox Private Network "provides a secure encrypted path to the web to protect your connection and your personal information anywhere and everywhere you use your Firefox browser." So my feeling is a built-in facility which is easy to use and provides useful VPN services to many people who might not otherwise go to all the trouble to set up a VPN, you know, seems like a good idea.

It, as we noted, encrypts and tunnels Internet browsing activity, but only your browser activity, through a collection of remote proxy servers which thereby mask the user's actual location and block third parties like your ISP or your hotspot provider, anybody who might be sniffing on you, including the government, for example, from snooping on your browser traffic, at least until it emerges from the other end of the VPN connection. Now, interestingly, the proxy servers used by Firefox Private Network are also provided by Cloudflare. So it looks like Mozilla and Cloudflare...

Leo: Wow.

Steve: Yeah, have agreed to provide strong privacy controls to limit what data Cloudflare may collect and for how long it may store any data. We've often on this podcast, and I heard you talking about it just the other day, about a VPN, we've talked about VPN services. And one of the many issues is whether they log; and, if so, what log retention policies they follow.

Leo: Right.

Steve: Cloudflare has stated: "Cloudflare only observes a limited amount of data about the HTTP/HTTPS requests that are sent to the Cloudflare proxy via browsers with an

active Mozilla extension. When requests are sent to the Cloudflare proxy, Cloudflare will observe your IP address, the IP address for the Internet property you are accessing, source port, destination port, timestamp, and a token provided by Mozilla that indicates that you are a Firefox Private Network user. We call this 'Proxy Data.' All proxy data will be deleted within 24 hours." So they're being very clear about what they are observing, collecting, and what their retention policy is.

So anyway, anyone who's interested, our listeners, again, only on desktop Firefox. It is slated to be available to mobile Firefox users, as well, once the VPN exits its beta stage. And although it's currently free, Mozilla has hinted that the company is exploring the possibility of adding value-added commercial service pricing options in the future so that it's able to be a self-sustaining service.

Anybody who has a Firefox account, for example, you use that in order to sync Firefox shortcuts and favorites and links and things between browsers. If you go to https://private-network.firefox.com, you can sign up and join the beta, and then all of your Firefox desktop browsing usage gets proxied by Cloudflare, and you are in a secure browser tunnel for all of the browser stuff you do, which I think seems like a good idea.

So last Tuesday was September's Patch Tuesday.

Leo: Yes.

Steve: And it did not disappoint.

Leo: Well, depends on what you were hoping for.

Steve: That's true.

Leo: There was a lot there.

Steve: It provided fixes for a whopping 79 vulnerabilities.

Leo: Geez.

Steve: Remember when it was 16, Leo? Remember those quaint days of yesteryear?

Leo: It's not getting better, is it.

Steve: No, it's really not. And 17 of those 79 vulnerabilities were considered to be critical. Among the many, we received a further fix for last month's very worrisome CTF flaws which were discovered and explored in excruciating detail by Google's Tavis Ormandy. As we'll recall, Tavis discovered how unprivileged attackers could launch their attack code with elevated privileges by leveraging this CTF client and server system in Windows. And we've long since been disabused of the notion that elevation of privilege is nothing to worry about because it can, as we have seen, really be leveraged to the advantage of attackers. So during the previous Patch Tuesday in August, Microsoft dealt

with one of the related vulnerabilities, CTF vulnerabilities. But at the time, they indicated that there was still more to come.

So as part of this month's offerings, Microsoft has released another fix for this range of flaws titled "Windows Text Service Framework Elevation of Privilege Vulnerability," and addressed another one. Quoting Microsoft, they said: "An elevation of privilege vulnerability exists in Windows Text Service Framework when the TSF server process does not validate the source of input or commands it receives." And that is, of course, what Tavis found, although he worked on it, I think, for a month.

"An attacker who successfully exploited this vulnerability could inject commands or read input sent through a malicious Input Method Editor (IME). This only affects systems that have installed an IME. To exploit this vulnerability, an attacker would first have to log onto the system. An attacker could then run a specially crafted application that could exploit the vulnerability to take control of an affected system." And you never want attackers to take control of your system. You're not going to have a good day. "The security update addresses this vulnerability by correcting how the TSF server and client validate input from each other."

So as we know, the other continuously troubled area of Windows recently has been Remote Desktop. So also in this month's patch batch we get four more fixes to the RDP's client-side fix. Remember that we saw this also the previous month. Microsoft was clearly looking at this code, the RDP code, not only on the server side, which has been a victim of exploitation recently, but also on the client side. And they have found it wanting. So there are four more fixes of what is really not such a big problem which Microsoft has discovered. But now that they're looking at it and giving it the focus of their attention, they're finding more things to be fixed.

I consider it really not such a big problem because being on the client side, this would only affect people who connected their Remote Desktop Protocol client to a malicious server. And I think most people are connecting them to their home base, which is probably not malicious. If it is, you probably have bigger problems.

Anyway, Microsoft again said: "Remote code execution vulnerabilities exist in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights." And, you know, blah blah blah, you'd have to connect to a bad server, or a man in the middle could also interject traffic that would cause a problem. So that was fixed last week.

Oh, we should also note that Microsoft has said that three of those four vulnerabilities have been publicly disclosed, and two of them have known exploits. So hopefully by now, since that was last Tuesday, everybody has run themselves an update and reboot cycle on their important machines and has got those fixed, even though I don't think it's that big a problem to start with.

One of those 17 critical vulnerabilities which was also fixed this month is a VBScript remote code execution vulnerability. So it's just as well, as we have previously noted, that Microsoft will be throwing in the towel on VBScript in favor of the now industry-wide standard ECMAScript, also known as JavaScript, since as we all also too well know, legacy usage and dependency will continue for VBScript forever. I'm sure there are corporations that have written gobs of VBScript stuff, and they need it to, even though it has no future, they need it to stay around. And so it's a good thing that Microsoft is continuing to fix it.

And Microsoft said: "A remote code execution vulnerability exists in the way VBScript engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user," blah blah blah.

So hopefully enterprise use is the only place we will see this, and that it will disappear from the public Internet, because at some point you're probably going to want to disable VBScript usage out on the public Internet. I mean, it's good that these things are being patched. But, you know, this has always been there, and you don't want to have your system taken over remotely by visiting a site that hosts a malicious ad because an advertisement that is being served from an ad rotating service could run script on your browser and do bad stuff to you. So not good.

And I just wanted to take a moment to make sure everybody knows about something I was completely unaware of. And Leo, I'm sure you know about this because apparently it's been around for a couple years.

Leo: Well, also I live in the future.

Steve: Oh, you have that benefit, don't you. You're bringing us wisdom from the future.

Leo: Yes. Yes, that's it.

Steve: I, however, code in assembly language, so I am stuck in the past.

Leo: Oh, my god, are you.

Steve: Chrome Remote Desktop.

Leo: Yeah.

Steve: Oh, my god.

Leo: Really. You're that excited, huh?

Steve: Well, it's just so simple.

Leo: Right.

Steve: It's so easy.

Leo: Right. I think they did it for Chromebooks initially because it just, you know, you kind of need it on a Chromebook.

Steve: Right. Well, in fact you could just consider that to be a remote desktop client, where you don't actually load any apps there, you just run things on a desktop at home.

Leo: Precisely, yeah.

Steve: So my beloved Lorrie had a need to work with a client of hers who was just really unskilled with computers. She was doing remote neurofeedback...

Leo: Oh, wow.

Steve: ...and needed to set up this client's computer. And, I mean, there was just, like, she had to get onto her desktop. And so I looked. I said, oh, yeah, no problem. Windows, it's built into Windows.

Leo: It's built in, RDP, yeah.

Steve: Yeah. And there is that, what is it, there is Remote Desktop Protocol, but there's Remote Assistance.

Leo: Right.

Steve: And so I showed her how that worked. And she, like Lorrie was saying, oh, you know, honey, that's...

Leo: This isn't going to work.

Steve: That's going to be too much. And so there was like, you know, a bunch of commercial services that were doing it. But they were like, you know, the good ones weren't free, and blah blah blah. And finally I stumbled on remotedesktop.google.com. And it's like, oh, my god. And so, I mean, so it's like - anyway, I just wanted to make sure, I wanted to bring it to our listeners' attention. I'm sure that our listeners are from time to time having to help somebody that really, you know, just like they should not have a computer. But they have one anyway.

And so, wow. In fact, I don't even think you need Chrome. You originally did. But now you need - they have revamped it. You need a browser that supports WebRTC. And maybe that's too - I think that you need WebRTC to be on the controller side. I think you probably still need Chrome, the Chrome browser, to be on the side which is taken over. So but, you know, again, Chrome is the majority browser on the Internet, and you just go to there, and you click a button, and it downloads an extension to Chrome, and you can then view their desktop. And, wow. So anyway, just a little heads-up because, boy, I mean, in terms of a slam dunk for helping somebody who really has a hard time pushing buttons, like do I click once or twice - well, actually that is a question for the ages - it's just a win. So, yay.

Leo: Yeah. And it's free.

Steve: Yeah. Yes, exactly. It's free. And works through NAT and, I mean, you know, because everybody...

Leo: Yeah, does NAT traversal, yeah, yeah, that's right, yeah, yeah.

Steve: NAT traversal. And I was just - I was very impressed with this thing.

Leo: Works with Firefox. At least that's - I just set it up, yeah.

Steve: Yes, yes. That is exactly what I was going to say. And so Firefox in addition. And of course that also probably means it will work with the new Edge, if it doesn't work with the old Edge. I imagine it probably does work with the old Edge. But we know it will work with the Edge based on Chromium. Chredge or something? What is it you and Mary Jo and Paul were calling the...

Leo: Chredge, yes, Chromium Edge, Chredge.

Steve: Chredge, Chredge.

Leo: WebRTC is such a great standard. You can use it for video calls, for phone calls.

Steve: Yup.

Leo: Really, this is really - it's working well. I think it's great. It's browser-based.

Steve: Yeah. It's really moving, moving to the future. Where you have been for quite some time, Leo.

Leo: I'm glad you finally got here.

Steve: Yeah. So Exim. Exim email servers are in trouble again. I wanted to make sure - this news is a little old because I just - it had been on my list of things to get to, and I haven't been able to get to it until now. But it's important.

We first talked about them several months ago. This was that bizarre, it takes a week to exploit the server thing. Remember, Leo, where you would be a client of a vulnerable server, and they were all vulnerable, and you'd basically create a bogus email and then send them a byte a minute so that the connection wouldn't time out, and then something would get tired after a week of waiting for this thing, this final email message to get sent. It wouldn't happen.

So then it would tend to - it would try to send you a bounce message. But in the envelope that you had sent, you had put shell commands, you know, exec shell commands in, like, the mail bounce or the reply-to, whatever it was, which this Exim server would execute. So even though you had to be patient, you would be able to execute as root any commands which you had stuck into the email envelope and then waited. Which I argued a worm would be able to take great advantage of. And in fact there were worms that were doing this, as it turns out, not surprisingly.

Well, unfortunately, Exim is back again with another problem. This one is way worse. The Exim maintainers have released Exim v4.92.2 after publishing an early warning two days beforehand to give sysops an early heads-up that they would really need to patch this as soon as this went public because they knew that bad guys were going to jump on it. And it affects all email server versions up to and including its immediate predecessor, 4.92.1. And just to remind everyone why this matters, Exim is a widely used, open source, mail transfer agent for all Unix-like operating systems - Linux, macOS, Solaris, et cetera. And it is currently behind nearly 60% of the Internet's email servers today. So it's the majority email transfer agent.

This new vulnerability is CVE-2019-15846, affecting, as I mentioned, all Exim servers previous to the one that was patched only recently which accept TLS connections. And of course that's now considered best practice. GRC, you know, accepts TLS connections. But the fault that was discovered allows attackers to obtain root-level access to the system by sending an SNI, that's the Server Name Identification, ending in a backslash null sequence during the initial TLS handshake. Whoopsie.

As we know, SNI is an extension to the TLS protocol which allows servers to host multiple TLS certificates on a single IP. It allows a connecting client to tell the server in the first TLS packet which server certificate it wants to use for this TLS connection. And according to the Exim team, since this vulnerability does not depend on the specific TLS library being used by the server, both GnuTLS and OpenSSL are affected. And though the drop-in default configuration of the Exim mail server software does not have TLS enabled by default, since TLS certs need to be supplied and configured, that makes sense. Still, some operating systems do bundle Exim with the default vulnerable feature enabled.

So what this means is immediately a large, large population of Exim servers are vulnerable. And there's no question. We did verify three months ago when the previous vulnerability was made public that Exim servers declare their version in their hello message when they answer a connection, which means it is very easy for Shodan to index them by version, and for bad guys to find them. And you don't have to wait a week now to take one over. You can do so instantly. So with any luck, this is old news to any of our listeners who may be responsible for Exim servers. If not, you want to update to 4.92.2 immediately.

Also, a follow-up from a listener last week - I'm not sure which space-time continuum we're in, Leo, but I think it was last week. I was complaining, or I mentioned the Firefox browser memory consumption problem and how I was recommending an add-on. I think somebody in the chatroom, because I remember you supplied the information on the fly, Leo, mentioned that there was an about:config switch in Firefox which was disabled by default. It was browser.tabs.unloadOnLowMemory. It defaults to false.

Leo: Right.

Steve: And I said, yay. I didn't know about that. I'm going to turn it on, and next week I will know because the whole process I go through for building the show is to have a bunch of tabs open. I had 40-some open at the beginning of production of this podcast.

Leo: Wow.

Steve: So I set it to true, and memory consumption immediately fell.

Leo: Woohoo. Yay.

Steve: So it works. So, yes. To all of our listeners, if you're a Firefox user, and you have multiple tabs open in a memory-lean machine - I only have 8GB, as I mentioned, on the Lenovo X1 that I use. I use it in a closed configuration with a Lenovo dock in my other location. But unfortunately, 8GB is all the RAM it's got, which is a little tight these days. And this really solved the problem for me. So thank you, listener or chatroom person, for mentioning that. It works great, and I wanted to let everyone know.

Also we've been talking about ransomware a lot recently because - ransomware. So I wanted to note something that someone tweeted in my direction, which was that Windows 10 Windows Defender includes a ransomware protection feature which enables various protections against ransomware. We were talking about, and will be actually in the future, Leo, in two weeks, talking about synchronization and how having file sync systems which store previous versions is good protection against ransomware.

Well, it turns out that Windows 10 also builds some in. However, it is disabled by default because it requires some handholding and tuning. And it's not for the faint of heart. But I wanted to point out that it is there, and it is useful, and it works. It involves two features. One is Controlled Folder Access, and the other is Ransomware Data Recovery. Controlled Folder Access is definitely disabled by default, and it will definitely cause you some annoyance while it's being trained. Which is why I'm sure Microsoft has it off by default.

And what really surprised me is that it even blocks Microsoft's own apps, like IE and Edge, which I thought, well, okay, maybe they're just trying to be really evenhanded here. But once it's been trained, it will definitely be useful until and unless it, too, is bypassed somehow. You know, everything ends up being bypassed eventually. But maybe it's rooted so deeply in the kernel that it's going to be difficult to have that happen. It will probably keep unknown baddies from touching your user data filled directories, you know, like everything underneath your documents, you know, the things you tend to do.

The second component is Ransomware Data Recovery, which automatically syncs those same common user data directories up with your Microsoft OneDrive to keep those files backed up. Anyway, so ransomware victims with this feature enabled can then use OneDrive to recover their files if they ever become encrypted with ransomware. And I don't know how Microsoft does this, but presumably there's something going on where it's not going to get fooled. If it already has a file that's been backed up, ransomware won't, you know, it won't overwrite that on OneDrive if it's changed by ransomware. Maybe some heuristic that Microsoft is employing where suddenly the entire file changes dramatically, Microsoft says, not so fast there. I wasn't able to get any specific information about how that works.

But I do know that Controlled Folder Access is a useful, but painful feature. I had to enable it toward the end of my work on the SQRL client because SQRL stores its user SQRL identity in a SQRL folder under the user's documents. And also SQRL has a self-install feature that really freaked out Windows 10 because installing themselves is what malware wants to do also. So that's how I learned a lot about Controlled Folder Access.

And essentially you're getting notifications constantly of things that are wanting to write into your documents folder, so you're having to say, you know, look at what it is and go, yeah, okay. Yeah, okay. Yeah, okay. Yeah, okay.

And so there's sort of an exponential falloff of yeah, okays that you're needing to explicitly do. But frankly, I like the idea of having to whitelist things because, again, the need to train them falls off pretty rapidly over time, and then you end up with a system that's pretty well locked down. So anyway, I just wanted to put that on everybody's map as something to consider.

Okay. You've got to look at the logo. It's animated. They did SVG animation on the header of the site. And it's just wonderful: S-I-M-J-A-C-K-E-R dot com. Simjacker.com.

Leo: So there's the SIM.

Steve: There it is.

Leo: But watch carefully. What?

Steve: Agh.

Leo: Turns into a voodoo mask.

Steve: It'll repeat.

Leo: That's really good. That's really...

Steve: I loved it. They did a really nice job. So unfortunately, that's the end of the good news.

Leo: That's the end of the funny stuff. Oh, boy.

Steve: That's - the rest is not funny. And when I read this, like, what? You what? It's a new SIM card flaw. And get this, not theoretical, not like some university saying, oh, you know, maybe if the moon is full and you click your heels three times you can leak some data from an Intel side channel. No. This is discovered being actively exploited in the wild, which allows attackers to hijack ANY, capital, all bold, ANY phone just by sending it an SMS message, which is like, what?

So this comes from AdaptiveMobile Security. And in their overview they said: "AdaptiveMobile Security have uncovered a new and previously undetected vulnerability and associated exploits, called Simjacker. This vulnerability is currently being actively exploited by a specific private company that works with governments to monitor individuals."

Leo: What?

Steve: Uh-huh.

Leo: Oh, man.

Steve: Yeah. "Simjacker and its associated exploits is a huge jump in complexity and sophistication compared to attacks previously seen over mobile core networks. The main Simjacker attack involves an SMS containing a specific type of spyware-like code being sent to a mobile phone, which then instructs" - and this is where I'm going, like, wait a minute, have we just jumped the shark here? - "instructs the SIM card within the phone to take over the mobile phone to receive and perform sensitive commands." And I did some digging around in Wikipedia. It's like, wait a minute, I thought a SIM was a ROM. How can a ROM take over?

Anyway: "The location information of thousands of devices was obtained over time without the knowledge or consent of the targeted mobile phone users. During the attack, the user is completely unaware that they received the attack, that information was retrieved, and that it was successfully exfiltrated. However, the Simjacker attack can, and has been extended further to perform additional types of attacks.

"Simjacker has been further exploited to perform many other types of attacks against individuals and mobile operators such as fraud, scam calls, information leakage, denial of service, and espionage. AdaptiveMobile Security Threat Intelligence analysts observed the hackers varying their attacks, testing many of these further exploits. In theory, all makes and models of mobile phone are open to attack as the vulnerability is linked to a technology embedded in SIM cards. The Simjacker vulnerability could extend to over one billion mobile phone users globally, potentially impacting countries in the Americas, West Africa, Europe, Middle East, and indeed any region of the world where this SIM card technology is in use."

They finished: "We're quite confident that this exploit has been developed by a specific private company that works with governments to monitor individuals. AdaptiveMobile Security has been working closely with the customers and the wider industry, including both mobile network operators and SIM card manufacturers, to protect mobile phone subscribers. We've blocked attacks and are committed to using our global threat intelligence to build defenses against these new sophisticated attacks that are circumventing current security measures."

So I have a lot of information here, but I had to dig down further. So I found a "how does it work." They wrote: "The main Simjacker attack involves an SMS containing a specific type of spyware-like code being sent to a mobile phone, which then instructs the SIM card within the phone to take over the mobile phone to retrieve and perform sensitive commands." So that repeats what I said earlier.

"The attacks exploit the ability to send SIM Toolkit Messages and the presence of the S@T browser on the SIM card of vulnerable subscribers." And I thought, what? Maybe we are in the future. "The S@T browser is normally used for browsing through the SIM card. The Attack messages use the S@T browser functionality to trigger proactive commands that are sent to the handset." And it turns out that, like, the SIM is in line between the radio and the rest of the phone handset functionality. Anyway, the responses to these commands are sent back from the handset to the SIM card and stored there temporarily. Once the relevant information is returned from the handset, another proactive command is sent to the handset to send out an SMS containing the information. So I thought, what the hell? An S@T browser of some kind on SIM cards?

So at this point I jumped over to Wikipedia to get a bit more background, and that just made things worse. Wikipedia says: "SIM Application Toolkit (STK) is a standard of the GSM system which enables the subscriber identity module" - which is what SIM, S-I-M, stands for - "to initiate actions which can be used for various value-added services. Similar standards exist for other network and card systems, with the USIM Application Toolkit (USAT) for USIMs used by newer generation networks being an example. A more general name for this class of Java Card-based applications running on UICC cards is the Card Application Toolkit." Okay. So there's just way too much technology which apparently some committee once upon a time said, oh, that'll be cool to have in there. Let's stick that in. And, like, nobody - everyone just kind of forgot about it.

Anyway, so the SIM Application Toolkit, this SAT, which is in all GSM network phones, "consists of a set of commands programmed into the SIM which define how the SIM should interact directly with the outside world" - what? - "and initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input."

Leo: Wow.

Steve: It's like, it what?

Leo: Who knew?

Steve: Yes, exactly. Well, unfortunately, bad guys. "STK has been deployed by many mobile operators around the world for many applications, often where a menu-based approach is required." Okay. Maybe back in the day of a flip phone, where you actually had a text screen that you had to, like, scroll through or something? But it turns out everyone stopped using it, but it stayed in there. And they give an example: "...such as mobile banking and content browsing. Designed as a single application environment, the STK" - this is still Wikipedia - "can be started during the initial power-up of the SIM card and is especially suited to low-level applications with simple user interfaces."

And they finish what I'm quoting here, saying: "In GSM networks, the SIM Application Toolkit is defined by the GSM 11.14 standard released in 2001." So, yes, for the last 18 years. Then they said: "From release 4 onwards, GSM 11.14 was replaced by 3GPP TS 31.111, which also includes the specifications of the USIM Application Toolkit for 3 and 4G networks." So in other words, we all have it. And if our phone receives an SMS that was carefully crafted completely without our knowledge or permission, things can be done to our phone behind our back.

Let's see. "AdaptiveMobile Security explained that their global threat analytics system allowed them to correlate the Simjacker sources with known malicious threat actors. As a result, they can state with a high degree of certainty that the source is a large professional surveillance company with highly sophisticated abilities in both signaling and handsets. These types of companies exploit the fact that mobile operators may incorrectly regard core network security as solved, if they deploy a standard GSMA-compliant firewall." But that's not the case.

So they've revealed the existence - "they" meaning AdaptiveMobile - the existence of the vulnerability and associated exploits that they call Simjacker. They believe this vulnerability has been exploited for at least the past two years by a highly sophisticated

threat actor in multiple countries, primarily for the purpose of surveillance. Other than the impact on its victims, from their analysis, Simjacker and its associated exploits is a huge jump in complexity and sophistication compared to attacks previously seen over mobile core networks.

I've got a bunch more information about IMEI recovery, location, data messages, a big graphic here in the show notes showing the way, on the way in, the SIM intercepts a Simjacker attack SMS and essentially takes over the phone and is then able to probe, execute commands on the device, obtain information back, and then forward it out to an accomplice device. And so at the minimum it's able to obtain location information, essentially pinging the phone without any notification of the user.

But it's also able to play a tone; send a short message; set up a call; send USSD information; send SS, whatever that is; provide local information, the IMEI, the battery, the network, the language, et cetera; power off the card; run an AT command behind the user's back; send DTMF commands; launch browser; open a channel; send data; get service information; submit multimedia requests; determine geographical location.

Anyway, so they said: "By using these commands in our own tests, we were able to make targeted handsets open up web browsers, ring other phones, send text messages and so on. These attacks could be used to fulfill such purposes as misinformation, by sending SMS/MMS messages with attacker-controlled content; fraud, by dialing premium rate numbers; espionage, as well as the location retrieving attack, an attacked device could ring another number, thus turning it into a listening outpost; used for malware spreading by forcing the browser to open a web page with malware located on it, which it would then execute; denial of service, by disabling the SIM card; or information retrieval, retrieve other information like language, radio type, battery level, and so forth."

So basically we all have this capability in any GSM network-participating phone right now. So all of those examples that we see in the movies where the person takes the SIM card out, those suddenly sound like a much better idea than they were before. Of course you take the battery out, too, and the phone is shut down.

Leo: Or completely, for no reason at all, break it in half and throw it out the window.

Steve: You've got to crack it in half, Leo, just for dramatic effect.

Leo: Breaks the hinge. That's all you're doing. Everything's fine.

Steve: I do have another graphic in the show notes which is interesting, which is a distribution, if you scroll way down, against a black field, a distribution of attack targets that they have seen. So it's an extremely long tail, but clearly a very few number of specific targets were receiving a high rate of probes about their location. They said: "In one country we are seeing roughly 100 to 150 specific individual phone numbers being targeted per day via Simjacker attacks." They said: "Although we have witnessed bursts of up to 300 phone numbers attempted to be tracked in a single day, the distribution of tracking attempts varies."

So anyway, this is being used for surveillance in targeted attacks. And the good news is it looks like these could be caught because they have to transit the mobile phone network. And right now there are no firewalls that are blocking this from happening. Basically it means getting smart about this at the mobile phone infrastructure level because it's certainly not the case that all of our SIM cards are going to be replaced any

time soon. But, boy, I mean, this looks like a capability that was overdesigned once upon a time, that had a brief window of usage, and then nobody ever turned it off or took it away or shut it down. And it's just a glaring vulnerability in GSM phones.

Leo: Oh, only GSM.

Steve: Yes. Only, well, GSM, SIM-based GSM. I'm not enough of an expert in other non-GSM networks. But there are alternative SIM-like systems in non-GSM phones.

Leo: Right. There are SIMs in LTE phones. But do you think that's a different kind of thing?

Steve: I'm not, again, not an expert enough to know.

Leo: Yeah, interesting. I bet it is the same. Why would, you know, they'd never take out a capability; right? When you can put in more.

Steve: Exactly. Wow.

Leo: Mark says it's the same. He says the only thing resistant is CDMA. Mark's a security expert and fan.

Steve: Ah, cool. And does anyone use CDMA anymore? Did that go away?

Leo: You know, some older Verizon and Sprint handsets maybe. But everybody's moved to LTE. CDMA over LTE in some cases. But I think you'd still be using the SIM.

Steve: Yes. In that case the underlying transport would be LTE still.

Leo: Right.

Steve: Wow. So anyway...

Leo: Not good. Not good.

Steve: Our listeners, in general we don't have anything to worry about. It's nice that this came to light. Certainly there are people somewhere whose location is, well, and you can imagine that this is the kind of thing that law enforcement could ask a provider to provide for a given individual. We want to know where they are right now, and there could be an answer from virtually any - virtually anybody can be targeted whose phone number is known.

Leo: Right.

Steve: By sending them an SMS message. Their phone will say, yup, here's where I am, and other stuff, too.

Leo: Wow. Wow. Just - and of course hijacked for malicious purposes, not merely spying on you. But, you know, you could make money off of it.

Steve: Right, right.

Leo: Well, well, well. Isn't that special. Thank you, Steve, for really cheering up - I think that's why people listen. They listen for the happy news here at Security Now!. And that's why they keep tuning in. They still haven't gotten any.

We do this show every Tuesday, 1:30 Pacific, except when we're doing it in the time zone shift thing.

Steve: Yes, when we are dropping through...

Leo: We're in our time tunnel.

Steve: ...a spatial rift.

Leo: When we're in the Star Gate, you never know when it'll be. But so we have recorded the October 1st show ahead of time. And I think we're going to record again on Saturday afternoon; right?

Steve: Yes, we are. We're going to record on Saturday afternoon for Tuesday.

Leo: Steve's headed out - when are you leaving?

Steve: I leave on Sunday.

Leo: Okay. Steve's going on his European tour to tell the world about SQRL. By the way, Mark was at the event in - where was it?

MARK: Orange County.

Steve: Oh, cool.

Leo: And he said there were over a hundred people there, and you asked, "How many of you listen to Security Now!?" And when everybody raised their hand, you said, "Well, let me put it this way. How many of you don't?" And it was three people.

Steve: Yeah. And I said, "Maybe you three should get a clue because, you know..."

Leo: Yes. Everybody else is listening. I hope you all got that clue. If you like Security Now!, tune in. We do it live, as I said. We won't be for a couple of weeks. But normally it's Tuesdays at 1:30 p.m. Pacific, 4:30 Eastern, 20:30 UTC. You can watch live at TWiT.tv/live. So we're not going to be back here until October 8th.

Steve: Correct.

Leo: October 8th we'll be back on our regular schedule. But as I said, we're not missing an episode. We recorded an evergreen for October 1st, and we're going to do one on Saturday. If you want to watch that, by the way, it'll be about 2:30 Pacific, 5:30 Eastern, 21:30 UTC Saturday, right after the radio show.

Steve: Even if we have to bend the space-time continuum to make it happen, Leo, we will...

Leo: Well, this one's not so bad because you're recording Saturday for Tuesday.

Steve: Yeah. So there'll be a less dramatic snapback when the fabric restores.

Leo: The rent is repaired. You can get copies of this episode. You know, it's all in order on the website. Go to GRC.com. While you're there, you can not only get a 16Kb version of this show, but 64Kb audio. You can also get a great transcription by Elaine Farris. She writes it all down. It makes it a lot easier to understand if you can read along.

We also have lots of other good stuff there, including Steve's bread and butter, SpinRite, world's best hard drive maintenance and recovery utility, GRC.com. Steve can be messaged there, GRC.com/feedback. But you can also "at" him on the Twitter. He's @SGgrc. And he takes DMs, as well, there. So if you have something secret to tell him, @SGgrc.

I will be also putting the show up on our website, TWiT.tv/sn. And when I say "I," I mean those guys down the hall because I'm out of here. TWiT.tv/sn. Or best thing to do, you know what, you should all be doing this, don't be one of those three people who says I don't know what you're talking about. Subscribe. Find your favorite podcast application or subscribe on YouTube, and you'll get it the minute it's available in the proper order. The packets will be reordered for your convenience. No buffering. Thank you, Steve.

Steve: Okay, my friend. I will talk to you Saturday afternoon, after The Tech Guy.

Leo: All right. All right. I'll see you then.

Steve: Bye.