Cryptographic Backdoors

Description: Following this slow week of security news, Leo and I first discuss the news surrounding how and why the U.S. was so sure that North Korea was behind the attack on Sony. Then we examine the cryptographic consequences of the British and U.S. governments' recent pronouncements that terrorist communications should not be allowed to remain secret.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-491.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-491-lq.mp3

SHOW TEASE: It's time for Security Now!. Leo Laporte and Steve Gibson. Coming up we've got a little bit of security news, and then Steve is going to do something quite surprising. He's going to go against his better political interests and judgment and actually explain why a cryptographic backdoor isn't necessarily a bad idea. You know what? He's right. Stay tuned. Steve Gibson and Security Now! up next.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 491, recorded January 20, 2015: Cryptographic Backdoors.

It's time for Security Now!, the show that protects you, your loved ones, and your privacy, and your security. And here he is, the Explainer in Chief. We're going to call you the Security Czar here at TWiT, Steve Gibson.

Steve Gibson: Oh, lord. Okay. I'll accept the title. The Czar.

Leo: You know, I was watching - it's amazing. Here we are, almost 18 months since the original Snowden leaks, and there are more every day.

Steve: That's the top of our news is - we didn't have much happen in this last week. It was relatively quiet. But what few things we did were big. I should explain to our listeners that I've delayed the Q&A that I had planned because for the last week I've been listening to all of the popular press, well meaning though they are, not being cryptographers, going nuts about the concept of the government mandating backdoors and how it weakens security. So that's the topic for today is cryptographic backdoors in the context of Cameron's and then of course our U.S. President Barack Obama's echoing

of this sort of vaguely stated intent.

But what I want to do is I want to get correct about the technology because that's what we do here. And everybody's got that wrong. It does not weaken anything to give the government access. That is, it doesn't have to. It shouldn't. And so what I want to do is I want to separate out the question of policy, which is absolutely a topic of debate, and discuss it with you some more, Leo, because we sort of kind of rushed through it last week and really didn't have a chance to look at the many different aspects of it. But I want to separate that from the technology because that's math. And we can give the government any kind of access we have to, if we have to. And I want to talk about, separately, the technology tradeoffs about that and how the fact is that, I mean, compelling as the term "backdoor" is, it's possible to have multiple front doors and for them to be every bit as secure as the security we have now.

Other than that, I want to talk a little bit about why the other - sort of like the only other big piece of news that occurred in the last week was we found out why it was that Barack Obama, during his final press conference of the year that we talked about last week, seemed so confident in pointing the finger at North Korea as he took off for his vacation to Hawaii. I have some sci-fi thoughts and recommendations, and then we'll get into our content. So I think, once again, a good podcast for everybody.

Leo: Lots to talk about. I was watching, and I recommend, it must have been a year ago, the "Frontline" piece, there actually were two pieces on the Snowden revelations and the NSA, they call it "the program" for capturing all the data. And it's really well done, balanced, and a fascinating piece. So I'm very interested in all of this. And I have to say, I among everybody else have been kind of uncritically saying, well, a backdoor makes the software broken. So I'm very interested in what you have to say there. And in fact...

Steve: Well, and you're not...

Leo: ...as soon as you mentioned that, I realized, of course, you could just give a key. You could have two private keys and give one to the government. But people like Cory Doctorow, knowledgeable fellow, that was his chief, in fact I think probably most of the people like EFF, that was their chief complaint, is that backdoor breaks the code. So I'm very interested in what you have to say about that.

Steve: Yeah. And so, yeah, because we're about technology here, I wanted to clarify that, yeah, and separate that aspect from the politics. But the politics are fascinating, too.

Leo: Oh, yeah. Oh, yeah.

Steve: So we'll talk about all of that.

Leo: All right. News of the week, I guess.

Steve: So, yeah. In a very light news week, we had one really interesting tidbit, which was the news was broken by an investigative reporter named David Sanger, who writes for The New York Times. I saw him interviewed yesterday. His story appeared in the Times yesterday. Headline was "NSA Tapped Into North Korean Networks Before the Sony Attack, Officials Say." And so my own headline for the podcast for this was "Let's Don't Underestimate the NSA." I think maybe there's sort of a tendency to think well, it's sort of big and bureaucratic and, you know, stumbling over their own feet. But the technology that's evidenced in the document - there was sort of a companion document that Der Spiegel published. I have a link to it. Actually I made a bit.ly link for the show, bit.ly/sn-491. And that takes you to a three-page PDF which is a couple pages from what looks like an online conversation. Anyway, I'll get to that in a second.

I first tried to sort of, like, paraphrase what David wrote. And I thought, okay, I can just do a better job if I just share just the first opening four paragraphs of what he wrote. He said: "The trail that led American officials to blame North Korea for the destructive cyber attack on Sony Pictures Entertainment in November winds back to 2010," so four years ago...

Leo: According to unnamed government sources. Very important to point that out.

Steve: Correct. He said: "...when the National Security Agency scrambled to break into the computer systems of a country considered one of the most impenetrable targets on Earth. Spurred by growing concern about North Korea's maturing capabilities, the American spy agency drilled into the Chinese networks that connect North Korea to the outside world, picked through connections in Malaysia favored by North Korean hackers, and penetrated directly into the North with the help of South Korea and other American allies, according to former United States and foreign officials, computer experts later briefed on the operations, and a newly disclosed NSA document."

He said: "A classified security agency program expanded into an ambitious effort, officials said, to place malware that could track the internal workings of many of the computers and networks used by the North's hackers, a force that South Korea's military recently said numbers roughly 6,000 people. Most are commanded by the country's main intelligence service, called the Reconnaissance General Bureau, and Bureau 121, its secretive hacking unit with a large outpost in China."

Okay. So what's really interesting is the dialogue in the document that David refers to which Der Spiegel published, which is a sort of a snippet of top-secret, marked as such, conversation where somebody wonders about the term "fifth-party collection." Like, what's fifth-party collection? And so it poses the question, is there fifth-party collection? And some individual responds yes. "There was a project that I was working last year," and we don't have any dates here, so this sounds like this is the four-years-ago, 2010 timeframe. "There was a project that I," says this writer, who's anonymous here, we don't have his name, either, or hers, "I was working last year with regard to the South Korean CNE program." CNE, of course, is the acronym for Computer Network Exploitation, sort of general penetration and exploitation.

"While we aren't super interested in [he writes] SK (South Korea)," and then in parens "(things changed a bit when they started targeting us a bit more), we were interested in North Korea, and SK puts a lot of resources against them. At that point our access to NK was next to nothing, but we were able to make some inroads to the South Korea CNE program. We found a few instances where there were North Korean officials with South Korean implants on their boxes, so we got on the exfil points and sucked back the data.

That's fourth party. However, some of the individuals that South Korea was targeting were also part of the North Korean CNE program. So I guess that would be the fifth-party collect you were talking about.

"But once that started happening, we ramped up efforts to target North Korea ourselves." And then he says, "(as you don't want to rely on an untrusted actor to do your work for you)." Meaning they weren't content to continue essentially looping through South Korea to get to, like, South Korea's penetration into North Korea to get to North Korea. Our NSA wanted our own direct connections. So they said, "But some of the work that was done there was able to help us gain access. I know of another instance, [and he says] I'll be more vague because I believe there are more compartments involved, and parts are probably NF," whatever that stands for, "where there was an actor we were going against. We realized there was another actor that was also going against them," meaning North Korea, "and having great success because of a zero-day they wrote. We got the zero-day out of passive and were able to repurpose it. Big win. But they were all still referred to as fourth-party."

So anyway, that's a snippet of sort of what appears to be internal NSA dialogue among people who have certainly a high degree of privilege to what's going on, where they're saying that, by initially getting in through some South Korean connections into North Korea, our networks, the NSA, had probes in North Korea. And so the balance of David's story, where he's explaining essentially what we now believe is going on, is that the U.S. was able to be very rapidly definitive, much more so than anyone in the security community believed. All we had was, oh, well, they were using some IP addresses. And unfortunately, while that might make the general public happy, those of us who knew better, knew that these were, like, widely known proxies that...

Leo: I just - I've got to say this, Steve. I can't let you go farther with that.

Steve: Okay.

Leo: This guy Sanger was the same guy who told us that there were weapons of mass destruction in Iraq based on anonymous government sources. He has been a channel in The New York Times for anonymous government sources before which are not credible because it's basically - he's repeating government propaganda. Now, the Snowden leaks no one questions.

Steve: Right.

Leo: And I think rightly so. So the theoretical possibility of this being true is actually very high. But I would not credit that New York Times article in the least. And I'm not alone. There's a very strong opinion piece on Errata Security by Robert Graham...

Steve: Ah, yes. We know him.

Leo: ...whom we know well, who says this is just not credible. It may be true; it

may not be. But when you get anonymous tips from government sources, it's not journalism to rehash them. It's merely repeating government propaganda. It's misinformation.

Steve: Interesting, yeah.

Leo: Just thought I'd point that out.

Steve: No, I'm glad.

Leo: Before we get too enamored of it.

Steve: For context.

Leo: Yeah. I mean, the Snowden stuff I completely credit. In fact, there was even some speculation in the past that that wasn't real. But I think we pretty much agree now there's no way that could be faked.

Steve: No, no.

Leo: And I trust Der Spiegel. But I don't know if you can trust this New York Times article. It kind of - so I've always said, well, why would the President and the FBI lie? And what Robert Graham says is just exactly like the run-up to war in Iraq. And in fact it's the same reporter at The New York Times who has the information. This guy has a history, a track record. And when the U.S. government decides it wants to do a little saber-rattling...

Steve: Yeah, good point.

Leo: ...he's the first person they call. So it doesn't confirm, it doesn't really confirm, in my opinion, this information.

Steve: Right.

Leo: Although we obviously do have the means.

Steve: Yeah. And I guess it feels to me like it's, from a technical standpoint, the internal NSA document feels right. I mean, it seems credible. It's somebody who feels like he's discussing among a trusted peer the kind of operation that they have in various facilities around the world able to do this kind of stuff. So again, you're right. We don't know one way or the other.

Leo: According to - this is Sanger. According to the officials and experts who spoke on the condition of anonymity - that always should be a red flag, when you read that. And he doesn't have any public, you know, anybody besides the Snowden documents to publicly confirm that.

Steve: Right.

Leo: And in fact all he's got is a quote from a cyberwarfare expert who says, "Attributing where attacks come is incredibly difficult and slow."

Steve: And that's what we've said from the beginning, is that it's just - it's so difficult to know definitively. And we've asked the question, was there information that the government had, that it wasn't disclosing, that allowed it to state as definitively as it did that North Korea was behind the attacks?

Leo: And to further muddy it, you've got that bastion of credibility, General James Clapper, who says, "Oh, yeah, I had dinner with the guy last fall, you know, the guy who did the attack." So come on. This seems a little self-serving on their part.

Steve: Yeah, especially Clapper. You know how I feel about him. We played the video...

Leo: He's already lied to us. He lied to us once.

Steve: Yeah. We played the video of him saying, "No, we're not spying on anybody, no, sir," while he was scratching his head and, like, which looked like a bad poker tell. Okay. So I wanted to share with our listeners my complete amazement over the fact that there appears to be a fabulous series starting on the Syfy Channel, which I know sounds like an oxymoron, I mean, that phrase, because I'm very picky about science fiction. And so it aired for the first time Friday, the first episode. First of all, the title is "12 Monkeys," which of course is a famous piece of science fiction...

Leo: Loved that movie.

Steve: ...that Terry Gilliam - yes, yes. People who have seen now the first hour episode think this blows the movie away. And I don't know where this came from because it is so unlike anything else that Syfy Channel typically airs in that it's really good. And I just - I hope it maintains. But I know we have tons of sci-fi interested listeners. So I wanted to make sure that everyone at least knew that this - I'm sure they'll be reairing it through the week, and the second episode will be this coming Friday. So "12 Monkeys" on the Syfy Channel.

I also saw, I don't know why, I guess it was because the Sunday shows were canceled for sports, I found myself poking around a little bit, looking for something to watch. And there was a movie, a 2014 movie that was not well reviewed, called "Automata," A-U-T-O-M-A-T-A. And, I mean, it's off of the chart. It's Antonio Banderas, Dylan McDermott,

and a barely recognizable Melanie Griffith. I remember I was looking at her, thinking, is that Melanie Griffith? Of course I don't think I have seen her since "Working Girl," so that's been a few decades.

Leo: Yeah.

Steve: Anyway, the movie was kind of haunting. It's only $3.99 on Amazon Instant Video, and I'm sure you can find it on whatever your source of movies is. Anyway, I provisionally recommend it. I don't want to get anyone's hopes up too much. I mean, it's got some rough spots. But there's a lot of it that's well done. And even the critics who didn't like it said, well, you know, it's got its moments. And it's interesting. And it actually comes - I've thought of it again because toward the end of MacBreak Weekly, or maybe it was in between shows, you were talking about this question of what happens as computers get more intelligent. And the concerns that some legitimate computer scientists like Kurzweil and so forth, Kurzweil I guess his name is, have, like, their worry about what happens when we actually succeed in making machines intelligent.

Leo: Oh, a lot of people worried about that, yeah.

Steve: Yes, and this is in...

Leo: Including Elon Musk.

Steve: So this is set, yes, this is set in sort of the post-apocalyptic, the sun has overheated, and the earth is sort of hostile to people, so we create machines in order to do a lot of the work. And they kind of get loose. Anyway, again, "Automata," 109 minutes long, not very, I mean, it's not fabulous. That's why you haven't heard of it before. But for our audience who are sort of forgiving because a lot of them do watch stuff on the Syfy Channel, I could recommend it for a few dollars.

Leo: Apparently also on Netflix for free if you're already a subscriber.

Steve: Oh, yay, good. Then in that case, give it a try because - and it has kind of a - you're not sure what's going on at the beginning. It's sort of an awkward start. But then you kind of get into the groove. And I liked it, I have to say, and I find myself kind of thinking about it, like affected by it, which doesn't happen that often.

Leo: Yeah, I use that as a metric. Did I think about it the next day?

Steve: Exactly.

Leo: Then, whether it was a great show or not, it stimulated some thought.

Steve: Yeah. It had some good moments. And speaking of a good moment - there's a transition for you, a segue. In the middle of December - I just ran across this in my email from Sue, she forwarded it to me - from a Jarred Sutherland. The subject was "Whew! SpinRite Success Story." And he said: "Steve, I've been listening to Security Now! for several years now and have been a fan of your site and research well before that time. I finally had a need for SpinRite for a friend whose Seagate drive which contained very important data went completely belly-up. Now, this made me panic for a very specific reason. I configured backups for this system, but missed a poorly placed directory." And he has in parens, "(online backup over a slower connection, so I was selective about which folders were chosen)." Which is to say he wasn't backing up the entire drive. He said, okay, I will back up the documents directory and so on, but there was one that got away from him.

He said, "So I was able to restore most of the data I needed from the backup, but not this particular crucial chunk. I was sunk, or so I thought. A combination of SpinRite on Level 2 and a bit of fridge time allowed me to mount this drive on my MacBook and pull the data off just in time. SpinRite saved my bacon. What a fantastic piece of software you have here. I will pass along my recommendation to any and all who end up in a position like me, or who don't want to by keeping a good eye on their drive. Thank you!!! [three exclamation points] Jarred Sutherland."

Leo: Nice.

Steve: And it's interesting because his mentioning the fridge reminded me that one of - we're sort of beyond this point now. But one of the arguments that we encountered early in the days of SpinRite was how could software fix hardware? It was like, I mean, skeptics were saying, you know, wait a minute. If the drive's bad, then software can't fix it. And of course we know that the reality is that there's a large band of gray between good and bad on hard drives, and that they actually deliberately operate kind of in the gray, relying on error correction to sort of keep them from going too deep into the gray or crossing into the dark. And that essentially the drive and the OS and everybody will give up and just say, okay, it's too gray. SpinRite comes along and says nothing is too gray. Unless it's really not even spinning any longer, we're going to pull that one last time back from the dark, into the light.

And of course SpinRite's able to do that. There are some instances where the drive has sort of crossed over. And one of the tricks is you change the temperature. You stick it in the fridge for half a day or a few hours, just to sort of throw in another variable. It's like the drive is normally running hot, and we can't get the data, so let's cool it off. And then you quickly plug it in and see if you can run SpinRite on it again, like in the area where it had a problem, or just start it over and sort of introduce temperature as another thing to try. I mean, at this point we're getting desperate. So refrigerator, fine. And sometimes, as many people have found, that's like the final little bit of magic to bring it back from crossing over to...

Leo: To the other side.

Steve: To the other side, exactly. So anyway, Jarred, thanks for sharing and reminding everybody about SpinRite.

So we've never - we're in our 10th year of the podcast - expressly talked about

backdoors. We refer to them many times sort of in an offhand fashion or tangentially, relative to something else. Like famously we were talking last year about this notion of a backdoor when we discovered that that dual elliptic curve digital random bit generator, remember the DRBG, when it was one of the four different algorithms in the NIST formal suite of pseudorandom number generators that was approved, and we started to wonder about where it came from and whether it was trusted because it sort of had appeared in our products, and it was slower than the other ones and had sort of an unknown back story.

So anyway, so then the reason this sort of came to the fore for me is, of course, in the last week, after the Paris attacks, as we just talked about last week, David Cameron has famously been running all over the place talking about how terrorists should not be allowed to communicate in a way that the government cannot decrypt if it wants to. And as I understand it, his statement has been stronger than the one the U.S. President Barack Obama echoed. Cameron came to the states, and they were together, and essentially Obama was saying something similar, although maybe not quite going as far as to say that we're going to have legislation to do this which, as I understand it, Cameron has been saying.

Leo: I think the President was a little bit cagey about how he supported this, yeah.

Steve: Right, right. And I want to talk about...

Leo: And, by the way, it would be terrible for U.S. tech companies like Microsoft and Apple and Google because who's going to want to use software with a backdoor?

Steve: Well, and, see, perfect segue because the backdoor is the term that everybody uses except, like, Barack never said that; Cameron never said it. No one has ever used the term "backdoor" except those reporting on this. And one of the problems, I think, is that that's the term we have. First of all, we've talked about how, when you, for example, have an exploit named Heartbleed, you give it a fun name, it gets a lot more traction than if it's some CVE numerical designation that no one can remember. And there's just this - there's a rich, deep history of backdoors in mystery novels and in sci-fi. And it has this...

Leo: You might remember this moment in a little movie called "WarGames."

MALE VOICE: I want you to take a look at this.

Leo: I think they talk about a backdoor here.

Steve: Yeah.

MALE VOICE: Hey, what's that?

MALE VOICE: I wanted Jim to see that.

Leo: No truth to the rumor that that's Chris Pirillo.

MALE VOICE: Wow, where did you get this?

MALE VOICE: I was trying to break into Protovision. I wanted to see the program for their new games.

MALE VOICE: Wait, Jim, I'm not through yet.

MALE VOICE: Remember you told me to tell you when you were acting rudely and insensitively? Remember that? You're doing it right now.

Steve: And a young Matthew Broderick.

Leo: Yeah.

MALE VOICE: Theaterwide biotoxic and chemical warfare. This didn't come from Protovision.

MALE VOICE: You bet it didn't. Ask them where it did come from, Jim. Go ahead, ask them.

MALE VOICE: I told you already.

MALE VOICE: Looks military to me, definitely military. Probably classified, too.

MALE VOICE: Yeah, but if it's military, why does it have games like Checkers and Backgammon?

MALE VOICE: Maybe because those are games that teach basic strategy.

MALE VOICE: Jim, how do I get into that system? I want to play those games.

MALE VOICE: You're not supposed to see any of that stuff. That system probably [unintelligible] their data encryption algorithm. You'll never get in there.

MALE VOICE: Hey, I don't believe that any system is totally secure.

Leo: I love this kid.

MALE VOICE: I bet you Jim could get in.

MALE VOICE: Yeah, I'll bet you he couldn't.

MALE VOICE: I bet you he could.

MALE VOICE: Well, you'll never get in through the frontline security. But you might

look for a backdoor.

Leo: A backdoor.

Steve: Okay. So, perfect segue. In computing, a backdoor is a method of bypassing the normal method of authentication. So whatever it is, it's a method of bypassing the normal method of authentication. A cryptographic backdoor is a secret. And I put in here, I was going to say a secret known only to the algorithm designer. And I put "initially" in parens, to highlight the fact that the problem is that of needing to keep a secret. So a cryptographic backdoor is a secret (initially) known only to the algorithm's designers or implementers. And being a backdoor, the knowledge of that secret allows some aspects of the difficulty of decrypting the encrypted content to be bypassed, thus substantially weakening the algorithm's guarantee or promise of security.

So a perfect example was if, for example, that dual elliptic curve deterministic random bit generator had been designed to be weak, then there would be some characteristics of it which, to be a good backdoor, would withstand direct scrutiny. Other experts could look at it and scratch their head and say, yeah, looks okay to me. And yet there would be some properties of it which would elude observation such that the people who knew the secret would have an advantage in some fashion, based on the purpose for which those random numbers were employed. So everybody has been correct in asserting that a backdoor, per se, weakens security. And we know that because what that says is that there's a secret, and secrets are notoriously difficult to keep such that, if it became known, then the security can to some degree be bypassed.

So the clip from "WarGames" is another perfect example. If there was a backdoor, then somebody installed it there, and these kids were going to attempt to discover it in order to go through the backdoor, the idea being that it's like it's another way in. But part of that is that it's not another front door. That is, it's not a sanctioned means for decrypting the content. It's secret. And when we were talking about Enigma last week, one of the strongest aspects of the Enigma technology was that the Polish mathematicians managed through a great amount of skill to reverse-engineer the entire machine itself, based on enough samples of its output. And yet, even having the machine, because it was a keyed cipher machine, if they didn't have the key, then having the mechanism didn't help them. So what's different here is a backdoor sort of breaks that rule. It says there is a secret defect that can be exploited to allow someone to essentially bypass the need for the key.

So the point is, the main issue that I wanted to bring up, and there's a lot to talk about this, is that absolutely nothing prevents current crypto from operating with multiple keys. And in fact we do that now. We believe that the way iMessage works is that every user of iMessage has a private key which never leaves their device. It's generated in their device as a public key pair composed of a private key and a public key, are generated in the cryptographic element, the secure element in the iPhone, and the private key never leaves. The public key is sent to Apple for key management. And when you are generating a message that is intended for multiple recipients, that message contains multiple keys.

Now, remember that public key crypto isn't used for bulk encryption because it's just way too slow. So this is why we also need, for cryptography, a source of really good random numbers. So we have a really good random number generator. We choose a random number which is used to encrypt the message. And then that random number is

encrypted with the public key of the intended recipient because only the person who has the matching private key can decrypt that random number back to what it was and then use symmetric encryption, or decryption in this case, to get the message back.

The point is that this makes encrypting for multiple recipients possible because you take that one random number, and you encrypt it first with one recipient's public key and attach that to the front of the message. Then you take again the unencrypted random number and encrypt it with a different recipient's public key and attach it, and then with a third, and so forth. So you can arrange to send a message that contains essentially multiple addressees, for lack of a better term, the point being that, when the message is received, the recipient will have the ability to decrypt one of those multiple keys to get the original random number which was used to encrypt the message and thus decrypt it.

So I'm not - and I want to make sure everyone understands, I'm not advocating this at all. I mean, as everyone knows, I aborted CryptoLink, the work I was going to do on a VPN, specifically because there was a threat that something like this could be coming along. And at this point in the evolution of information technology and networking, we're sort of at an inflection point, I think. I mean, it'll be interesting to see how the next few years go because the one argument that cannot actually be made is that necessarily allowing the government access, some means of access to our communications, weakens it.

Now, the problem is also that - and you'll probably remember the exact phrase, Leo. I couldn't remember what it was. But it's something, there's an old saying, something like once you tell one other person a secret, it's no longer a secret.

Leo: Another great Ben Franklin quote, I'd say.

Steve: Something like that. And so we cannot argue against the fact that there's a tremendous burden of responsibility associated with managing this. But here's the way it would work, just to, like, lay out the theoretical framework. And that is that the U.S. government, I'm sure the NSA or the FBI, somebody who knew what they were doing - law enforcement, broadly - would create a master public key pair. The private key would be well guarded. The public key everyone would know. That is, that would be - it would be like, you know, go to the website. Download our public key.

And so in this - and again, I want to make sure everyone understands I am not advocating this. I'm just - we have to talk about the technology separate from the ethics and all the politics and everything else. But the technology would be that, presumably, a law would have been established which does require that any legal encrypted traffic be decryptable by duly empowered law enforcement. And the technical means for achieving that would be that, when we're going through the process of any, quote, "legal" under this draconian law, but still, if it happens, the way we do that is, while we're going through this process, in that keying phase, the U.S. government's public key is used also to redundantly encrypt the symmetric key, and that's part of the payload of the message. So it is as secure as the math, subject, of course, to the management of this key.

So we don't have a secret like the "WarGames" guys or like the classic notion of a backdoor. What we have is a redundant keying of all legal cryptography. And I'm being careful with my phraseology because we'll talk about the point you raised last week, Leo, that, well, the bad guys won't use that. Of course they'll use illegal cryptography or cryptography which cannot be decrypted, which does exist and will always exist. And hopefully this argument will keep this draconian "1984" Big Brother crypto from ever

happening.

But just as a matter of technology, then, the idea would be that this cryptography that was legal under this draconian law would all carry a key that could be decrypted only by the U.S. government's law enforcement private key, which they would have to keep absolutely secret. And presumably there would be some process. The NSA would do bulk data collection of maybe everybody. And then when they recognize that some terrorists have been operating under their nose, they would pull the communications from that group of people and pull the headers off the packets, send that somewhere to have those keys decrypted, and then get them back, and then be able to decrypt back into plaintext. I mean, it's burdensome. But anyway, my main motivation was just to bring the point up that we don't need a backdoor because the technology we have today could allow that.

So this is obviously still fraught with problems because, as you immediately mentioned correctly last week, it is math. And if there are, quote, "legal" cryptographic systems under such a law, all that will do is it will create an underground of cryptographic systems that don't have the government key on it, for anybody who wants to encrypt data that can't be decrypted under this technology.

Leo: This is actually Skipjack, which was, is, a crypto system proposed by the NSA. Remember the Clipper Chip, which is, by the way, despite all the hoorah about it, in our TVs today. But that used Skipjack. And the idea was there was an escrow process for a second government key, and that that key would be held in escrow and would need legal authorization for releasing. I'm going to put...

Steve: Yeah, and...

Leo: Go ahead.

Steve: And that's a very good point. In my model, there's one super galactic master government key. But a safer way to do this would be, for example, if Apple wanted to do commercial cryptography for the privacy of its users, subject to such a law, then they could give the government an Apple iMessage private key, and then the Apple technology would always incorporate the matching public key as an additional key in Apple communications. And similarly Google could do it. And the point is anybody who wanted, any commercial entity that wanted to sell crypto in this climate could produce a public key pair and turn over the private key to law enforcement agencies so that they're able to decrypt the traffic, given proper means and needs and protocol and so forth.

Leo: I guess, you know, it reminds me of this conversation over Skipjack. And one of the issues - I'm looking at a testimony from 19, I don't know, '94, I think, from Whit Diffie, '93, about Skipjack. And one of the things he points out is that - and he doesn't have a problem with the key escrow. But he says, if you don't make the algorithm for Skipjack public, it can't be vetted by - we've talked about this many times - can't be vetted by crypto experts, and therefore we can't be sure it's secure.

Steve: Yeah. And so that was 22 years ago or 23 years ago, back when we were sort of still thinking of - remember that, like, RSA, the famous RC4 cipher that has now been discredited because of the way it was implemented in the early WEP WiFi, that was a

secret. It was proprietary. There was a time when these algorithms were not published, were not vetted by the academic or the crypto community. And we just sort of had to trust that they were good. And the good news is we're past that point now. Now we've got highly vetted, scrutinized, I mean, we're actually - we're using public competitions in order to choose what the next cipher will be. So arguably as democratic and academic a process as we've been able to come up with so far, where, again, it's the algorithm itself is solid, and it's the key that is the secret, which is much stronger crypto.

So what do you think is going to happen, Leo? I mean, you're as clued in to all of what's going on as any of us.

Leo: Well, I don't know about that. I know you listened to our conversation on TWiT with Iain Thomson.

Steve: Oh, my god. I also wanted to say, fabulous panel on TWiT on Sunday [TWiT-493]. Really, really good...

Leo: So Iain Thomson of The Register. And he's a Brit, of course, and gave us kind of the British perspective on why Cameron would say such a thing, whether it's political or real, et cetera. We had Ben Thompson from Taipei, Taiwan. He's probably the smartest analyst out there.

Steve: They're really, really smart.

Leo: Isn't he great?

Steve: Really sharp.

Leo: His website, Stratechery, is for me must-read stuff. And they're just so great, so smart, and it was a lot of fun. And who was the third? Now I've forgotten. I got Ben - it was the two Thom(p)sons, the Thom(p)son Twins.

Steve: A gal.

Leo: Oh, of course, Serenity Caldwell, the great Serenity Caldwell for iMore. So, yeah, I thought it was a good conversation. And Iain, you know, I said, "Iain, does Cameron mean this to be a law?" And he said he thinks he does. I said, "There's certainly political motivations." You know, his party is being pushed from the right by Ukip and others. And so you want to look strong on terrorism. But I think the consensus was that perhaps Cameron doesn't understand the technological issues.

But I have to say, I just accepted uncritically this idea that a backdoor weakens encryption. I mean, if Cory Doctorow says it, it must be true. But you're absolutely right. When you started the show I said, well, wait a minute. Let me do the thought experiment.

Steve: Right.

Leo: Of course you could have some sort of secure key escrow. We'd have to trust that this escrow systems works and doesn't have leaks. But if you believe that strong encryption is effective, hackers are no more likely to break that than your key.

Steve: Right.

Leo: A private key's a private key.

Steve: And one thing, one thought I had was whether posing the question, isn't metadata enough, that is, we've argued that metadata is a big intrusion as it is, even without knowing what the conversation is. Knowing what the network of connected people are is a huge intrusion. And I wonder if that's not enough of a compromise.

But I listen to the talk. I'm an avid politico. I follow politics. I listen to these guys talking and this argument of, wow, how can we allow conversations to occur that we can't monitor? And, I mean, we know how. We believe that there are other means for acquiring that same information, you know, plant bugs in the people's machines, microphones near them, I mean, do other things rather than just the opportunity for wholesale decryption of everyone's private communications. But I just - I don't have much faith in the understanding of how intrusive that would be within our lawmakers.

Leo: Yeah. I think that's the problem. And it's not going to take long before somebody, if they haven't already, pulls Cameron or Obama aside and says, "Excuse me, you understand that this would be devastating for the economy of U.K. or the United States, that no one would buy products from the United States ever again?" I mean, it's just - I think it's a nonstarter. Although I've had lots of email and tweets from listeners in the U.K. who say, "Oh, you don't understand, they mean to do this." And even Iain Thomson said nobody probably would have believed the proposal a few years ago that all Internet traffic be filtered in the U.K., and it is. So, yeah, maybe, I mean, I don't - maybe it is something that they could do. But, boy, they'd have to isolate themselves as a country.

Steve: And we do know, for example, that corporations are increasingly proxying their networks with hardware that allows them to inspect in the SSL the TLS traffic of all of their users. That's happening because more and more traffic on the Internet is becoming encrypted. And it's just not feasible for a corporation not to be able to see into the traffic that is entering its corporate network. So they're intercepting with HTTPS proxies in order to perform malware and traffic inspection increasingly. And we know that there are educational systems that are doing the same thing.

So, I mean, it's tough. In terms of legal processes, one of the things that I was imagining was that - imagine an environment where it is illegal to use encryption that cannot be turned into plaintext. So that, if you do encrypt, then, if asked, you must be able to decrypt on demand or suffer the consequences of being unwilling to provide decryption for what's encrypted. I mean, maybe that's sort of a half measure.

Anyway, it'll be interesting to see. And mostly what I wanted to make the point was that, unfortunately, we really don't have the argument from an academic standpoint, from a technical standpoint, that giving the government access weakens our crypto. It would be an additional layer of headache and management. But if commercial entities doing crypto gave the government, you know, created a second key and gave the government a private key that allowed them access, that doesn't weaken it at all, unfortunately, subject to the need to manage that properly. But we see people able to manage. All of our certificate authorities are able to manage their...

Leo: That's how it's done; right.

Steve: ...private keys so that no one else is able to get it. Anyway, I wanted to put that on the radar because...

Leo: I think you're right. And that's why we love you, because you're a stickler for accuracy, even if you agree with the sentiment behind the inaccuracy.

Steve: Yes.

Leo: Did you get this from Carey Parker? I just wanted to mention this. It's called "Firewalls Don't Stop Dragons."

Steve: No, interesting.

Leo: Yeah. He said he sent you one. So he said he wasn't sure if he got the address.

Steve: It might have gone to our corporate mail...

Leo: Probably did, which means you'll get it eventually.

Steve: Yes.

Leo: "A Step-by-Step Guide to Computer Security for Non-Techies." He writes, "As a software engineer, political junkie, and concerned citizen, I felt the need to do something about the current sorry state of affairs with regard to security and privacy. I think most people are just too intimidated by technology, so they just throw their hands up." So he's written a book on how to secure your computer, how to get your privacy. He says, "I've been listening to Security Now! for probably four years. I never miss an episode. It was a real inspiration to me. And I've included multiple references to Steve and the podcast in the book."

Steve: Ah.

Leo: So that's cool. He doesn't mention where you can get it. I would hope it's on Amazon. I think probably everything is. And it looks pretty good. I've just flipped through it. I just got it while we were talking. But he talks about LastPass and, you know, all the stuff that you need. It seems like it would be a useful - how to create a master password. And we talked about how to use a song lyric to create a password.

Steve: Yeah.

Leo: And it's all in here. So I think he's done, you know - two-step authentication. I think he's done a great job. And he's obviously been heavily influenced by you. So...

Steve: Well, and it looks like the notion of firewalls is sort of a generic term because he's talking about all kinds of different...

Leo: You've got to do something. It's not about firewalls particularly, it's about how you've got to do more than just have a firewall or a - he talks about the "Christmas Story," "Be sure to drink your Ovaltine." Remember that? He used a secret decoder ring, and that's what the secret message was, "Drink your Ovaltine." So I kind of like this, just flipping through it. So I just thought I'd mention it, and since he is a fan, and he mentions the show. It's called "Firewalls Don't Stop Dragons." I think it's self-published by Carey, C-A-R-E-Y, Parker.

Steve: Nice.

Leo: And thank you, Carey, for passing this along. We probably should have saved it for the feedback episode because that's next week; right?

Steve: I'm sure we will - I didn't even look in the mailbag. I wanted to, but when this issue of the backdoors came up, I thought, no, we have to just clarify that one technical issue that unfortunately we don't have that to fall back on. So I'm sure there'll be lots of questions, maybe about Enigma. That was a super popular episode last week. So, yes, Q&A. And then everybody wants the DeTor episode.

Leo: Gotta do it.

Steve: Which, you know, it'll be the one that follows unless, you know, hell breaks loose in the meantime. But believe me, it's like right there in my notes to talk about how much we can trust Tor. Oh, and there it is on Amazon.

Leo: It is on Amazon, $17.43.

Steve: Nice.

Leo: Just came out. And we were talking last week - I'm going to throw one more thing in, and then we're going to wrap it up. We were talking last week about the historical inaccuracies in "The Imitation Game." You and I both loved it as a movie.

Steve: Great movie.

Leo: I'm sure it will - it was nominated for nine Academy Awards, I think. Was that the one? No, "Birdman" was. But I think it was...

Steve: I think, like, seven.

Leo: Yeah, quite a few, and Benedict Cumberbatch was nominated for Best Actor. It was nominated as Best Picture. But we did talk about the fact that in some ways it slanders Alan Turing's memory, which is sad, saying that he was a craven traitor, in effect. So somebody in the chatroom said this, and I meant to mention it, "Cryptonomicon," which is my all-time favorite book, I mean, just the greatest book...

Steve: Neal Stephenson, yup.

Leo: Brilliant guy, great writer, I mean, really one of our best writers. And he happens to be technically super literate, super right on. They talk about Enigma a lot in there in an historically accurate fashion. So if you want a great novel that is about crypto, that is fun to read, I mean, it's something great, and it has quite a bit of Alan Turing and Enigma in there, it's "Cryptonomicon." It's not a historical - well, it is, kind of. It's a novel with historical stuff in it.

Steve: Yeah, and it's long. It'll keep you going.

Leo: It's so good.

Steve: It'll keep you going for a while.

Leo: So good. Hey, Steve, thank you so much. Yes, feedback next week, god and hackers willing. If the good lord's willing and the creeks don't rise, we'll do questions and answers next week. You can ask your question at GRC.com/feedback. Don't email Steve. You can also tweet him, though. He is @SGgrc on the Twitter.

Steve: I try to keep an eye on my feed and use that.

Leo: Good way to interact with him. And of course while you're at the site,

GRC.com, pick up a copy of SpinRite, world's best hard drive maintenance and recovery utility. And then that's the only thing he charges for. The rest of it, there's so much great stuff, and it's all free. Lots of good information from the wide-ranging mind of Steve Gibson, GRC.com. He also has 16Kb versions of this show. He's got transcriptions there. We have high-quality audio and video from the show at our site, TWiT.tv/sn, for Security Now!. And of course you can always subscribe at your favorite podcast pavilion, iTunes or whatever you like to use.

Steve, have a great week. Thank you for - I know politically you're on the side of people who hate this idea, this David Cameron idea. But this is what I love about you. The fact is a fact, and we've got to be honest about the facts.

Steve: Yeah.

Leo: Thanks so much, Steve. We'll talk again next week on Security Now!.

Steve: Thanks, Leo.