Listener Feedback Q&A #1

Description: Leo and I discuss questions asked by listeners of our previous episodes. We tie up loose ends, discuss a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world "application notes" for any of the security technologies we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-016.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-016-lq.mp3

Leo Laporte: This is Security Now! Episode 16 - your questions, Steve's answers. Steve Gibson is on the line via Google Talk from his...

Steve Gibson: Hey, Leo.

Leo: ...lair in Irvine. Hi, Steve.

Steve: My fortress of solitude.

Leo: Every - we decided every Mod 4 podcast we're going to start taking questions and responding to them. Is that the idea?

Steve: Yup. Yup.

Leo: Yeah. And this is Mod 4, Episode 16.

Steve: Yup, so episode numbers that are evenly divisible by four will be Q&A. And it's really nice because lots of people are posting questions to the form at securitynow.htm on my website at GRC.com. I'm pretty much keeping up. I mean, I am at the moment up to date. And I'll sort of see, like, a question that's asked many times in different ways. And it's like, okay, this is something that, you know, we need to deal with. And also there are issues that come up that really aren't big enough to be a whole half-hour Security Now! episode, but are, like, it's a real good point. And so it really helps me. Also a lot of people are, you know, they have different experiences. For example, we've talked about GoToMyPC. A huge number of people have said, hey, what about LogMeIn.com?

Leo: Right, right.

Steve: And so, you know, there's another system that is free for their minimum service, that allows people to access their computers remotely. So it allows us to, you know, to bring those things to light, too, basically closing the loop of feedback with our listeners.

Leo: So let's close the loop. And we start with our first question. And this, again, it's a composite of a number of questions along these lines.

Steve: Exactly.

Leo: Referring way back to your passwords episode, which, gosh, that was one of our very earliest episodes, wasn't it.

Steve: We did, I think, the first couple episodes on passwords.

Leo: Yeah.

Steve: After the Zotob worm. That was the very first one.

Leo: Yeah. And that was a great topic. The need for using strong passwords that can't be guessed makes sense. But writing them down and keeping them in my wallet scares me. What if my wallet fell into the wrong hands? What should I do?

Steve: Ah. And many people have mentioned that. It's like, hey, you know, they like the idea. I mean, they get it that using a password that's complex and has, like, upper and lowercase and just gobbledygook makes total sense to them. But, and then that means you have to write it down. Otherwise you're never going to be able to remember it and get it right again. But what if someone discovered that?

Leo: Right.

Steve: And my idea is that, okay, write down a variation of it. For example, maybe write it down with the first five letters from the end on the front. That is, make a simple change to it when it's written down that only you know. So you have a secret way of turning what you wrote down back into what your real password is.

Leo: So somebody finding the wallet's not going to have anything.

Steve: Exactly. And even if they tried to use it, you know, it's not going to work. And they'll go, okay, well, I guess this isn't the right thing. Or...

Leo: I do that. I just shift the capitalization in a certain way that is according to a rule. And that won't work...

Steve: That would be good as long as where you were logging into...

Leo: Was case sensitive, yeah.

Steve: Exactly, was case sensitive.

Leo: Most places are.

Steve: Or maybe just tack on your own secret five characters to the end of everything that's written down.

Anyway, the point is - and people can figure out their own algorithm because we don't want to give it away because otherwise we've lowered the security. But do something to what you write down in a uniform way that, you know, only you know. And so you've still got an aspect of it that is secret.

Leo: And this isn't - by the way, as soon as we finished that podcast, I started changing all my passwords using this portable password policy that you came up with. And I do it only on the low to medium security sites. I have to have stronger passwords on my bank and so forth. But I'll tell you what I - you know, it's not exactly this, but it's like this. I will take the name of the site. So if it's Google, without the dotcom, just Google, and then I will intersperse the letters with the last four digits of my Social Security number.

Steve: Nice.

Leo: And that works. You know, as somebody pointed out in another email, if a couple of webmasters got together and looked at my passwords, they'd be able to figure out how I was doing it. But first of all, that's unlikely. And that's why I only use it in lower security issues.

Steve: Yeah. And another point has been brought up, actually, another question that I've had several times that this now occurs to me, is many people wrote in saying, okay, but what about a situation where there's a password policy that forces me to change the password every so often?

Leo: Yeah. I hate that.

Steve: That breaks the algorithm approach completely.

Leo: Right.

Steve: The only thing I could suggest is maybe put a serial number on the end, you know, 000, 001, 002. Again, technically you would know, like, what the password was before, if you knew what it was now. But it would allow you to quickly try a few things to get the one that's correct. And again, it's a way of mutating an existing password, making a slight change to it. Still, the bulk of it is completely random and high security.

Leo: Also you created a password page at GRC.com/passwords that generates, you know, truly random strings for wireless encryption.

Steve: Well, and it's just great raw material. It's raw material for any time someone needs a password, you know, chunk.

Leo: So people wrote and said, okay, fine, but how should we manage that password? You know, for instance you have guests who are wanting to log onto your wireless network. Do you give them, the guests, the password? How do you do it? It's so long and difficult to handle.

Steve: That's a very good point. I sort of glibly said in a podcast, oh, just cut and paste, without thinking it through. Because, you know, somebody who comes to your home isn't yet on your network. So cut and paste what?

Leo: Right.

Steve: I have a couple thoughts. One would be, if you have a floppy drive, of course, if people still have diskette drives, you could just use that to move the password over to their machine. Failing that, USB drives are more and more universally available now that would allow you to get into their machine. Or, if they could

get on the 'Net any way, and then, for example, you email it to them or, like, leave it on Google Mail, for example, and then you briefly log on, download...

Leo: On their machine, yeah.

Steve: On their machine, you know, just in order to get it over to their machine.

Leo: I think I like the USB Key. I think that's a great idea. People more and more are using USB Keys to store stuff like that. And that's a very good use for it, I think.

Steve: And, you know, frankly there's been a lot of issue about - and as we look at these questions, this problem of merging security and lack of security continues to create problems. So another possibility is, if this person doesn't need security while they're at your house, just shut down your encryption. Just, you know, with a...

Leo: Oh, yeah.

Steve: ...button on your browser, turn off your encryption...

Leo: Let them use it, yeah.

Steve: ...while they're visiting. You know, don't you do anything, but...

Leo: It's just temporary.

Steve: ...don't do any online banking with all your neighbors. But, you know, like, while they're there...

Leo: Yeah, that's fair.

Steve: ...you know, you accommodate them. And then when they leave, you switch back up to strong encryption.

Leo: Here's a question that addresses something that we're in the middle of right now. Is it possible to use a public computer in a hotel, a library, an airport, with total safety? What are the security and privacy concerns?

Steve: Well, now, that's a really good question because that's a little different than sort of the VPN topic that we're going to continue talking about for the next couple episodes. This is, like, you go to a library and want to do something. The problem is, even if you logged into Google Mail, for example, you could use a secure connection to Google Mail to prevent your dialogue from being listened to. But you're using somebody else's hardware and, you know, essentially booted with somebody else's software. So you don't know there's not a keystroke logger monitoring everything you type at the keyboard prior...

Leo: Oh. So even if you had a VPN, they could keep track of that.

Steve: Exactly.

Leo: Oh.

Steve: I mean, if you use GoToMyPC, if you do LogMeIn, or like that SSL-Explorer that we talked about that allows...

Leo: Doesn't matter.

Steve: Yeah.

Leo: Doesn't matter. You're still getting your keystrokes logged.

Steve: So it is a - and in fact, anecdotally we hear that those computers in public locations tend, you know, like script key guys like to install even like a hardware keystroke logger, just inline in the keyboard.

Leo: And that's undetectable. You cannot detect that.

Steve: Yeah. And so they, you know, some kid sticks it in the keyboard, sits back and pretends to be reading a magazine while other people come up and use the computer. Then they unplug it, take it home, and dump out everything that was typed.

Leo: Oh. So what can you do about that?

Steve: Don't use public machines.

Leo: [Laughing]

Steve: No, I'm not kidding. There is no - again, there's just no...

Leo: Can't be secured.

Steve: There's no safe way. Even if it's not a hardware keystroke logger, it could be something in software that somebody else has deliberately installed to hack the machine. So, and it's an important lesson, I think, overall, in terms of a security policy, is having known control of the platform that you're using.

Leo: Hardware control, yeah.

Steve: Yeah, it's your laptop, you're carrying it around, you don't loan it to somebody who you don't trust because, you know, in general you tend not to because presumably you've got other stuff on the laptop that is yours. So maintaining physical control of the computer is definitely part and parcel of being able to be secure using that machine. So you really need to remember that you can't use somebody else's computer that you have no security oversight on in a secure fashion. Sure, it's safe to go Google and browse around and not do anything important. But be very careful, not even logging into Google Mail on a public hotspot machine, because anything could be happening there.

Leo: Wow. That's a good warning. Several times, another questioner asks, you've mentioned that hubs are less secure than switches. What's the difference between a switch and a hub, and why do hubs allow you to see the entire network? Are switches one-way devices like NAT routers?

Steve: Okay. That's, again, a question that's come up a number of times. The idea between a switch and a hub is that, first of all, only with current 10BaseT technology - you remember that there was - I've lost my vocabulary. Was it 2BaseT?

Leo: Oh, the old coax, you mean?

Steve: Yeah. With coax you actually had an electrically shared connection.

Leo: I remember that because, if you unplugged your computer from the network, the whole network would die because it was serial.

Steve: It was a nightmare.

Leo: It was terrible.

Steve: But you were actually...

Leo: Had these T connections everywhere.

Steve: You actually had multiple computers on the same physical wire. Well, the way 10BaseT works is different. You have a single computer connected to a hub or a router so that each computer is electrically on its own set of wires, which is really important. Inside the hub, now, inside a hub or a switch is essentially a little mini NIC, a little network interface, just like you have on your computer for every one of its connections. With a hub, anything that any one of those wires receives is sort of mindlessly sent back out of every other one of the connections.

Leo: That's what it means not to have any routing. It's not routed. Everybody gets a look at every packet, and then the one that's for you, you take.

Steve: Well, routing...

Leo: Kind of; right?

Steve: We have to be, yeah, we have to be careful of words because routing is something else. The right term would be "switching," where the idea would be there's no switching, so that what one port receives, all other ports hear. And so that's a hub, where you actually - everybody's sort of on - they're not quite on the same wire electrically, but they're all seeing any information that anyone sends. So the reason this is a problem in a hotel is that you could have a huge hub or a set of hubs where something that one computer on the 12th floor sends to the Internet, literally every other machine in the physical hotel is able to sniff that, and essentially receives that traffic.

Leo: You know me and physical analogies. I've got one for you.

Steve: Oh, good.

Leo: That will explain this. So it's as if you're in an office, a crowded office, and somebody wants to pass a phone message to you. They can come in the door and shout the message. You'll get the message, but so will everybody else in the office.

Steve: That's perfect.

Leo: That's a hub.

Steve: Yes.

Leo: If you had a switch, you would be divided up into different rooms in the same office. There'd be other people in your room. But the person who comes in and shouts the messages is only heard by those people in your room, that is, that segment on the switch.

Steve: Well, actually a switch is even better than that. It is exactly like someone coming in and whispering just to you.

Leo: Oh, really. Oh, I thought a switch divided the network into segments that were still public.

Steve: No.

Leo: Oh, okay.

Steve: What happens...

Leo: So my analogy doesn't work, then. All right.

Steve: Yeah. I mean, it's sort of tricky because what happens...

Leo: Because I was going to say a router is like somebody calling you on the phone and saying that message directly to you.

Steve: A switch does that, too.

Leo: A switch does that, too. Okay.

Steve: What happens is a switch learns which MAC address, which physical NIC is on each of its segments. Now, if you had a master switch, and then it was connected to other switches, and then they were connected to NICs, so you sort of have a hierarchy? In that case, the switch at the top of the tree would learn, like, maybe that there were 10 NICs that were connected to its first port because that then connects to another switch that learns which NIC is on each one of its ports.

Leo: Right.

Steve: So it is possible for a switch to send multiple traffic down one of its connections that's then further subdivided by another switch or a hub out further away from it. But essentially, the bottom line, no one listening to traffic on a switch is able to ever hear anything other than what's bound for it.

Leo: It's the guys coming up and whispering in your ear.

Steve: Exactly.

Leo: Okay.

Steve: Just like it's whispering in your ear. In fact, it's funny that hubs are becoming endangered now. It's hard to find hubs because switch technology is coming down in price, and it's just better. So I literally, because I'm in, you know, sort of in the network end of the world, I've purchased a bunch of hubs, just sitting in boxes, before they disappear completely.

Leo: I have some I can give you, Steve, if you really want some.

Steve: Well, because they're so useful for me. I want to be...

Leo: Well, in our own...

Steve: I want to be able to sniff the traffic on my own network and watch other computers talking to each other. You cannot do that if you use a switch to connect all your computers together.

Leo: To understand this really requires an understanding how Ethernet, which is a networking protocol that is being used, works. It's a broadcast protocol. Without any special switching, it will just send everything to everybody.

Steve: Yeah. In fact, in one of our earlier...

Leo: And that's inefficient; but, well, it's actually got some efficiencies and some inefficiencies.

Steve: Well, it's inefficient because you start having packet collisions.

Leo: Right.

Steve: The way Ethernet works is that, essentially, anyone can talk on the wire at anytime they want. If two people talk at the same time, they will collide. Their packets literally collide and scramble each other's bits on the wire. But each of them is listening to the wire as they're talking. So in the old days, when you literally were all on the same wire, or even today if you're on a hub instead of a switch, if two computers on a hub send at exactly the same time, their packets will collide. But because they're all hearing what everybody else says, they hear their own collision, and they realize, oops, somebody was talking, started transmitting at exactly the same time I did. So what they do is they back off, they wait a random amount of time and retransmit. Well, the chances of a second collision are low. But if it happened, then they would, again, they'd wait a random amount of time and try again. The point is, this technology, it's called CSMA, Collision Sense Multiple Access. That's the original brilliant Ethernet technology that Bob Metcalfe invented back in the old days.

Leo: And that's why people came up with switches, because on very large networks you were getting so many collisions that you wanted to kind of segment your network to make it more efficient, to reduce collisions.

Steve: Well, that's exactly right. If your network gets huge, and you've got a certain number of computers, what's happened is the Ethernet starts to fail because you end up with a much - the rate of collisions starts going up so high that no one is able to get their message through without somebody else stomping on it.

Leo: Right.

Steve: And a switch is a store-and-forward technology. It receives the packet; it looks at the MAC address to see where it's bound for. It looks up in a table that tells it which ports the MAC addresses are connected to. And it resends that packet only out on that one port. That's that switching behavior. And that prevents your network from collapsing as it gets really big.

Leo: All right. Let's move on because we have a lot of questions. I want to get to as many as we can. This is a very interesting one from a Good Samaritan. He says, there are a number of unsecured Wi-Fi access points in my neighborhood. Is there any way I can contact them, aside from knocking on doors, and warning them about the security issues that they're facing?

Steve: That's an interesting question. I thought about it when it was asked, when I received it from the web page. Certainly anything he would do over Wi-Fi would be illegal. I mean, in the early days of filesharing, there were - remember where we had open filesharing ports? There were people who would put text files on other people's desktops telling them that their - I never did this, but...

Leo: This is not nice.

Steve: That's not a good idea. I mean, it's illegal for someone to alter anyone else's computer, even if you have the best of intentions.

Leo: You mean like Sony?

Steve: Yeah, exactly.

Leo: Okay, let's not - we'll get into that later.

Steve: So unfortunately the only thing I could suggest is what this guy suggested, maybe like printing up, you know, Xeroxing some leaflets, some little information pamphlets, and say, hey, I don't know who you are, but my computer can see your network, and it's not secured. It's wide open. I'm not touching your network, and I never have. But you ought to go start listening to Episode 1 of Security Now! with Gibson and Laporte...

Leo: We wouldn't mind that.

Steve: Exactly.

Leo: Do a little ad for us.

Steve: Again, there's no way it is not illegal. And believe me, you could piss off some knee-jerk neighbor who could have the cops out, and it would be a problem.

Leo: You don't want to do that, yeah.

Steve: Nope.

Leo: Here's a fellow who's been listening well, I think. He's using WPA, which is the encryption that you recommend for wireless networking. He's using the Pre-Shared Key, the PSK version.

Steve: Right.

Leo: And TKIP. He says he's using a killer key from your passwords page. But since AES encryption is better than TKIP, which you said still uses the RC4 encryption from WEP, I'd rather use AES. My vendor doesn't offer it. What is a boy to do? Or girl, I'm not sure.

Steve: This, again, is sort of a composite question that many people have asked. They recognize that, okay, they're happy they are no longer using WEP. But they know there's something more. They're, like, using WPA instead of WPA2. They know that there's something more. Or there's, like...

Leo: That's good enough, isn't it?

Steve: Yes. And that's my point, is there's nothing wrong with RC4. This AES...

Leo: It was how it was implemented that was bad.

Steve: Yes. RC4 is a fantastic cipher, extremely random. You mix that with your clear text, you get undecipherable crypt text. There's just no way that anyone is going to be able to crack it. So I really think that any concern about going beyond basic WPA with a pre-shared key, and especially if you're using one of those gobbledygook 63-character passwords from my passwords page, I mean, you are just nailed down. You are super secure. And there's another reason not to go further. You might be able to get, like, one computer and your access point to hook up. But the further you push the encryption, the more problems you're going to have with other devices. Somebody comes over who doesn't support - they may support WPA with a pre-shared key, but not the higher level that you're using. So WPA with a pre-shared key is so strong, you just really - you can stop there with confidence.

Leo: If you don't want to bother with proxies or VPNs at a public hotspot because you're just doing email, how secure are the secure features of web mail systems? He asked about - or this person asked about Google Mail. But I'm actually curious. I use FastMail, which is an IMAP service, but it does SSL. Am I secure? Is he secure?

Steve: Yes. Yes. Now, we've got to be a little bit careful when we say "public hotspot." As long as we mean you use your computer that you have controlled and public connectivity...

Leo: A public terminal is another problem entirely, as we talked about earlier.

Steve: A public terminal, as we discussed before, that's just a big no-no. There's just no safe way to do that.

Leo: Okay. But your password is sent encrypted. Your entire transaction is encrypted. And most of these services, I know Google and FastMail do this, you can click a box to say, yeah, I'm on a public network. Don't, you know, make sure that nothing gets saved and all that stuff.

Steve: Yes. I would say that it is completely safe. SSL will protect everything you do once it's connected. So, for example, if you use https://gmail.com to get onto Google Mail, and make sure that it keeps you on a secure connection as you move around the website - I believe it does - then you're safe. As long as all you do is email that is over that SSL connection from a public hotspot, you have nothing to worry about.

Leo: And listen next week because we are going more into detail on how to create a VPN that you can use to be secure all the time.

Steve: Excruciating detail.

Leo: Oh, man. No, let's not get started, because I've been playing with some of the things you're going to suggest. And "excruciating" might be the right word.

Steve: Yeah.

Leo: Is it possible, one listener asks, to compromise a NAT router or a NAT router modem? Here's what happened. Normally ZoneAlarm is silent on his PC. A few weeks after resetting the NAT router he began to get a couple of ZoneAlarm alerts from real IP addresses. He reset the NAT router again. That made it go away for a few weeks. But it comes back. Is he being corrupted? Is he being compromised?

Steve: Yeah. I would bet money - you know how we've talked about the moment you put a NAT router in, your personal firewall goes silent because there's no way unsolicited traffic is able to enter through the NAT router any longer.

Leo: Any alerts you get will be from outgoing, outbound traffic, not incoming traffic.

Steve: It'll be your own applications asking for permission to use the Internet, exactly. I would bet anything this guy's got Universal Plug and Play enabled on his router. And that is a big no-no. Universal Plug and Play is an insecure technology that Microsoft created which allows - basically, it's sort of their zero administration effort. The idea is they want their MSN Instant Messaging and things just to work. They don't want to ask users to open ports through their router, to have to do, like, static open ports. Basically, Universal Plug and Play allows the computer to tell the router to open ports. And what's worse, it doesn't show in the user interface. You can't go to your router and see what ports have been administratively opened behind your back. It's really bad. And so this sounds like exactly what's happening here is that something in the user's computer - and that's the other problem. It could be malicious. It could be a trojan that doesn't want to get cut off from the outside world. It installs itself. It uses Universal Plug and Play to bring his router defenses down deliberately so that unsolicited junk is now able to enter through his router. You absolutely have to disable Universal Plug and Play, and then reboot your router. Otherwise...

Leo: And that will be somewhere in the router settings, if you log in or out.

Steve: Yeah, it'll always be in the user interface. And the good news is most of the routers I've seen seem to have it disabled by default...

Leo: Oh, that's good.

Steve: ...because they're recognizing it's a problem.

Leo: Oh, that's interesting. That's something new. Maybe because of you. I don't know.

Steve: Well, I've been pounding on people about it.

Leo: Good. What are your feelings, another writer asks, on file and print sharing on a home network if you have a NAT firewall, you know, you're behind a router? I know that XP has a fit about the security issues when you set sharing up. It really does. It warns you several times.

Steve: Oh, yeah.

Leo: But it is a prime reason I have a home network. I want to be able to use one printer on the network. All my machines, I want to be able to share files. He's not alone. Everybody, I think, wants to

do that.

Steve: Yup.

Leo: In addition to being behind the router, the NAT firewall, I have also installed NetBEUI on all my PCs, XP Pro and Home, plus 2003 Server - and that's because filesharing's a little easier over NetBEUI, I'm sure - and have unbound file and print sharing from TCP/IP, so that it is only accessible via NetBEUI.

Steve: Oh.

Leo: Was that a good idea?

Steve: This guy, he's...

Leo: That's clever, isn't it.

Steve: Well, he's read my ShieldsUP! pages. That was what I discovered years ago, was that you did not need TCP to do filesharing. NetBEUI was Microsoft's original protocol...

Leo: Used to be called NetBIOS.

Steve: Well, actually...

Leo: Pretty much the same, isn't it?

Steve: Yeah. They're certainly related, although they are different technologies.

Leo: Oh, okay.

Steve: NetBEUI's an actual transport protocol. What's cool about NetBEUI is it is a non-routable protocol. It is unable to get away from your local network. There's no IP address in NetBEUI. It's all only for a LAN, not for a WAN. Now, if listeners don't know what we're talking about, this is all about what ShieldsUP!, the original security stuff on my website, is about. And it shows you how to do this thing called unbinding TCP/IP from file and printer sharing and using NetBEUI instead. I mean...

Leo: Isn't he protected, though, anyway?

Steve: Yes.

Leo: Because he's got the router protecting...

Steve: I was just going to say, he's a real suspenders-and-belt guy who's got, you know, super level of protection. So he would be safe using NetBEUI even without a router because...

Leo: Because port 139 is blocked by the router.

Steve: Yes.

Leo: And nobody's going to be able to make any NetBIOS calls.

Steve: Well, and NetBEUI doesn't have ports. I mean...

Leo: Oh, it doesn't. Oh, I get it. All right, okay.

Steve: I mean, it's completely - it's a non-Internet protocol.

Leo: I see.

Steve: And so by...

Leo: So what is port 139? That's a NetBIOS - that's a filesharing port, isn't it?

Steve: Yeah. It's NetBIOS over TCP.

Leo: So that's what we're disabling.

Steve: Exactly. And so by unbinding file and printer sharing from the use of TCP, you're, like, in a whole different networking realm that can't go anywhere. I mean, he is super safe.

Leo: Good. Good job, in other words. But not necessary as long as you block those ports. If you get a green light from ShieldsUP!, you're stealthed on port 139 and the filesharing ports. You don't - that's enough.

Steve: If you're behind a NAT router, you're safe anyway.

Leo: Anyway.

Steve: Yup.

Leo: Okay.

Steve: Because NAT protects you.

Leo: Right. You've said that SSL connections are not susceptible to man-in-the-middle attacks, but I've read that they are. I want to believe you, but why do others think that SSL is susceptible to MITM attacks? And when an SSL or VPN authorizes, what stops someone listening to the packages each way to figure out the keys? So first let's start with what is a man-in-the-middle attack?

Steve: Okay. In fact...

Leo: I have no analogy for this one. You're on your own. I mean, I could do it, but I'm going to let you

do it.

Steve: We're going to start the beginning of the New Year talking about the way the Internet works - what's ports, what's IP addresses, what are packets and all that.

Leo: Oh, good.

Steve: Then we're going to talk about crypto because we really need a foundation to understand some of this more advanced stuff. So it's probably the wrong time for me to answer this because we don't have enough foundation for me to talk about how SSL security works and how man-in-the-middle attacks can be avoided. I wanted to bring up the question because so many people are asking it.

Leo: A man-in-the-middle attack is when somebody kind of poses as the receiving or the sending site.

Steve: Yes.

Leo: And intercepts traffic.

Steve: Yeah. The idea is that it's one thing to passively listen to packets going in both directions. And that was the second part of this question was, if someone listened to this session, this SSL or the VPN connection being established, why doesn't that give them all the information they need to decrypt the whole conversation?

Leo: Right.

Steve: Because, after all, they've heard everything that both sides have sent back and forth to each other. I mean...

Leo: But that's public key cryptography. That's the whole point of public key cryptography.

Steve: Exactly.

Leo: In the old days, if you had a decoder ring and, you know - or you had to send the guy the decoder ring; right? And if anybody intercepted the decoder ring, he could copy down the algorithm and then send the decoder ring on, and you're cracked. But because of public key cryptography, I can send you the public key, and it's still useless. Is that basically it?

Steve: That's it. And that's probably all we should say for now.

Leo: It just means it's possible to exchange a key without compromising security. You still need the personal, the private key to decrypt.

Steve: It's sort of like, okay, I could explain this now...

Leo: Let's save it.

Steve: ...but people would get more confused...

Leo: Let's save it.

Steve: ...and everyone's eyes would cross.

Leo: That happens anyway. Let's not...

Steve: So I want to explain this. It's so cool how this works.

Leo: It is. It is.

Steve: And I think people are going to get a big kick out of it. But if we do a partway job, people will just end up being more confused.

Leo: So just answer this question. So man-in-the-middle is not possible with a properly implemented SSL?

Steve: Oh, boy. We're going to get into trouble, Leo.

Leo: Okay. You could say - you could fudge it. You could say "in some cases."

Steve: If it - no. There's just no simple way to answer the question. SSL is susceptible to man-in-the-middle attacks if authentication is not involved. A man in the middle, there's no way for a man in the middle, who's somebody who's not just passively listening, but is actually able to impersonate the people at either end, that is...

Leo: That's why these certificates are so important. Certificates are the authentication you're talking about.

Steve: Certificates are an aspect of authentication. But again, here's where we really need to get careful with our definitions.

Leo: Okay.

Steve: So there's just - we're going to have to wait.

Leo: Okay.

Steve: People are going to love this...

Leo: Stay tuned.

Steve: ...when we explain it, yes.

Leo: By the time you've listened to Episode 99 of Security Now!, you will be the next Bruce Schneier.

Nintendo just launched its Wi-Fi service for the Nintendo DS. You can now go to McDonald's and play games against other DS people. The problem is the device doesn't support WPA encryption. The DS only has WEP. Many small portable devices are like this. Any suggestions for a home network where we might want to use these devices and still be secure? In other words, if I've got a DS, and I've got a WPA-encrypted network, I can't use the Wi-Fi.

Steve: Yeah. And this sort of question has come up in many different flavors. For example, there's some people that have their TiVos on a wireless connection.

Leo: Right.

Steve: But TiVo only supports WEP. It doesn't support WPA.

Leo: Right.

Steve: They want to run their whole network on WPA, but now the TiVos are stranded.

Leo: Now, Palm did the right thing. They support WPA.

Steve: Oh. In fact, Leo...

Leo: Which is nice.

Steve: ...I took one of my hairy - I was going to say "hairy-ass passwords" - from my own passwords page. I mean, this thing just makes your eyes cross. 63 characters, it looks like, you know, the computer is badly broken. I did, I copied and pasted it using a little SD card into my Wi-Fi, my new TX, dropped it in, and it connected right up to my network.

Leo: Isn't that great.

Steve: Oh, using real strong WPA encryption.

Leo: But so if you have a DS, you just - either you don't use it on the network; or you set the network for WEP during that time; or actually, as you mentioned earlier, you could just turn off security during the time you want to use it.

Steve: The thing that I've suggested to people whose email addresses I had was - and actually they wrote back and loved the idea. So I guess maybe it's feasible. It's possible to run two networks.

Leo: Oh.

Steve: There's nothing to prevent you from having your - and this actually solves the problem of people coming over to your house, also.

Leo: So have an insecure network and a secure network.

Steve: Exactly. You might want to run MAC address filtering and hide your SSID so that your neighbors are

not using - I mean, I would suggest having one that is WPA running at full security, and probably just leave the other one wide open. Don't even bother with WEP security on the other one if you really don't care. But do use MAC address filtering...

Leo: Just to keep it out of prying eyes.

Steve: ...to keep your neighbors from using it by mistake. Then your TiVos can connect, your Nintendo DS can connect, your neighbors who bring their laptops over...

Leo: Real quickly, what would the topology be? You would have, okay, I have my cable modem or DSL modem. It's connected first to the insecure access point, and that's bridging to the secure access point?

Steve: There are levels of security that you could go through. But as long as you've got a switch on your router which is isolating the traffic from each other, you're going to be very secure.

Leo: Ah. So you have a router connected to the cable modem and a Wi-Fi access point coming off that router...

Steve: Yup.

Leo: ...that is open.

Steve: And it's not going to see any of your - and none of your encrypted traffic would ever be decryptable anyway because you're on WPA.

Leo: Right. So a modern router is going to have a switch, and it's going to be - that'll be sufficient. An older router might not, but...

Steve: Yup.

Leo: Okay. Let's see. We only have a few more minutes. Let's get a few more in here. What's the security of the Windows Remote Desktop? Is it safe? Is it secure? Do you recommend using it at a hotspot as a kind of VPN?

Steve: Ah. That's a great question. And we're going to do one whole episode on Remote Desktop security and securing Remote Desktop because it's a really nice way for people who are interested in not using a third-party service like GoToMyPC or LogMeIn.com, for them to be able to access their machines. Microsoft has tried for years to make this secure. And they still haven't got it right. It is deeply encrypted. With XP you're using 128-bit RC4 encryption cipher. So it is extremely encrypted. It is, however, susceptible to a man-in-the-middle attack, like we were saying before. There are even freely available tools - this Cain & Abel tool has a Remote Desktop Protocol man-in-the-middle logging and interception capability that basically someone can sniff that traffic - actually can't sniff it. I need to be careful here myself. They have to actively modify the initial log-in dialogue to insert themselves in the middle. But these tools are available and are known. Then they are able to record everything you do with your Remote Desktop. Now, this is one of those deals where someone says, okay, c'mon, Gibson, you know, it's encrypted, it's secure, it's not susceptible to passive eavesdropping. Isn't that good enough? I have to say yes, probably it is.

Leo: But you should beware that there are holes.

Steve: Yes. It is - and there again, that's always where we draw the line. I want to tell people what is possible, let them decide whether they care or not.

Leo: Whether it's probable.

Steve: Exactly. Microsoft has the problem that they are not securely authenticating. There is no authentication technology in Remote Desktop, and no secure certificates. They actually tried to fix this earlier this year and still didn't get it right.

Leo: Essentially what you're saying is that it's secure, but it's not perfect.

Steve: It is deeply encrypted. It's very strongly encrypted. No one sniffing the traffic would ever be able to get it. And the only vulnerability in the desktop protocol - which is what they're using, RDP, Remote Desktop Protocol - is that, if somebody really wanted, I mean, like, knew you were going to be using Remote Desktop, got all set up, and managed to intercept and modify your traffic on the fly, I mean, it's much more of a theoretical vulnerability. But it exists, and it has been exploited, and the software is on the 'Net that allows it to be done. Then somebody could, essentially without you knowing it, monitor everything you did remotely - mouse movements, typing on the keyboard, capturing your keystrokes, logging in with your email client, running on the other machine and so forth. So it is, like, a theoretical exposure.

Leo: All right. We are out of time. I wish we had more. But, you know what, we will do more. Every fourth episode we'll answer more of your questions. So keep them coming.

Next week, Steve, are we going to finally find that holy grail of safe computing on the road?

Steve: We're going to address a whole next aspect of VPN, the so-called PPTP, Point-to-Point Tunneling Protocol, and IPSec VPNs, which are implemented by Microsoft and by so many of the later model consumer Small Office Home Office, the SOHO routers. We're going to talk about that works and how, unfortunately, Microsoft has deliberately made their built-in Windows client incompatible with any, well, almost all of those routers.

Leo: So that's...

Steve: But still some good solutions are available.

Leo: Do we have a silver bullet, a magic...

Steve: We're on the way. We're on the way.

Leo: All right, okay. We're getting close. Okay. Well, ladies and gentlemen, that's it for this episode of Security Now!, Episode 16. Thanks for all your questions. If you want more information, show notes are on GRC.com/securitynow.htm, as is a 16KB version of this show, and transcripts, too, in all sorts of formats, so you can follow along with the home version of Security Now!.

Our thanks to the folks at AOL Radio who broadcast Security Now! on their podcast channel and very graciously provide us bandwidth so that we can offer this podcast to you absolutely free at AOLmusic.com. I'm Leo Laporte for Steve Gibson. Thanks for joining us in Security Now!. We'll talk to you next week, Steve.

Steve: Bye, Leo.

Leo: Thanks.