NFC - Near Field Communications

Description: After catching up with just a tiny bit of security news (it was a very quiet week in security), Steve and Leo take the podcast's first-ever comprehensive look at the emerging and increasingly popular NFC (Near Field Communications) technology, which is now present in tens of millions of cell phones and other mobile and fixed-location devices.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-372.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-372-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, the Explainer in Chief, and he's going to talk about NFC chips. They're in many new smartphones, but not Apple's iPhone. What is it? How does it work, and what are the security implications? Near Field Communications, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 372, recorded October 3rd, 2012: Near Field Communication.

It's time for Security Now!, the show that protects you and your loved ones online with our man, Steve Gibson, our Man on the 'Net, Steve Explainer in Chief and guy at GRC.com who gives us so much great stuff. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always.

Leo: Good to see you. We've been talking before the show about sci-fi, our favorite topic. And coffee.

Steve: Yup. Movies, debates, politics.

Leo: Politics. It's like, this is all our favorite stuff: red wine, politics, coffee, and movies. Sci-fi.

Steve: Yeah, there you go.

Leo: There you go. That's all you need in life. And then you throw in a little Security Now!, and you're set.

Steve: You've got the day covered.

Leo: So last week you said you might talk about NFC today. Is that our topic?

Steve: Yes, that is our topic. I have been reading about it since then. Actually I'd started a little bit before then, also. I've completely satisfied all of my curiosity. I know everything I need to know about it for now. And by the end of this podcast I imagine that all of our listeners will feel the same.

So it's interesting. We'll set it relative to the other sort of environmentally competing technologies. There's of course WiFi, Bluetooth, RFID, even IRDA, kind of. And here's NFC. So how does that fit into this spectrum of connections and communications between our devices? What are its problems? What are its promises? I mean, I have to say, now that I have really come up to speed and get a good sense for where we are at this moment, I appreciate more than I did a week ago how odd it is that it wasn't part of iPhone 5.

Leo: Oh, interesting.

Steve: Because, I mean, the industry, the rest of the cellular phone industry has left Apple behind in NFC. I mean, virtually all the other phones have near field communications. And this makes the iPhone conspicuous in not having it. Now, it's true that we're at the early stage of the adoption curve. And people have various theories about why Apple chose not to do this, like that it's hard to do radio in a metal case, except, well, the phone is a radio, so I don't buy that. I also read someone saying, well, Apple doesn't want to be the leader in this. They would rather wait till things settle down and not be a first mover. It's like, well, okay, maybe. I just don't really get it. But at the end of this podcast we will all know what it is and sort of have that whole question mark resolved for the time being. And from then on we'll just be tracking the mistakes that everyone makes in implementation.

And in fact I'm going to kick off with that because our old friend Charlie Miller, who we know as the great Pwn2Own multiple-time winner, and he wrote the "Hacking Mac OS X" book, he gave a presentation on hacking near field communications at this most recent Black Hat 2012 Conference a few months back. So, oh, and I just tweeted, by the way, for anyone who's interested, I just tweeted a link to his presentation's PDF. So for anyone who wants to delve deeper than I'm going to, that's a great place to look at hacking near field from that end. And we have very little news, a little bit of news which I'll wait until we get started.

Leo: All right. And then NFC, the subject of the day.

Steve: Yes, exactly.

Leo: And I will be interested in the security issues because if, well, if we're going to start using it for payment, that's going to be big issue.

Steve: Yes, baby.

Leo: All right. Let's do the news before we get to NFC.

Steve: Well, there wasn't much that happened. As we know, some weeks are so busy we don't have a chance to talk about anything else. And every so often we run across a week where almost nothing happened, which is, I guess, from a security standpoint probably a good thing. We talked last week about the expectation that the NIST, the National Institute for, now I've forgotten...

Leo: Standards of Time?

Steve: Standards of Technology? Anyway, NIST...

Leo: I'm sure the chatroom will tell us momentarily. The National Institute of Standards and Technology.

Steve: That's right. That they were on the verge of choosing the hash from among the final winnowed-down contenders. And they did that yesterday, on October 2. They did not choose Bruce Schneier's Skein.

Leo: Aw.

Steve: As I was sort of just hoping they would because I know and like Bruce. However, they did choose one that was co-designed by someone we know of because he was also the co-designer of Rijndael, which was chosen to be the next-generation AES, the Advanced Encryption Standard cipher. Now, we're not sure how to pronounce this. It's...

Leo: Keccak.

Steve: First of all, you could just say SHA-3, SHA-3, which is like saying AES instead of trying to remember how to spell Rijndael, which actually I have a macro now in my brain which spells it for me when I put my hands on the keyboard. But K-E-C-C-A-K.

Leo: The press release says it's "ketch ack," or "catch ack."

Steve: And that's what I've seen is catch, C-A-T-C-H, phonetically, again, C-A-T-C-H and then A-C-K, catch ack, which looks good enough to me. Anyway, so a team of

cryptographers chose this. It is very, very fast. In their work they're getting a byte of hash for every 12.5 cycles on an Intel Core 2 CPU. But it also is very friendly to hardware implementations which are able to run it even faster. And I have not looked at it deeply yet. I think that I probably will because we've talked about other hashes, and this is going to be at some point adopted. But as we said last week, there doesn't seem to be any hurry towards it because this was started, what, eight years ago in '04, when we believed that AES-2 might have some long-term problems. So the NIST decided to be ahead of the game this time and have a replacement hash ready. And it turns out SHA-2, the SHA-2 family of hashes, like SHA-512, for example, that we were talking about last week, is still holding up very well and seems plenty strong.

Anyway, Wikipedia wrote, "Keccak uses the sponge construction in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted. In its largest instance, the state consists of a 5x5 array of 64-bit words, so 1600 bits total. Reduced versions of the algorithm are defined for smaller power-of-two word sizes 'w' down to one bit," which would give us 26 bits of total state since we have a 5x5 array of bit sizes. So 5x5 obviously is 25, and we had a one-bit thing. That'd be kind of cool to have a one-bit hash. I've got to look at that. Anyway, "While smaller state sizes can be used to test" - of course I guess it wouldn't be hard to guess which the hash was. Anyway, "While smaller state sizes can be used to test cryptanalytic attacks, intermediate state sizes" - for example, a word size of 4 with 100 bits of state, or a word size of 32 with 800 bits - "also provide practical, lightweight, alternatives."

So what all that means is that we have a new hashing standard whose word size is dynamically variable. And what excites people about this is that it is extremely different from the existing SHA-2 family. So cryptographers like that because they explain, if it turns out that the SHA-2 family do develop some sort of problems, or, that is, we learn something about them that we don't now know that weakens them, this Keccak, which has now been awarded SHA-3 status, it's so different that any problems SHA-2 has, SHA-3 absolutely will not have.

So anyway, that's our news for the week. We now have a next-generation hash standard. The feeling is there's no big hurry to implement it. I'm sure people will do hardware implementations. There will be referenced software implementations in all the various languages, so you could choose whatever you like. And perhaps because it is faster than SHA-2, if there's some reason, for example, in a closed system, where you're the only one who is using the SHA-3 results, you might just go ahead and choose to use it, where its speed or its scalability are of use to you. Whereas, for example, the existing SHA-2 family have the advantage of already existing universal adoption. And so, for example, you could send somebody a file and say the SHA-512 hash of this is the following, and they're able to reproduce that, and you know that they're able to do that. Whereas right now we have zero adoption level of the successor. But we have chosen it. So that's cool.

Leo: You know, I thought the other thing I found interesting in their description of this, they said it seems unlikely, the difference in design and implementation from SHA-2 means that it seems unlikely that any attack that attacks SHA-2 would then be useful attacking SHA-3. So they intentionally chose something that deviates sufficiently from SHA-2 that one attack couldn't theoretically attack both. Somebody would have to come up with two different ways of attacking. Which is clever.

Steve: And when we discuss it, as I imagine we will at some point, it will doubtless seem like serious propellerhead-level technology. But to the cryptographers, what they really like about it is that it's extremely simple. That is, they think of it as extremely

cryptanalyzable. So it's not like it's some random bizarre mess that might have unexpected behavior which isn't obvious on its surface. Instead, it is an extremely transparent clear construction, which makes the cryptographers very comfortable that they can see what it's doing. They understand how it works and why. And they're able then to represent that it looks like it's going to be very secure. So anyway, we have our next-generation hash. We don't need it. But we do have it.

Leo: Yay.

Steve: And nothing came onto my radar in the security space besides that this week. I'm sure I could have dug around and found some things, but there wasn't anything that seemed very important. So that's all I have on that side.

Leo: You know what, it's okay. Doesn't have to have an hour's worth of tech news every week.

Steve: In keeping with that spirit, I thought I would, I mean, I know all of our listeners know about SpinRite and how it operates and what it does. So I thought I would just share a nice tweet that I saw come through my feed. Someone whose handle is @TALK_HARD tweeted: "My main HD crashed in the middle of the night! Thank God for SpinRite and @SGgrc!!! Recovered the entire 1.5TB drive OS and all!" So thanks for sharing that, @TALK_HARD.

Leo: All right. Now let's talk about - I'm putting my box away. Let's talk about near field communications.

Steve: Okay. So probably the best way to introduce this is to summarize a bit of the dark side. I mentioned Charlie Miller at the top of the show. The title of his talk, which he gave at the recent Black Hat 2012 Conference a few months back was "Don't Stand So Close to Me."

Leo: [Laughing] I don't think this is what Sting was thinking about when he sang that song, but all right.

Steve: No. "An Analysis of the NFC Attack Surface." And I should preface this by saying, what Charlie looked at, to his credit, is the current state of implementation. So I'm largely going to talk about the technology of NFC because that's where we are today. But there's nothing fundamentally insecure about NFC. As we have seen so many times, it's the way it was implemented which is the problem. Now, having said that, there's, as our listeners know, there's a fundamental tension, I guess maybe is the best way to put it, any time you have radio because you have variations in distance. We've got famous uses of Pringles potato chip cans to create focused-beam WiFi that allows much greater ranges than people were anticipating. So the idea of something wireless immediately creates some tension which we need to do the right thing with.

But so in the preview before his talk, Charlie put together a couple paragraphs to sort of tease his presentation. He said: "Near Field Communication (NFC) has been used in

mobile devices in some countries for a while and is now emerging on devices in use in the United States. This technology allows NFC-enabled devices to communicate with each other within close range, typically a few centimeters. It is being rolled out as a way to make payments, by using the mobile device to communicate credit card information to an NFC-enabled terminal. It is a new, cool, technology. But, as with the introduction of any new technology, the question must be asked what kind of impact the inclusion of this new [functionality] has on the attack surface of mobile devices. In this paper, we explore this question by introducing NFC and its associated protocols.

"Next, we describe how to fuzz the NFC protocol stack for two devices, as well as our results. Then we see, for these devices, what software is built on top of the NFC stack. It turns out that, through NFC, using technologies like Android Beam or NDEF content sharing" - which I'll define and explain later - "one can make some phones parse images, videos, contacts, Office documents, even open up web pages in the browser, all without user interaction. In some cases, it is even possible to completely take over control of the phone via NFC ... stealing photos, contacts, even sending text messages and making phone calls. So next time you present your phone to pay for your cab, be aware you might have just gotten owned." So that was the introduction.

Leo: That's depressing. I had higher hopes for this.

Steve: [Laughing] It really is.

Leo: Wasn't that the idea, though, that this is an RFID with a near field, a very limited range?

Steve: Yes. So that is exactly what it is. Probably the way to characterize this best is to think of this as almost contact where you're using radio to replace actual connections. Probably many of us have seen traditional smart cards where on the backside of the card, or sometimes on the front, there's a little sort of a pad of gold contacts. And so you slide your card into a reader, and it comes into contact with those contacts on the card.

Well, contacts are problematical. In engineering terms, they're actually expensive. It's one of the reasons, for example, that we're seeing a movement towards serial devices rather than parallel devices. Original hard drives were the so-called "parallel ATA," the PATA. New drives are "serial ATA," SATA, because even though parallel would allow you to move more data across channels in parallel, it turns out that our technology's gotten so fast that interconnection ends up being a greater problem than speed. And even the PCI bus is a serial bus rather than a largely parallel bus, as the original PC buses were.

So this is a step sort of one step further, to remove the electrical contacts from the interface and just do it over radio. And exactly as you said, Leo, RFID was the precursor technology for this kind of application space. Yet NFC is deliberately designed for much shorter range. When I drive through the toll road transponder, I've got the little transponder in my window. That's an RFID transponder that is being read at a distance of, what, maybe two or three meters from my car windshield. And many people are familiar with those toll road-style transponders.

The range for near field is on the order of an inch, 2.54 centimeters. So that's, like, 2.5 centimeters is one inch. And even in Charlie's paper he talks about having experimented with this. And in the real world the maximum range is, he says, two to three centimeters,

so that's right in this, like, one-inch region. The term "near field" comes from the original expression of the way electromagnetic radiation radiates. The traditional radio that we're used to operates in what's called the "far field." This was all laid out back in the mid-1800s, in the 1860s, by a Scottish physicist and mathematician named James Maxwell, the so-called "Maxwell's Equations," which are really - they're hairy partial differential equations which describe how electromagnetic propagation works.

It turns out that there are different properties of propagation which apply when you are within only a few wave lengths of the radiating surface, the antenna, as opposed to when you are many, many wave lengths away. One way to think of it is that, if you're really far away from an antenna, even though that antenna has a physical size, it looks more like a theoretical point source to you, so that the wave fronts are coming more in a coherent fashion. But when you're very close, then you're able to sort of feel the physical distribution over the span of the antenna.

So there's a very different set of properties between near field and far field. And this involves a complex interaction between electrostatic fields involving charges and electromagnetic fields involving a magnetic field. So to sort of place this on the spectrum of things, near field operates at a relatively low frequency. It's right in the middle of the shortwave band. You'll remember from your licensing, Leo, that short wave is between about 3 and 30 MHz.

And the near field spec - and all of this has been ratified and unified. There's an NFC forum that maintains the specifications. There's about 160 companies that are now members and signed on to support NFC-compatible stuff, whether it's phones or passive tags, NFC tags or whatever. But there's a good set of unifying standards to keep everybody talking on the same, literally on the same frequency, but also with compatible protocols. So NFC is just about right in the middle of the short wave band, which runs between 3 and 30 MHz. It's at 13.56 MHz. By comparison, for example, Bluetooth is around 2400 MHz, which also is 2.4 GHz. WiFi is around the same place as Bluetooth and also at double that, at about 5 GHz.

So of course WiFi was designed to replace LAN wiring. Bluetooth was designed to replace cell phone cables. And similarly, NFC was designed to replace sort of the existing contact smartcards. So the technology involves a coil antenna, some sort of printed coil, and typically one chip over on the tag side. You can have, in the way near field functions, there's normally a master and a slave, the master being the controlling party in this two-party communication. Near field is always a 1:1 pairing, that is, a 1:1 relationship. There's nothing, for example, like a LAN where you have multiple devices all communicating at once, nor even in Bluetooth where you have the so-called PAN, the Personal Area Network.

In near field, again, the way to think about this is they tried to design it so that it was very much like having a smartcard with contacts, but we removed the contacts. So everything about this is designed to be in physical proximity, but not an electrical connection. Instead, it's a short distance radiation connection. So, for example, they have this notion of a - they call them in the forum, and formally defined in the spec, they call it a "Smart Poster," where at some point in the future there may be a poster hanging up on a wall, and there will be the sort of the near field logo, which people over time will get to recognize, sort of a stylized "N" that looks a little bit like a lightning bolt. And that will be your cue that underneath that "N" on the poster is an NFC transponder.

So it has no batteries. It just sits there waiting to receive power from someone's cell phone, typically. So you would essentially touch your cell phone to the poster. You don't actually have to physically touch it, but it's just sort of easier because you've got to get

about that close to it. And the field, the radiated field from the cell phone's near field master, essentially powers up the chip in the transponder. And so this 13.56 MHz frequency provides power to the chip. The chip then modulates the power in its coil to essentially put a load on the transmitter.

So the transmitter can sense that it's being loaded down because its magnetic field has coupled with the magnetic field of the transponder in the poster. And by altering the load that the transponder puts on its own coil, the transmitter is able to sense that, and they're able to communicate. Communication can be bidirectional, and it can be simultaneous, and there is in the specification a means for dealing with collision. So if, for example, there was - I don't know, I mean, collision is not something you would encounter often because the distance of this whole system's operating is so sort. But they do have collision avoidance approaches in cases where you had two transponders too close to each other.

So the first mode of operation is that, where you have an energizer and a passive source of information, essentially. And, when energized, the passive source of information gives up what it's got, whatever it might be. And, for example, in the case of a poster, in the so-called "NFC poster spec," you receive a little burst of information which actually moves at a pretty good rate. With a 13.56 MHz carrier, the information is set at 1/128th of that, which of course we know is 2^7, so that's a nice power of two. Which means that the tag is able to clock its data slaved off of the receiving signal. So it's sort of a self-clocking format, which is good for making these tags passive and non-battery powered and very inexpensive.

But, for example, when it's energized, the tag actually comes up and is in an idle state. And then there's a command-response protocol which has been defined. So this is all much more sophisticated, again, sort of next generation from what we have from the early RFID tags, which are much simpler and simply send back a static fixed serial number to identify themselves. Here the tags are able to be field programmed. You can actually buy paper rolls of these things that are sticky on one side that have, for example, in one case, 144 bytes of nonvolatile memory which can be selectively made read-only so that you can put data into this through the field and then set write-only bits on all or a portion of this data. And then, through a series of commands, you're able to later query the tag for its contents, but have no permission to modify it. So there's that first mode.

Then there's also the mode where you have a device pretending to be a tag, that is, it might be an active device which is not actually a passive tag, but it's pretending to be one. So the interaction is exactly the same as in the case where it actually was a passive tag. And then in the third instance you actually have a peer-to-peer relationship where both devices are actively generating their own local near RF field, and then they come into physical proximity with each other and are able to initiative a handshake and exchange data.

So what do we do with this? Well, for one thing, we have, for example, this Smart Poster notion, which is one of the predefined specifications, where a burst of data might contain a title and a URI, that is, a URL-style universal resource string, which we're used to from Internet URLs, containing a reference to a web page, or an image on the 'Net, or some other sort of addresses accessible to the device that is receiving the information. In this poster format they talk about a so-called "action record," where the device you are pinging, querying, suggests what action should be taken given the URI that it has sent you, and there's an icon record so that it might also present on the screen some sort of information that the user would be given and take advantage of in order to sort of define what it's doing.

So that's sort of the whole scope of what near field is. It is short physical proximity, on the order of an inch. There have been some experiments where they have beamed power at a tag that was further away and had the tag modulate their beamed field and receive it. So we have some of the problems that we've got with any time you remove electrical contact and switch to radio, you're making some assumptions about the radiated power of the thing that is powering the device and your ability to sense its loading down of your field. So distance is somewhat fuzzy. But itself, the near field spec just says this is the frequency we operate at, here's the protocol for the way these devices communicate, and on top of that people can put whatever they want.

So one of the other application areas, aside from the so-called Smart Poster, is this notion of using a near field communication to bootstrap into a more potent communication. For example, we've talked about the problems of establishing a passphrase on a WiFi hotspot. If you've got a very complex, crazy passphrase, it can be difficult to enter that into another device. If instead your WiFi router came with a near field-capable radio as part of it, then you could, for example, get your cell phone onto that WiFi router just by tapping the cell phone against the router. And so the idea would be that, in that application, they would exchange the information over a bandwidth-constrained, because I don't know if I mentioned that it's about 106Kb per second, so it is dramatically slower than WiFi or Bluetooth. But the idea is, I mean, that's all the speed you would need for a Smart Poster to send you a URL or to perform some simple credit transaction with a near field terminal.

But the idea would be, in the mode where you have a WiFi hotspot, you would tap two devices together. They would exchange information about the other much more capable protocols, which then come into service as you pull the devices apart. And that's one of the frequently mentioned applications for this is - in fact that's the way the Android Beam functions is, that you've got two Android phones which don't yet know about each other. You tap them together. They use NFC to handshake and agree upon crypto-level data which they then use to encrypt and exchange files over their WiFi connection because they've got a much more capable WiFi radio, capable of much higher bandwidth and much greater operating range. But you want that to also be secure. So by briefly bringing them together, you essentially synchronize them, and then you pull them apart and establish the communication that way. So it's a cool technology, Leo.

Leo: You know, the thing about Apple not adopting it, the only reason I was hoping they would adopt it is because it would obviously jumpstart it; right?

Steve: Yes, yes.

Leo: But I think that it is new, and nobody's using it yet. So, I mean, very few. Peet's uses it, a few places like that, Peet's Coffee here in San Francisco.

Steve: Yeah, and as I mentioned, I have it in my BlackBerry phone, which I've had for about a year and a half.

Leo: That's interesting.

Steve: It's like, okay. It's nice that it's there. I have it turned off. And that's one of the

other things that Charlie's takeaway from his presentation was - so what Charlie found was not surprising. It's very much like the exact same domain of problems that we've seen over and over, which is that sometimes the people who are implementing this don't get all the details right. There's nothing fundamentally secure or insecure about near field communication. It's just a short-range means of exchanging relatively low bandwidth, that is, 106Kb per second, data between two devices, one of which may be completely passive and have none of its own local power source. Yet you can still write to it in an EEPROM sort of fashion and read back from it.

But what happened was some of the early implementations, for example, didn't require any user interaction. And that's his main takeaway is, yes, it's less convenient if you have to acknowledge a near field event, but so much more secure if the user is required to accept, to look first at what is about to be done and then say, okay, yeah, that looks like something I want to do. And some of these early implementations for the sake of, oh, how sexy it is that you just bump it up against a poster or you tap two devices together and this all sort of happens by magic, with no user intervention required, as we well know, the flipside of that is going to be problems with security.

Leo: So would you - well, I mean, I don't know. So you would use it if it were widely available, or...

Steve: So I would have it off. I would have the radio off all the time. This parallels our recommendation for Bluetooth. You'll remember, Leo, that time I came up to do a show with you in Vancouver, and it was on the whole Bluetooth security and pairing, and I had an application I brought with me that showed us all the Bluetooth radios within range, and virtually everyone in the studio had their Bluetooth enabled on their phones.

And this was at a time when Bluetooth was still not really solid. I mean, it's gotten a lot more secure, mostly because focus has been put on the security aspect. But there were ways early on that Bluetooth could be used to suck people's address books and contact lists and calendars and things out of their phones. So back then the advice was, if you don't know you're needing it, turn it off. Keep it off all the time because, well, and if nothing else, you're saving power because power is a scarce resource on a phone. So keep your Bluetooth off unless you're using it.

Now, of course, where we've got, for example, a law in California forbidding people from using their hold-it-in-your-hand handsets, there has been a huge jump up in Bluetooth being used to communicate with the little in-ear headsets. And so I imagine it's on a lot more often. What you definitely want to do is turn off pairing so that it's not sitting there broadcasting itself and trying to hook up with every Bluetooth radio in the area. But I would say the same advice applies for near field. On my BlackBerry I've got it...

Leo: But it's a lot shorter range; right?

Steve: Yeah. Oh, I mean, it is. It's one inch. It is going to be absolutely difficult...

Leo: Yeah, the attack surface, there's no magic that you could get to it from across the room, or is there?

Steve: Well, that's the problem with radio is there's nothing - it doesn't absolutely drop off. It sort of fades out. And it fades out very quickly. But we've seen situations where somebody with a focused antenna can beam power over a much larger distance and establish a radio link where it wasn't expected, where the assumption was that you're okay. I remember you and I talking about Bluetooth; and, like, there was a window of opportunity during Bluetooth pairing where an eavesdropper had some advantage. And you and I on this podcast years ago talked about going out into the middle of a parking lot where you could see all around you...

Leo: I could find my car.

Steve: ...that nobody was within 10 meters, or 30 feet, which is the nominal range of Bluetooth in order to do your pairing, so that you didn't have to worry, just during that brief moment, anybody being able to eavesdrop on you. So this is a lot better. I think there's no question this is going to take hold. This is going to get traction. People are going to like it. Again, people like convenience. And so the convenience factor is going to drive this forward. It creeps me out just because I - and I'm sure it does some of our listeners because we've seen over and over and over how many ways there are for these things to go wrong and that, when faced with a choice between security and convenience, initially the industry chooses convenience. And it's only after it gets burned a few times it backs off and says, oh, okay, I guess maybe have to ask before we do that.

Leo: So maybe Apple's wise to wait.

Steve: I just - I'd like to have it in the phone. Leave it off. Turn it off by default. But have it there so that, I mean, it just seems like a bullet point missing. I don't know when they are going to do iPhone 6. Maybe that's already in the works, so they've got it coming soon. But, boy, I think it's 40 million devices now have near field.

Leo: Wow.

Steve: And all of the new smartphones do except coming from Apple.

Leo: Yeah, certainly my Sun Galaxy S3, the Galaxy Nexus have NFC. I'm surprised your BlackBerry does.

Steve: Yeah. I wonder if - do you know if the Nexus 7 does? I don't remember seeing it. I don't think it does.

Leo: I don't think so. That's interesting because that's a tablet, not a phone.

Steve: Right. But still, I mean, I think...

Leo: HTC does not apparently put it in their One X. The new Lumia 920 will, I know, for the Windows Phone folks. So I don't know, I mean, that's a big number, but I think that it's certainly far from universal. Nexus 7 does, according to Didao [ph] in our chatroom.

Steve: There are some beginnings of security protocols. One of the things that I encountered when I was looking at this is that RFID had absolutely no provision for encryption, but NFC does. So we're not seeing it deployed yet. But, for example, I can imagine a scenario where future laptops will have an NFC logo on their, like, front surface down by the touchpad, in front of the keyboard, and you might authenticate by bringing your phone to your laptop briefly.

Leo: Oh, yeah, wouldn't that be neat.

Steve: Which is not a difficult, exactly, not a difficult thing to do. And so we begin to get aspects of multifactor authentication that way, too. I mean, I think we're going to be seeing more of near field in the future. I'm sure this is not the last podcast we'll be discussing it. Unfortunately, any future podcasts will be probably talking about what went wrong rather than how it works.

Leo: Right. NFC, the horror, the horror. That'll be some future date. Episode 472, perhaps. Considerate's saying in the chatroom that according to Wikipedia the distance record for detecting Bluetooth is 1.78 kilometers. So for a 30-foot, nominally 30-foot. So you make the point exactly. That's, you know. Of course it has to do inductance, which is more difficult than just a radio.

Steve: Yes, that is true. Because it is near field, the field falls off very quickly.

Leo: But so does RFID; right? RFID is an inductance-based system. And that works great, you know, you go through a toll booth, that's...

Steve: I think it was 10 centimeters was the number I saw in the forum for, like, their maximum theoretical range. And so, what's that, about...

Leo: It's not far.

Steve: ...4.5 inches or so?

Leo: 2.54 centimeters to the inch.

Steve: Yeah.

Leo: So whatever.

Steve: Oh, yeah. So 20 - wait. Yeah, so I don't know.

Leo: Divide by two.

Steve: Four or five inches.

Leo: By the way, correction, apparently the HTC One X does have NFC. Somebody has one in the chatroom, says no, no, mine has it.

Steve: I really do think it's on its way.

Leo: Majority of new smartphones, yeah.

Steve: Yeah, I think Apple's decision not to include it, I don't understand it in the iPhone 5. But this is going to be - I think this technology is going to take hold. And we're going to see it used a lot. I'm not so sure I'm a fan of bumping it up against random posters because that just seems...

Leo: We have an NFC chip on the wall as you come into the Brick House. We have a guest tile, and you tap it, and it'll check you in on Foursquare. It doesn't, by the way, doesn't do the check-in all the way. It just launches Foursquare, says you're here, and then says would you like to check in.

Steve: Nice.

Leo: Yeah. And I think that's probably how most people will implement it. That's using Samsung's built-in software on the phone.

Steve: Yeah. One thing we've not talked about yet is QR codes. That's also on my list of things to - of, like, technology to...

Leo: That's kind of the competing the technology for this.

Steve: Yeah. And of course that's optical as opposed to radio. And to me that seems a lot - actually I'm seeing QR codes all over the place now. They're beginning to get some traction.

Leo: I saw a gravestone with one.

Steve: [Laughing]

Leo: I kid you not.

Steve: You are here.

Leo: Yeah. I don't know, maybe it pulls up a page with his life story. I don't know. I didn't take a picture of it. I should have.

Steve: No kidding. Was it etched or...

Leo: Yeah.

Steve: Wow. Well, there's a geek.

Leo: Well, and it's also somebody who has a lot of faith in the technology. Like 50 years from now are people going to be able to read QR codes?

Steve: On my headstone. Yeah, that's a very good point, Leo, yeah.

Leo: Steve Gibson is the Explainer in Chief. There's actually a Tumblog, "WTF QR Codes." Thanks to Jesse in our chatroom for this. Like, why is there a QR code here? And there's lots - so it's cute. It's like - let me see if - so people are putting them everywhere. Here's one, fish on a grate.

Steve: I guess that's one of the cool aspects of the QR code is, because it is optical, it's even lower technology than a passive near field tag. And all phones now have cameras.

Leo: Just need camera software, yeah.

Steve: Even the iPhone 5.

Leo: Yeah. Yeah.

Steve: It is a neat technology. I'll just remind our listeners that I just tweeted the link to Charlie Miller's presentation, which I think is 40-some pages and lots of neat pictures and diagrams and technology. He spends much less time on how it works that I just have and

much more time on what he did to break it, which is, I guess, I mean, it's certainly of interest to our listeners and the topic of the podcast. But I just sort of shrug a little bit. It's like, yeah, well, it's not NFC's fault. It's that the people who did it made some mistakes and, more importantly, never put in a confirmation. Do you want to do this?

Leo: Right.

Steve: And I think that's just crazy.

Leo: But that's implementation specific. You could, I mean, for instance, you use Google Wallet, it will give you a PIN. So that's something the app should do. But again, well, maybe - no, because if you don't do it in the app, if you don't require it, then you could hack it silently.

Steve: Right.

Leo: Yeah. Steve Gibson's the Explainer in Chief at GRC.com. That's where you'll find him. His Twitter handle is @SGgrc. When you go to GRC.com, pick up a copy of SpinRite. You never know when you might need it. It's the world's best hard drive and maintenance and recovery utility. And, you know, it's Steve's bread and butter. So, yes, let's everybody buy it. But there is a lot of free stuff there, including 16Kb audio versions of this show for the bandwidth-impaired and full transcriptions, which Steve pays for, at the Security Now! pages there. And of course his show notes. We also have show notes on our wiki, thanks to some guy whose name we can never remember, but I will find it out for next week. We also have full quality audio and video versions available on the TWiT page, TWiT.tv/sn.

Steve: I'd also remind people that a side effect of Elaine's fantastic transcripts is the entire textual content of all 371, soon to be 372, podcasts are searchable. And when I encountered Charlie Miller's name in the Black Hat Conference, I thought, Charlie Miller, I'm sure we've talked about him. So I went over to GRC.com/sn.

Leo: See? Yeah, search right through it.

Steve: And in the search field I put "Charlie Miller," and bang, there was a complete chronology of all of our discussions of Charlie. So I was able to remind myself exactly what it was that Charlie had done in the past and why he was so familiar to us and our listeners. So it's very handy. If something comes up that you sort of think you remember hearing about, you can just go over and quickly find the references to it. It's really handy.

Leo: I love the Internet. Speaking of which, I found an ABC article that says "Digital QR codes offer interactive cemetery experience. Funeral directors are seeing an increase in demand for gravestone bar codes."

Steve: No kidding.

Leo: That is just...

Steve: Wow. That's...

Leo: ...crazy. Crazy. We do this show every Wednesday, 11:00 a.m. Pacific, that's 2:00 p.m. Eastern time, 1800 UTC, on TWiT.tv. Tune in live. We can interact through the chatroom. And as you can see, I use the chatroom a lot to flesh out the show, so to speak.

Steve: Yes, and GRC.com/feedback. We'll have a Q&A episode next week. Let me know what's on your mind, what you're curious about, any questions that the NFC technology brought to mind, and we'll talk about them next week.

Leo: Thank you, Steve.

Steve: Thanks, Leo.

Leo: See you next time on Security Now!.