PPTP and IPSec VPN Technology

Description: In our continuing exploration of VPN technology for protecting network users on networks they don't control, Leo and I discuss the oldest "original" VPN protocols: Industry standard IPSec, and Microsoft's own PPTP and L2TP/IPSec. We examine and explain the trouble with interconnecting Windows machines to third-party VPN routers and examine the many reasons these older technologies are probably not optimal for on-the-go road warriors.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-017.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-017-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 17 for December 8, 2005, continuing VPN solutions. Steve Gibson is joining us via Google Talk. And we're ready...

Steve Gibson: Hey, Leo.

Leo: ...to continue - is this Episode 4 of VPN? Episode 3? We've been doing this...

Steve: I think this is actually our third.

Leo: Third.

Steve: We talked about the theory of VPN first, what's the concept of tunneling packets through another protocol. Last week, of course we talked about SSH tunnels and SSL tunnels. And this week we want to talk about basically sort of the granddaddy protocol of VPN, which is a point-to-point tunneling protocol, PPTP, which was originated by Microsoft; and then sort of the formal IETF standard, which is IPSec tunneling, to create a virtual private network extension.

Leo: So this is really the alphabet soup edition.

Steve: Uh, yeah. We have a few more to go. We're going to talk about some open source VPN solutions and some public services in the next week or two. But I wanted to talk about the VPN that most people already have, basically, if they're using Windows. Even Mac supports PPTP VPNs. And of course many people have VPN endpoint NAT routers. And there are issues with interconnecting all this. So that's sort of where I wanted to go.

Leo: It's a big topic and an important topic because, frankly, secure networking, secure online use is, you know, top of mind for everybody these days.

Steve: Well, I can tell you that there's been a phenomenal response in the postings that we've received about this topic. People who are roaming around, the so-called "road warriors," who are in hotels or in open

Wi-Fi, they understand that, you know, their traffic is very vulnerable without creating a secure connection. So that's, of course, what VPN offers.

Leo: Well, let's start with a kind of circle around for last week's episode. Because even though it was a question-and-answer episode, we created some more questions.

Steve: Well, yeah. I think I overstated the security offered by switches versus hubs in responding to one of the questions that we'd seen many times, like, you know, is a hub much more secure than a - I'm sorry, is a switch much more secure than a hub, because it doesn't allow you - a switch doesn't rebroadcast all of the net's traffic out of every port. A number of people said, wait a minute, there are ways to breach the security of a switch. Well, that's not really true. There are ways to breach the security of an Ethernet LAN, and we're definitely going to be talking about those. But I first - I don't want to freak everyone out with that until we provide some solutions which they'll already have implemented or be ready to implement after we talk about these VPN solutions. So it's really not that the security of a switch is unbreakable. It's that the security of the Ethernet itself, it was never designed, like many of our protocols, never designed with security in mind. So it is true that you cannot passively sniff the LAN's traffic on a switch, whereas you can with a hub. But it is also true that there are active means of subverting the entire network that we'll be talking about in the future. But I just wanted to go on the record and clear that up.

Leo: That ARP poisoning that the guy was talking about; right?

Steve: Exactly.

Leo: We'll save that for another...

Steve: Also, I mangled an acronym, and I hate when I do that, especially acronyms that I know so well. I talked about CSMA, and I called it Collision Sense Multiple Access instead of Carrier Sense Multiple Access. And it has a CD on the end which stands for Collision Detection.

Leo: All right.

Steve: So the real acronym for Ethernet is CSMA/CD, which is Carrier Sense Multiple Access with Collision Detection, which...

Leo: I admire your engineer's drive to precision and clarity.

Steve: Well, the only way...

Leo: But I don't think most people care that much.

Steve: That's the only way I could code everything in assembly language, if I paid attention to the carry bit.

Leo: Everything matters in assembly.

Steve: And in following up one last point, which was our discussion of how virtually impossible it is to use a public access point, that is, like a public terminal in a hotel or in a library. Even, you know, like we were explaining, even keystroke logging could be installed on that machine and, in fact, has been found in public terminals. Many people wrote with various, like, clever means to get around that. For example, if you open Notepad, you could type a couple characters in on your password, then switch to a different application, type some nonsense, go back to notepad, type a few more, go back to something else, type some nonsense. The point is that, if you could - if something was only able to see your keystrokes and not things you were doing

elsewhere on the multi-windowed interface, then you could even use, like, cut and copy/paste in order to end up assembling your final username and password that a keystroke logger would be blind to. And there's, you know, any number of variations of that concept. And I thought those were clever and certainly worth mentioning.

Leo: Knock yourself out, kids.

Steve: There you go.

Leo: If you really want to do that. But I guess it is one way that you could use a public terminal and be fairly assured of safety. Unless somebody's got a camera over your shoulder, and then forget it.

Steve: If you really have it.

Leo: All right. Let's go on. PPTP, Point-to-Point Tunneling Protocol.

Steve: This is the original protocol which every version of Windows from 95 on has had built into it. There are a number of ways to use the protocol. And because they're built into Windows, they're sort of compelling. The problem is that Microsoft's first implementation had some very serious security vulnerabilities in the way the tunnel authenticates itself. And even the second one ends up being prone to ready abuse. So Microsoft is deprecating the use of it. They call it "non-strategic for the future," and they're moving to what they call L2TP, which is Layer 2 Tunneling Protocol, which is protected by IPSec, which is the standard IP Security Protocol. But it is in everyone's machine. And in our show notes I've got some links to some pages that show, for example, how you can, with no additional software, how you can just use the built-in New Connection Wizard in Windows XP, or there's a variation of that in Windows 2000. Just step through the Wizard and basically interconnect two machines using this VPN.

Leo: They call it VPN, but it's using this Point-to-Point Tunneling Protocol.

Steve: It is. Well, it would be a Point-to-Point Tunneling Protocol VPN. I mean, it truly is a Virtual Private Network where the client machine is acquiring an IP from the machine it's connecting to, which is essentially extending the entire network through to the other machine. It's worth mentioning that, when we were talking last week about SSH tunneling, there we're really not using a VPN solution. It's a secure protocol tunnel which uses proxy servers in order to basically fool your clients into routing their traffic through the tunnel, as opposed to a true VPN, which is what we're talking about this week, that actually gives your client an IP from the server. And it's like it's on the server's local network, and it's being secured through this encrypted tunnel. So these are true VPN solutions.

Leo: I remember using corporate VPNs that used this PPTP. You had to use Windows pretty much. Macintosh and Linux didn't support it very well because it's a Microsoft protocol. The rest of the world's not using PPTP.

Steve: That's true. And in fact, the routers that people can buy recently now, these so-called VPN endpoint routers, they actually are a VPN server. And you remember a couple of weeks ago I started talking about my quest for the holy grail. Well, the holy grail was to need no client software on a machine out on the Internet. You're in an open Wi-Fi hotspot; you're a road warrior in a hotel. You realize that, because it's on a LAN, which is inherently unsafe, or your radio, which is inherently unsafe, you really need to encrypt your traffic, at least until it gets out of that danger zone.

A number of people have said, hey, Steve, you know, it's cool that you're talking about VPNs. But, you know, once you get your traffic decrypted, it's going out over the Internet anyway, isn't it? So what's the point? Well, the point is you want it encrypted while your traffic is crossing the area of highest danger. Which, for example, in a hotel setting is a network you don't control, or in open Wi-Fi is where your traffic is inherently sniffable by anybody who is able to be within range. So, sure. All Internet traffic as it passes over the Internet, unless it's explicitly encrypted by an SSL connection, it's going to be in the clear. But there you just have safety in numbers. It's, you know, a huge tunnel, an amazing amount of traffic going by, very unlikely

that anyone is going to find it. But again, it's prone to targeted attack, but not sort of just general, you know, general let's see what we can pick up with our antennae attack. But these VPN routers, my hope was that we'd be able with a Windows machine to connect to a VPN router.

Well, it turns out that Microsoft has deliberately chosen to stick their head in the sand and not support the protocol in their built-in Windows client that everybody else does. Microsoft supports this L2TP, this Layer 2 Tunneling Protocol, which is incompatible with just standard IPSec VPNs, which is what all of the endpoint routers support. So it turns out that my search for the holy grail, that is, no software installed in a laptop, and you can connect to your VPN router at home, is deliberately not possible using just standard Microsoft client. Now...

Leo: And why would they do that? Is there a compelling reason to do that?

Steve: I've got some links in our show notes, in the episode notes, that show them defending this position for, like, page after page after page. It's like, no, we don't believe that the standards yet exist, blah blah blah, I mean, it just goes on and on and on. It's like, okay, Microsoft, you know, if you don't want to do it, just say so.

Leo: Yeah.

Steve: For whatever reason, they just don't want to do it.

Leo: So as far as you can tell there's really no legitimate reason, it's just they don't want to do it.

Steve: I'm sure there's no legitimate reason because everybody else has, and everybody else is interoperable. Now, if you had a Netgear router or a D-Link router or a Linksys or any router that really offered good peer-to-peer VPN endpoint support, which is what any of these VPN routers do, they offer - unfortunately, it's not free, but it is very nice - they offer inexpensive clients, about $39 typically, for the Netgear, the D-Link, or the Linksys. In fact, I think Linksys's client may be free. But it wasn't clear from their site. They have something you can download for free. It may be that it's available. Although I don't know how interoperable it would be with other manufacturers' systems.

Leo: So they have this router. I put it on my system. Does it say on the box "VPN Router"?

Steve: Yes.

Leo: Yes. So I should look for that.

Steve: And they're generally a little more expensive than the sort of generic non-VPN routers. But it's about $129-$139, something like that.

Leo: Now, and then I run this software on my laptop at the hotel where I'm worried about security.

Steve: Yes.

Leo: It connects to my router at home. And here's my big question. And this is - I've been trying to, you know, in parallel with you, trying to set this up to make it work. I understand it lets me get to my home network and see my machines and stuff like that. Can I then surf out onto the 'Net, as well? I mean, can I use my Internet connection at home to surf the 'Net?

Steve: Well, you're a member of your local network. And I think we talked about this once before, and I had

not yet achieved that.

Leo: Yeah. In theory, it's doable.

Steve: Well, what actually put me off of it is that there are still some problems even with doing that. The problems are, first of all, there is a problem with using IPSec through any NAT routers because the IPSec technology inherently, by design, protects its packets from being changed. It's a packet authentication technology that basically signs every packet so that any change will be detected. Except that NAT routers change packets. They have to. That's the way they work. As you know...

Leo: They re-address them. They change the address on them.

Steve: Exactly. Now, there are actually two encryption technologies for IPSec: one called AH, which is Authenticated Header; and one called ESP, which is, I can't remember the acronym. It's like...

Leo: Extrasensory per- no.

Steve: Encapsulation Security Policy or Protocol. Encapsulated Security Protocol. The AH approach does include the IP address of the packet. Well, we know that has to change. So AH can never be routed across a NAT router. However, the ESP encryption stops a little bit short. It doesn't change the IP address. It does change the inner packet address. So it's possible to route that. What happened is, people recognized that IPSec would not be very useful if it was unable, if it was absolutely unable to ever transit NAT routers because, of course, NAT routers are - you're going to find them in any hotel, any Wi-Fi hotspot, and of course in any home environment.

So what they did was they created a next-generation technology a few years ago called, unfortunately, NAT-T, or NAT-Traversal. Now, this is different than just regular NAT traversal that we've had with packets crossing regular NAT routers. This is special - NAT-T is the acronym you want to look for, NAT-T, NAT-Traversal for IPSec. What this NAT-T does is it wraps the IPSec packet in another wrapper of UDP - the standard UDP, you know, versus TCP, the Datagram Protocol - that then allows the packet to run through a NAT router, for example, in a hotspot, traverse the Internet, come through another, like, user NAT router, and then, since the protocol is recognized - if it's recognized, I should say - by each end, then this allows IPSec to work through NAT without any problems.

Leo: So basically it's saying to IPSec, look, you don't have to change the packet, it's fine, we'll wrap it up in a wrapper that will keep its integrity from point to point. Then once it's inside the network we'll unwrap it, and then the router can re-address it.

Steve: Exactly. Now, Microsoft silently added this technology in XP Service Pack 2. So it does exist in Service Pack 2, even though Microsoft is hostile for their client hooking up to endpoint VPN routers, unfortunately. However, all of the very latest VPN routers also support it. For example, Netgear has an FVS318, like Frank Victor Sam 318. It's in its third version right now. The Version 3 router does support this NAT-T traversal. However, versions 1 and 2 don't. And unfortunately they're not upgradeable to support this. So if you had an earlier version of this particular router, you'd be out of luck. But if you've got a Version 3 router, you're okay. Similarly, all of the current D-Link VPN routers also support this. The problem is, it's very poorly documented on anyone's side. I had to contact D-Link and get a hold of a technical guy and say, okay, which of your routers support this? You don't talk about it anywhere. Well, they all do. However, only some of the latest Netgear routers support it. They do have a PDF that shows a spreadsheet of what features are supported. And there's a line item, so they're beginning to recognize that this is an important thing. But it still is sort of just on the emergence of being widespread.

Leo: So if you want to use a Windows computer to access your home network, and you have purchased a router that supports VPN, that must support also NAT-T, the NAT- Traversal, so your client can get into your network.

Steve: There are two ways, though, that a router can support VPN. So we want to be clear about this.

Routers for a long time have supported what's called VPN traversal - or I'm sorry, VPN passthrough. VPN passthrough acknowledges the problem of changing the port as the packet emerges from the NAT router. So what VPN passthrough does is, for one VPN connection, that is, if you're connecting to one remote server, the router recognizes, oh, look, this is UDP port 500, which is what IPSec uses for its transport. It deliberately leaves the port alone. It leaves it as 500 when it comes out the other side of the NAT router and puts it out onto the Internet specifically so that the IPSec packet is not broken. So the idea is this would allow somebody working at home who had to have a VPN connection to their corporate server, it would allow them to still get a VPN connection to their corporate server, even if they've got a NAT router in their home environment that would normally break VPN because it's just, you know, VPN, you know, IPSec cannot traverse through NAT. So VPN passthrough is different than a VPN endpoint. When you've purchased a VPN endpoint router, you've got a router that you can actually VPN to. It's the server of the VPN connection. So exactly as you were saying, Leo, you're out roaming around the Internet somewhere, and you use one of these third-party clients, you know, probably the same client whose router you purchased, just to make sure that there's not going to be any interoperability problem. And it allows you then to connect to your network at home.

Leo: I'm so confused, Steve. You've completely left me in the dust. Can we kind of boil this down to a series of recommendations? Or no?

Steve: Well, okay.

Leo: Look, let's get back to our original premise. I'm at a hotel.

Steve: Yes.

Leo: Or I'm actually - this is perfect because I'm planning to do this. Tomorrow I'm going to get on a plane. I'm going to go to a hotel. What should I do at home so that I can safely use that hotel network?

Steve: If you have a VPN endpoint router, that is, a router that is clearly a VPN router...

Leo: And it'll say so on the box...

Steve: You probably paid extra for it, so you may know that...

Leo: You'll know.

Steve: You know that you have it, even if you've never been able to use it before.

Leo: Which I haven't, okay.

Steve: Then you will need to purchase their matching client software because, unfortunately, Microsoft's built-in client technology won't connect to an endpoint router.

Leo: It's intentionally disabled in this LTPTPT2P2.

Steve: Yes. They just - they will not support it.

Leo: They don't want to, okay.

Steve: They won't do it.

Leo: For unclear reasons.

Steve: So you could then use this client software that you purchase for about $39 to connect to your router at home.

Leo: Okay.

Steve: Now, that would get you to your home network.

Leo: Right.

Steve: You could then basically do anything you wanted to with very good security using your home network. I should mention, though, that you will want to use a Pre-Shared Key, much as we've talked about with WPA technology...

Leo: So you have to set that up before you leave.

Steve: You do need to set it up before you leave. Now, the other problem is, and this is why I haven't pursued this all the way, is it turns out that ISPs or hotels can be...

Leo: Don't tell me they block the port?

Steve: Yes. That's the problem with this failing the holy grail solution also is - aside from needing to buy additional software - because you're using standard IPSec or Point-to-Point Tunneling Protocol ports - 1723, 1701, 500 - those could be administratively blocked if, for whatever reason, someone didn't want you to be using VPN within or through their network.

Leo: Do you think they're commonly blocked? Is that...

Steve: Yes. And in fact, I know that they are because I've run across sites which are trying to offer this as a service. And they say, well, if PPTP doesn't work, try using IPSec, you know, hopefully one or the other will.

Leo: Now, PPTP won't work if you're trying to use a Windows box because you'll have to use the LP2P, which Microsoft prevents.

Steve: Well, it turns out that we...

Leo: Is that right, or am I...

Steve: ...we've mentioned - kind of. We've mentioned one nice-looking service called PublicVPN.

Leo: Right.

Steve: PublicVPN.com. And it's something I would recommend for people as a possible solution for sort of, you know, in this myriad of solutions. It's inexpensive. It's $5.95 a month, or $59.95 for a year. They're

running servers that support Microsoft's PPTP and this Level 2 Tunneling Protocol, L2TP IPSec. What it means is that you need no client installed. They support all Windows platforms and the Mac platform, allowing you to create a secure connection to their server which would get you out of the danger zone. If you were in a hotel, for example, Leo, with your Mac, for $5.95 for a month you could get an account with them and connect to them, getting your traffic encrypted as it leaves the hotel's LAN, travels the Internet to them, where it would be decrypted and dropped out onto the Internet.

Leo: And it uses SSL, so it's unlikely to be blocked.

Steve: No, it uses - and that's why, again, it's probably not a great solution for someone traveling a lot...

Leo: Because...

Steve: ...because it does use the standard...

Leo: PPN.

Steve: ...PPTP and L2TP blah blah blah.

Leo: Yeah, yeah, yeah.

Steve: So but, you know, it's there. And we've talked about it before; so I wanted to, like, wrap that up when we were specifically talking about it.

Leo: There's another one called HotSpotVPN that might be...

Steve: Now...

Leo: How about that one?

Steve: Yes. I'm just...

Leo: It's less expensive.

Steve: I'm just opening a dialogue - actually it's more expensive. They have a special of $8.88 per month at the moment.

Leo: Oh.

Steve: Otherwise it's like $11 or $13 or $15, depending upon how many bits you want your key length to be, which actually is pretty hokey since even 128-bit key would be fine.

Leo: Plenty, yeah.

Steve: These people are an SSL-based VPN. But I haven't yet finished my dialogue with this guy to figure out exactly what it is they're doing. So we will definitely...

Leo: No endorsement yet, but we're looking at it.

Steve: Yeah, no endorsement yet. But we'll come back to it. Ultimately, Leo, you and I are going to take a look at this OpenVPN service, and another one that I have found called Hamachi, which both look like they're very interesting solutions.

Leo: It's not merely yellowtail tuna, it's a VPN solution.

Steve: Exactly.

Leo: Okay.

Steve: However, for the sake of completeness, for people who have VPN endpoint routers, want to know how to use them, I can guarantee them they cannot connect with a Windows client. They need to purchase the client from their supplier.

Leo: Because that uses the NAT-Traversal.

Steve: Yes. And also they need to make sure they have either updated their firmware or that their particular VPN endpoint does support the NAT-Traversal. Otherwise they absolutely won't be able to connect from a hotel. And even if it does, they are subject to the VPN packets being filtered by policy by the hotel or - for example, maybe somebody wanted to VPN from their corporate environment to their home to get a file or to check up on their systems there or something. They might well find that their corporate firewall is blocking outbound VPN connections, even while allowing incoming VPN connections from people that were outside the corporation coming in. As a corporate policy, they might be really locked down. So there are problems with standard VPN technology being used all over the place, even if you're got a VPN router. I'm still aiming at coming up with a better solution, and that's what we're going to talk about next week.

Leo: Good. I'm exhausted. Okay. So I just want to recap so that people aren't completely left in the dust. And if anybody's still listening, they're very brave. Because this was complicated, and it had a lot of acronyms in it.

Steve: It did. Although, based on the feedback we've had, this is the discussion people want because they...

Leo: Well, yeah.

Steve: ...want to understand the limits of virtual private networking.

Leo: And we all want to solve this problem of how do I use a network at a hotel safely? And if you're not clear why we want to solve this, listen to some of the earlier episodes, particularly, I think, Episode 14, where we really talk about why it's just not safe to use a hotel's network.

Steve: Well, and Leo, in all honesty, we haven't yet really explained the danger. I don't want to really do that until we have some solutions in place.

Leo: It's worse than you think.

Steve: You mentioned ARP poisoning, and it's a horrible problem.

Leo: Okay, okay. Don't, don't - because you're going to scare people. You're going to scare me. I got ten days on the road coming up. Hotel access for all ten days. Okay. And you still have not found the holy grail for me. And I've been trying all these solutions, you know, SSH tunneling and OpenVPN and so forth. And so, well, all right. And I'm worse because I'm on a Mac. Does that make it worse or better? At least I don't have to deal with Windows blocking IPSec.

Steve: True. The Mac does support PPTP, although it turns out that that is subject to man-in-the-middle attacks. It has no strong useful authentication, and it has been cracked by various tools that are able to insert themselves. And in fact, we're going to show how easy that is to actually do in the real world.

Leo: All right.

Steve: We're going to get the solution, but we need to create a nice foundation here first.

Leo: Oh, it's so frustrating. Well, it's good. No, and so I understand people really want to know this. And it was complicated, but we're laying the foundation for why...

Steve: We've ended up choosing something else.

Leo: We have to go a particular route.

Steve: Yes, exactly.

Leo: Okay. And it's just - it's interesting. All right. So thank you very much, Steve, for explaining this. And as difficult a subject as it is, even a dunce like me, I think I've understood it. If you want to know more, the show notes are available at GRC.com/securitynow.htm. And they are very helpful for kind of elucidating this because you've got pictures, you've got a graph, it makes it just much easier to understand.

Steve: Yes. And, in fact, for this episode I have an extensive list of links that people can poke around at if they want to fill in the gaps.

Leo: And thanks to Elaine who's going to transcribe all this and make sense of it. You can even reread it slowly. And maybe reading out loud with your mouth moving will help.

Steve: I had one person named Andrew posted a comment. He said, wow, your podcasts have really picked up speed. I got a kick out of that. I thought that was a nice analogy.

Leo: Does he mean they're getting more complicated?

Steve: I think they've really got his interest.

Leo: Good. Well, and we're not always going to do this kind of high-level stuff. We're going to mix it up. But frankly, this is an issue for everybody, that everybody has to solve. And, you know, we will get - you think the next episode we'll finally get this holy grail thing?

Steve: Yes. We're going to talk about the very interesting cross-platform solution called OpenVPN. People who want to do a little research ahead of time can put "OpenVPN" into Google. They'll find a ton of links. It's a very popular-looking solution. But it's not zero-configuration by any means.

Leo: Right. I know, I've been trying, and I can't figure it out. And who knows, it'll happen in seven days. We could find out there's a horrible hole in it, and then we'll have to find something else.

If you want to read those transcripts that Elaine works so very hard on, of course, again, GRC.com/securitynow.htm. Steve also hosts 16KB versions of this for easy download. And we have decided that we're going to put together some audio CDs of the year when we get to January so that you can buy it as a portfolio and give it to your favorite IT person. We'll let you know about that. If you want to listen on AOL, we're on part of the AOL Radio on the Podcast Channel. So tune in there. And we thank AOL for providing that and for providing the bandwidth for Security Now!.

All right. I have a plane to catch. Steve Gibson, thank you very much. I really appreciate your explaining this and all the work that you must have to do to understand it yourself.

Steve: Thanks, Leo.

Leo: It's a tangled web we weave.

Steve: Talk to you next week.

Leo: That's it for this edition of Security Now!.