
# Fingerprint Biometrics

**Description:** After catching up with the week's news, and following the news that Apple's new iPhone Touch ID system was spoofed within days of its release, Steve and Tom take a much closer look at the technology and application of Apple's Touch ID system, examining the reports of its early demise.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-423.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-423-lq.mp3

---

SHOW TEASE: Coming up on Security Now!, I'm filling in for Leo again. And Steve Gibson and I have got some great stuff to talk about. There's more NSA news, seems like there's more every week. We've got some of that. Also we'll find out what about iOS7 is really frustrating Steve, and it's not the fingerprint sensor. In fact, we've got a whole explanation of what's good and what's bad about fingerprint biometrics. All that and more coming up.

TOM MERRITT: This is Security Now! with Steve Gibson, Episode 423, recorded September 25th, 2013: Fingerprint Biometrics.

It's time for Security Now!, the show that attempts to keep you informed about the safety hazards of the Internet, and sometimes the wider world, to help you stay safe online. I'm Tom Merritt, filling in for the vacationing Leo Laporte. He's gone for two more weeks, so I get to do this show one more time. I'm excited about that because I get to do the show with this guy, Steve Gibson, the man behind GRC.com, ShieldsUP!, SpinRite, and so much more. Steve, it's a pleasure to do this show with you. Thanks for letting me co-host.

**Steve Gibson:** Oh, likewise, Tom. It's great. We get along well.

TOM: We've got some fingerprint biometrics to talk about today, amongst other news.

**Steve:** Well, yeah. As soon as the news of the fingerprint reader came out, our listeners will remember me saying, well, let's see how long it takes before the reader is spoofed. And I'm finding myself reacting to the fact that people are saying it was hacked. To me, it was spoofed, it wasn't hacked. A hack would be something that circumvented the need for it. But spoofing is, I mean, that's the right term. Fake fingerprints were made. And we talked a little bit about the technology. The fact that it was a capacitive technology as opposed to a photographic technology meant that inherently you would need a 3D finger. And of course it didn't last a week.

So I figured it'd be a great topic for today since it's obviously very topical. It's in the news. And I wanted to also put it into perspective because one of the groups that performed the hack said, see, nanny nanny nanny, we told you fingerprints were no good. But a different guy who did it says, you know, the topic of his posting was "How I hacked Apple's Touch ID, and why I still think fingerprints are great." And both of these really - the reason I think I want to share them mostly is they really take us into the technology that had to be developed in order to do this, which is also sort of interesting. And of course we've got a whole bunch of news of the week. So a great podcast.

TOM: Yeah, it's a great - I'm really interested in talking about this, too, because what these - you can use "hack" in sort of the broad sense of messing with stuff to apply to it here. I know what you mean. It's not actually changing the sensor or getting in there. But these ways of going after it, they show the limits of it. Nothing is a hundred percent secure ever. So to me what these show is not that, oh, see, fingerprints are bad. It's that, if you're going to use a fingerprint sensor, you should know that these are the limits to what it's going to be effective at and what it won't be.

**Steve:** Exactly. What I want to do is I want to bring back some perspective of - and in fact, even in this context I think a week or two ago I talked about front door keys that are also not - that are not unique. But they're in the physical world, and they're good enough to do the job. And a fingerprint and what you have to go through to spoof it and the fact that it's a real-world, physical attack that involves proximity, in that sense it's completely different than anything that can be done to us from China or Russia, purely electronically, with a zero-day sort of thing. So it does really put us, I think, in a different class of security. So I want to just take a really good overview of what this means in the context of security and convenience because really those are the two terms that apply.

TOM: Yeah. Watch out for those boxes of fingers being shipped over from other countries. Okay, Steve. Let's get into some of the security news, starting with - oh, yeah.

**Steve:** Yeah, now...

TOM: With the NSA. Back again.

**Steve:** We can't get away from it.

TOM: NSA and RSA. We've got two different SA's.

**Steve:** Yes, we do. We shouldn't be away from it until it sort of dies down...

TOM: Sure, of course.

**Steve:** ...of its own accord. Now, many people apparently misunderstood what I was saying in the last couple weeks about this so-called backdoored dual elliptic curve programmable random number generator, or deterministic random bit generator, I think is what - DR, whatever it was - when I was saying that nobody would use it. I wasn't saying nobody has ever used it. I said anyone who knew anything would be crazy to use it. So that was my point, was that in this collection of four pseudorandom number generators that the NIST had standardized on, it was, like, it was ridiculously bad. It was hundreds of times slower. It was questionable from even before the ink was dry on the standard. And it was sitting next to three others that were faster and clearly secure, where from day one this stepchild was just wrong. And then we find out that it's the default random number generator used by RSA's suite of security libraries.

[Silence]

TOM: It just kind of leaves you speechless, doesn't it.

**Steve:** Okay. Let me say that again. The RSA, the arguably sort of premier commercial provider of security technology and software, the inventors of standard factorial-based public key encryption, the designers of all these technologies, they, in commercializing this, they created a suite of libraries. There's Crypto-C, Micro Edition Suite, Crypto-J, Cert-J, SSL-J, Crypto-C, Cert-C, SSL-C, all these packages. There's something called the BSAFE Toolkits, they call them. And what we learned from a letter that RSA sent to their major clients and customers is that they needed to change the default pseudorandom number generator used in all of this for, I think it was like 2007 or 2008, I mean, for like many years, because the default was this last orphan child random number generator. That's what the BSAFE Toolkit suites used by default. They had other PRNGs in there. But if you didn't explicitly select and tell the package to use a different one, this is what you got. And it is impossible to explain this. I mean, this is just - the security industry was stunned. I mean, arguably, we should have known. But it was just - you just - RSA would be the last person you would expect to do this.

TOM: RSA is synon- I mean, I know most of the audience knows that they're synonymous with encryption. In an episode of "Agents of SHIELD" that premiered yesterday, they throw out RSA in there as sort of like, yeah, we're using RSA, like...

**Steve:** The guys, yeah.

TOM: If Joss Whedon writes that in the script, that means that this is permeated into the consciousness of the culture; right?

**Steve:** Okay. So Matthew Green, whom we've spoken of recently, the Johns Hopkins cryptographer, he wrote - and I'll just quote the top of his posting. He said: "In today's news of the weird, RSA," and he says in parens "(a division of EMC)" because they got bought by a bigger fish, "has recommended that developers desist from using the" - and he says in parentheses "(allegedly)," and then in quotes, "backdoored" - and that's the other thing, too, is that our listeners understand, because we covered this in detail, what we know about this. And we don't know anything. But there's every reason to be as suspicious as we should be. And that's all the reason anyone needs never to use it. I mean, because it's not like it's the only choice. It's like the worst choice, in terms of performance. Oh, and in fact, in trying to defend it, the CTO of RSA said, well, you know, there are purposes for having slow algorithms. It's like, what?

TOM: Like what?

**Steve:** Well, for example, when you want to strengthen a password, you run it through a hash many, many, many hundreds of thousands of times. But that's slow hashing functions.

TOM: Yeah, that's not the same thing.

**Steve:** It's completely distinct, yes, from a slow random number generator. Normally you need those at very high speed and very high quantity. We were talking about how entropy gets drained from operating systems that maintain entropy pools and that - so operating systems are thirsty for new entropy because the random number generator is taking up the entropy in order to do a really good job. So this is just - this is unbelievable.

But anyway, so continuing what Matt Green said, he said: "...developers desist from using the (allegedly) 'backdoored,'" in quotes, "Dual_EC_DRBG random number generator, which happens to be the default in RSA's BSAFE cryptographic toolkits." And then Matt writes: "Youch." He said: "In case you're missing the story here, Dual_EC_DRBG (which I wrote about yesterday)," he says, "is the random number generator voted most likely to be backdoored by the NSA." And of course he doesn't mean voted literally. No vote was taken. But we all agree.

He says: "The story here is that, despite many valid concerns about this generator, RSA went ahead and made it the default generator used for all cryptography in its flagship cryptography library. The implications for RSA and RSA-based products are staggering," writes Matt. "In the worst case, a modestly bad but by no means worst case," he says, "the NSA may be able to intercept SSL/TLS connections made by products implemented with BSAFE."

TOM: B-UN-SAFE.

**Steve:** Oh, goodness, yeah. "So why would RSA pick Dual-EC as the default? You got me," he says. "Not only is Dual_EC hilariously slow, which has real performance implications, it was shown to be a just plain bad random number generator all the way back in 2006. By 2007, when Shumow and Ferguson raised the possibility of a backdoor in the specification, no sensible cryptographer would go near the thing. And the killer is that RSA employs a number of highly distinguished cryptographers. It's unlikely that they'd all miss the news about Dual_EC. We can only speculate about the past." So, I mean...

TOM: Can you make a stab at why?

**Steve:** Well, NSA. Again, we will never know. We don't actually positively know there's even a problem. But there's certainly grounds - there's grounds for concern. The magic numbers used in this particular elliptic curve, remember I said elliptic curves are fine, but specific ones, because there's an infinitude of them, specific ones are chosen for various reasons. So the researchers, Shumow and Ferguson, verified that it was possible to have a backdoor such that getting a few random numbers from this generator would allow you to get the entire future, to essentially capture its state. And once you have the whole state of a random number generator, because it is deterministic, you can simply project that state forward into the future.

So it's impossible to excuse this. No one would have chosen this. Someone did. And, I mean, there's, like, there's no better place to plant a trojan than in RSA's toolkit, which is used pervasively as a building block because no one wants to write all this complex crypto stuff themselves. It's used pervasively in commercial products as a building block for everything. So, I mean, this is the nightmare scenario. And we know how crucial random numbers are. It's the basis for secrecy is that you choose a random number which is unpredictable by your adversary, and then you encrypt it in order so the other side can decrypt the random number, then they have it, and then you both use that for the actual - to run the cipher. So anyway, the incredible good news, I mean, this is another example of the positive fallout that Edward Snowden created. None of this would be happening if he hadn't sacrificed his way of life.

TOM: You mean no one would know about it.

**Steve:** Correct, I'm sorry. None of the revelations would be occurring. And, I mean, this has now been killed. This may have been the coup that the NSA has had, and it's dead.

Well, it will be as soon as they root this out of all the products that have it.

TOM: Sure. Well, this seems to be the smoking gun that goes along with the story that said NSA had broken encryption, and everyone was saying, well, they can't have broken encryption. Bruce Schneier was saying, "Trust the math." This could be the explanation of it. They didn't have to have broken anything. They had something that was already broken, essentially.

**Steve:** There could very well be people back in Langley who are just not happy today.

TOM: Oh, I'm sure.

**Steve:** Because their big feather that they had managed to insinuate out into the industry - and, I mean, also, the problem with this is that it is not just the NSA. There are other smart people in the world. And especially when you aim them at something, and you give them a place to go dig, they can find answers. So if other people, not the government, I mean, you could argue that the U.S. government, the NSA having this is bad enough. But this has always been the argument against allowing any kind of security vulnerability, even one that seems to be asymmetric in nature, where only if you had a secret would it be vulnerable. The problem is, those secrets cannot be kept. The fact that Edward Snowden happened demonstrates the NSA could not keep their own secrets.

TOM: Right. And what the NSA would like to say is, yes, but if Snowden had kept his mouth shut like he should, this wouldn't be happening. That he didn't is a fact. And the fact is, if he didn't keep his mouth shut, if he did keep his mouth shut, somebody else might not have kept their mouth shut, just proving the point that you can't keep the secret.

**Steve:** And the fact that there are other smart people implies that, if we allow known weak crypto with suspected backdoors to go into heavy use, then it may very well be that there are other people far from Langley, Virginia who are also not happy because who's to say that they haven't independently cracked this. And that's the danger. It's not just, I mean, if there is a crack, and it requires keeping a secret, the huge breakthrough in our understanding of how to secure privacy is that algorithms must be public. The idea that you have - and even RSA is guilty of this. They had some, RC6 may still be, but RC4 was for a long time, and then it kind of - it got loose from their control. The idea is that you want to have the algorithms be open and then - but be secretly keyed. Here we have an algorithm that is inherently flawed because it's based on some keying material no one knows the providence of. We don't know where it came from. It just, ooh, magic numbers. You know, trust us. And, no. We can't do that.

TOM: TNO, yeah.

**Steve:** Yeah. So...

TOM: I was just going to say, I think the lesson here - because I'm sure there are people in our audience even who say, well, you know what, I want the NSA to have an advantage; I'm not one of these people who is against them. And that's fine. I probably disagree with you, but that's fine, to be on that side of the argument. However, it's not necessarily, as Steve is saying, about just the NSA. You don't know who else has the ability, or has had the ability for a long time now, to take advantage of this same backdoor.

**Steve:** Yeah, and they're not going to tell you. They don't want to disclose - they don't

want to disclose that. It's probably, if it exists, it is a super-secretly guarded secret. And they're chortling around with their ability to capture some random numbers and then know the future. Which is the end, which kills crypto.

TOM: And even The New York Times now understands that backdoors are bad.

**Steve:** I was impressed by this, actually. This meant something to me because it was the Sunday review section. It was put up in the paper by The New York Times Editorial Board. So not just one random crank, I mean, but this was their formal statement. They said: "In 2006 a federal agency, the National Institute of Standards and Technology" - NIST we've talked about - "helped build an international encryption system to help countries and industries fend off computer hacking and theft. Unbeknown" - unbeknown? Well, that's what it says. Unbeknown. I guess I can put a "st" in, unbeknownst.

"Unbeknownst to the many users of the system, a different government arm, the National Security Agency, secretly inserted a 'backdoor' into the system that allowed federal spies to crack open any data that was encoded using its technology." Now, again, we don't know that. So this is dumbed down for the general population. Unfortunately, it's also a little overblown. But our listeners understand suspicion is enough, and we've got plenty of suspicion, when there doesn't need to be any.

So going on it says: "Documents leaked by Edward Snowden, the former NSA contractor, make clear that the agency has never met an encryption system that it has not tried to penetrate." Well, that's probably true. "And it frequently tries to take the easy way out. Because modern cryptography can be so hard to break, even using the brute force of the agency's powerful supercomputers, the agency prefers to collaborate with big software companies and cipher authors, getting hidden access built right into their systems.

"The New York Times, The Guardian and ProPublica recently reported that the agency now has" - meaning the NSA agency - "now has access to the codes that protect commerce and banking systems, trade secrets and medical records, and everyone's email and Internet chat messages, including virtual private networks." Again, that's a little overstated, but okay. "In some cases, the agency pressured companies to give it access." Now, that we do know. "As The Guardian reported earlier this year, Microsoft provided access to Hotmail, Outlook.com, SkyDrive, and Skype. According to some of the Snowden documents given to Der Spiegel, the NSA also has access to the encryption protecting data on iPhones, Android and BlackBerry phones.

"These back doors and special access routes are a terrible idea, another example of the intelligence community's overreach. Companies and individuals are increasingly putting their most confidential data on cloud storage services and need to rely on assurances their data will be secure. Knowing that encryption has been deliberately weakened will undermine confidence in these systems and interfere with commerce. The backdoors also strip away the expectations of privacy that individuals, businesses, and governments have in ordinary communications. If backdoors are built into systems by the NSA, who is to say that other countries' spy agencies or hackers, pirates and terrorists won't discover and exploit them?"

TOM: And we've been saying they probably already have, yeah.

**Steve:** Oh, yes. The government can get a warrant and break into the communications or data of any individual or company suspected of breaking the law. But crippling everyone's ability to use encryption is going too far, just as the NSA has exceeded its boundaries in collecting everyone's phone records rather than limiting its focus to actual suspects. Representative Rush Holt, Democrat of New Jersey, has introduced a bill that

would, among other provisions, bar the government from requiring software makers to insert built-in ways to bypass encryption. It deserves full Congressional support. In the meantime, several Internet companies, including Google and Facebook, are building encryption systems that will be much more difficult for the NSA to penetrate, forced to assure their customers that they are not a secret partner with the dark side of their own government." Wow.

TOM: Good on them for pressuring Congress, yeah.

**Steve:** Yes, yes. And the idea, I love the idea that we could see some legislation that forbids the government from asking for this because then any companies approached are completely free to say, first of all, no; and also to say, hey, guess what the NSA just asked us to do illegally? So this is a step forward.

TOM: Yeah, absolutely.

**Steve:** Yeah. I was pleased and impressed.

TOM: I'm not sure how much I feel Google and Facebook are the folks I want leading the charge on building new encryption standards. I don't think it's bad to have them in there. I prefer distributed open source solutions to that. That's why this next story both scares me and heartens me. What does Torvalds have to say about inserting backdoors?

**Steve:** I know. I just got a big kick out of this. And this, of course, came out last week. He was - well, anyway. So I'm stuck on his name because I know he pronounces it apparently Linus [Lee-nus].

TOM: You can say Linus [Lie-nus]. I say Linus [Lin-nus], which is probably...

**Steve:** Sort of a compromise, yeah.

TOM: Yeah.

**Steve:** Anyway, so Linus or Linus or Linus, who created the open source Linux operating system...

TOM: LT.

**Steve:** ...22 years ago, of course we all know, "took the keynote stage at the LinuxCon conference, along with fellow kernel developers, to talk about the state of Linux kernel development. Throughout the hour-long session, which occurred on September 18th, the panel was peppered with a barrage of questions on a wide variety of topics, with the outspoken Torvalds providing all manner of colorful comments. Torvalds was also asked if he had ever been approached by the U.S. government to insert a backdoor into Linux. Torvalds responded 'no' while nodding his head 'yes,' as the audience broke into spontaneous laughter."

TOM: Classic. It's classic Torvalds. He's hilarious, if you've never actually heard him speak.

**Steve:** And the problem is I wouldn't have been laughing.

TOM: Well, it's not funny. It's funny the way he delivered the answer.

**Steve:** Correct.

TOM: The actual answer is no laughing matter, you're right about that.

**Steve:** It's funny, have you tried saying no and nodding? It's amazingly difficult.

TOM: It's hard. Yeah, it's like patting your head and rubbing your tummy at the same time. No. You have to think about it.

**Steve:** Yeah, it requires a lot of deliberate override of what's natural. Anyway, I loved that. And here's another piece of information. So he says no while he's nodding. So, yikes. At least...

TOM: It's an elegant way to deliver a complex piece of information, which is usually in these cases, if you have been approached, the government then says you can't tell anybody we approached you.

**Steve:** Of course, yes. And this was brilliant. So hats off to him. And further evidence of the pressure that manufacturers of pervasive systems, even something like this, I mean, the much-heralded open source, I mean, I don't know how he would do it if he chose to. But of course he never would, so...

TOM: No. Good man. I hope.

**Steve:** Changing the topic...

TOM: Yeah, I was going to say, hopefully we've got one iOS7 security thing to talk about when we get to fingerprints later on in the show. But there's other flaws. Whenever there's an iOS update, there's always going to be flaws that surface. And hopefully none of these have to do with the NSA. What are they?

**Steve:** So, okay. What intrigued me about these, I found three different problems that have been reported. But from the standpoint of being a developer, and just sort of - problems have a feel. It's one thing to have, like, an obscure buffer overrun in some library that was written 10 years ago, that if you dance in a full moon in the dark with touching your nose and send in a certain thing, this will happen. That's one thing. These feel different. These feel like they are characteristic of a system which is getting overly complicated and is beginning to show its age. And that's sort of sad. I mean, these are mistakes that are a consequence of complexity. And as we know, security and complexity are enemies of each other. It is difficult for anything really complicated to also be secure.

And what unfortunately Apple has done is they have added feature on feature on feature on feature. There are little pathways, little cracks through the system that they obviously didn't foresee. So the first one is just kind of a - I get a kick out of, reported by a number of different people. The Find My Phone feature, much heralded in iOS7, can be disabled by putting the device into Airplane mode. Okay, well, that's not surprising because Airplane mode, of course, shuts down all communications because otherwise we're told we're going to crash. Okay. So the problem is in iOS7 this can be done when the phone is locked with a passcode, meaning not by its owner, but by a thief, as the voice-activated assistant, Siri, which is available by default while the phone is locked, can be verbally instructed to put the phone into Airplane mode.

TOM: That's just one of those ones where they weren't - they thought, oh, well, putting it in Airplane mode, you should be able to do that. That's not a security flaw. Oh, wait a

minute. Yes, it is.

**Steve:** And then the problem is Siri is still accessible, as we will hear in the third one, which is another Siri accessibility problem. She's accessible while the phone's locked. So first thing the thief does is have Siri put the phone in Airplane mode for him, and now he doesn't have to worry. Now he can attack the phone and not have to worry about Find My Phone being activated remotely. It can't be, because it's disconnected. Wow.

Now, this one, apparently there was a soldier who had a lot of time on his hands, and he was bored. Maybe he was on guard duty. Jose Rodriguez in the Canary Islands somehow worked his way through this little gem. Anyone can exploit the bug by swiping up on the lock screen to access the phone's control center. We'll be coming back to the control center later because I have a peeve of my own about that.

TOM: I'm going to do this along with you.

**Steve:** So you swipe up on the lock screen to access the phone's control center. And then opening the alarm clock, holding the phone's sleep button brings up the option to power it off with a swipe. Instead, the intruder can tap Cancel and double-click the Home button to enter the phone's multitasking screen.

TOM: So far so good. It's working.

**Steve:** That offers access to its camera and stored photos, along with the ability to share those photos from the user's various accounts, essentially allowing anyone who grabs the phone to hijack the user's email, Twitter, or Flickr account. And then people who wrote about this said: "The far-reaching nature of this breach through the steps described above offer unfettered access to a user's photos and the sharing functions of those photos. That includes access to social media accounts and emails. And by selecting the option to send a photo by iMessage, it also allows complete access to the user's contacts, and all information stored therein." So, I mean, this is just a classic mistake and then a wedge that pries open access to other parts that are needed in order for the first phase to function.

TOM: I got into my App Store, too.

**Steve:** "Apple has reportedly acknowledged the mistake and pledged to rectify it in a later software update. Until this gap is patched, users can prevent this from happening to them by disabling access to the Control Center on the lock screen. Go to Settings, then Control Center, then swipe the option to Access on Lock Screen so that it does not display on the lock screen." So another little mistake. It's like, oh, won't these features be nice. But they do kind of combine in a way that wasn't expected. Okay.

TOM: There you go. Off.

**Steve:** And finally, finally, this is an interesting one. For pre-iPhone 5s devices, it's assumed, being upgraded to iOS7: "If you have an iPhone 5 or older and have updated your operating system to Apple's new iOS7, you should be aware that the password or passcode required on your phone's lock screen no longer prevents strangers from accessing your phone." No longer prevents them from doing it. So this occurs after the upgrade. "They can use Siri, the voice command software, to bypass the password screen and access your phone instead. Simply hold down the Home button, even while the phone is locked, and wait for Siri to ask you what you want. From there, we accessed Facebook, Twitter, text messages, email, and phone calls..."

TOM: Really?

**Steve:** "...all on our iPhone 5."

TOM: Really, Apple? Really?

**Steve:** "We even got access to our contacts app. Access is limited. You can't see anything on the phone beyond the lock screen and the Siri interface, so you can't play Candy Crush" - oh, darn - "for instance. But you can do a lot of important basic phone stuff on someone else's phone. Email, calls, text, and social media are probably the majority of time spent in mobile phone use. You can stop Siri bypassing your password by reducing access to Siri in the Settings. Go to Settings > General > Passcode Lock [enter the passcode] > Allow access when locked > Siri > switch from green On to white Off."

TOM: So this is an example of a default being in the wrong position.

**Steve:** Exactly. Exactly. Now, they say: "Here's one theory: On iPhone 5s, the new iPhone, access to the phone is through a fingerprint security device called Touch ID," which of course is the topic of this podcast, "which utilizes the Home button as the fingerprint detector. Only the person who owns the phone can open it. If you're running iOS7 on an iPhone 5s, it would be impossible to unlock the phone by pressing the Home button. The problem is that, on earlier devices, pressing the Home button brings up Siri, not the fingerprint detector. That would explain the non-obvious workaround inside the Settings section."

TOM: I think they should make Siri be able to recognize the owner's voice.

**Steve:** Yes. I was thinking the same thing. It's like, eh, you don't sound like Jack.

TOM: Right.

**Steve:** Now, I put this note in my show notes when it first popped onto my radar, middle of last week.

TOM: This is funny.

**Steve:** And I didn't know whether we would be talking about it, say, not yet, or yes. But for those who don't know, there is a fun website: IsTouchIDHackedYet.com. And of course it now offers the news, yes. And in fact, what was really cool was that, when it initially appeared, people began posting donations for - pledging that they would offer the person who first hacked Touch ID, and again I say "spoofed," X amount of money. And I remember seeing the figure $16,000 at one point. I haven't added it up. I don't know where it is. There were some, even after it was shown to be spoofed, some thousand dollar donation. So it's like, okay, well, that helps pay for the materials that were required.

TOM: Yeah, no kidding.

**Steve:** Now IsTouchIDHackedYet.com says "Yes" and provides some background information and a list of all the nice sponsors who provided lots of money.

TOM: That's great. That's really funny.

**Steve:** Yeah.

TOM: So what's Apple saying about Touch ID?

**Steve:** Right. There is, naturally, there are various types of support pages. There's the page that shows how to do it and how to use it. There's also a support page in their knowledge base that sort of helps to put it into context, which is useful to share and provide some additional information. I'm sure we're going to be learning incrementally more about it as time goes on. They said: "To configure Touch ID, you must first set up a passcode. Touch ID is designed" - and this is crucial wording. And this did exist prior to the spoof. So this is Apple's pre-hack or spoof position, which is right.

They said: "Touch ID is designed to minimize the input of your passcode; but your passcode will be needed for additional security validation, such as after restarting your iPhone 5s; when more than two days, 48 hours, have elapsed from the time you last unlocked your iPhone 5s; or to enter the Passcode and Fingerprint settings." So they understand that in situations where maybe asking Touch ID to provide more security than it should, the phone will fall back to prompting you for your passcode.

Then Apple continues: "Since security is only as secure as its weakest point, you can choose to increase the security of a four-digit passcode by using a complex alphanumeric passcode." So here they're teaching us about switching to the full keyboard and using something long. They say, skipping over that: "You can also use Touch ID instead of entering your Apple ID password to purchase content from iTunes Store, App Store, and Book Store. You will be asked to scan your fingerprint with each purchase. If Touch ID does not recognize your finger, you'll be asked to try again. After five failed attempts," and this comes up later today, "you'll be given the option of entering your Apple ID passcode. In addition, you will need to enter your Apple ID passcode after restarting your iPhone 5s and enrolling or deleting fingers."

So they have backed it up with essentially requiring two-factor authentication in those instances where maybe you have less - they're trying to suggest things that a bad guy might do or you do infrequently or, for some reason, you haven't apparently had access to your phone for some length of time. They're using the metrics they can to say, in this instance, give us additional confirmation that you're still you. So that's certainly reasonable.

TOM: Yeah. And this is the thing that made me positive about Touch ID when I first heard the announcement was that they weren't switching over to say, we're relying entirely now on your fingerprint for access to the phone, which would have been a horrible thing.

**Steve:** Right, right.

TOM: Now, what about where they store my fingerprint? That's getting a lot of attention, a lot of discussion.

**Steve:** Yeah. And we don't know enough. I mean, this is where Apple ID - I'm sorry. Apple ID. Apple is generally more secretive than I would like about security. Apple is not open to the degree that other companies are. So they're not telling us yet. I expect over time - this is what I mean by we'll be learning more. They end this page by talking about what they call the "Secure Enclave." So they have their own term.

TOM: Wow.

**Steve:** Touch ID, they say, "does not store any images of your fingerprint. It stores only a mathematical representation of your fingerprint. It is not possible for your actual fingerprint image to be reverse-engineered from this mathematical representation." That's all good, and this is what I conjectured a couple weeks ago when I was talking about the topology of features. "iPhone 5s also includes a new advanced security architecture called the Secure Enclave within the A7 chip, which was developed to protect passcode and fingerprint data. Fingerprint data is encrypted and protected with a key available only to the Secure Enclave. Fingerprint data is used only by the Secure Enclave to verify that your fingerprint matches the enrolled fingerprint data. The Secure Enclave is walled off from the rest of A7 and as well as the rest of iOS. Therefore, your fingerprint data is never accessed by iOS or other apps, never stored on Apple servers, and never backed up to iCloud or anywhere else. Only Touch ID uses it, and it cannot be used to match against other fingerprint databases."

So a couple things. Because of where we're going to go with our next story, it's interesting and key that it is not backed up to iCloud, they say. And I will say, what they described is entirely possible from a pure architectural standpoint. It is certainly possible to create essentially an environment where you can send in, that is, you have a write-only ability to send in fingerprint enrollment data, and no ability to read it. So it's write-only for enrollment. And similarly it is submission-only for a candidate to ask about matching. And what you get out is just go, no go. That is, it just says yes, this matches sufficiently; or, no, it doesn't.

So, I mean, this is all good news. They're not storing prints, so they're not in there anywhere. They're storing structural information, the so-called - again, I'm hypothesizing - some topological representation of features which have been found. And they're storing it in a custom-designed, not just saying, I don't know, like not having a software in iOS that has set aside some chunk of EPROM somewhere. This is hardware on the chip, designed for this data to live there, such that you can only send fingerprint image data in. You can only say "learn this" or "compare this." And so this is all good news. I think they've done the right thing. And significant that it's not backed up. It cannot come out. It only goes in. So...

TOM: Isn't there a networking security system like that where you can only send in on one channel, or one cable, or one connection, and out on a - there's an entirely separate one?

**Steve:** Yeah. In fact, we've talked about that a couple times. Ethernet itself, the actual physical wiring, is one twisted pair that goes in one direction, transmitting, and a different twisted pair that goes in the other direction, receiving. And there are systems, cables you can actually make, there are even little connector boxes that deliberately drop the other direction. So you electrically cannot send data in the other direction. And there are even fiber optic links where you've got a photo diode and a photo receptor and a piece of plastic in between, and there just isn't any way for data to go...

TOM: That's the one I remember you talking about. I think that's the one I'm thinking of right there, the fiber optics system. That's really cool. GeekCanuck says he's going to start making rainbow tables for fingerprints. Do you think that would get him anywhere?

**Steve:** Rainbow tables. I don't think so. Okay. So we don't know exactly, we don't yet have details on what they're looking at. There are sort of two levels of features in fingerprints. The so-called "minutiae," and that's actually the term they use, the "minutiae," are sort of the subfeatures, like broken ridges or sort of ridges that merge, or ridges that form a little disconnected island, where...

TOM: So kind of the imperfections, huh.

**Steve:** Yeah, they are. Now, the larger details are what we normally see if you just, like, looked at your fingerprint on a glass. You would see humps, and you would see what's called a "whorl," is where the ridge goes out and kind of does a loop and then goes back the same direction it came from. So you have this ridge reversing course and going off the fingerprint, back where it came from. You have other ones that just go up and then sort of come back down and continue going off in the same direction. And then you have some that are just not connected to the edges of the fingerprint in any way, sort of at the top level. And we don't really know exactly what they're doing. But the articles we'll be covering here toward the end of the podcast give us some sense for what was necessary in order to defeat it.

TOM: Yeah. All right. Our last main story here in the news, when I read the headline, it kind of threw me. And then when you read the story you start to realize, well, maybe I should have guessed this. "Google knows nearly every WiFi password in the world?"

**Steve:** Yup. Now, and this is - what's interesting is this is even not news. I mean, this is not startling except in the context now of post-Snowden era. As far back as in June of 2011, a guy named Donovan Colbert, writing for TechRepublic, describes stumbling across this fact on a new ASUS EEE PC Transformer tablet.

So back in June of 2011 he wrote the following: "I purchased a new ASUS EEE PC Transformer tablet last night after work. I brought it home, set it up to charge overnight, and went to bed. This morning when I woke I put it in my bag and brought it to the office with me. I set up my Google account on the device and then realized I had no network connection. So I pulled out my Virgin Mobile Mi-Fi 2200 personal hotspot and turned it on. I searched around Honeycomb" - which of course that was the version of Android, right, back then on the tablet? - "looking for the control panel to select the hotspot and enter its encryption key. To my surprise, I found that the EEE Pad had already found the Virgin hotspot and successfully attached to it.

"As I looked further into this puzzling situation, I noticed that not only was my Virgin hotspot discovered and attached, but a list of other hotspots were also listed in the EEE Pad's hotspot list. The only conclusion that one can draw from this is obvious: Google is storing, not only a list of what hotspots you have ever visited, but any private encryption keys necessary to connect to those hotspots.

TOM: Which does all make sense. Google keeps a profile for you to make it easy when you turn on a new Android device and load all of your settings.

**Steve:** Exactly.

TOM: Why wouldn't your WiFi password be one of those things?

**Steve:** And that is going on to this day, two years later, more than two years later. And thus the genesis of the headline, "Google knows nearly every WiFi password in the world." They're saying with the massive number of Android devices which are backing themselves up to Google's Cloud, and the default setting is to back up the settings of the device, and that includes your list of known-to-that-device previous hotspots and the encryption keys for them, those are up there. And we also know that you can, if you attach a new device, it will automatically - and synchronize to the Google Cloud, it's automatically configured with that information. So what we now know is that Google has that stuff, and Google has the ability to decrypt it. And the NSA has the ability to ask

Google for that, if they want it.

TOM: Well, and that's the key; right? Because you can also phrase this story "Google knows every email in the world" because there are so many Gmail addresses that they probably know a large percentage of the email because they're either being sent to or sent from Gmail accounts. And you can make a similar argument about documents. It all pretty much hinges on client decryption, which is what happened when he set up his PC Transformer, he put in his password, how secure that is, and whether Google can get into your private profile and hand it over to somebody if somebody comes knocking with a subpoena. Or not, in some cases. They don't even need them.

**Steve:** Well, actually we do know that they can. We know that they're now boasting good physical datacenter security and good encryption in the datacenter, but that they can remove it. I mean, they have access to our data. And many people have verified that through clever tests of changing their password before synchronizing, and then Google finds them and synchronizes. So it wasn't using their password, blah blah blah. So we understand that our link to Google is encrypted. But once there, we're now depending upon their encryption, which they have the ability to break, being strong. And of course the integrity of all the employees who have access to our data.

TOM: Right, of course. There are Snowdens on all sides of the equation.

**Steve:** Uh-huh, yeah.

TOM: So you have your own list of iOS7 errata, things you think Apple should publish?

**Steve:** Yeah. Like Sarah, I ordered my phone very late in the morning, or, wait, very late in the night, early in the morning, actually, shortly after midnight. I'm just getting a black one, but they said they'd ship it sometime next week. So it's like, I'm not desperate for it. But all my other iOS devices are switched over to 7. And one of the things that I do often, have always done in the old days, pre-7, I'd lift the screen up and then slide to the left to get the control panel. And I would adjust the brightness because - and I find I do it several times a day because the auto adjust is useless to me. It never seems to - I thank them for trying, but they don't seem to know what I want.

So I'm manually adjusting the screen. And sometimes it's glaringly bright, so I'll bring it down. Sometimes I'm out in the sunlight or in a lighter setting, and so I crank it all the way up. But it's something I'm doing all the time. So but I immediately recognized there was a problem because of course the new way is, from any screen, you drag up from the bottom, and up comes a handy control panel. Unfortunately, to make it more visible, Apple dims the rest of the screen, and the panel itself is not very bright. So in raising the control panel where the brightness setting is, they're dimming the screen so I can't see how bright the setting is I'm trying to make. And I was reminded of - you're probably old enough, Tom, I hope, to remember pre-remote controlled TVs.

TOM: Oh, yeah. I was the remote control.

**Steve:** You'd be sitting on the couch across the living room from the family's TV screen, and the volume would be too low. So you'd get up and go over there to turn the volume up. But now you're standing at the TV, and so of course it's louder. So you adjust the volume, then you sit down, oop, now it's too loud. So you get up again and turn it down. So my point is, of course, where you're sitting, you can't adjust the volume, and when you get there, it's different. Similarly, you can't change the brightness on the iPad without it changing the brightness for you so you can't tell what brightness you're going

to have once you're through changing the brightness.

TOM: And you can't use the hack that Bill Merritt used, which was to tell his son Tom to go change the volume without him getting up from the couch. That's no way to do that with your phone.

**Steve:** Exactly. Okay. A little louder, Tom. Oh, a little - okay, that's just perfect, yeah. Okay, now, the other thing that occurred to me, actually it has been a problem for me, is - and I worried about the TWiT studio - is the local bandwidth congestion on one's network of having multiple iOS devices in the house with the auto app update turned on. A couple days ago I was unable to watch you guys live. It was pausing constantly. And I was getting a little spinning disk, and then it would try again, then it would pause. And I thought, what is going on? Because, I mean, I'm the master of my domain. I know what's happening all the time here.

And so I closed the stream from you guys and looked over at my router. And I've got a big iron Cisco industrial router. And normally the activity light flickers routinely because I have a live connection to GRC's servers, and I have a protocol that I developed for synchronizing, like when we hear "yabba dabba do" here it's because I'm sending UDP packets querying for a status update, and they come back through the multiple layers of NAT that way to get to me. So there's a little constant activity. I know what my network looks like. And this thing, the light was on hard solid. And I thought, what is going on?

So I fired up my packet sniffer. I saw a huge amount of TCP traffic going to one IP. It was somewhere in Englewood, Colorado, the network where it terminated. I didn't have a clean lookup, a reverse. And I thought, you know, I'll just bet it's my iPads because I have a couple of them and an iPhone here, all that are cruising. And sure enough, I shut them down, network went back. And then I was able to listen to you guys without any trouble. And I then, because it just sort of annoyed me, turned off auto update on all of those. You go into the iTunes Store setting over in the left-hand column, and there's an option for things that update. You can turn off auto update. I'm just going to switch back to, first of all, allowing them to accrue for a while, and then updating my master copy of iTunes on a Mac, and then synchronizing the pads to get the most recent app.

And so here was my concern was that it's one thing for me to have my little network disturbed by a couple iOS devices. I can't imagine the TWiT studio with everyone there having a phone, and suddenly Elements, which is like a gig-plus, decides it needs to update on all of them.

TOM: Oh, yeah.

**Steve:** So I'll mention this to Leo, too, just to be aware that it could really warp the bandwidth of the TWiT studio.

TOM: And it could do that in any kind of large situation. I thought immediately of universities because I remember when the iPhone first came out, and it was always trolling for WiFi access points. Some sysadmins at universities got upset about that. This is much worse than just looking, pinging the access point. This is, like you say, in some cases large amounts of data getting downloaded.

**Steve:** I mean, most of the time. And we know how rapidly these apps are being updated. They're constantly being updated. And if you're like me and Sarah, and the app count you've lost control of, there's just a lot happening.

TOM: What's your most hated UI change? This is interesting.

**Steve:** Pure gripe. It turns out that I use the app history all the time. So I would, again, I would lift up the screen using a four-finger swipe, and there in order of reverse chronological recency are the icons of all the apps I've used, however many could fit across the bottom. And then if I needed to go back further, I'd scroll to the right in order to get the next most old ones. And of course I know the icons perfectly. I know what every one of them is. So of course what Apple has famously done is they've screwed that up completely. Now when you do that you get big thumbnails of the last screen state of each of these, and then the icons are widely spaced out. So that if you get, like, three, one in the middle and two on the edges, because they've been forced apart by the size of the thumbnail that is hovering over them, it's just - it's a catastrophe for me. I mean, it's, like, just disastrous. So...

TOM: You know what bothered...

**Steve:** I hate it.

TOM: You know what bothered me the most about it is a lot of times I'll just close all of those, right, as a way to track down a particular battery drainer usually. And now you've got to swipe the screen away, that little freeze frame of the screen state that you were talking about. That's so much slower than just having them all jiggle and then tap tap tap tap tap and get rid of them.

**Steve:** Yup. Yup. In fact, I'm glad that Sarah showed that on the show, where you can, while you're looking at that history view, you can drag the big thumbnail screen up and off the top, and it goes away. So it's at least one way of closing apps, and also contracting your history again. But I'm really, I mean, this is - I don't know how I'm going to get used to this because I feel like being able to see whatever it was, like 7 on an iPad, I mean, there's like - everything that I had been doing, I could just quickly jump back to. And yes, you can do the four-finger swipe sideways to kind of go back in time. But it just was so easy to quickly lift the screen and say, oh, that's the one I want; and, bang, I was there.

TOM: Yup.

**Steve:** I've lost that now.

TOM: It's just not as convenient. I use that a lot, too. I haven't noticed it being a big problem because usually the one I want is close. It's not very far away. So I always had to swipe maybe a couple of times anyway. But, yeah, I know what you mean. On to the miscellany, then?

**Steve:** Yeah. I mentioned a few weeks ago the TV series "Orphan Black."

TOM: Mm-hmm, big fan.

**Steve:** Yes. And I'm through with the first - I'm halfway through. I'm through with the first of two disks because I got it on Blu-ray. And I just wanted to say that I'm stunned that that's one actress.

TOM: I know. She is incredible, isn't she.

**Steve:** That's, yes, that's what I come away feeling. I mean, overall, it's a nice series, I

mean, it's interesting. I like it. It's just like sort of a good procedural thriller. But for me, what stuns me is that she isn't actually cloned.

TOM: Right.

**Steve:** I mean, it's like the parts she plays are phenomenally different from each other. Sometimes a little overboard, like to make them distinct. But believable. But as I'm looking at these people, I'm having to remind myself, this is actually the same person because she does just an amazing job. And I don't think it's just hair and makeup. I think it's she becomes these different people. So that's what, for me, that's the most fascinating part of the series, which is it's just amazing.

TOM: I remember watching that first episode and thinking, okay, they're visually different, but how long can she really keep these characters separate? And she really - you forget. You forget while you're watching it that it's Tatiana Maslany, or however you say her name, I apologize, Tatiana, is doing all of those parts. I agree. She's incredible.

**Steve:** So I also wanted - we've mentioned on the podcast several times the TV series "Homeland," of which Leo and I are both huge fans. I'm, like, a hyper fan. I just - it was so good the last two seasons. I'm hoping they're able to keep it going. But it does...

TOM: Were you happy when Claire Danes got her Emmy?

**Steve:** Yes. Yes. I mean, she does a fabulous job, also. And I just - everything about it I really enjoy. And I wanted to make a note that it returns to the air this coming Sunday for our listeners who don't already have systems set up to capture it.

And then this is just completely random, but I just - this happened this morning when I was putting the show together, and I just thought, you have got to be kidding me. I've always had my domains at Network Solutions. That's, you know, back in the day they were the guys. They were where you got domains. I mean, we registered GRC.com at the same time that Microsoft registered Microsoft.com. I mean, I've had the domain that long. And so there wasn't all these alternatives. So, and inertia has kept me there, and it's a pain to move everything, and I've got a bunch of stuff there.

Anyway, they've recently just been spamming me with marketing propaganda. I mean, it's really getting to be annoying. And then this morning was - I just looked at it, I thought, no, no, no, no. A domain that I have, I got a free registration for it in .biz for one year, $0. And I thought, first of all, I thought, what? It's like, I was confused. Was my account hacked somehow? Did somebody register this for me? Or like, what, what, what? Then I realized what this is. It is pure bait and switch. It is we're going to give you an existing domain in the .biz top level at no charge for a year, hoping you will use it. Because then you're stuck. And I just want to flip them the bird and just say, you know, that is just slime.

TOM: I moved all of my domains with concierge service. And they're not a sponsor of this particular show. They are a sponsor on the network, but Hover, you just call them up. You tell them your domains. They do all the hard work for you. And then you do all the confirming and everything, so it's secure. But that was nice.

**Steve:** Yeah. I just looked at this, it's like, you've got to be kidding me.

TOM: Yeah, that's annoying. That's super annoying. So you're working on a ton of stuff.

**Steve:** Oh, boy, I am. So I just wanted to give our listeners a - I finished the work on this first phase of the SpinRite R&D. We have full pre-AHCI support, which was the PCI Ultra DMA controllers, which virtually everybody has in their machines for the last couple years, although the newer machines have their motherboards set to AHCI, which is the next-generation controller. That's the next thing I'm going to support. What's somewhat amazing is that we achieve 100% success on all controllers that anyone in the newsgroups, and we have hundreds of people have tested this on hundreds of machines, have in their possession. Many AHCI controllers turn out to do double duty, and so we already work with those, and many RAID controllers. We're now able to penetrate what I call "thin RAID," where it's a RAID feature, but it's actually just a bunch of disks, and the software provides the RAID functionality. And so it calls itself RAID in the system. We run on all of its drives. There was only one true, apparently true RAID by HighPoint Systems, where at this point we're unable to operate on. And we may be, once we add AHCI support.

And we're getting stunning performance. Because I built my own extended real-mode operating facility, essentially, that I talked about once before, and my own extended memory manager into this technology, so we're in real mode, running DOS, yet we have access to all of the machine's memory. We only need 32MB, but that's vastly larger than the buffer we were using before. It's the largest buffer drives can use. But that's getting us, on a Level 2 fast recovery scan, we're seeing, like, 93 minutes per terabyte. So now multi-terabyte drives can be scanned and data recovery performed on them in a couple hours. So that's really going to be very cool. And of course, as I've said, I've committed, a free upgrade to all of this for current 6.0 owners.

At this point now I've stopped work on that because I am frantically, feverishly, fervently working on documenting the identification authentication system that I've come up with. And I'm going to try to have that as our topic for next week, Tom.

TOM: Great.

**Steve:** I think I probably can. Because I know that I've piqued everyone's curiosity, to say the least.

TOM: Yes.

**Steve:** It's holding up. I've got pages now of clear documentation and diagrams. And I've thought things through all the way, which is what I was wanting to do, but I wasn't letting myself really spend the time until I got SpinRite, this first phase, nailed down. And it's looking good. So I think that'll be the big reveal a week from now.

TOM: So no Q&A next week? We push that off one?

**Steve:** I'm willing to for this.

TOM: Nice. I'm excited about this. I can't wait to hear about it.

**Steve:** And I'd love to do it with you, and then I get to do it with Leo again the next week. So that's...

TOM: Oh, yeah, there you go. Perfect. Everybody wins. All right, Steve. Let's get into Touch ID. Let's get into fingerprints. First of all, there have been some cool hacks. What are these hacks that people have been doing? I love the Chaos Computer Club one, frankly.

**Steve:** Yeah. Well, okay. They're basically one, that is, there is one way to do this. And so I want to share the "nanny, nanny, nanny" posting, which I've edited a little bit just so that it reads better on the podcast. And this was the original claim that was met with some skepticism until a good video was being made. There was some concern that the video wasn't really very good. And I'll make a couple comments about that whole notion, too. But this is sort of the - I want to show both sides to this coin. These are the guys who think fingerprints are an absolutely bad idea, period, and you'll certainly get that sense from them.

So this is the official statement from the Chaos Computer Club, who were the first people to spoof Apple's Touch ID. They said: "The biometrics hacking team of the Chaos Computer Club (CCC) has successfully bypassed the biometric security of Apple's Touch ID using easy" - we'll see about that - "everyday means. A fingerprint of the phone user photographed from a glass surface was enough to create a fake finger that could unlock an iPhone 5s secured with Touch ID. This demonstrates again, they say, that fingerprint biometrics is unsuitable as an access control method and should be avoided. Apple had released the new iPhone with a fingerprint sensor that was supposedly much more secure than previous fingerprint technology. A lot of bogus speculation about the marvels of the new technology and how hard to defeat it supposedly is had dominated the international technology press for days." Okay, well, I didn't see that, but I also wasn't looking for it. But I will take their word for it.

TOM: I don't know about dominated, but it certainly was talked about. I'll give them that.

**Steve:** Yeah. Starbug, who performed the defeat, said: "In reality, Apple's sensor is just a higher resolution compared to the sensors so far. So we only needed to ramp up the resolution of our faking technology. As we have said now for" - actually it says "for more many years" - "for many years, fingerprints should not be used to secure anything." These are the anti-fingerprint people. "You leave them everywhere. And it is far too easy to make fake fingers out of lifted prints."

Okay, unquote. So back to the announcement. "First, the fingerprint of the enrolled user is photographed with 2400 dpi resolution. The resulting image is then cleaned up, inverted, and laser-printed with 1200 dpi onto a transparent sheet with a thick toner setting. Finally, pink latex milk or white wood glue is smeared into the pattern created by the toner onto the transparent sheet. After it cures, the thin latex sheet is lifted from the sheet, breathed on to make it a tiny bit moist and then placed onto the sensor to unlock the phone. This process has been used with minor refinements and variations against the vast majority of fingerprint sensors on the market." We'll talk about all this in detail, what they were achieving with this, in a second. But then they posted an update:

"The process described above proved to be somewhat unreliable as the depth of the ridges created by the toner was a little too shallow. Therefore, an alternative process based on the same principle was utilized and has been demonstrated in an extended video available. First, the residual fingerprint from the phone is either photographed or scanned with a flatbed scanner at 2400 dpi. Then the image is converted to black & white, inverted, and mirrored. This image is then printed onto a transparent sheet at 1200 dpi. To create the mold, the mask is then used to expose the fingerprint structure on photo-sensitive printed circuit board (PCB) material. The PCB material is then developed, etched, and cleaned. After this process, the mold is ready. A thin coat of graphite spray is applied to ensure an improved capacitive response. This also makes it easier to remove the fake fingerprint," so the form's mold release. "Finally, a thin film of white wood glue is smeared into the mold. After the glue cures, the new fake fingerprint is ready for use."

So Frank Rieger, spokesman for the CCC, who posted this, quoted himself, saying: "We hope that this finally puts to rest the illusions people have about fingerprint biometrics. It is plain stupid to use something that you cannot change and that you leave everywhere every day as a security token. The public should no longer be fooled by the biometrics industry with false security claims. Biometrics is fundamentally a technology designed for oppression and control, not for securing everyday device access." Interesting. Anyway, continuing...

TOM: I suppose he has a perspective.

**Steve:** Yeah. "Fingerprint biometrics in passports has been introduced in many countries despite the fact that by this global roll-out no security gain can be shown. iPhone users should avoid protecting sensitive data with their precious biometric fingerprint, not only because it can be easily faked, as demonstrated by the CCC team. Also, you can easily be forced to unlock your phone against your will when being arrested. Forcing you to give up your hopefully long passcode is much harder under most jurisdictions," that is, the difference between something you have and something you know, and we'll be talking about that here at the end, "than just casually swiping your phone over your handcuffed hands. Many thanks go to Heise Security team which provided the iPhone 5s for the hack quickly. More details on the hack will be reported here." So that's the statement from the people who say this is all dumb.

Now, Marc Rogers also defeated this, but he's a little more forthcoming about what it took. And he posted a blog posting titled "Why I Hacked Apple's Touch ID and Still Think It Is Awesome." So Marc wrote: "By now, the news is out Touch ID was hacked." And of course, again, I say "spoofed." This was a spoofing attack. We have the word. It's the right word. "In truth, none of us really expected otherwise. Fingerprint biometrics use a security credential that gets left behind everywhere you go, on everything you touch. The fact that fingerprints can be lifted is not really up for debate. CSI technicians have been doing it for decades. The big question with Touch ID was whether or not Apple could implement a design that would resist attacks using lifted fingerprints, or whether they would join the long line of manufacturers who had tried, but failed, to implement a completely secure solution.

"Does this mean Touch ID is flawed and that it should be avoided? The answer to that isn't as simple as you might think. Yes, Touch ID has flaws; and, yes, it's possible to exploit those flaws and unlock an iPhone. But the reality is these flaws are not something that the average consumer should worry about. Why? Because exploiting them was anything but trivial. Hacking Touch ID relies upon a combination of skills, existing academic research, and the patience of a crime scene technician. First, you have to obtain a suitable print. A suitable print needs to be unsmudged and be a complete print of the correct finger that unlocks a phone. If you use your thumb to unlock it, the way Apple designed it, then you are looking for the finger which is least likely to leave a decent print on the iPhone.

"Try it yourself," he writes. "Hold an iPhone in your hand and try the various positions that you would use the phone in. You will notice that the thumb doesn't often come into full contact with the phone; and, when it does, it's usually in motion. This means they tend to be smudged. So in order to hack your phone, a thief would have to work out which finger is correct and lift a good clean print of the correct finger.

"Next you have to" - and he has in quotes - "'lift' the print." Oh, and I've made a little editorial comment here. The Chaos Computer Club article rather glibly glosses over this next part because Marc writes: "This is the realm of CSI. You need to develop the print using one of several techniques involving the fumes from cyanoacrylate" - superglue,

commonly known - "and a suitable fingerprint powder before carefully and patiently lifting the print using fingerprint tape. This is not easy," says Marc, who has done it. "Even with a well-defined print, it is easy to smudge the result, and you only get one shot at this. Lifting the print destroys the original.

"So now what? If you got this far, the chances are you have a slightly smudged 2D print stuck on a white card. Can you use this to unlock the phone? This used to work on some of the older optical readers, but not for many years now" - because they've gone capacitive, and we'll talk about that in a second - "and certainly not with this device," meaning the iPhone 5s. "To crack this control you will need to create an actual fake 3D fingerprint" from this 2D image. Creating the fake fingerprint is arguably the hardest part and by no means easy. It is a lengthy process that takes several hours and uses over a thousand dollars' worth of equipment, including a high-resolution camera and laser printer. First of all, you have to photograph the print, remembering to preserve scale, maintain adequate resolution, and ensure you don't skew or distort the print." All very good points which CCC didn't mention.

"Next, you have to manually edit the print to clean up as much of the inevitable smudging as possible. Once complete, you have two options." He mentions the CCC method: "Invert the print in software, print it onto a transparency film using a laser printer set to maximum toner density, then smear glue and glycerol on the ink side of the print and leave it to cure. Once dried you have this thin layer of rubbery dried glue that serves as your real print." Okay. And but then he says that apparently he was the user of the more elaborate approach.

He says: "I used a technique demonstrated by Tsutomu Matsumoto in his 2002 paper, 'The Impact of Artificial "Gummy" Fingers on Fingerprint Systems.' In this technique, you take the cleaned fingerprint image and, without inverting it, print it to transparency film. Next, you take the transparency film and use it to expose some thick" - and he goes back through the whole PC board routine, exactly as the CCC guys posted in their update. So Marc winds up saying: "Using fake fingerprints is a little tricky. I got the best results by sticking it to a slightly damp finger. My supposition is that this tactic improves contact by evening-out any difference in electrical conductivity between this and the original finger.

"So what have we learned from all this? Practically, an attack is still a little bit in the realm," he says, "of a John le Carr novel. It is certainly not something your average street thief would be able to do; and, even then, they would have to get lucky. Don't forget, you only get five attempts before Touch ID rejects all fingerprints from then on, requiring a PIN to unlock it. However, let's be clear: Touch ID is unlikely to withstand a targeted attack. A dedicated attacker, with time and resources to observe his victim and collect the necessary data, is probably not going to see Touch ID as much of a challenge. Luckily, this isn't a threat that many of us face.

"Touch ID," he concludes, "is not a 'strong' security control. It is a 'convenient' security control. Today, just over 50% of users have a PIN on their smartphones at all. And the No. 1 reason people give for not using the PIN is that it's too inconvenient. Touch ID is strong enough to protect users from casual or opportunistic attackers, and it is substantially better than nothing."

So I liked that because I think that really puts this into context, which is what we need. I would argue that having something that is very good, but not perfect, then allows you to use a much stronger passcode because you need to use it much less. You don't need to use it every time you turn your phone on, every time you unlock it to get access to it. That's the annoying thing. You only need to use it in those instances where the phone feels, oh, it's time for me to make sure this is the same person. And that's infrequent

enough that you can afford that one to be much more burdensome. And that's going to be what most people who try to hack this and fail a couple times, or five times, and then it's game over, with all the other caveats.

So anyway, this is why I'm still a fan of this technology. I think in terms of real-world use, if this moves from 50% unlocked iPhones to 100% some lock, and frankly a very good lock in most cases, then this is a huge step forward for Apple.

TOM: I think a lot of people are getting caught up in the semantics of this; right? I mean, I actually think Marc Rogers is making it sound more complicated than it is. I think if someone really put their mind to it, they could probably do this. Not that any of us have cyanoacrylate just laying around the house. So it's a fair point that this is not easy. And I think the Chaos Computer Club tried to make it sound a lot easier than it was, too. But really to me that's not even the most important part, is this easy, is this hard. The most important part is the point you get to at the end, which is how often is it really going to be taken advantage of? How likely is it that some, like you say, like a casual thief is going to go to the trouble to do all of this? More likely they'd just make you unlock it before you hand it over to them. Right?

**Steve:** Well, precisely. Yes. And, I mean, one thing to remember, too, is that, if there's a weakness, it's that, I mean, anybody who really wants security will use a really long passcode. Period. I mean, that's what they will do. Or they'll use Touch ID until they start - until they do a border crossing, because now we're seeing stories about devices being confiscated at international border crossings. And it's like, okay, so you turn off your fingerprint, and you only use your super long passcode there. And then, once you regain control, you switch back. So it's worth planting in people's minds that it is subject to that because, at the border crossing, you can imagine a situation where some authority says, "Put your finger on your phone." And if you haven't turned it off, you could arguably be compelled to do that. Whereas something you know that's in your head is much more difficult for you to be compelled to disclose. And recent appellate court decisions have ruled that it's against the law to force, to compel someone to incriminate themselves under the Fifth Amendment of the Constitution.

TOM: Unless you're at the immigration checkpoint.

**Steve:** Yeah.

TOM: Yeah.

**Steve:** Yeah. So I guess I think this is good news. I think the key is for people to use it with an understanding of its limitations.

TOM: Exactly.

**Steve:** It's funny, as you were talking, I was thinking, the scenario that I could imagine, although I don't think it likely, is for some reason some whiz kid wants access to his parents' iPhone, which for some reason they don't give. Because he's a whiz kid, his parents are leaving fingerprints all over the place...

TOM: He's like, I know where the super glue is. I've got some cyanoacrylate.

**Steve:** And Dad left a nice perfect thumbprint on the whiskey glass last night. I'm going to dust that and lift it. I mean, maybe just for kicks to see if he can do it. But, I mean, I really do, I mean, for example, making sure that the photo is square on, that it is 1:1

scale, that's obviously critical. That it isn't - that there's no trapezoidal distortion in either way. I mean, I could see that it would take something to make this work. And because this is capacitive, because it actually senses the presence or absence of substance over the sensor, that's what that means, as we were talking about it before. It's actually, it's the 3D-ness of the ridges of your finger that this thing is sensing, in the same way that a stud finder is able to find a wood stud behind the wall. But what's happening is it puts out a capacitive feel, an electrostatic field, and the so-called dielectric constant changes, depending upon whether there's air or a solid there.

Similarly, when you put your finger on the sensor, there is air where you've got ravines in between the ridges, and this sensor is able to sense that it is a change in capacitance from that to where the skin is in contact, just like a stud finder that people have been using for decades.

TOM: In that Chaos Computer Club video, if I'm seeing it right, they just wrap the fake fingerprint around a real finger; right?

**Steve:** Yeah.

TOM: That's all they needed to do. You don't need to make a fake finger.

**Steve:** No.

TOM: Just wear it.

**Steve:** You just end up with like a little snakeskin sort of very thin thing. But it's got - and the whole idea of using toner was that toner is 3D. And you can feel, if you, like, rub your fingers on a Xerox copy that uses toner, you can feel that it is 3D. And so that's what they need was they needed to create, turn the image from a two-dimensional to a raised event. And so the whole concept of going to the PC board is there you have a printed circuit board, is a much thicker layer of copper than the toner is thick on paper. So they use the image to photo etch the copper away so you end up with raised copper, which is more raised than toner. Then you smudge the insulating material, the glue or latex, into that. And then when you peel that out, you've got an image of the fingerprint in relief, essentially, thanks to this little printed circuit board.

So, yeah, it can be defeated. But, boy, I think both locking it, five times to lock - and it'd be nice, frankly, if Apple turned that number down, or if that were user controllable.

TOM: If that were - yeah, exactly.

**Steve:** I'd set that to one. If it proves to be reliable enough, if you don't get it the first time, sorry, enter your passcode.

TOM: Yeah. And that way, if somebody says we're going to force you now, you're at the border, you don't have Fifth Amendment rights right now, put your finger on that, you put the wrong finger on it.

**Steve:** Yes.

TOM: Oh, sorry, I messed up. I thought it was my right hand, it's my left hand.

**Steve:** And, oh, my god, and you know, I haven't had to use my passcode for so long, I've forgotten it.

TOM: Can't remember what the passcode is, yeah. No, exactly. I think this is really important because people - and it's fun. I understand people are getting caught up into, like, well, how difficult is this, and could I do it myself, and is it possible that this is easier than, like, trying to attach some kind of bot to the phone and crack into the passcode. Those are all fair exercises. But in the end...

**Steve:** Why do people climb mountains?

TOM: Yeah, exactly.

**Steve:** Why do people climb mountains? Because it's there, and they want to look around from the top. And it's like, okay, here's a high-volume consumer fingerprint scanner. Let's find out what it takes to crack it.

TOM: And I'm glad they did.

**Steve:** I am, too.

TOM: Because now I know, okay, that's how much I could rely on that sensor. I'm not going to - and you know what, this informs my use of my phone, too. It also informs what I'm going to allow to be stored on that particular computer, and what connections it's going to make. Because you know it has that level of security.

**Steve:** Right.

TOM: So it's all good stuff. Well, Steve, thank you.

**Steve:** And if it's easy to turn it off, then you could do that intelligently. If you understand that your phone has valuable data, while it's really in your control, you get the convenience of using your thumb or whatever finger you choose. When it might have, for some reason, you have less control over it, then you could just turn that off and just fall back to your really long passcode.

TOM: You mentioned it earlier in the show. How much more secure is this than a house key?

**Steve:** Yes, exactly. I mean, that's the other thing we forget, is that a house key is actually not very secure. It exists in the physical world. Some guy has to be there at your door trying keys. But it's like a fun experiment is it's often the case that somebody else's, one of somebody else's many keys will unlock your front door because statistically there just aren't that many of them. So again, the idea is this probably has, well, Apple is claiming a one-in-50,000 false positive rate. So, and they actually get their statistics a little bit wrong because they believe that that means that after 50,000 tries you'll succeed once or something like that. I can't remember exactly what they said, but it's like, okay, that's not quite the way statistics works, Apple. But still, the idea being it's very unlikely that a stranger's fingerprint is going to also unlock your phone. And that does the job.

Just like it's very unlikely that a specific person's key is going to unlock the front door. But you get enough people together, and the chances are that someone's key will. And actually, you also have the problem with the birthday attack. If you've got a bunch of people together, the chances are very good that someone, any pair of someone's front door and someone's keys could be unlocked. Similarly, if you got a whole bunch of

people together with their phones, and everybody tried everybody's phone, then the birthday attack statistics come into play, and it becomes, again, much more likely. But those are all sort of synthesis exercises. I just think it's - I can't wait to get mine and to play with it. I think it's going to be a lot of fun.

TOM: Well, thank you, Steve. As always, fantastic show, and a good explanation. I'm really looking forward to next week. And I hope you're able to pull that together for next week because I'm looking forward to hearing about this new authentication scheme. Doesn't involve fingers, does it.

**Steve:** No. No fingers.

TOM: Okay. I'll keep my fingers to myself. You can find Steve's work at GRC.com. You have a fingerprinting service, totally different kind of fingerprinting service, that I noticed at the top of the show, allows you to detect when your secure connections are being intercepted and monitored. But go check out...

**Steve:** I did that all pre-NSA. But there's been a surge of interest in it because of course suddenly people actually realize, oh, maybe there is some pressure being put on connections to be intercepted. So I've noticed a resurgence of interest in that.

TOM: SpinRite, of course, all kinds of great things. And you can find all of our show notes and things like that at TWiT.tv/sn. Anything to tell folks about before we head out of here?

**Steve:** I think everybody knows that I keep the low-bandwidth versions of these, as Leo describes it, for the bandwidth-impaired. Elaine likes to use it because she's got a satellite link to wherever she is out in the boonies somewhere, and so it preserves her bandwidth. And of course she famously does transcripts for all the podcasts, which we have at GRC.com/securitynow.

TOM: Check them out. Thanks, everybody. Oh, yeah, go ahead.

**Steve:** I was just going to say that I'm really sure we're going to do, I mean, I'm as sure as I could be that I'll be ready next week. I'm going to show it to some close friends and to have other eyes on it and to get some scrutiny. Maybe, I mean, there's always a possibility that someone will see something that I just could not see because I was its own parent. So I may announce that it's busted already. I hope not. We could do a Q&A, in which case you submit questions to GRC.com/feedback.

TOM: Excellent. Thanks, everybody. And you'll tune in next week to find out. We'll see you then.