CryptoSystem Backdoors

Description: Steve and Leo discuss the deeply troubling recent news of possible legislation that would require all encrypted Internet communications, of any kind, to provide a means for U.S. law enforcement "wiretap" style monitoring.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-268.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-268-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 268, recorded September 29, 2010: CryptoSystems Backdoors.

It's time for Security Now!. Ready to get, prepared to get protected on the Internet? Let's do it. Steve Gibson is here. He is our host and the guy in charge at the Gibson Research Corporation, GRC.com, author of SpinRite, the world's best hard drive maintenance and recovery utility, but also the first antispyware. He's a big security guru, and we're so glad to have him in our fifth year of protecting you online. Hey, Steve.

Steve Gibson: Actually, sixth year.

Leo: Going in, yeah, we've completed five.

Steve: Yeah.

Leo: So in our sixth year.

Steve: In our sixth year. Hi, Leo. Well, I'm a little depressed this week.

Leo: What? No, Steve.

Steve: Yeah, I am.

Leo: Why?

Steve: Well, I mean, I always recover from these things. But I actually had a hard time sleeping Monday night because of some news that was reported in The New York Times, which is what was so disturbing about the current administration's intention to submit to Congress, as soon as it comes back in session after the new year, after the midterm elections, under apparently pressure from the FBI, to cause backdoors to be installed in all cryptographic communication systems on the Internet so that law enforcement - under court order, but still - has the ability to break the encryption.

Leo: Well, we've seen in the past how much government has, how much regard for subpoenas and warrants. So that's really bad news. Because once that's in, then you have weak encryption.

Steve: Well, and it won't work. I mean, the horses are out of the barn.

Leo: The bad guys will always have good encryption.

Steve: Yes. Good encryption, perfect, bulletproof, uncrackable. It's all out there. It's all open source. Everyone knows how to do it. So what it will do is it will create an underground of communication systems which still cannot be cracked, which the bad guys will use. Meanwhile, commercial products, I mean, I'm directly affected by this because of CryptoLink and my plans to do a Trust No One VPN. I mean, that's why I couldn't sleep Monday night. It's like, no.

Leo: Oh, man.

Steve: I mean, this is really bad.

Leo: Well, we're going to talk about this.

Steve: Yup.

Leo: This is of course a very good subject. And it's not the first time this has come up. Maybe we can do something about it, too. But this is a good subject for us.

Steve: Yup. We're going to talk about it. We do have security updates and news that I think everyone is going to find interesting. A new, well, first, the problem we talked about last week, the zero-day flaw which was causing all of the ASP.NET web developers to scrambled around - remember, that's the one where it was discovered being exploited that by probing a website - and Microsoft admitted that this affected millions of websites. By probing a website with incorrectly encrypted replies, the way the website's error responses, the error pages came back, gave up information about the crypto, the specific

crypto key that was in use, which allowed then bad guys to successfully crack the crypto on those sites in order to reveal usernames and passwords and get into encrypted sessions. So the short-term fix was - and this was what Microsoft's formal recommendation was, is don't ever give any different error messages. Like, consolidate all possible errors into just a simple 404 sorry-that-didn't-work error in order to prevent this information leakage.

Well, the problem was bad enough that Microsoft did an out-of-cycle update. And Tuesday of this week many people noted that, whoa, wait a minute, this is not the second Tuesday of the month. That was last Tuesday. And but sure enough, Microsoft said we've got to get this thing out because it was being used in targeted attacks. So that happened. And people who are XP SP3 and later all received that update for all versions of Windows and .NET that were affected. So that happened, and it's good. Unfortunately, we have a new zero-day vulnerability.

Leo: Oh, geez.

Steve: In Windows. Just can't get away from those. That seems to be happening more and more now. This is the ActiveX object which is in a DLL, msnetobj.dll. That contains the code which Microsoft uses with their digital rights management technology to obtain a license. And unfortunately it's been found - in the wild again, being exploited - that that DLL contains multiple remotely exploitable vulnerabilities such that a user simply enticed into visiting a malicious web page can have arbitrary code downloaded and executed on their machine. Microsoft has acknowledged this, confirmed that it's a problem, but we don't have an update yet. And not, I mean, this just happened, so not even any timeframe or anything. It's not clear yet how widespread this is. But it was found in the wild happening. And so there's a URL which - it's a URL-triggered exploit. So a website knows how to malform its reply to this DRM DLL in a way that allows it to send code to people's machines. So here, get one more way into Windows, that we're learning about only because we're seeing it being actively exploited.

And also just last week we were talking about the leakage, the confirmed leakage from Intel, essentially, Intel's technology which they license, the HDCP, High Definition Content Protection, which is used for essentially content in motion over cables and things, not stored on the disk. Blu-ray technology uses a different encryption. But once it's out there, essentially what Intel wanted was something that was very fast to implement in hardware so that it would give you security, but you didn't need a big, powerful, number-crunching processor to do it. So they wanted to be able to, like, sort of quickly stream this around and, yet, as it moves across interfaces in one's, like, entertainment system, or even inside of a computer, at no point would the content be - could you find a place you could tap into it in order to get it in plaintext form.

Well, already there is software on the 'Net which works. The website is www.cs.sunysb.edu/~rob/hdcp.html. And from his documentation on that site, he says, "The HDCP cipher is designed to be efficient when implemented in hardware. But it is terribly inefficient in software, primarily because it makes extensive use of bit operations. Our implementation uses bit slicing in software to achieve high speeds by exploiting bit-level parallelism. We have created a few high-level routines to make it as easy as possible to implement HDCP as shown in the following example." And then the source code for this can be downloaded.

And he did some benchmarks on his software. It is able to process 640x480 pixel frames using only a single core. He has a benchmark with a Xeon 5140 running at 2.33GHz, and

it's able to successfully, that is, all software is able to successfully process 181 frames per second at 640x480 resolution. A Core2 Duo P9600 running at 2.53GHz is able to process 76 fps, still faster than real-time, so that's fine, although it's a small frame, of course, 640x480. And then he says decryption of 1080p content is about seven times slower. But decryption can be parallelized across multiple cores. So a high-end 64-bit CPU should be able to decrypt 30 fps, 1080p content, using two cores, and about 1.6GB of RAM.

So the fact that they're using that much RAM tells me that what he's done is he's basically created a table-based system where he's using precomputed results of bit-twiddling. See, when he talks about the problems of doing this in software, we know from our series on how computers work that there are some things that software instructions were designed to do. But it turns out that programmers typically don't have a great need for bit-level operations. They exist, but you can't do many things at once. You have to sort of like test each bit individually and make decisions.

Well, you probably want to do that all at once. So table lookup approaches is a way of getting around that. You trade the lack of instructions for building tables once in memory and then just referencing table entries to sort of give you the result of many operations with a single reference to memory. So I would imagine that's why he needs 1.6GB of RAM. And of course what this means is, as I also said last week, there will be hardware to do this in no time. I mean, now here we have a software implementation, someone who's just a hobbyist can take a field programmable gate array and say, hey, I'm going to put this into hardware. It'd be fun. And I'm sure it'll happen.

Leo: Wow. Didn't take very long.

Steve: It didn't.

Leo: What was that, a week?

Steve: And, see, that's, frankly, it's one of the things that I love about the 'Net is that's the way the 'Net is. Here's some guy, and what, SUNY SB is...

Leo: State University of New York.

Steve: New York, yeah.

Leo: I don't know where SB is [Stony Brook], but...

Steve: Yeah. And I appreciate that this, I mean, this is the spirit of the Internet. And we're going to be covering some stories here shortly which demonstrate that this is under threat, essentially, which is, I think, really too bad.

So I've avoided drawing conclusions so far about whether the Stuxnet worm - which we've discussed on several occasions, which has been around for a long time, and we've talked about it because it won't go away - whether it's targeted at Iran. The problem is

there isn't any way to know for sure. And I'm reluctant to draw conclusions that a lot of the press, like can you say theregister.co.uk, who delight in this kind of spectacle, are drawing. We know more than we did before. And still it's a maybe. Maybe it's a stronger maybe than before. But Iran has disclosed that about 30,000 IP addresses within their country have been infected by Stuxnet. But it's a Windows-carried worm. And remember that it was found to already have in it four different zero-day Windows exploits. So the developers are extremely good. The other speculation being made, which again, all it is is speculation, is that people who have studied it are so impressed by it that they're saying this has to be state-sponsored malware, that is...

Leo: Oh, boy.

Steve: Yeah. And so...

Leo: We've been waiting for this kind of thing.

Steve: Yeah.

Leo: But if you think about what they're attacking, it kind of makes sense.

Steve: Well, yes. The speculation - again, that's all it is - is that the Bushehr nuclear reactor, which is about a few weeks to go online, a few weeks away from going online...

Leo: There are quite a few people, not merely Israel, but there are quite a few people who would like that not to go online.

Steve: Yes. Yes. So it's a big event. And some UPI photos, UPI press posted some photos of the inside of the reactor control area that showed that it was the Windows-based, Siemens-based PLC, which is precisely what this worm targets.

Leo: Right, right.

Steve: Last week there was a really good expert on industrial control systems, Ralph Langner, who published an analysis of the worm. He said that this is a thing that specifically targets Siemens software systems, industrial control systems. He suggested that it may have been used to sabotage Iran's nuclear reactor. Langner is a Siemens expert who simulated a Siemens industrial network, then analyzed the worm's attack. And I'm reading from one of the online reports. It said one of the things that Langner discovered is that when Stuxnet finally identifies its target, it makes changes to a piece of Siemens code called Organizational Block 35. I love that. It'll be the name of a movie one of these days, Organizational...

Leo: OB35.

Steve: OB35. This Siemens component monitors critical factory operations, things that need a response within 100 milliseconds. By messing with Operational Block 35, Stuxnet could easily cause a refinery's centrifuge to malfunction, but it could be used to hit other targets, as well. And this is somebody else quoting, said, "The only thing I can say is that it is something designed to go bang."

"Whoever created Stuxnet also employed four previously unknown zero-day attacks and a peer-to-peer communications system, compromised digital certificates," as we know, "belonging to Realtek Semiconductor and JMicron Technology" - we talked about how, coincidentally, or maybe not, they were in the same office park - "and displayed extensive knowledge of industrial systems." Still reading, "This is not something that your run-of-the-mill hacker can pull off. Many security researchers think that it would take the resources of a nation state to accomplish" this.

Leo: Aha.

Steve: So again, speculation. I've avoided it until now. But I thought we have to talk about it.

Leo: Can I say this is better than a bomb? This doesn't kill anybody. And if it takes the plant offline, yay.

Steve: Yeah, well, yeah. I mean, we - yeah. Potentially, yeah.

Leo: Yeah, I mean, come on.

Steve: Yeah. I mean, the expectation is this is not for energy generation, this is for bomb-making, fuel...

Leo: Right, uranium enrichment, yeah.

Steve: Yes.

Leo: Now, we don't know. And if it's just a power plant, that's a shame. But everybody seems to agree that that's not what's going on. Unfortunately, well, unfortunately or fortunately, this probably isn't a long-term hack; right? I mean, this is just a - this is just a road bump.

Steve: The jig is up now. I mean, Organizational Block 35 will be protected. They will make sure, I mean, Iran said this thing did not get into the reactor. It's crawling around all over outside, but it didn't get in. So, I mean, if that was its intent. We just, again, it got in many other places that had Organizational Block 35 altered also. So again, it's just you can't say that was - no one knows that was the target. But it qualifies. And it's certainly high profile, which is really the only reason it all comes up.

Leo: And Dr. Mom and some others in the chatroom are saying, well, this could have, I mean, if it had caused a meltdown, it could have had horrendous, disastrous impact, worse than bombing it, maybe. So I shouldn't say it's better than bombing.

Steve: Speaking of which, rapidly making its way through the Senate is a bill which many people are upset about. It's called the "Combating Online Infringements and Counterfeits Act."

Leo: Don't get me started.

Steve: I know. COICA. People who want to read about it can look - the EFF.org site has it. And the URL that I have here in front of me is wrong, but it's just www.eff.org/coica, which has a bunch of resources. Here's the deal. And this is why people are so upset. It is a law which, if passed, and it's in the process of being passed, apparently, or getting ready to be, "making its way through the Senate" is the quote, it creates two new U.S. Attorney General-controlled DNS blacklists - it's the first time we've ever had anything like that in the U.S. - which would be required by law to be enforced by ISPs and domain registrars. The reason there's two lists, one you have to follow; the second you are strongly encouraged to follow, but it isn't - you're not breaking the law as an ISP or a domain registrar if you don't.

So what we're talking about doing is, for the first time ever, empowering the U.S. Attorney General to censor the Internet for everyone in the U.S., so that domains that exist we would not be able to find. We would put them in, and it's not even clear what we would get - a redirect or a 404 page doesn't exist error, it's not clear what would happen. But citizens of the United States would be unable to go to pages, domains, that were on this list. And as you can imagine, I mean, this is a dramatic change. This is all of the Internet no longer being available.

And I was just, as I was putting this report together and, for example, had that page showing the HDCP software decryption, I mean, this is the freedom that the Internet has created. And we're talking about maybe sites like RapidShare and quasi-legitimate sites that somebody somewhere decides that this is - no doubt driven by the MPAA, our Motion Picture Association, another...

Leo: Oh, yeah, and RIAA and all those groups, yeah.

Steve: Exactly. And they're just saying, oh, yeah, we need a way to take these sites down. The problem is, there are already legal means for dealing with this kind of online technology, online content that people want to bring down. There are processes for allowing our legal system to go and do takedowns.

Leo: That's what's wrong with this. It kind of bypasses due process. That's what in my opinion is wrong with it.

Steve: Yes, exactly. And you can imagine, over time, it'll get easier to put sites on this list. It'll be like, wow, this works really well. Let's expand this a little bit.

Leo: Well, as the EFF has pointed out, every new technology has been fought as copyright violations by rights holders, including VCRs, player pianos. We wouldn't have them if this law had been in effect in 1920. So one thing we know for sure is people who own rights today are not the best people to ask when it comes to what the future is going to look like. And giving them this kind of power is just a bad idea. Not, you know, it's not like you and I are pro-piracy. That's not what's going on here.

Steve: Absolutely. Of course not. I mean, I'm a publisher of intellectual property. I make my entire living on the fact that people honor my copyrights. And I respect their purchases. I don't do anything to keep them from copying the product. I just hope they won't.

Leo: Well, and this is funny, I think really this is where education is going to help. There is still this stupid notion, and we're going to - it also applies to the backdoors that we're going to talk about later in the show...

Steve: Oh, yeah.

Leo: ...that this kind of stuff hurts bad guys. It doesn't. Bad guys get around this stuff routinely. It only impinges on honest people. And that's what's really crazy about this stuff.

Steve: And Leo, this isn't what the country, this isn't what the United States has stood for.

Leo: No.

Steve: Since its founding, since it was founded. I mean, it's just...

Leo: It's a shame.

Steve: The idea that we would be in a country that doesn't let us go to some domains where people outside the U.S. - I mean, we invented the Internet - people outside the U.S. are able, with their DNS servers, to get to sites here that we can't.

Leo: And again - correct me if I'm wrong, but it does seem to happen - without due process.

Steve: Yes. And it will not work. That's the other thing. There will be ways around it.

Leo: Pirates will get around it, of course.

Steve: Yeah. I mean, I would immediately do something to get around it, if it weren't illegal to do it, and I'm sure it would be. So I'm proscribed from doing that.

Leo: So guess who gets around it? Crooks.

Steve: Yeah.

Leo: Honest people who obey the law are the ones who are hurt by this.

Steve: Well, and you end up with cat and mouse, too. You end up with those sites that are blacklisted register under a different name. And for a while they're there, until the blacklist catches up with them. And then they move again. I mean, the whole thing is just brain dead. It makes no sense. But we have a problem, and that is that we're dealing with technology that the legislatures probably don't understand. And who knows what the unintended consequences are going to be. But the idea that we're facing state-sponsored censorship of the Internet...

Leo: Welcome to China, folks.

Steve: Exactly. It does give us pause. And unfortunately, it's driven by commercial interests.

Leo: Of course.

Steve: I mean, that's what's behind this is commercial interests.

Leo: It's not in the public interest.

Steve: No. I saw somewhere, and I couldn't find it again, I just wanted to mention this because we've talked about it a couple times, the judgment came down about the school district that was spying on students who took school laptop property home whose administrators had installed some webcam-based technology. Remember that some parents were suing the school because their son or daughter were being spied on, and one of the teachers confronted them with a photo of them in their...

Leo: Eating candy.

Steve: Eating candy in their bedroom, saying that this is not conduct becoming a student.

Leo: You're popping pills.

Steve: Anyway, the charges were dropped...

Leo: Oh, no. What?

Steve: ...against the district, saying that there was no malicious intent.

Leo: Oh.

Steve: So the prosecution was unsuccessful.

Leo: Wow. That's kind of stunning.

Steve: I know. I saw it, and I just thought, oh, well, who knows. Somebody had a good defense attorney and managed to get these people off, so...

Leo: It's tough to sue government agencies. In many cases it's illegal, or you can't. And I think judges almost always are going to err on the side of caution there, so...

Steve: Yeah.

Leo: I guess the judge deemed that no criminal activity occurred.

Steve: Right. Well, and I hope that - this got a lot of press. And I hope that lessons were learned, even if...

Leo: Exactly. I think that's the case.

Steve: Yes. It's hard to imagine that lessons were not learned.

Leo: I don't think there's many schools will do that again.

Steve: No. It really did get a lot of noise. So that's good. I have no errata, and just a short little SpinRite note from a happy user, because we have got a lot of content to cover. It was just an email we received with the subject of "Testimonial." And Bill Pomeroy wrote, he says, "I've owned a copy of SpinRite 6.0 and its earlier cousins since their birth." So 20 years. "Fortunately, I haven't had to rescue any of my hard drives during all that time, until yesterday. SpinRite was just one of those must-have programs

that I kept at hand. Yesterday

Win XP SP2" - oh, good for you, Bill, you're still where I am - "on boot would only blue screen. Chkdsk /f and /r produced only more blue screens. I inserted my bootable SR 6.0 CD, and after completing a Level 2 procedure I was back in business. I don't know how much I've spent on SpinRite over the years, but whatever it was, yesterday made it all worthwhile."

Leo: That's so great.

Steve: "Thank you, SpinRite."

Leo: That is a nice story.

Steve: Neat story.

Leo: We are going to talk about backdoors in cryptosystems and why the federal government is going after it.

Steve: Yup.

Leo: It's not the first time, and I suppose it won't be the last time. But this is one we want everybody's who's listening, who understands the issues, and that's the key, to listen, to understand it better, and then go fight this. But we'll talk about it in just a second. This is just, oh, I'm so glad you're covering this, Steve. All right, Steve. Take a deep breath.

Steve: Yeah. Okay. So let me start by reading a quote from the then-director of the FBI, Louis Freeh, back in 1997, who was speaking before a Senate Judiciary Committee and said: "For law enforcement, framing the issue is simple. In this time of dazzling telecommunications and computer technology, where information can have extraordinary value, the ready availability of robust encryption is essential. No one in law enforcement disputes that. Clearly, in today's world and more so in the future, the ability to encrypt both contemporaneous communications and stored data is a vital component of information security.

"As is so often the case, however, there is another aspect to the encryption issue that, if left unaddressed, will have severe public safety and national security ramifications. Law enforcement is in unanimous agreement that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism. Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes. For this reason, the law enforcement community is unanimous in calling for a balanced solution to this problem." So that was 13 years ago.

Leo: Oh, really. Oh, wow.

Steve: 13 years ago. 1997. What happened on Monday was that Charlie Savage, who reports for The New York Times, wrote a story whose headline was "U.S. [Tries] to Make It Easier to Wiretap the Internet." And I'm going to read this:

"Federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is 'going dark' as people increasingly communicate online instead of by telephone." Because of course they've got the telephone wiretapped already. "Essentially, officials want Congress to require all services that enable communications including encrypted email transmitters like BlackBerry, social networking websites like Facebook, and software that allows direct peer-to-peer messaging like Skype to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.

"The bill, which the Obama administration plans to submit to lawmakers next year, raises fresh questions about how to balance security needs [with] protecting privacy and fostering innovation. And because security services around the world face the same problem, it could set an example that is copied globally. James X. Dempsey, vice president [of] the Center for Democracy and Technology, an Internet policy group, said the proposal had 'huge implications' and challenged 'fundamental elements of the Internet revolution,' including its decentralized design. 'They [are really] asking for the authority to redesign services that take advantage of the unique, and now pervasive, architecture of the Internet,' he said. 'They basically want to turn back the clock and make Internet services function the way ... the telephone system used to function.'

"But law enforcement officials contend that imposing such a mandate is reasonable and necessary to prevent the erosion of their investigative powers. 'We're talking about lawfully authorized intercepts,' said Valerie E. Caproni, general counsel for the Federal Bureau of Investigation. 'We're not talking expanding authority. We're talking about preserving our ability to execute our existing authority in order to protect the public safety and national security.'

"Investigators have been concerned for years that changing communications technology could damage their ability to conduct surveillance. In recent months, officials from the FBI, the Justice Department, the National Security Agency, the White House, and other agencies have been meeting to develop a proposed solution. There is not yet agreement on [some] important elements, like how to word statutory language defining who counts as a communications service provider, according to several officials familiar with the deliberations. But they want it to apply broadly, including to companies that operate from servers abroad, like Research in Motion, the Canadian maker of BlackBerry devices. In recent months, that company has come into conflict with the governments of Dubai and India over their inability to conduct surveillance of messages sent via [BlackBerry's] encrypted service.

"In the United States, phone and broadband networks are already required to have interception capabilities, under a 1994 law called the Communications Assistance to Law Enforcement Act (CALEA). It aimed to ensure that government surveillance abilities would remain intact during the evolution from a copper-wire phone system to digital networks and cell phones. Often, investigators can intercept communications at a switch operated by the network company. But sometimes like when the target uses a service that encrypts messages between his computer and its servers they must instead serve

the order on a service provider to get..." an unscrambled version.

"Like phone companies, communication service providers are subject to wiretap orders. But the 1994 law does not apply to them. While some maintain interception capacities, others wait until they are served with orders to try to develop them. The FBI's operational technologies division spent $9.75 million last year helping communication companies including some subject to the 1994 law that had difficulties do so. And its 2010 budget included $9 million for a 'Going Dark Program' to bolster its electronic surveillance capabilities. Beyond such costs, Ms. Caproni said, FBI efforts to help retrofit services have a major shortcoming: the process can delay their ability to wiretap a [suspect] for months. Moreover, some services encrypt messages between users, so that even the provider cannot unscramble them. There is no public data about how often court-approved surveillance is frustrated because of a service's technical design.

"But as an example, one official said, an investigation into a drug cartel earlier this year was stymied because smugglers used peer-to-peer software, which is difficult to intercept because it is not routed through a central hub. Agents eventually installed surveillance equipment in a suspect's office, but that tactic was 'risky,' the official said, and the delay 'prevented the interception of pertinent communications.' Moreover, according to several other officials, after the failed Times Square bombing [in] May, investigators discovered that the suspect, Faisal Shahzad, had been communicating with a service that lacked prebuilt interception [capacity]. If he had aroused suspicion beforehand, there would have been a delay before he could have been wiretapped.

"To counter such problems, officials are coalescing around several of the proposal's likely requirements: [1] Communications services that encrypt messages must have a way to [unscramble] them; [2] Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts; and, [3] Developers of software that enables peer-to-peer communication must redesign their service to allow interception. Providers that failed to comply would face fines or some other penalty. But the proposal is likely to direct companies to come up with their own way to meet the mandates. Writing any statute in '[technologically] neutral' terms would also help prevent it from becoming obsolete, officials said." Which is to say, make it broad.

"Even with such a law, some gaps could remain. It is not clear how it could compel compliance by overseas services that do no domestic business, or from a 'freeware' application developed by volunteers. In their battle with Research in Motion, countries like Dubai have sought leverage by threatening to block BlackBerry data from their networks. But Ms. Caproni said the FBI did not support filtering the Internet in the United States.

"Still, even a proposal that consists only of a legal mandate is likely to be controversial, said Michael A. Sussmann, a former Justice Department lawyer who advises communications providers. 'It would be an enormous change for newly covered companies,' he said. 'Implementation would be a huge technology and security headache, and the investigative burden and costs [will] shift to providers.'

"Several privacy and technology advocates argued that requiring interception capabilities would create holes that would inevitably be exploited by hackers. Steven M. Bellovin, a Columbia University computer science professor, pointed to an episode in Greece" five years ago: "In 2005, it was discovered that hackers had taken advantage of a legally mandated wiretap function to spy on top officials' phones, including the prime minister's. '...[I]t's a disaster waiting to happen,' he said. 'If they start building in all these backdoors, they will be exploited.'

"Susan Landau, a Radcliffe Institute of Advanced Study fellow and former Sun Microsystems engineer, argued that the proposal would raise costly impediments to innovation by small startups. 'Every engineer...'"

Leo: Like you.

Steve: Yeah, like me. "'Every engineer who is developing the wiretap system is an engineer who is not building in greater security, more features, or getting the product out faster,' she said. Moreover, providers of services featuring user-to-user encryption are likely to object to watering it down." Oh, gee, you think? "Similarly, in the late 1990s, encryption makers fought off a proposal to require them to include a backdoor enabling wiretapping, arguing it would cripple their products in the global market. But law enforcement officials rejected such arguments. They said including an interception capability from the start was less likely to inadvertently create security holes than retrofitting it after receiving a wiretap order. They also noted that critics predicted that the 1994 law would impede cell phone innovation, but that technology continued to improve. And their envisioned decryption mandate is modest, they contended, because service providers not the government would hold the key."

This is the final line: "'No one should be promising their customers that they will thumb their nose at a U.S. court order,' Ms. Caproni said. 'They can promise strong encryption. They just need to figure out how they can provide us plain text.'"

Leo: Yeah. It's called a paradox. An oxymoron.

Steve: So here's the problem. First of all, I mean, we can all sympathize with law enforcement's dilemma because everything that Louis Freeh said 13 years ago is coming to and has come to pass. Skype's encryption is very good. They did it right. And how many times have we talked about the fact that encryption technology today is done?

Leo: Right.

Steve: I mean, it's bulletproof. We have Rijndael running with a 256-bit key that is a simple mathematical algorithm, and we have no means - none - for cracking it. It is uncrackable. Now, the problem is, and we said this a little bit at the top of the show, is this is too late. I mean, I completely sympathize with what law enforcement wants to do, with the dilemma they have. But this technology exists. It is in the public domain. It is in open source tools all over the world. It's already escaped. And there's nothing they can do about it.

And so here I am, looking at my next product, CryptoLink, that I've talked about often, which, I mean, I have a design. It's laid out. I'm going to talk a little bit about it because we'll talk about what it means to put a backdoor in something like this. But, now, one of the things I was proudest about is that CryptoLink would have an open protocol - I mean, the code itself is going to be mine, closed; but the protocol that it implements is going to be published and open and subject to peer review. I want that. So that guys who have more of an attack mentality than the guy who invented it here mentality can look at it and say, this really looks good, I mean, it's so simple. And it's like, yes, I know, it's really simple. And the simpler it is, the more easy it is to know that it's secure.

And so what does this mean? Does this mean that the FBI would capture data on the wire, which they cannot read because it's encrypted, and then I guess get a court order, and then bring the data to me with the court order and say, "The law says you must decrypt this for us, this which your product encrypted." Okay, so...

Leo: Well, that's not so bad because then you would have the keys, not them.

Steve: Correct. And that's one of the notes that was in the article that Charlie published says that the individuals would have the keys. So I'm assuming that that's the case. Now, of course, this creates a vulnerability because I could be compelled to decrypt something, not only by court order, but at the point of a gun.

Leo: By a bad guy.

Steve: Exactly. If something is sufficiently valuable, now I'm exposed. And I didn't want that. I mean, I was so jazzed that CryptoLink would be like my ultimate expression of TNO, Trust No One, not even me; I mean, that an individual could rekey their copy of CryptoLink anytime they wanted, and at any time, for whatever reason, and start fresh, and no one would have any knowledge of what their key was. But now...

Leo: How is this different than maybe putting the keys in the hand of the user, and then the court order or the police go to the user and say, well, you've got to give up your keys. Then that leaves you out of it.

Steve: Right. It leaves me out of it. The problem is that, now, let's see, that's just it, is that I was assuming that that scenario I just painted is the way it would work. But it's sounding like maybe the FBI wants real-time monitoring. I mean, maybe they...

Leo: That's what they need; right? They need a hole that they can open and leave open.

Steve: And they're comparing it to the phone system, where they're able to tap somebody's phone. So now they're saying we want to be able to tap somebody's computer.

Leo: Exactly.

Steve: And any dialogue back and forth - and, I mean, they single out peer-to-peer, talking about, you know, Skype. And as we know, Skype is a point-to-point technology. The central server is used for presence establishment, so that you can see your Skype contacts that are online. But the Skype technology is beautifully designed so that it's a point-to-point encryption. So if the FBI is saying that Skype needs to be able, Skype corporate needs to be able to give them wiretapping-class access to Skype communications, well, that absolutely requires a redesign. That's like, okay, now, that

means all of Skype's communications has to go through a central location where it is decrypted, or could be, and made available so that it's no longer point to point.

I mean, if that's what it takes, if that's what this law says, I won't ever write CryptoLink. I mean, that's not what I want to do. I want a point-to-point, VPN-ish-like product. I mean, this legislation is threatening that. It says, as I understand it, that there will be a law, if this horrible thing should pass, which will require wiretap-class access to all encrypted commercial products and software and services. Now, and again, all that does is it creates an underground of TNO technology that I have no interest in developing for bad guys. I certainly would never do that. And I would hate to think that my crypto system would be used by terrorists. But, I mean, that's a problem that technology always creates. Technology is neither good or bad. It's a capability, and it's the application of it which then requires morality and ethics and responsibility. It's always been the case. That's what technology is. So, what do you think?

Leo: Well, as they're saying in the chatroom, and this is quite apt, law enforcement can always propose things that would make their life easier. Random door-to-door searches would make it easier to enforce laws. So that has never been the sole criterion, in the U.S., anyway, for our laws. That's why we have a Constitution. The Constitution protects us against random door-to-door searches very specifically. The interesting issue is there is no right, some say, a right to privacy in the U.S. Constitution. So that's one issue is there isn't any specific prohibition - of course the founders didn't really consider encryption when they wrote the Constitution. So I guess the question is, how far is too far for law enforcement to push it?

Steve: Well, and there's a precedent established already with that CALEA act where we know that, given a court order, our law enforcement is able to tap our phones. They're able to tap phones and cell phones. Cell phones use an encrypted technology which is decrypted for them, so they're able to tap them. Now, I mean, one of the problems is this raises all kinds of interesting practical problems because how does the FBI know, I mean, encrypted communications, as we've often discussed, is pseudorandom noise. How does the FBI know...

Leo: What to listen to?

Steve: Yeah, what software is on a machine? I've done a lot of research over the last couple days, listening to what everybody is saying about this. And as you can imagine, this is a huge kerfuffle. I mean, there's people blogging, their fingers are smoking, they're blogging so fast. I mean, there was more than a thousand articles - I did a search on Google News - a thousand articles that were launched since Monday when this New York Times article came out, and bloggers going crazy. So some of the people have said that law enforcement does have a means to solve the problem, and that's by getting to the endpoints. That is, if they want to monitor someone's computer, they have a means...

Leo: Go to the person.

Steve: Yes, to put some spyware, some legally mandated spyware, and there is such stuff. The FBI has their own spyware, like a keystroke logger and that ilk, which they can

and do currently install surreptitiously in people's machines, after they get a court order to do so, which puts them under surveillance and feeds everything they're doing out the same Internet connection to the FBI. So the person doesn't know. So essentially what the FBI is doing is they're getting all of that before it's encrypted by this suite of now existing crypto-based products. I mean, if mine, if CryptoLink were sitting there on the system, and somebody were using it, all you see, I mean, CryptoLink's data doesn't identify itself. Maybe that's going to be a requirement of the law, that encrypted data have beacons in it, tags.

Leo: [Rumbling]

Steve: No, I mean, think about it.

Leo: Of course. They need to.

Steve: Yes. Somehow they would have to be able to say, oh, what programs, what software has created this pseudorandom noise? So there would have to be little markers every so often in the data stream that identified what software and version and so forth this was, only for the purpose, because I wasn't going to put it in otherwise, only for the purpose of making it identifiable to a third party, presumably law enforcement, and we hope law enforcement.

The other problem is, it does then begin, I mean, even that starts to crumble privacy because then anybody can be looking at the communications and see what tools you're using. If the FBI can determine it, so can anybody else. So now there's information disclosure when before all I was sending was pseudorandom noise. Not anymore. I and everybody else, if that's what we have to do. And, if we're talking about, like, having to re-architect the products as was described, such that point-to-point communications can no longer be point-to-point, that is, the FBI wants real-time wiretap monitoring of the same class they have with the phone system, well, now you can't do a VPN. It's illegal to have an encrypted connection between two points is what this says, is that the law will require somehow that something sends a copy somewhere else or stores it or makes it available somehow. I mean, this is hugely sweeping from an architectural standpoint.

Leo: I just - I hope - and by the way, this is not the first time they've tried to do this, and in the past it has been prevented. So I hope that cooler heads will prevail here. I think law enforcement acts as if it has the right to wiretap; and that, if technology comes along and makes that impossible, that they have no other means for enforcement. And I find that just difficult to believe. And we've got to underscore the fact which you said at the very beginning, that this doesn't prevent people from using strong encryption. Bad guys will still have access to strong encryption which cannot be broken.

Steve: Yes, and that's what they'll use.

Leo: And they'll just use it.

Steve: Yes. Exactly. And so here's this law which potentially would hugely inconvenience, I mean, to the point where I won't create such a product, I mean, I just, I won't do it.

Leo: And to no purpose because...

Steve: Precisely.

Leo: ...it accomplishes nothing.

Steve: Huge inconvenience, and the bad guys will still use the free open source tools which already exist. There's already audio communications clients, point to point, that are free, that you can use, that are well encrypted because it's so easy to do. So it doesn't solve the problem. It creates a - so, what, you catch the dumb criminals who use the commercial software. But everyone will know now that backdoors are installed in all of this stuff. So the bad guys will find the stuff that doesn't have backdoors in it. I mean, it just - it boggles my mind.

And then I'm wondering, wait a minute, what about outside the country? Because we have had, in the past, an inside/outside the country situation. You'll remember, Leo, that the very first version of Netscape Navigator had a 40-bit encryption and a 128-bit encryption. The 128-bit encryption was much stronger than the 40-bit. But encryption back then was classified by this country...

Leo: Right, munitions, it was munitions.

Steve: It was a munition. And so...

Leo: And that, look how well that worked.

Steve: Uh-huh. So you were unable to export it from the country because it was a munition. So Netscape created a watered-down 40-bit key for their SSL - as we remember, they invented SSL - to create strongly encrypted connections. And that was the exportable version. So the U.S. would allow Netscape Navigator to be downloaded by anybody in 40-bit version. The problem was, what we all wanted, even us in the U.S., was the 128-bit version, and we couldn't get it. You had to go through all, jump through all kinds of hoops to get the strong one, proving who you were and where you lived and that you weren't ever going to let it go, you weren't going to send it to anybody and so forth, such that nobody used it. We all used the 40-bit one, which took about a week to crack back then, and just sort of held our breath. And it was like the best, that's all we could get, so that's what we used. And so there was this notion of inside the country/outside the country.

Well, so could I create CryptoLink in the TNO fashion that I want to for sale outside the country, and then have, like, the backdoor spying version - this is why I couldn't sleep Monday night. I'm so upset by this. It was like, oh, I mean, it just - oh. Well, I guess we can hope, and certainly do, that this just won't happen, that enough people will explain

to our legislators that there are - I mean, the more I think about it, the more I think of technical hurdles and technical problems. And again, I would like the FBI to have the tools that they need. But the technology to escape surveillance exists. The technology is out there. It's free. It's algorithms. It's math. It exists. It's done.

And so unfortunately, as communications does move more to the Internet, the Internet is going to "go dark," in their jargon, as we encrypt. I mean, how many times have you and I talked about wishing everything was encrypted? Like forced HTTPS we talked about a few weeks ago, and websites forcing SSL. I mean, we see this as a good thing because we're good guys who don't want to be spied on when we're at Starbucks and open WiFi locations. And I'd love to create a super robust, absolutely killer VPN to offer this kind of technology - which, again, exists, it's just math - offer it to people. And that's under threat now.

Leo: It just reminds me so much of the discussion of copy protection, of DRM. It seems like in this case the motion picture industry, the recording industry is kind of hand-in-hand with law enforcement in the sense that they would like to use technical tools to prevent something they don't like. The problem being that DRM doesn't work because it only hinders honest people, and crooks just go right around it. And so DRM solutions are ineffective. And it's been proven they're ineffective.

Steve: Yes.

Leo: They just don't work. And I think that this is analogous. It's not exactly the same, obviously, but it's analogous. Once it's possible to get around this stuff, the bad guys will. Now, I've talked to law enforcement people, and they say, oh, you'd be surprised how dumb crooks are. And so their point of view is, yeah, I mean, a smart crook can evade wiretapping, as well. But most crooks aren't smart, so we get them. So their point of view is, no, we just want to have a backdoor because most crooks won't be smart enough to use PGP or some truly encrypted solution. They'll just use, "Oh, hey, Skype works."

Steve: And so here's the problem is that what they want to do, it sounds like, could fundamentally force architectural changes on existing services, like Skype is a perfect example because you and I are talking over it right now. We have an encrypted connection directly between the two of us. Nobody can decrypt it. No man in the middle can intercept this dialogue you and I are having and block it. And this was negotiated when we connected, and Skype Central was not involved.

Now, if a law is created that requires that, even with a court order, that somehow this conversation can be overheard over the Internet, then that changes the architecture of the Skype product. And I see that as a huge issue, a huge problem. So now, what, both of our Skypes feed a stream to a third party, which we assume no one is listening to most of the time, but we now know somebody might be, if they have the legal right to do so. I mean, again, I have no problem with that.

The problem I have is that this isn't easy to do. I mean, it isn't. DRM, I would argue, for example, is maybe less onerous because, although people chafe at the idea that they can't make personal copies and so forth, but basically you put the DVD in your player, and you press play, and it plays. And it plays just as well if it's copy-protected and if it's not. Here, we're talking about fundamental requirements that change the way stuff

works and that wouldn't be effective anyway. Oh.

Leo: I guess that's the big one, isn't it. It wouldn't be effective anyway.

Steve: Yeah. Yeah, now, I do take issue with the critics saying, because I want full honesty here, with the critics saying this weakens some of these technologies. The fact is, for example, if, I mean, I've already - I've designed, I designed Monday evening, as I was recovering from this news, it's like, okay, what am I going to do about this? It's like, I mean, and I posted, my original posting to my newsgroups was, "Well, it's over. I'm not going to do CryptoLink. I will not do this."

And then I thought, well, you know. And then some people said, oh, Steve, but we want it, and we trust you. And if you were forced to reveal our communication with a court order, then fine. Don't give up on something that's going to be so cool and offer so many unique features, blah blah blah. And so I thought, well, okay, maybe. I mean, again, if I have to - there's no way that I'm going to be, like, involved in every dialogue with every CryptoLink customer, that is, running their traffic through my server. That will never happen.

Leo: No no no no no no. People will probably hear this and say, well, what can I do? And what I would suggest, the people who prevented this last decade are still around. You can still donate to them. And I'd encourage you to do so. It's called the Electronic Frontier Foundation.

Steve: Well, and in fact, yes. All, everyone listening, EFF.org - sorry to interrupt you, Leo, but...

Leo: No, no. Go with it. Run with it.

Steve: EFF.org is on top of this. There's four links on their home site right now that...

Leo: And COICA or whatever it's called, too.

Steve: Yes, the earlier thing we talked about.

Leo: The DRM issue, yup.

Steve: Yes, using DNS blacklists, government mandated. Both of those issues they're on top of. And they've got some forms that allow you to write to your senator. And, I mean, absolutely, this is somewhere where voices need to be heard. I'm delighted that people whose jobs and livelihoods are fighting against this kind of problem - again, I want to be so clear. I have friends in the FBI years ago who, back when we were doing all the denial-of-service stuff and so forth, I mean, we've had lunch, and we've talked about this problem. I'm so sympathetic to the problem, that there is this fundamental problem with their ability to surveil traffic on the Internet. But there are problems that don't have good

solutions. This doesn't have a good solution. And if a point-to-point encryption is outlawed [laughing], I guess...

Leo: EFF quotes the 1999 Ninth Circuit Court of Appeals decision in the Bernstein case that says, "Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb."

Steve: Low ebb.

Leo: "The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost." This is the Court writing. "Government efforts to control encryption thus may well implicate, not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty." That's the Court, folks.

Steve: Yeah. And one other point that I heard made that I think is a very good one is that law enforcement is complaining about the rise of the Internet. But a lot of communications is not encrypted. I mean, these dumb criminals are dumb, and they write email, and they use unencrypted technology. And the fact is, I mean, the truth is the FBI was having a field day with tapping into unencrypted communications which bad guys are using right now. Yes, encryption is a problem. But the fact that there's also still a preponderance of non-encryption, and that it's over the Internet, and that you don't know when you're being tapped, means that in fact there's a huge amount of useful information that is doubtless being filtered through right now, as we speak.

Leo: Yeah, I guess if a crook's dumb enough, they're not going to be encrypting. If they're smart enough to use encryption of any kind, they're going to use strong encryption. So maybe that dumb crook analogy doesn't work. I donate monthly, I'm a sustaining donor to EFF. I encourage everybody to do that. EFF.org. They use the money to go to court.

Steve: Yes.

Leo: Not only to raise awareness. But they go to court. They file amicus briefs, they challenge, they are court focused. And that's what makes them so effective. This is...

Steve: And they defended Dan Bernstein in his suit against the federal government, saying...

Leo: They won that case.

Steve: Yes.

Leo: So we owe them for that in 1999. And if you want to continue to fight, I think the EFF is a great place to do so. They also, as you said, they have emails and stuff you can send. But EFF.org. I think, you know, take that indignation and put it to good use. Steve, I'm glad you raised this issue. I think it's so important.

Steve: Well, I mean, I'm stalled at this point. I mean, I have other stuff I have to get to before I start writing CryptoLink. The architecture is in place, the technology is in place. It's just...

Leo: Well, remember, it's not law yet. Attempts to make this law in the past have failed. I'd go ahead, Steve. Have faith.

Steve: I don't have any.

Leo: That good will prevail.

Steve: I can spend some time on SpinRite. That'll make lots of people happy. This is going to happen probably early next year. So here we are toward the end of September. So it's only a few months. Besides, I still have some other stuff I've got to get to before I was going to start anyway. So, I mean, one thing, it's like, I mean, literally, if this shuts down, if this forecloses the ability to point-to-point communication, then...

Leo: It's not going to happen.

Steve: Well...

Leo: We've got to fight it. We've got to fight it. We've got to fight it.

Steve: Well, believe me, I'm ready for a fight. But I am glad that I didn't already invest two years in CryptoLink and then have this happen. It's like [laughing].

Leo: This isn't going to happen. Web5517 says politicians always win in the end. That's wrong. The people always win in the end. Politicians might win in the short term, but we always win in the end. We will win in this one. EFF.org.

Steve: If people care. If people care.

Leo: Well, that's our job.

Steve: Yeah.

Leo: And everybody who is listening's job as a good geek. This is where your ability and your knowledge of this stuff comes into play. You can't sit on your butt. Take some time off from World of Warcraft and get out there and raise awareness, write some emails, and make it happen.

Steve: Yeah. Go to EFF.org, and they provide some forms that make it easy for you to send notes to your congressmen and senators, your representatives in Washington. And now's the time. We need to stop this.

Leo: Steve Gibson...

Steve: I mean, again, I'm sorry the FBI is dealing with encryption. It is a horrible, horrible problem. But it's math, and it exists. And there just isn't a way around it. We now have the ability to encrypt, I mean, what's next? TrueCrypt on people's hard drives? It's going to force a backdoor for TrueCrypt so that they can decrypt on demand? I mean, this is - we can't let this erosion happen.

Leo: I couldn't agree more. Steve is at GRC.com. That's where he lives, the Gibson Research Corporation. That's where we find SpinRite, the world's best hard drive maintenance and recovery utility. You'll also find every issue of this show, all 268 episodes, both in 64KB, the high-quality audio, as well as 16KB audio. He has transcripts up there of each and every show, as well, for those of you who like to read along while you listen. And we provide audio and video at our site, TWiT.tv/sn for Security Now!, TWiT.tv/sn. And when you're there, you can subscribe on iTunes, the Zune Marketplace. Whatever aggregator you use will work with that. And YouTube and all the other places. Steve...

Steve: And next week we've got a Q&A.

Leo: Good. So how do they ask questions?

Steve: GRC.com/feedback. That'll take you to a web page with a form. Send me what you're thinking about. We'd love to hear reactions to this. And we will do that next week.

Leo: Excellent. Thank you, Steve. We'll talk again next week on Security Now!.

Steve: Thanks, Leo.