Virtual Private Networks (VPN): Theory

Description: Leo and I first follow-up on the past two episodes, discussing new developments in the continuing Sony Rootkit DRM drama, and some confusion over the crackability of WPA passphrases. Then, in this first of our two-part series on VPNs, we discuss the theory of VPN connections and tunnels, explaining how they work and why they represent such a terrific solution for anyone on the go.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-014.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-014-lq.mp3

Leo Laporte: This is Security Now! Episode 14 for November 16, 2005: VPNs. And Steve Gibson and I are here in the dark Call for Help studio.

Steve Gibson: A quiet studio.

Leo: They're on a lunch break.

Steve: Yeah, perfect.

Leo: Everybody's run away to get their wraps. But we're going to talk about - actually, let's start by talking about issues that came up from our last episode.

Steve: Yeah, there's been some additional news over on the Sony front.

Leo: Okay.

Steve: Sony has now backed away officially from offering copy-protected DRM-based CDs. All of this rootkit nightmare that they've stumbled into has caused so much trouble that they've said, okay, we're going to remove...

Leo: We give up.

Steve: Exactly. We give up. We're going to remove this from our stuff and, apparently, even recall existing inventory that's out in the retail channel. I mean, it's been a huge problem.

Leo: I did notice that they said "remove temporarily." So I think they're reserving the right to put copy protection in, but just not that copy protection.

Steve: One of the nicest things I read somewhere - and I can't remember now where it was, it was in the

last week - somebody was interviewed and said Sony needs to understand that, while it is their intellectual property, it's their copyrighted material, it's not their computer.

Leo: Right.

Steve: It's the user's computer.

Leo: And I'll be honest, from reading the comments from Sony executives, I don't think they get that yet.

Steve: No.

Leo: They still believe that they, in pursuit of protecting their intellectual property rights to that music, can modify your system. And I think that that's - they're going to try some other way of doing it.

Steve: Well, and that's of course the good thing about this as a precedent-setting event, is that hopefully this is going to demonstrate to people where the boundaries are for DRM, what you can and you cannot do. And there was also a report that this is apparently installed in as many as 500,000 machines.

Leo: One expert said that, yeah.

Steve: Are now carrying this technology.

Leo: And those machines in all likelihood are never going to be disinfected. It's too difficult to do, and their users probably don't even know they're infected.

Steve: I was going to say, yes. We're certainly reaching with our podcast, you know, an upper-end, technically competent, you know, really aware audience. Most people who just stick the audio CD - I mean, I don't play audio CDs in my computer...

Leo: Right.

Steve: ...because, you know, it's just not something I've ever done. It just sort of seems wrong to me.

Leo: But what I do is I rip them. I do put them in there to copy.

Steve: Absolutely, to move them to your players.

Leo: Yeah. And that is, you know, the key there is not to play it. You press the Shift key not to run the autorun. But I have to point out something. Now, I don't - I haven't verified this, and we're going to get a disk, and you're going to verify this.

Steve: Yup.

Leo: Somebody said that, even if you say no to the EULA, it's already too late; they've already installed the software.

Steve: Oh.

Leo: They haven't activated it.

Steve: Ah, interesting.

Leo: But it is on your system already.

Steve: Wow.

Leo: So it's not running. The EULA is required before they say, okay, autorun.

Steve: Right.

Leo: The EULA is what puts it into the registry or whatever so that it starts every time you boot your machine. But even before the EULA, the EULA runs as a consequence of having installed the software. So I haven't verified that. But if that's the case, I mean, it's just a mess.

Steve: Yeah.

Leo: It's just a nasty mess. Okay. So that's the Sony rootkit. Let's talk a little bit about WPA because that's what we talked about last week.

Steve: Right. It's interesting. I got one comment back from someone who had a point that I wanted to bring up. And he said, hey, Steve, I took offense or objection or exception to you saying that WPA was completely uncrackable. He said there are WPA cracking tools that are already out.

Leo: Yes.

Steve: And I wrote back because he gave me an email address. And I said, yeah, you're right, except that those are only useful if people have weak WPA passwords. So WPA with a really, really random gibberish passphrase, which is a pain to establish once, but once done, I mean, it is truly uncrackable. And I did something between the last podcast and now because a couple of people said, hey, you know, how do I get a really good random password? And they provided some links to some existing online password generators. The problem is that those password generators aren't running over SSL, and they're not perfectly written. For example, they don't have an expiration date on the page, which means that an ISP could cache and would cache that page locally, so that somebody else might get the same page that you got and would get your passwords. And okay, that's not a big problem. But I thought, okay, GRC should have a password generator. So I wrote one: www.GRC.com/ - in your honor, Leo, I made it four letters - p-a-s-s.

Leo: Easy to remember.

Steve: "Pass." Or...

Leo: Or "password."

Steve: ..."password" or "passwords." And people can put .htm on the end if they want to; it'll ignore it. Doesn't matter. Anyway, what it is, is it's very cool. If you just go to, you know, HTTP, that is, not "S," just regular - you know, as most people would, they just stick GRC.com/passwords in their browser - it'll see that

you're trying to access GRC's password generator over a non-secure connection that anyone could sniff, that is, you know, may be available, open, and certainly that proxies can cache. It'll say, oh, no no no. It'll automatically redirect your browser to a secure version, set up an SSL connection, then on the fly use extremely good cryptographic random number generation to create three different passphrases: a hex 64-character passphrase...

Leo: 63.

Steve: Actually 64. It turns out that WPA has two modes that it can operate in. And the Windows WPA client accepts either one.

Leo: Oh, okay.

Steve: And that is, you can actually give it - 64 hex characters is exactly 256 bits. So you can actually give it the actual encryption key. Or you can use a 63-character passphrase which can be any kind of alphanumeric mumbo jumbo. So the second version is a 63-character, any printable ASCII, I mean, backslashes, colons, dots, periods. It looks like your computer is broken...

Leo: Right.

Steve: ...when you see this. And then, since I wanted to make sort of a general-purpose solution, and I also heard that some hardware might not be compatible, might not be actually on the WPA spec, so that if you put the passphrase into two devices, you would not be able to connect because some hardware wouldn't be handling all the funky characters correctly.

Leo: Right, right.

Steve: So the third version that comes out on my page is only alphanumeric. It's all alpha, you know, A through Z, upper and lowercase, and 0 through 9, which will be acceptable by anything, and is still sufficiently random that, you know, it's going to be very solid. So there's now a new little service at GRC. [Perfect Passwords: GRC's Ultra High Security Password Generator, at www.GRC.com/pass or www.GRC.com/password or www.GRC.com/passwords.]

Leo: It's probably beyond the scope of this, but I'm just curious. We've talked before about random number generators on computers not really being real, they're pseudo-random number generators.

Steve: Yes.

Leo: Because it's hard to do real - it can't do real random. How did you - what are you using for your random algorithms that you know they're cryptographically strong?

Steve: I have a crypto license from RSA Security themselves. I own what they call the BSAFE cryptography library, which is what I use over on my server side stuff. I seed it with a whole bunch of stuff, like how many processor cycles the clock has run since it was powered up, and the phase of the moon, and the NIC address, I mean, it's just a whole bunch of stuff, and some other information that only increments and never decrements. So I'm sure I will never repeat these. And, you know, my page, my passwords page, is a super-safe place to get passwords.

Leo: Great.

Steve: And a user might not want, you know, even trusting me as much as they would, might not want to

take them as-is. So you could take, like, do it three times. Oh, the other cool thing is, just refresh the page. Every time you refresh, a whole new set of, you know, pseudo-random passwords.

Leo: So do three of them and take a third from each.

Steve: Exactly. Or take it and chop it and swap pieces around or whatever.

Leo: Right. As long as it's 63...

Steve: But it is super, super random.

Leo: Would you recommend using 63 characters, just to make sure it's compatible?

Steve: Yes.

Leo: Yeah.

Steve: Yeah. I don't know...

Leo: That's random enough.

Steve: I mean, well, okay. It is so uncrackable at 63 characters, no one is going to have that in a dictionary. And it would take them forever to, like, come up with that.

Leo: And we should point out for the people who are going to be semantic purists, it's not uncrackable. It's practically uncrackable.

Steve: Yes.

Leo: In any practical sense.

Steve: In the lifetime of the universe.

Leo: Yeah. Sometime it could get cracked. And it might happen less than the lifetime of the universe. But...

Steve: By bizarre chance.

Leo: Right.

Steve: Or by, you know, if you just chose random passphrases, you know, one in a gazillion gazillion possibilities.

Leo: Right. So mostly uncrackable.

Steve: Yeah. Anyway, it's there if anyone wants to take advantage of it.

Leo: Not theoretically uncrackable. All right. Now, let's get to VPN. This is something that's used by businesses all the time, Virtual Private Networking. It allows a telecommuter to log into the business network in a secure fashion. Can it also be used by the home users?

Steve: Well, absolutely, and in fact that's really sort of our focus for the podcast. This follows perfectly on the three segments that we've done so far on WiFi and, you know, on the security aspects of wireless networking. Because the idea is, you know, basically we talked about open access points. We talked about weak WiFi security. And then finally we talked about WPA, you know, honest-to-God serious industrial-strength security. So the next thing really to talk about within this context is how can you be secure when you're at Starbucks, or you're, you know, using a public access point...

Leo: Yeah.

Steve: ...where it's not your network, you're not able to secure it, you have no administrative control over it, but you want to use the access point in a secure fashion.

Leo: More and more access points are offering security of some kind or other. But still, a lot of them don't.

Steve: Well, as a telecommuter, say, like, here I am staying overnight in a hotel in Toronto.

Leo: Right.

Steve: I want to be able to plug my computer, even not WiFi, I want to plug my laptop into the hotel network.

Leo: You don't know what's happening there.

Steve: I have no idea what's going on. And in fact, it was interesting. A column in InfoWorld two weeks ago, Roger Grimes was quoting a gal who is a security person, who travels around a lot. She said half of the hotels - I mean, she's, like, on the road all the time, a real road warrior. Half of the hotels that she's in are using hubs and not switches. Meaning she...

Leo: Means you're all on the same network.

Steve: Yes. Well, they're not only the same network, but they're a shared segment. So if she turns on Ethereal to do packet capture...

Leo: Could see anything.

Steve: And she does. She says in a typical evening stay - and there's a password capturer called Cain.

Leo: Yes.

Steve: She uses Cain. And Cain is smart about various protocols. It knows what it's seeing in packets that go by. She typically sees more than a hundred, the number that was quoted in the article was 118 in-the-clear passwords for people staying in the hotel. I mean, she literally captured their information.

Leo: Well, I know that's the case because I'm staying in a hotel now that offers free WiFi. And when I open my iTunes, I can see other people's iTunes libraries. So we're on the same segment.

Steve: Right. Well, you're WiFi, so you're inherently - you're in the same atmosphere, you know, you're on the same planet as other people.

Leo: There is a little - they must be doing some firewalling or blocking of some protocols because I can't actually see their music. But I can see their shared libraries.

Steve: Well. So, you know, you and I...

Leo: So how do I protect myself?

Steve: You and I have talked about using and needing a personal firewall. I mean, on my laptop...

Leo: I did do that.

Steve: ...I've got XP.

Leo: Yeah.

Steve: And I've got Service Pack 2.

Leo: I turned on my firewall.

Steve: So I've got its firewall on. So I know I'm okay as far as that goes. But, you know, I am not going to do anything where I need privacy, which, you know, even...

Leo: Well, my data's in the clear.

Steve: ...checking email.

Leo: Well, then, that's the problem.

Steve: Yes.

Leo: As soon as I log onto email, my email password and log-in is visible.

Steve: Yes.

Leo: Now, I use SSL for my email, so fortunately I think I'm all right.

Steve: Yes, you are, in fact, because SSL creates - and that's a perfect segue into this. SSL creates a secure connection which is actually not a tunnel. A tunnel is a different thing. But it creates a secure transport for everything that happens afterwards. And that security is negotiated before any user data passes through the

connection.

Leo: Even my password?

Steve: Yes.

Leo: Okay.

Steve: Yes.

Leo: So as soon as I'm in that SSL mode...

Steve: Yes.

Leo: ...on that port, everything is encrypted.

Steve: The original negotiation, first a TCP connection is established. So the SYN packets go back and forth with the TCP connection. Then a security channel is established within that connection.

Leo: And then I enter my password.

Steve: And then you actually have a user data, an application-level channel between the endpoints.

Leo: So that's pretty safe. When I do FTP, and I upload to my website - which I do, in fact, from the hotel fairly frequently - if I'm using plain old FTP...

Steve: Yup, ports 21 and 22.

Leo: ...and that gives them an access to my website.

Steve: Well, and anyone could have the file that you were transferring.

Leo: Well, and also what happens is a lot of times people use the same password for their FTP to upload to the website as their administrator log-in or their SSH log-in.

Steve: Right.

Leo: So that really opens you up to somebody hacking your website. So that's why I use secure FTP when I transfer.

Steve: Right. Okay. So...

Leo: But I'm still open to everything else.

Steve: Going to the next...

Leo: So what do I do?

Steve: Yes. Going to the next level is this thing called a VPN. Now, the reason it's available to end users - there are a couple ways it's available. And this week I want to talk about sort of the theory and the technology of a VPN...

Leo: Okay.

Steve: ...and not get into all the detailed specifics. We're going to do that next week because it's a big topic. I don't want to try to cram too much in and miss stuff. So the theory of VPN, Virtual Private Network, the key concept is what's called a "tunnel." With a tunnel, you establish a connection between endpoints. And we've talked about how packets are used to move data over the Internet. One of our future podcasts, we're actually going to talk about how the Internet works and get into that in more detail. But for now, it's sufficient to know that data travels in packets. The packets have, like, an address information on the front, the so-called header of the packet, where it's the source IP, the destination IP, the source port, the destination port, and some other stuff. That is normally visible to anyone who's sniffing the traffic. And it gives the IP of your machine, where it originated, and the IP of where it's heading. And also, from looking in the packet - normal Internet packets are not encrypted in any way. They're just so-called plaintext, as the crypto term is. So anybody, again, sniffing the traffic can see what it is that's going on and understand what the traffic is.

Now, what the VPN does, which is unique and special, is it essentially encapsulates the packet. Every packet coming from your computer is encapsulated. It's wrapped in another packet where your entire packet is the payload, the data of this VPN packet. So the IP addresses, like where your data is going to, ends up being in the data of this so-called VPN tunnel packet.

Leo: So even that's not visible.

Steve: Even - exactly.

Leo: Well, how does addressing happen, then?

Steve: Well, what happens is, you always establish a VPN, this so-called VPN tunnel, between two points which are both aware of this VPNing. Normally...

Leo: So you have a client and a server.

Steve: Well, actually you have peers.

Leo: They're peers, okay.

Steve: Yeah. It's VPN peering. So, for example, you could take two VPN routers and peer them together, and they would create a tunnel. Or, most often, telecommuters would have a VPN client in their system, and they'd be dialing into, like, a VPN pool in their corporate environment or - and this is what we're going to talk about in detail next week - their own VPN router at home. Because you can now get consumer VPN routers which would allow you to dial into your home - to essentially use the Internet to get you to your home router over a secured channel. Then you have access, not only to any machines you have at home, but to the Internet, just as you would at home, out from that router.

Leo: So once that tunnel is established, it's hardened. Nothing inside can be seen, including the addresses on the packet.

Steve: Well, that's the key is that - so first we have this notion of wrapping a packet in, like, a super packet, in this encapsulation packet. There's also seriously strong, industrial-strength encryption going on. So, and the encryption technology is something our more techie listeners may have heard of called IPSec. IPSec is an IP standard for endpoint-to-endpoint security that establishes extremely strong, you know, virtually uncrackable encryption. So every single packet is scrambled when it's put into this VPN packet.

Now, an interesting little tidbit is that Microsoft Service Pack, I think it was the first Service Pack 2, broke VPN because what happens when you wrap a packet is it gets bigger. And there are limits to the size that packets can be as they travel over the Internet. So what should happen, what has to happen, is that your packets, your source packets, before being wrapped, need to be made smaller so that, after the VPN wrapper is added, they'll still be within that 1500 bytes. Microsoft forgot that and ended up breaking VPN, which was a good lesson to all the people in corporate America who are not installing service packs and major patches without really testing them first to make sure that they don't break critical things. And it was, you know, Microsoft quickly scrambled to fix it. But they did break it with that security update.

Leo: Interesting.

Steve: So essentially...

Leo: It's fixed since, but...

Steve: Oh, it was immediately fixed. And it's like, oh, oops, we're sorry. We won't do that again.

Leo: When corporate America howls, Microsoft probably jumps a little faster than when you and I howl.

Steve: Oh, absolutely. Yeah, we know how fast they jump when I howl.

Leo: Not at all.

Steve: No, not at all. So anyway, the idea is that this VPN tunneling establishes a secure channel. Now, somebody sniffing the traffic is just out of luck. They could know by looking at the IP address or port number that it's a VPN channel because VPN channels tend to use specific ports. But they won't even know where you're going...

Leo: They can't see any addressing.

Steve: ...because your entire packet is encrypted. Even your headers are encrypted. So they see nothing. They will see the endpoint of the tunnel, wherever that is, but not know anything about what you're doing because what happens is, at the receiving end, the outer wrapper is removed from this packet. Then whatever it is inside that just looks like static, looks like noise, it's decrypted back into your original packet, and then it's dropped onto the network. So what this does is, for example, if you were using a VPN router as your normal home router, you could, from being remotely located somewhere, you could connect to it through any open environment, in the hotel environment that we were talking about before, or WiFi.

Leo: Right. The only issue sometimes with VPN is that those ports may not be open.

Steve: Ah, yes, and that's where we're going to talk about problems with VPN and things that can go wrong. Sort of the, you know, here we're talking about the theory. We're going to talk about the practice of VPN and things that people need to be aware of. And if you thought that WPA was acronym stew, with RC4 and TKIP and, you know, AES and enterprise blah blah blah, I mean, this VPN stuff is - when you look at one of these VPN clients that you have to, like, add the numbers to and configure, you just glaze over because there's IKE, Internet Key Exchange; there's the IPSec; and, you know, 3DES and AES and so forth. But there are ways that you can configure all of this for maximum compatibility. And that's what we're going to talk about

next week is how - basically, now everyone knows they want VPN because, I mean, it really is cool. It allows you, with total confidence, to use your computer anywhere. I mean, even if you go to a friend's house, use their WiFi and VPN back to your home, then you get out on the Internet from there, and you have access to any machines that you have at home. It's a real win.

Leo: Sounds like something everybody should be doing.

Steve: It's a great solution.

Leo: And there are services out there that you can do this through, as well, yeah.

Steve: Right. That's the alternative. In our earlier show we had some show notes...

Leo: We mentioned a couple of services, yeah.

Steve: ...with three of those. And Google had a VPN service for a while, which I guess they then shut down.

Leo: Well, because Google was, at least in San Francisco, offering WiFi. And they plan to, I think, roll this out nationwide. They do have a secure WiFi. And for a while people had figured out how to hack it and use it...

Steve: Ah.

Leo: ...going through the Google servers, the Google VPN servers, even on your own access point. I don't know if that hole is still there. It sounds like it's not. But there are ways you can do this, as you said, for yourself. There's services you can use...

Steve: Well, and if between now and next week's podcast people, like, have to do something immediately, Anonymizer.com, they have a service where they will anonymize just a few things, like web surfing, where you use them as a proxy to, like, filter and anonymize your web search. And they also have exactly what we're talking about, is a secure tunnel. And the other cool thing about this...

Leo: They use SSL, which is a little more transparent. You don't have to worry about ports because SSL ports are almost always open.

Steve: Correct. And but the other cool thing I want to make sure I don't forget about tunneling is nothing, nothing knows what traffic you're sending through a VPN tunnel. It's, literally, it is impossible for anything to know. So people, for example, have problems if they're telecommuting because, like, port 25 for SMTP, for email, might be blocked by the hotel, who doesn't want spam being sent. The beauty is, through a VPN tunnel, if you can establish the tunnel, once that's done, you could do anything. Nobody can block any specific behavior you have because it's...

Leo: Because they can't see it.

Steve: It's just static. It's noise.

Leo: Yeah, yeah.

Steve: It's completely transparent.

Leo: So Part 2 of VPN next week on implementation, how you can do it. Can we throw in a little bit of stuff on SSH tunneling, as well?

Steve: Oh, yes.

Leo: Because that's another way to do it.

Steve: Yes, for sure, and SSL.

Leo: Yes.

Steve: And I want to say that we've been getting so many questions that we're going to start a practice of doing some Q&A podcasts.

Leo: Maybe once a month we'll just go through questions and responses...

Steve: Well, being the mathematician, I'm thinking any podcast that's divisible by four.

Leo: Okay.

Steve: So here we are...

Leo: This is 14.

Steve: ...on number 14. We'll do VPN next week. And so 16 will be...

Leo: Okay.

Steve: ...our first Q&A podcast. So every...

Leo: Okay, Mod 4. Security Now! Mod 4.

Steve: Security Now! Mod 4. And so people who are submitting things on the securitynow.htm page at GRC, believe it or not, I read all of that. I mean, it's a job reading everyone's submissions because we get a ton of stuff.

Leo: Lot of useful stuff.

Steve: But it's great feedback for me because I know what stuff, you know, we missed, what we need to cover. And so every fourth episode - you know, again, if something critical happens, like did happen with the Sony DRM stuff, we'll hold off, you know, and cover that, and jigger our schedule around.

Leo: Right.

Steve: But, you know...

Leo: I like the Mod 4. We're going to have to stick to that Mod 4.

Steve: I like that. It's good.

Leo: It's easy to remember.

Steve: Yup.

Leo: It's like leap year. But let's not get like leap year because then there's always those exceptions.

Steve: Every 400 years there's not one.

Leo: Yeah, and the century mark and all that stuff. If you want to know more, of course, Steve puts up great show notes at GRC.com/securitynow.htm. Not only show notes, but there's also a lo-fi 16KB version for people who don't have the bandwidth or the storage; also transcripts in a variety of formats. So, in fact, the transcripts have proven very popular.

Steve: Yeah.

Leo: Do you want to give credit to the woman who does those for you? Do you remember her name?

Steve: Her first name is Elaine.

Leo: Thank you, Elaine.

Steve: She's spectacular.

Leo: That's really a nice thing to do.

Steve: I mean, she is just super.

Leo: All right. Well, we really appreciate it. It makes it much more accessible for people who can't listen to the podcast or want to share it.

Steve: And she's going to have to be transcribing what I just said. Flattering her.

Leo: She'll be smiling.

Steve: Elaine, you deserve all the praise that I can give you. You're fantastic.

Leo: And of course thanks to the folks at the AOL Radio, the podcast channel there, who not only broadcast Security Now! on their podcast channel, but also provide us with the bandwidth. AOLmusic.com is the URL for that. We'll be back next week talking about VPN implementation unless something awful happens again. But that's what we're here for.

Steve: Yup.

Leo: Security Now!. Steve Gibson, thanks a lot.

Steve: Always a pleasure, Leo.

Leo: Safe trip home.