SECURITY NOW!

Transcript of Episode #30

Cryptographic Issues

Description: Steve and Leo open their multi-week discussion of the operation and technology of cryptography. This first week they start by examining the social consequences and ethical implications of common citizens being empowered with freely available cryptographic technology that no force on Earth - no government agency, no corporation, no private individual - can crack within their lifetimes.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-030.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-030-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 30, for March 9, 2006: Cryptographic Issues. Steve Gibson, a good afternoon to you.

Steve Gibson: Hey, Leo.

Leo: Leo Laporte here. And today we begin a series on something I think everybody wants to know more about: cryptography.

Steve: Yeah.

Leo: This is going to be exciting. Today we're going to cover cryptographic issues, societal issues and so forth. But over the next three or four episodes, a lot more, including how it works fundamentally. Any issues we want to cover from previous episodes before we dig in?

Steve: No, I think we're pretty clear to start. I want to - I'm excited about this. I know that a lot of people are interested in what cryptography is, sort of on the technical side - how it works, you know, what are public keys and private keys and certificate authorities and signing chains and all of that. And so over the next few weeks I want to really - I want to take our time, explain this stuff very clearly so that we've created a real foundation of understanding how these basic technologies interrelate with each other. And then of course they're all about how we're using the Internet today, you know, OpenVPN that we've talked about for remote secure access uses certificates. We know that secure web browsing uses certificates. You know, what does that mean? What is a signing authority? And, I mean, really how does this stuff work? And I think what's surprising is that it can be explained in a way where people are going to go, wow, I get that. I mean, they're going to come away with an understanding of it.

But before we really got into the technology side, I wanted to talk this week about sort of the - kind of the ethics of crypto because something has happened that is significant, just in the last decade or so. And that is that end users, just regular people have, thanks to the academic community really getting involved in crypto, have acquired access to free, simple, usable technology which no government, I mean, not their own government, no one else's government, no corporations, no one can crack.

Leo: Now, this is no accident because, in fact, Phil Zimmermann of PGP, which was really the first, you know, widely accessible public key cryptography, did have an agenda. He wanted to create a strong cryptography that the masses could use, not just - I mean, political dissidents, in fact, it's widely used by them, people who are in fear of their life, but also here in the United States who didn't want a government eavesdropping on them.

Steve: Well, of course, yeah. PGP stands for Pretty Good Privacy, which I always appreciated that acronym because, I mean, it is way more than pretty good.

Leo: It's a little self-deprecating, unnecessarily so. It's strong crypto.

Steve: If you use it, it's all you ever need privacy.

Leo: Yeah, yeah.

Steve: And it's interesting, too, because you know of course there's been all this controversy in the United States recently about this warrantless NSA surveillance of U.S. citizens where, you know, post-9/11 the George W. Bush administration took it upon themselves to change the way they got permission for basically eavesdropping on U.S. citizens, doing so-called "warrantless surveillance," meaning that they wanted the right, and have taken the right, to eavesdrop on any conversations which, basically, which they wanted to, in the interest of United States national security.

Leo: Well, and that's what's changed since Phil came up with PGP. This is, you know, all his work was pre-9/11. Well, it's changed a lot since 9/11. However you feel about this, there certainly is a legitimate cause for concern that terrorists are now capable of hiding their tracks by using widely available crypto. I mean, there was a news story recently that said Skype, which is secure, could be used for making phone calls without any possibility of wiretapping.

Steve: Yeah. Well, it's interesting, too, because there are the people who say, hey, I don't care if the government wants to listen to what I do, to my phone calls, to my Internet access and so forth. You know, and their argument is, I'm not doing anything wrong so I have nothing to hide.

Leo: Right.

Steve: And they argue that, hey, if you're not doing anything wrong, what are you worried about? And at the same time we know that there are commercial interests that would apparently like to know what we're doing with our computers. I mean, I guess corporate espionage is a real thing. And so you could imagine executives in a corporation spread out over the Internet wanting to hold a teleconference where they absolutely are sure that nobody, from a corporate espionage standpoint, nobody can listen in on their conversations.

Leo: And this is where it gets dicey. I mean, there is - you know, we're balancing public interest and public safety with a right to privacy and a right to free expression. You know, it's not for you or me to decide about this, but certainly we should talk about the issues that are raised.

Steve: Well, and you were talking about how, okay, terrorists could use cryptographic VoIP, like Skype apparently provides, in order to have conversations in plain sight, so to speak, that no one is able to decrypt. At the same time there's - and we would all agree that that's, like, a bad thing. We don't want people plotting against the health and welfare of citizens of other countries, you know, in their midst and being able to do so. But you also - and I'm not suggesting that that's a good thing by any means. But if that weren't available, wouldn't these bad people, these bad actors, find some other means for communicating?

Leo: Perhaps, perhaps. You know, I've asked Phil Zimmermann this pointblank, specifically. And he says you've got to take the good with the bad. And in his opinion - well, first of all, this cryptography's out there. It's probably too late to even debate this.

Steve: The horses have left the barn.

Leo: Yeah, and had a long time ago. Even when the United States was trying to classify it as munitions and prevent it from being exported, it was there. It was out. So maybe it's a moot conversation.

Steve: So the argument there being that, you know, sort of like guns, I guess, you know, it's like...

Leo: Bad guys have them anyway, so...

Steve: Exactly. Even if it's illegal, bad guys will still use it, breaking the law in order to use it to hide their actions.

Leo: Right, right, precisely. It's there. It's out there. You can argue back and forth. But the fact is, everybody has access to it. I use it all the time. I sign every email I send with a PGP cryptographic string. It's not encrypted, but the email is signed so that you know it came from me and that it hasn't been modified.

Steve: And that's for authentication of the stuff you send.

Leo: Right, that's a very valuable thing.

Steve: Well, and we're talking about OpenVPN. Well, an OpenVPN connection, the type that - and I'm still working on the guides, that's coming along, so people are going to get that. But an OpenVPN connection cannot be cracked by anybody. I mean, no government will be able to eavesdrop on the traffic over the OpenVPN connection. Now, we're doing it because we don't want script kiddies and hackers and malicious people who are snooping on the Internet to have access to our traffic. And so the question will be, I guess, then, well, should the government have a backdoor to these kinds of technologies?

Leo: No. Let me think about that or a second. No. And the reason is because, while the government's benign now, we can't always be assured of that. And we know that PGP is used by dissidents in fear of their lives in many totalitarian governments. In fact, that's why Phil created it, he says, is for countries where you couldn't speak freely and you needed this.

Steve: So, well, of course there was that whole Clipper chip during the Clinton administration, where Clipper was going to be a federally mandated and approved technology that would specifically have a backdoor that would allow, you know, "citizens" to communicate with relative security, but anything the government needed to decrypt that was Clipper encrypted, they'd be able to access.

Leo: Yeah. And...

Steve: And of course it...

Leo: ...of course that went down in flames.

Steve: It died big-time. Nobody wanted that kind of technology.

Leo: Now, that was pre-9/11, as I remember.

Steve: Oh, yeah.

Leo: So I wonder what the climate is today. Let me ask you. Do we know for sure that there aren't governmental backdoors? For instance, Skype isn't saying whether there's a governmental backdoor. They're not asserting that there is not.

Steve: Actually, they sort of imply - and this is what makes me nervous about it. They sort of imply that they will cooperate with anyone that they need to. Also you'll note that you may have an encrypted Skype connection to Skype. But when you use SkypeOut, for example, to transit onto the public telephone system in order to use the Skype service to bridge into the normal audio telephony world, you're decrypted, which means that Skype has to be able to decrypt your encrypted connection themselves. I mean, I have to tell you, Leo, I've actually been, you know, for a while I was thinking about writing my own VoIP system from scratch. Then it turns out that the Skype that we're using right now and upgrading equipment and things rendered that unnecessary. But I've been considering maybe doing a little VoIP encryption tool myself, just because it would be nice to be able to have a conversation. I mean, not that I have anything to hide, but it's just - it's creepy thinking that you might be listened in on, and you'd like to know that that's not happening.

Leo: Well, now this puts you on the hot seat. What about terrorists using it, Steve?

Steve: Well, I mean, that's the double-edged sword. You could argue that people have a valid reason for having a private conversation. I mean, and the U.S. Constitution is all about this. I mean, there is protections in the way the United States was formed because the people who wrote the Constitution came from an oppressive government that didn't have these kinds of protections. And, you know, we're seeing a lot of erosion of those kinds of civil liberties.

Leo: Mm-hmm.

Steve: And I don't mean to get this all political, I mean, because it's about technology. But it's always the case that technology and the evolution of technology creates these sorts of dilemmas.

Leo: Absolutely. And this is right on the hot border between politics and technology right now. So these things do need to be addressed. Sounds like you come down, and I think I agree with you, strongly on the side of freely available crypto. It does make it really hard for police agencies. And I don't know what the answer is to that, I really don't.

Steve: Well, you know, my feeling has always been, the one lesson we learn and we see over and over is you cannot legislate against technology. You know, technology is a force of nature. I mean, literally it is. But it's something you can't say, oh, this exists, but we don't want you to use it or to do it. I mean, well, sorry, but it exists, and so we're going to. And you've raised a really interesting point that I think is a great topic for this first podcast on crypto, and that is, how do we know the government can't listen in on things? We ought to talk about it now, and then we'll talk about the math and the way the stuff works in following weeks. But what is so cool about contemporary cryptography is that there is no hocus-pocus. There is nothing unknown about the way it works. We're not requiring any sort of, like -remember the classic cartoon where there's a blackboard, and a professor is jotting down all these super fancy formulas and equations and things and gets the whole board filled, and it looks like he runs into a dead end or something and gets stuck. And so he writes down on the blackboard, "...and then a miracle happens."

Leo: E=MC2. Amazing. Exactly.

Steve: And so what's so cool about modern cryptography is that we know exactly how it works, and we know why it cannot be cracked. Now, there are some assumptions that crypto is based on. For example, it's based on - some crypto, very popular crypto, is on the incredible difficulty of factoring because no one has ever been able to figure out a way to factor really big numbers fast.

Leo: So if a big number is the product of two primes, it's very difficult to find those two primes; and those, in fact, end up being the keys. Is that correct?

Steve: Right. You use two really large prime numbers, and you multiply them. So now you've got basically a number twice as long as either of those. And it turns out that it is just mathematically incredibly difficult. I mean, and the beauty is, now, all these academicians, super powerful mathematicians who we have to presume are as good as anyone the NSA or any other government security agencies have, cannot come up with a way of reversing that process. So in general, crypto is about some so-called "one-way functions," things that are easy to do in one direction that you just - you can't undo that in any reasonable amount of time. Now, and so the beauty is that the strength of the crypto is solely the infeasibility of mathematically doing something. And everybody in the world has pounded on it, trying to come up with a way to, like, you know, test it and see if there's a way of beating it. So we can presume that unless there's like, for example, the NSA actually did have some means for reversing this process that no one believes they have - and they're probably really pissed off right now that they don't have some way of doing that - then crypto is secure.

Leo: I can't help but think that there's somebody listening to this deep within the recesses of Fort Meade...

Steve: Giggling?

Leo: Giggling, smiling a big grin, saying, well, what you don't know won't hurt you.

Steve: Or kind of looking at his buddy in the other cubicle, giving him a thumbs-up.

Leo: Do you think? I mean, there really is no evidence that this has ever been solved. And it would be - mathematically it would be a big deal.

Steve: Well, yes. It would basically - the prime factorization problem is the foundation of one class of crypto. It's the way a lot of our public key technology works that we'll be explaining in detail in a couple weeks. So that would just collapse if this prime factorization problem were solved.

Leo: It's not that it can't be done, it's just that it takes such a long time that it's not feasible.

Steve: Well, it's that no shortcuts have been found.

Leo: Right, right. Again, that we know of.

Steve: Well, exactly. No shortcuts have been found that anyone knows of. And only very clever approaches that still involve lots of brute force processing is the only way that people have been able to deal with this. So, for example, people have, you know, cryptographers have said, okay, the problem is this hard. So the NSA would have to have, or a government agency like with government-level funding...

Leo: The Soviets.

Steve: Exactly, well, they would have to have a computer that was able to do this much work in this much time, that would be this big, that would cost this much in, you know, in 1990, and it would cost this much in 2000, and this much in 2010. So, I mean, the crypto people have got curves and charts that show the rate of processing growth against all the best methods known of cracking this stuff and saying that that means that a key of this length is this secure, that it would take a machine of this much power, this many centuries, in order to crack the key, knowing everything we know now. And then they extrapolate into the future the rate of processing growth and so forth in order to say, okay, nobody is going to figure out your credit card number.

Leo: I suppose. Although, as in "Fallen Dragon," at some point there will be, you know, enough processing power somewhere to crack all this, and we'll have to come up with something new.

Steve: Well, it certainly is a matter of processing power. That is to say, the goal that you're trying to achieve, for example, in this one instance of prime number factorization, the goal is well known. It's like, here you have this really large number, and you know for sure that it's the product of two primes. So it's not like you don't know how to crack it, it's just that you can't. And again, that's the beauty of modern cryptography is it relies not at all on obscurity.

Leo: Right.

Steve: All of this has been published in mathematical journals. One of the constant background projects is prime number factorization. The world's best math genius guys, you know, cut their teeth early in their careers on prime number factorization to see if they can come up with some way that no one else has thought of. And, I mean, it's incredible what amount of science and math has been applied to this, and it isn't budging. It is holding solid. No one has made any substantial progress in decades. So, I mean, it really looks like this is a problem that, no matter how clever you are, can only be attacked with brute force. And so we know what brute force requires in terms of processing, given all the cracking technologies that have been put together. And so we can say, okay, if a government-level processing power worked on this thing for a thousand centuries, they would be able to crack it. But by then it would have zero value.

Leo: Let's talk a little bit about how crypto is used because, I mean, when you say "crypto," of course you assume that what we're talking about is taking an email message, scrambling it so it can't be read by anybody but the intended recipient. But it's really used for many, many more things than that.

Steve: Well, for example, we were just talking about HotSpotVPN or OpenVPN using crypto just because we want to make sure that no one in the local environment could be sniffing our network connection and know what we're doing. And as we all know, whenever we're entering our credit card information, crypto is used only between the client browser and the ecommerce server, just as it crosses the Internet. As soon as it gets to the server it's decrypted back into plain text, as it's called, so that the ecommerce server is able to process our credit information.

Leo: Does digital rights management also rely on crypto?

Steve: Oh, yeah, yeah. Basically they're trying to do things which a consumer will not have the information to undo. I mean, I'm skeptical about any form of DRM standing the test of time. The problem is that you need to, for DRM, you need to put into the end user's home a device which itself is able to decrypt the content.

Leo: Otherwise you wouldn't be able to play it.

Steve: Yeah.

Leo: Your DVD player knows how to decrypt a DVD. It has it built in.

Steve: It has to in order to give you back the original picture. And so their solution is, now there's all this, you know, the HDCP technology trying to push the crypto all the way out to the display device so that you can't capture the signal going from the DVD player to your screen. But still the projector or the TV set, it has to know how to decrypt this. And there are lots of smart people in the world, and lots of reverse engineers. And there are people who are going to be annoyed by the entertainment establishment trying to basically protect the entire channel right up to your retinas.

Leo: Crypto is also used, as I mentioned, in digital signing. It's not used - in digital signing it's not used to hide text, but it's used to validate text. Is it the same kind of crypto?

Steve: To authenticate, yes.

Leo: To authenticate, yeah.

Steve: Authentication is a really interesting branch and is something we will be talking about here in the next couple weeks because, exactly as you say, the idea is that you want to sign a document. You can leave it in plain text. But you want to come up with a way of verifying two things: You want to verify with signing that no alteration has occurred to the document from the time it was signed by its author; and you want to also verify that it actually was created and signed by the person who you believe it was. And so it provides that level of sort of an envelope around the document which anyone can read, but nobody can modify, and no one can forge the signature of the document.

Leo: So it's pretty widely used in a lot of different areas. Any other areas that we may not know about that crypto is in use? I'm trying to think. Copy protection. Encryption, of course. Digital signing and authentication. It's used in Voice Over Internet or any kind of transaction over the Internet like secure transactions on your credit cards or VPNs.

Steve: Well, and of course, you know, people who are doing for-pay TV delivery, either cable boxes or satellite, they're also using crypto...

Leo: Sure.

Steve: ...in order to protect their channel so that only users who are paying for their services are able to receive them.

Leo: Video on your TiVo is encrypted so you can't steal it.

Steve: And in fact that's another - the satellite or the cable box is another example of content providers trying and failing, again, to protect their content because there's all kinds of satellite and cable box, you know, decloaking and hacking and content-stealing technology around because it's virtually impossible, I would say, to protect something all the way to the end of the channel. And in fact, one thing we haven't talked about, Leo, and this is a perfect answer to your question is, as we know, Microsoft Windows and Intel are moving crypto into the platform so that there will be technology in every single next-generation PC which will be involved in giving the operating system and the hosted software a tighter grip over what the end user is going to be able to do.

Leo: And that's controversial on both sides. The government doesn't like it because they want a backdoor. And consumers don't like it because it builds DRM into the system.

Steve: Yeah. I mean, it really is a war of rights.

Leo: Yeah. Fascinating stuff. There have been many great books written on cryptography. It's a field that has been important in so many ways, from Napoleon's army to the Enigma during World War II. and of course now to PGP and the politics of terrorism. So this is going to be a great subject. How many episodes are we going to devote to this?

Steve: I think probably about four, actually. We're going to start with how the not-so-secret decoder rings work next time, which is a perfect intro to symmetric cryptography. We're going to talk about symmetric ciphers next week, then asymmetric ciphers the week after. Then probably hashes and how signing works, and then sort of put all these pieces together because what's so cool is these are some very clear and easily understood building blocks that you can then literally assemble in different ways to perform really cool and very different sorts of jobs in crypto. So it's going to be neat.

Leo: Good. Steve Gibson, always a pleasure. I know there will be great interest in this. And more and more I'm hearing from people who are saving the shows and sharing them with other people, people who are in the field who use it for education; people who are not in the field but want to be in the field and are learning more; and a lot of people who understand security but want their friends, family, and co-workers to understand it a little bit better, too. So you're doing a great job, and we thank you for your hard work.

Steve: Glad to do it, and we'll talk to you next week.

Leo: All right. Everything is online at GRC.com/securitynow.htm. That's where Steve keeps the transcripts for this, thanks to Elaine, who types this up with her little fingers as quickly as she can right after we finish the podcast.

Steve: By the way, I got a little note from her this morning because the weather is looking pretty bad where she is in California. She may be - she wasn't sure, if she lost her satellite uplink, whether she'd be able to get the transcripts on time. But she said she stayed up too late last night almost finishing "Fallen Dragon."

Leo: Oh, she's reading it.

Steve: Yeah, I sent her a copy.

Leo: I can't stop. You're a pusher. I can't stop. It's getting very exciting right now.

Steve: Very cool.

Leo: It really is, yeah. If I didn't have so many darn podcasts to do, I'd be finished. By the way, while you're there, there's also a 16KB version of the show, 16kbps, so that, if it's too big a download for you to get the full-quality version, get the low-quality version, that's fine. And show notes with lots more information and links in a place where you can give Steve some feedback, great forums. It's all at GRC.com. That's where you'll find SpinRite, as well. That's the program that makes this all possible, Steve's disk maintenance and recovery utility, guarantee you the best one in the business.

Steve: I think it is.

Leo: If you can't recover it with SpinRite, you can't recover it with software, that's for sure. GRC.com. Hey, thank you so much, Steve, we really appreciate it. Don't forget, folks, if you like the show - somebody asked me this, and I want to kind of underscore it. They said, well, I've donated to TWiT. Does that count donating to Security Now!? Absolutely. But if you haven't donated, and you listen to any of the podcasts on TWiT.tv, your donation would very much be appreciated. It certainly helps us keep doing these kinds of things. It pays for our bandwidth, our server costs, our site redesign, all the expenses, equipment expenses and so forth. You can find the Donate buttons at TWiT.tv. Steve Gibson, we'll see you next week for more on crypto - Crypto 102, I guess we'll call it.

Steve: Yeah. And we want to remember to thank AOL for...

Leo: I almost didn't, didn't I. Thank you. I don't want to get them mad at us because, gosh, they push a lot of bandwidth for us at AOL Podcast Channel. We broadcast this show, by the way, at AOL.com/podcasting, and that provides us the bandwidth for the show. Steve, thank you for reminding me.

Steve: No problem.

Leo: Have a great week.

Steve: Talk to you next week.

Copyright (c) 2006 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/