Hamachi Rocks!

Description: This week Leo and I discuss and describe the brand new, ready to emerge from its long development beta phase, ultra-secure, lightweight, high-performance, highly polished, multi-platform, peer-to-peer and FREE! personal virtual private networking system known as "Hamachi." After two solid weeks of testing and intense dialog with Hamachi's lead developer and designer, I have fully vetted the system's security architecture and have it running on many of my systems. While I am traveling to Toronto this week, Hamachi is keeping my roaming laptop securely and directly connected to all of my machines back home. Don't miss this one!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-018.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-018-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 18 for December 15, 2005: Hamachi. Hamachi is a kind of sushi, isn't it.

Steve Gibson: Yeah. It's funny, I asked the developer, a guy named Alex Pankratov, where he came up with the name Hamachi. And he explained that he had been doing some work on an IPSec VPN tunneling technology prior to this, and that they were calling it TUNA, T-U-N-A, as Tunneling Architecture. And so when they started on this Hamachi project - I'm sorry, when they started on their second-generation project, that's what this evolved into, they thought, well, what are we going to call this? And so, what is it, yellow-fin, yellowtail...

Leo: Yellowtail tuna, yeah.

Steve: Yeah, yellowtail tuna is Hamachi. And so that's the name of this. What it is, you know, we've talked now extensively for many weeks about SSH tunnels, about the concept of tunneling, about SSL, about the traditional IPSec, Microsoft's L2TP, IPSec, the original PPTP, Point-to-Point Tunneling Protocol, blah blah blah, you know, VPN, endpoint routers and all that. All of this really results or boils down to what do users actually use to solve these problems? We've talked about, you know, what it is that the problem is that VPN technologies solve. Hamachi - I am so excited about this, Leo - it's a secure-from-the-ground-up, lightweight, free, peer-to-peer system that does NAT traversal, so it solves NAT traversal, firewall traversal. And essentially it allows people to build ad hoc local area networks. It's interesting, when I first installed it, it assigned my machine an IP in the 5. range.

Leo: I never heard of that.

Steve: Well, there isn't any. You know, as we know...

Leo: 10 is the lowest you can go; right?

Steve: Well, as we know, there are three networks that people are familiar with if they've looked at the inside of their NAT routers. It's typically 192.169 dot something dot something.

Leo: That's kind of reserved by the numbers folks for private networks.

Steve: Exactly. In fact, there's an RFC, it's RFC1918, talks about these three networks. There's 192.169.*.*; there's 10 dot anything anything anything; and then another one is 172.16 through 172.31. So those three subnets are set aside for use in private networks. And so you typically find that behind NAT routers that are routing those private addresses out onto the public Internet space, the point being that those are so-called nonroutable subnet ranges, or IP ranges, because no routers on the Internet would know how to forward a packet. Well, this 5. network is reserved by the IANA, the Internet Assigned Numbers Association.

Leo: Assigned Numbers and Addresses.

Steve: And Addresses.

Leo: Jon Postel's IT Group, which I think has been subsumed by ICANN.

Steve: Probably.

Leo: I think so, yeah.

Steve: Anyway, so there are no 5. IPs. Theoretically there could be someday. But the reason Alex chose this 5. is that he knew - he needed to give IP addresses to computers that were running Hamachi that would not collide with either IPs out in the public space or any of these three subnets which they might be running behind NAT routers. So he needed sort of like a third class of IPs. And so IPs that have never been issued was where he went. And so, you know, what, is it 16 million? I don't know, I can't do the math here on the fly. But it's...

Leo: It's four bytes.

Steve: It's, well, three bytes.

Leo: Three bytes.

Steve: So it's 24 bits. It might be, I think it's 16 million is the total number of IPs that are from 5.0.0.0 to 5.255.255.255. Okay. So what's cool about this is, well, there are so many things that are cool about this. When you install Hamachi on your system - oh. It's multiplatform. Right now it's just emerging from beta. It's available right now for Windows and Linux platforms. And as soon as it gets finished, as soon as the 1.0 version is released for Windows and Linux, shortly thereafter he will be releasing it for the Mac.

Leo: Is this the holy grail? Because you were looking for a free solution that allowed anybody to tunnel out and have secure networking no matter where they were, in a hotel, in an airport, on a Wi-Fi. Is this that holy grail?

Steve: This is absolutely part of the holy grail.

Leo: What's wrong with it?

Steve: Well, the thing I was actually looking for initially was a way to, with no client software on your machine, to connect to a VPN router that would get you into your network or out to the Internet.

Leo: But we now know that that's not possible. That's not going to happen.

Steve: It doesn't exist. Actually, I should mention that several people have brought up the fact that there are some obscure routers, for example, the SMC Barricade, there are a couple versions that do support PPTP routing themselves. So that's certainly, I mean, there are some that you can connect to with Windows. But they're not these, you know, the major mainstream routers. And again, the problem there would be that you might find yourself blocked by the environment where you were. You might find that your hotel was not allowing VPN, or their router does not support VPN passthrough, so you'd still have problems getting to your router at home.

Leo: Hamachi doesn't have that problem.

Steve: No. In fact, well, so it's multiplatform. When you install it on your machine, the Hamachi server issues a 5. IP that your machine statically and permanently and forever has. That's its IP in this 5. address space. It never changes. Now, you can transport your setup to a different machine if you had some reason to. But the point is, that's an IP that you can write down, you can configure it into links and do whatever you want to with it. So you install this Hamachi client on whatever set of machines you want to.

Leo: This would be at your home, probably, yes?

Steve: Well, at your home. I've got it running in my co-location in my server space.

Leo: So you could install it on your web server.

Steve: Absolutely. I mean, well, and I'll explain why. Because then what happens is you create ad hoc subnetworks of these machines. For example, I've got one called Gibson Research Corporation. And in that I have joined all of my various Hamachi-equipped machines into that network. You give it a long password. I got a password from my passwords page at GRC.com, you know, one of these 63-character nightmares, dropped it in, it hashes it, and that authorizes that machine to join a network that you've created. Now the machines can see each other. So what this does is it creates a secure, encrypted, peer-to-peer tunnel between any of the machines that are on the network.

So, for example, many people have written saying, hey, I love using Remote Desktop, but I'm concerned about its security. What should I do? Well, they should be concerned about its security because Remote Desktop does not have strong authentication. So it is subject to man-in-the-middle attacks, and it can be compromised. In fact, the current version of the Cain & Abel Cain tool has the latest support for the current RDP protocol, which allows - and, I mean, it actually builds a file, when you're running Cain, of everything you do over your Remote Desktop session. So here Hamachi solves the problem of wanting one computer to connect to and control another.

Leo: This is within your LAN.

Steve: Within, well, within the LAN that you create.

Leo: Right.

Steve: So you're able now to securely and safely use Remote Desktop through this Hamachi link with absolutely no concern that it can be eavesdropped upon. I've spent - I started talking to Alex on December 1st, and here we are on the 15th. I spent two weeks back and forth with him, asking him, I mean, bugging him to death, asking him very detailed questions about, okay, what about this? Are you hashing this password? Is it stored on the machine? You know, everything. He has done this, I mean, perfectly correct. The client builds an asymmetric key pair, a so-called public key pair. It gives the public one to the server so that the server can be used as the key distribution mechanism.

Leo: So you could dial into the server and say, what's the public key.

Steve: Yes. And you're able to also see it in your client if you want. But the nice thing about the server having the public key is then other clients that you agree you want to have connect to you, they receive the key from the server. Basically Hamachi is a zero configuration VPN peer-to-peer system. It does NAT traversal so that you're able - two people behind NAT routers, it will connect them. His server does not forward any traffic. And in fact it is not a relay. It actually establishes direct point-to-point connections between the machines.

Leo: So this is how he avoids the router issue, the firewall issue. He has a third point, a middle point that you both make outgoing connections to which - and then he connects you.

Steve: Yes.

Leo: Ah.

Steve: It's like a rendezvous or a liaison server.

Leo: Yeah.

Steve: So he looks, he basically figures out how your router is working, characterizes your router, and then works out - he tells then both clients over a TCP connection how to find each other. They find...

Leo: This is without opening - doing any port forwarding or...

Steve: And that's the other cool thing, is that if you had a VPN router, if you had any server running on your system, you'd have to have static ports open in order for you to be able to connect to it from the outside. Not so with Hamachi. It makes outgoing connections to the server, maintains a static TCP connection, then when you want traffic to go between machines, it's able to negotiate that directly.

Leo: Using a random IP - a port that - it does use a port, though, doesn't it?

Steve: Well, it's able to work through the local NAT router's port. So it works with whatever port the NAT router has assigned to outgoing traffic. Well, so it solves that problem. The security is complete. As I was saying about the asymmetric key pair, your private key never leaves your client. So you don't even have to trust the Hamachi server. The Hamachi server cannot be part of an attack on your system. It wasn't until I really understood this that I was willing to run these clients on my servers in my co-location. I mean, there is no way for the Hamachi system to access my stuff, even if it wanted to.

Leo: But it has the public key.

Steve: It's got the public key. But it doesn't have the private key for any of the clients. And you create the authorization when you initially create a connection between these endpoints. So it's extremely fast. The other cool thing is, for people who are, like, running around, doing telecommuting, one option, of course, is to run an email client on your laptop. Then you've got the problem of synchronizing your email, like if you're on the road and you download a bunch of stuff, then you've got it on your laptop, it's not back on your main system. So a cool solution for turning this into a system to give you Internet access, which it doesn't natively do, is instead, if you're using a Windows-based system, use Remote Desktop, which is now secured by the Hamachi system, and it's made accessible. If you were using Remote Desktop without Hamachi, you'd have to have port 3389 wide open to the world. Everyone knows 3389 is Remote Desktop Protocol, and so you're potentially vulnerable to, I mean, anyone knows you've got that open and soliciting a connection. If you use Hamachi to give you the same functionality, a direct point-to-point connection, it's encrypted and strongly

authenticated, which Remote Desktop Protocol won't do. You still have a point-to-point connection. So all you do is you bring up your desktop at home and use its web browser, use its email client, and use its connection to the Internet.

Leo: I've seen you do this, and it's pretty fast.

Steve: Oh, well...

Leo: I mean, it feels - I mean, it's fine.

Steve: Well, yes. And of course everyone knows about VNC. VNC is the...

Leo: It's a little slower.

Steve: ...is open source. It is also cross-platform.

Leo: Right.

Steve: That's the problem with Remote Desktop is it's a Windows-only technology.

Leo: Although there are clients for other platforms.

Steve: Ah. Well, in that case...

Leo: So I could use my Mac to surf to my Windows machine using Hamachi, and then use my Windows machine on my Mac desktop as if I were using a Windows machine, including surfing out. So let's step back and talk about the process of putting Hamachi on, what you need to do to install Hamachi. You need a - there's a client, and there's a server; yes?

Steve: No. It's just - it's a single...

Leo: Single program.

Steve: ...a single program. The website is - and if you just put Hamachi into Google you can get there. But it's...

Leo: H-a-m-a-c-h-i.

Steve: It's www.hamachi.cc. Alex is up in Vancouver, and so he's got a .cc on the end of his URL. You'll go to his site, download his client, currently for Windows or Macintosh - I'm sorry, Windows or Linux, and then Mac is coming soon. Installing couldn't be any easier. You simply run the setup, you go through a little wizard-based install to basically, you know, tell it where you want to load it on your hard drive. It sees that it's being installed in a system that it hasn't installed before. There's a negotiation with the server where it assigns it a unique IP. Your client produces its own asymmetric key pair, which it then uses to perform strong authentication. You do that on a couple other systems. Now, one trick is, he is assigning IPs sequentially. When I installed it on my second machine, for example, one of mine was 5.11.66.114. That was the first one I installed. What's very cool is I can tell you the IP. It doesn't matter. You can't get to 5.

Leo: Right.

Steve: I mean, it doesn't exist on the Internet. So, and what's really cool is my machine will always be 5.11.66.114. When I installed it on a second machine, it was, like, .120. I thought, oh, they're, like, so five people had installed it between the time that I had. So I quickly installed it on three more machines so that I could get IPs...

Leo: Sequential numbers.

Steve: Exactly, that I could get IPs that were sort of near each other.

Leo: Now that we've made it famous, it may not be easy to do.

Steve: You're going to be quicker. But...

Leo: So the Hamachi server, his server is assigning the IP addresses and keeps track of those.

Steve: It's doling them out.

Leo: So each one is unique.

Steve: And it's also, when your client builds the asymmetric key pair, it's then used for authentication and encryption. The client gives its public key to the Hamachi server so that it's able to then distribute it to anybody else who you authorize to connect. So you install it in a few systems.

Leo: And you don't have to. You could have it only on one system. But it's nice to have it on a bunch of systems.

Steve: I don't - who would you talk to if you only...

Leo: Well, okay. You only need it on a laptop and a desktop.

Steve: Oh, exactly.

Leo: But you installed it all through your office and in your co-lo and everywhere.

Steve: Yes.

Leo: Why did you do that?

Steve: Well, because I wanted to play with it. I wanted to get an understanding...

Leo: But you can also log on to any of those machines now from your remote client.

Steve: Well, yes. You can ping them. It supports Windows browsing directly. So you can right-click on any

machine in the list and browse the directory on those drives, do some standard Windows filesharing drag-and-drop. If you have...

Leo: Do you have to set up filesharing in Windows?

Steve: No, no.

Leo: Hamachi handles that.

Steve: Because it's inside Windows already, so you don't have to do that explicitly. So once you've got it installed on a few machines, then you start creating one or more of your own networks, where you define which machines get to participate. So, for example, you would create a network - I created Gibson Research Corporation. It wants a password. So I went to my passwords page, came up with this nasty 63-character random ASCII thing and dropped it in. Well, of course, because Alex is a crypto guy, it digested the 63 characters with no trouble at all. Nobody will ever get that password. I mean, I won't, if I ever lose it.

Leo: Yeah, don't lose it.

Steve: So I put it in a text file. I took that to a couple other machines, joined them to the Gibson Research Corporation network...

Leo: You only have to authenticate once, though; right? I do remember that, okay.

Steve: Exactly. Well, and in fact, one of the questions I asked him just before I came up here to Toronto to do this podcast with you is I said, wait a minute, what if I was at the TechTV studios, and I wanted to join a TechTV machine temporarily to my prized, super-secret, I don't want to, like, risk anybody ever getting in there network. What do I do afterwards to, like, remove all trace? Well, again, they did this thing perfectly. The password that I use is never written to the hard drive. It's hashed into a long token. And that's then used to validate this machine against my network. So then I would connect. I'd see all my machines there. I have now, by, you know, roaming around - oh, and since it's free, I don't even have to carry it with me. I go to any machine.

Leo: Just download it.

Steve: I just download it, install it. I would have to keep my wacky 63-character key around. So that allows me to join a machine into my super-secret private network, do whatever I want to. When I unjoin it, it can never come back because the key is not stored locally. It's only used to authenticate against the server. So I never need to worry again about someone following in my tracks and reconnecting to my network after I've gone.

Leo: Just uninstalling Hamachi is sufficient to...

Steve: Or actually, as people will see from the user interface, there's a Join and a Create Network. And then there's a Leave Network. So if I just left my network...

Leo: You could even leave Hamachi there.

Steve: I could leave Hamachi there.

Leo: So we'll download - there's a single file we download that we install. We authenticate. We create a key.

Steve: Actually it's all done for you. You don't even see any of that.

Leo: It's all wizards doing it all?

Steve: All of that is just done transparently. It's literally a zero configuration peer-to-peer system.

Leo: It traverses firewalls and NATs without - absolutely transparently because...

Steve: Deeply encrypted.

Leo: Yeah.

Steve: So, for example, it's our solution for hotel travelers, for Wi-Fi users. The one gotcha is you've got to have a machine somewhere for you to connect to. So you'd need to leave your home computer running with Hamachi on in order for you, in a Wi-Fi hotspot or in a hotel, to connect to it. But it is absolutely free. Now, they will have a premium version that will, for example, add some additional features. For example, it'll run as a service in the background, so you won't see it as an app on our desktop.

Leo: Oh, it is an app right now.

Steve: Yes. The free one won't relay at all. But there are some really nasty NAT routers. If you had a recalcitrant non-peer-to-peer-friendly NAT router on each end that Hamachi would not be able to negotiate a tunnel directly. So you would have to use the premium version...

Leo: Which would provide that third point that you'd connect to.

Steve: Yes, in order to use Hamachi as a relay. And that's really fair, too, because...

Leo: It's fair because you're using their bandwidth.

Steve: You're using their traffic. You're using their bandwidth, exactly.

Leo: So normally you're not. Normally you only use it to authenticate, to handshake. Once the handshaking is done, you have a direct peer-to-peer connection between your home and...

Steve: And it's fast. It's as fast as it could be between those two endpoints.

Leo: And now the only addition is - okay, so that gives me access to my computer at home from the road. And as you said, if you want to surf the 'Net or go out, you would just run Windows Remote Desktop, and in effect you'd be using your home computer, kind of like a GoToMyPC solution or a Citrix solution. You'd be using your computer to do the surfing.

Steve: But for free.

Leo: But for free, right.

Steve: Because you're using your own system instead of somebody else's system.

Leo: Is it a tunnel? It's a tunneling solution.

Steve: It is. It is a virtual private network, peer-to-peer secure tunneling system that, I mean, I can't find a single fault in it. I mean, I'm using it. I'm in love with this thing.

Leo: And it's absolutely free, from Hamachi.cc, if people want to download it. And we're not done with VPNs.

Steve: No. We've got one more week. We're going to talk about...

Leo: Well, what more is there to say? You've come up with the holy grail, Steve.

Steve: Well, there's one more solution we have to talk about because it's very popular, and that's the OpenVPN system. And that's next week.

Leo: Okay. And we also have found a commercial provider, HotSpotVPN, that works very well.

Steve: Yeah.

Leo: Using OpenVPN.

Steve: We're basically, so next week we're going to talk about, I mean, I hope everybody listens to this.

Leo: I'm going to install Hamachi right now.

Steve: We'll go to www.hamachi.cc.

Leo: Yeah.

Steve: Play with it. It is a super cool system.

Leo: Well, and because I run a web server that runs Linux, I can install it on my Linux web server. And all of that stuff will be - in fact, my web hosting company won't block it because it looks like normal traffic; right?

Steve: Well, that's the other - yes, that's exactly right. The other cool thing is that, because it's running through a tunnel, no hotel can block it. And say that somebody working for a corporation had, you know, Gestapo firewall people who didn't let anything in or out, yet you wanted to access your network at home. You know, Hamachi would allow you, if you have the ability to install Hamachi...

Leo: As long as you can install software; right.

Steve: As long as you can install software on your corporate computer, this would allow you to literally, on your desk, have access to your home computer. Also...

Leo: You can't run this off a USB key because it does have to modify Windows. You couldn't just run it as a standalone application off a USB key.

Steve: Don't know. I think it installs information in the registry.

Leo: It must modify Windows.

Steve: Or maybe in the directory. I'm not sure. The other thing is, we've had some people, for example, in prior months of TechTV, wanting - gamers who wanted to know how they could - how he could set up his Xbox to game with somebody else. And the only solution we had at the time was VPN endpoint routers, to use VPN endpoint routers.

Leo: This would work for that.

Steve: Hamachi is a perfect network for gamers. Okay, so next week we're going to talk about OpenVPN in all of its various forms. Because the reason I want to talk about it is there's so many ways it can be used, the HotSpotVPN being one of them, a commercial service. And there are a number of others that are also completely free.

Leo: It sounds like Hamachi is something that everybody would want to set up now, just to establish a connection between you on the road and your home system. If you were able to run Remote Desktop, you could then use it to do the kinds of things you would do at your home system, like surf the 'Net and so forth.

Steve: Exactly, and that gives you Internet access.

Leo: That gives you your Internet access.

Steve: Yes. And also access to all your files at home.

Leo: Now, when I log on, I use SSH to log on to my web server. I'm essentially doing the same thing. I'm setting up a tunnel. The only difference is, of course, I have to leave port 22 open so that I can log in, and I have to have - and I only have command line access to the server.

Steve: Well, the other problem is, SSH is a TCP protocol.

Leo: Oh.

Steve: Tunneling TCP through TCP is problematical because TCP is itself an error correction guaranteed packet delivery protocol. When you tunnel one of those protocols within another of those protocols, they're not talking to each other because they're sort of separate sheaths that are carrying your data. You can get very bad performance when you tunnel TCP in TCP. This is one of the things that's given VPNs a bad name. The other...

Leo: They seem slow because they're trying to do that.

Steve: Well, yeah. In fact...

Leo: Well, what's the solution to that?

Steve: ...the computers are fighting. The solution is to use UDP as the transport protocol. There you're sending packets only when you need to. So the internal TCP protocol gets encapsulated in UDP, and that's what Hamachi uses. And also because UDP translates through NAT routers and traverses NAT routers far more easily.

Leo: So it's - in fact, and I saw you, you gave me a little demonstration. You were sitting here on the set in Toronto, and you were logged on to your computer in Irvine, California.

Steve: Looking at my desktop.

Leo: And I have to say it looked every bit as fast as if you were actually there. Now, that's partly because Windows Remote Desktop is efficient, but also because that UDP transport is not slowing you down.

Steve: It's the right way to do a VPN. Now, the one other glitch that VPN - the thing that hurts VPNs is, when you encapsulate packets, you make them bigger. And so what can happen is your packets can be fragmented because they won't traverse the Internet because they end up being too big when they're wrapped in the packet. Hamachi fixes that and knows how to change the stack in your machine so that the TCP packets it generates are already shrunk, so that when it's encapsulated, it still fits in within what's called the MSS, the Maximum Segment Size, so that it won't fragment the packets. So you get, I mean, really good performance. In fact, I have, using Remote Desktop before, I have forgotten sometimes that I'm not on my computer. I mean, it's just not a painful experience.

Leo: For Windows and Linux users, this is just a remarkable solution. I mean, it gives you complete remote access to your home system. And because you put all of your computers on this thing, you've got a menu of all the computers at home that you can access. In fact, not only does it give you such good access, you were able to shut down one of those...

Steve: Here it comes.

Leo: ...computers by accident.

Steve: I knew. Yes.

Leo: Can't get to it right now.

Steve: I meant - I was reconfiguring it, and I meant to remotely choose Reboot, and I chose Shutdown, and it powered off in Southern California. It was like, oooh.

Leo: And there's no way to turn it back on from here.

Steve: Nope.

Leo: So that computer is now inaccessible. So one little word of warning. It's so much like the real thing, you could actually make a mistake and shut it down.

Steve: You need to be careful, yeah. You don't have the power button next to you for the computer that you're talking to.

Leo: It's a really - it sounds very - sounds like it is the holy grail, very close.

Steve: I had my fingers crossed while I was vetting the security architecture, thinking, oh, this, I mean, oh, and the UI is polished. I mean, it's a professionally assembled, beautiful piece of work. I mean, I can't recommend it highly enough.

Leo: He's giving it away for free, but the good news is - and I say this is good news - he has a business model where he can make money on it, and that means he will keep developing it, and there's a chance...

Steve: Well, and what's interesting, too, is...

Leo: It's a real product.

Steve: ...he had said that he will sell the server side also. It's hosted on Linux. So he's not just going to be the sole source of the Hamachi protocol.

Leo: That's a good idea. If I'm a company, and I want to set up, you know, have a large number of telecommuting workers, I create a Hamachi server at our home base, and I control it all. I don't have to worry, I know it's secure because I'm in charge of it. Boy, that's a great idea.

Steve: Yeah. And he's got online forums where people can ask questions. I'll be surprised if anybody has a question. I mean, it is so simple to use. The graphics are beautiful.

Leo: I got a question.

Steve: You can see the status of the different machines. Yeah.

Leo: When is the Mac client coming out?

Steve: What he said is, it's at very late beta stage now. I've never had a problem with it.

Leo: That's encouraging.

Steve: Yeah. So it's, like, it's almost there for Windows and for Linux. And as soon as that happens, he's going to do the Mac. So he's absolutely committed to a Mac-based platform.

Leo: For Mac to work you'd need something like Windows Remote Desktop. There is Apple Remote Desktop, but it's fairly expensive.

Steve: Or to hook your Macs together.

Leo: Yeah. Well, yeah, absolutely, you could do it that way. That's great. Hamachi.cc. And of course the show notes and a 16KB version of this show, as well as transcripts, are all available at

GRC.com/securitynow.htm.

Steve: There's one more issue I have to cover because it comes up so many times. I talked a couple episodes ago about the idea of, well, about the problem people are having when they have followed our advice and beefed their Wi-Fi, their wireless technology in their home, up to WPA, or in some cases just added full, you know, the strongest WEP encryption that they could if they don't have WEP-compatible hardware. Other stuff that they had, like their TiVos, for example, or PDAs...

Leo: Don't work.

Steve: ...that don't support, exactly, that don't support the WPA are in trouble. I mentioned, oh, well, there's nothing to keep you from running two wireless networks at home.

Leo: One secure and one relatively insecure.

Steve: Yes. And when I said that, you asked me right then on the spot, what would the architecture be? Which router would go where? Well, I punted the question because...

Leo: You fooled me. I thought you answered it.

Steve: No. I had to think about it extensively. Because of something known as ARP poisoning, it's different to answer the question if we assume everybody is passive than if we assume you could have an active attacker who could reorganize your networks by sending ARP replies. Very early in 2006 we're going to do a podcast about ARP poisoning and what that's all about and why it's a concern. What this means, though, for now, is - and I've gotten pencil and paper and really thought this through. If you put the insecure network inside and the secure network outside, the problem is it - because, as we know, NAT routers are like one-way valves - the insecure network would have upstream access to your secure resources, which is a bad thing. If we reverse it, if we put the insecure one upstream and the secured one downstream, sort of inside, you still have a problem because now the insecure network is on your perimeter, and it could potentially see the traffic coming from your secured network.

Leo: And it could be ARP poisoned.

Steve: Well, exactly. Passively, the response from passive listening is different. But in this day and age we need to assume, you know, any possible attack, certainly, that we know about. So the answer is, anyone who wants to run two wireless networks, they have to...

Leo: Need three routers.

Steve: Yes. They do. You have to have a Y architecture. You have your main router on the border that is not - that's just - it's a wired router. You then plug each of your wireless into it. So essentially you'd have three subnets. You'd have...

Leo: Otherwise your traffic's passing through the insecure network.

Steve: Yes.

Leo: This way you can make it a tributary. The insecure network is somewhere off by itself.

Steve: And ARP packets never traverse a router. ARP packets - ARP is a nonroutable protocol. It's only used, after all, for associating Mac addresses and IPs within a LAN. So basically you would have three LANs. You'd have the outside LAN that feeds the two inside LANs. So you'd have 192.168.0 something on one of them; 192.168.1 dot something, and 192.168.2 dot something. And so that's the architecture.

Leo: Are you going to draw this up and put it on the website?

Steve: Yes, we're going to do a page.

Leo: Do a little map.

Steve: In fact, the page I showed you earlier that we'll be talking about in the show...

Leo: Yeah, the ARP poisoning...

Steve: Yeah, that was a page that grew out of my need to lay some foundation for this.

Leo: All right. GRC.com/securitynow.htm. We thank the good folks at AOL Radio for providing the podcast channel which this show and all the other TWiT shows appear on, AOLmusic.com; and of course they also donate bandwidth, which saves us a packet of money.

Steve: Makes it possible.

Leo: I don't even - it makes it possible, that's the truth of it. We'll see you next week on Security Now!. We're going to talk about OpenVPN and a good commercial solution that is very easy to implement. In fact, I've been using it, and I've been very happy with it.

Steve: I am, too, yes. I wanted to give it a couple weeks of play before we got everyone revved up for it.

Leo: But meanwhile, enjoy your sushi treat from Steve Gibson.

Steve: Oh, it's so good, Leo, oh.

Leo: Now, next week is Christmas week. So we might - I guess we'll just do the podcast as usual.

Steve: Yeah, works for me on Thursday.

Leo: Okay. I might have to do it a little earlier because I have to go visit family.

Steve: I'm around.

Leo: Well, I'll tell you what. We'll deliver it on Thursday, by hook or by crook.

Steve: Absolutely.

Leo: And then we'll be back the week after Christmas because, well, we have no life. Thank you. On behalf of Steve Gibson, I'm Leo Laporte. Thanks for joining us. Stay safe, stay secure. We'll see you next time on...

Steve: And have some Hamachi.

Leo: Have some Hamachi on Security Now!.