



# SECURITY NOW!



Transcript of Episode #19

## VPNs Three: Hamachi, iPig, and OpenVPN

**Description:** Leo and I wrap up our multi-week, in-depth coverage of PC VPN solutions by discussing some aftermath of the zero-configuration Hamachi system; introducing "iPig," a very appealing new zero-configuration VPN contender; and describing the many faces of OpenVPN, the "Swiss army knife" of VPN solutions.

High quality (64 kbps) mp3 audio file URL: <http://media.GRC.com/sn/SN-019.mp3>

Quarter size (16 kbps) mp3 audio file URL: <http://media.GRC.com/sn/sn-019-lq.mp3>

---

**Leo Laporte:** This is Security Now! with Steve Gibson, Episode 19 for December 22, 2005: VPNs, The Final Chapter.

**Steve Gibson:** The final frontier.

**Leo:** The final frontier. Steve Gibson, Happy Holidays to you. Thanks for joining us, even though we're so close to Christmas, for this Security Now! episode. You helped us out on TWIT, too, on Sunday. That was nice.

**Steve:** We're doing it a little bit early this week...

**Leo:** Yes.

**Steve:** ...to kind of give people some clearance from the holidays.

**Leo:** Give me some clearance.

**Steve:** We're not going to miss a beat. We'll do one this week, and then of course Episode 20 will be next week, which will be our Mod 4 Q&A episode.

**Leo:** Right, our usual we-answer-your-questions. So get them in to [GRC.com/securitynow.htm](http://GRC.com/securitynow.htm).

**Steve:** Oh, Leo. After...

**Leo:** That was not a good thing to do.

**Steve:** Oh, God. After last week's Hamachi, you know, I used to be saying, oh, yeah, I'm keeping up, I'm reading everything that's coming in. I am so buried under stuff.

---

**Leo:** Yeah, that's all right. People will have to - do, I'm sure, understand that you can't respond to everything. And we'll try to respond to as many as we can.

**Steve:** I can't even read everything at the moment. It's just...

**Leo:** Yeah, it's amazing.

**Steve:** It's been phenomenal.

**Leo:** Well, before we get into the final chapter of VPNs - and we're going to talk about OpenVPN this week - let's follow up on a few things from previous weeks, some corrections, updates, and Hamachi updates.

**Steve:** Yeah, some errata.

**Leo:** Errata.

**Steve:** First of all, everybody is writing to me about this article from earlier in the year, talking about cracking Wi-Fi protected access, cracking WPA. And, I mean, I just - people keep posting this link to me. I meant to bring it up last week; but, as you know, I forgot my little errata notes at the beginning of the show, so we had to wing it.

WPA has not been cracked. WPA is not prone to cracking. The article is at [Inferno.com](http://Inferno.com). And it was back from May, I think, or maybe it was March. No, yeah, it's March. So, you know, nine months ago. It's a two-part article that goes into excruciating detail about brute force attacks on WPA. Well, that's what we've talked about. We know that WPA is susceptible to an offline brute force attack, that you can capture a couple of packets and then take those home with you and pound on that data, trying either dictionary attacks or every possible key. Which is why the passwords page at [GRC.com](http://GRC.com) was created, to give people these really nasty long WPA keys that nobody is going to be able to, you know, in any reasonable amount of time, recreate.

So I want everybody who's been concerned about what this article means - and by the way, I mean, I don't blame anyone for being confused. This thing was deliberately created, it seems, to be extremely confusing and alarming. But WPA is not cracked. There's no simple way to breach it as long as you use a really good passphrase.

**Leo:** It is kind of a shame. I guess [Inferno](http://Inferno.com) decided, well, let's go for the big headline, get a lot of attention, a lot of traffic to our page. But everybody knows, I mean, many protocols, not all, but almost all protocols are subject to brute force attacks. That's, you know, bad password, no security. We know that.

**Steve:** Yeah. And what you hope is that it's not subject to anything else, which is clearly the concern that this article raised. Now, also we've already begun to see the emergence of WPA brute force cracking tools floating around in the hacker sites. So that's something else that I saw in the last couple weeks is that we're beginning to see that emerge. So as we told people before, WPA is safe as long as you use a really good passphrase.

**Leo:** [GRC.com/passwords](http://GRC.com/passwords). And you can get a good one.

**Steve:** Yup.

**Leo:** All right.

**Steve:** Now, one other little loose end was we've talked about the problem of distributing those super-secure passphrases and talked about the idea of using the standard little USB, you know, drive dongle. One other thing occurred to me, and that is that those little mini CD-Rs would work. You could take maybe 10 passwords and just burn them on a CD-R. There they're going to be involatile. It's easy for you to move them around from machine to machine. Every machine that you run across is going to have a CD-ROM drive now. And that way it's extremely simple to move this really long password that you wouldn't want to have to type in manually.

**Leo:** Of course, the CD-Rs, you're not going to change it very often. But I guess that's kind of the idea anyway.

**Steve:** And that's the whole idea is you don't want to change this super-bizarre password. And in fact, that's why I was suggesting you might put 10 of them on there. You might start off just using the first one. If for any reason - you, for example, had to disclose it to a friend who came over, you know, for example, move them onto your WPA network by giving them that password. Then, if you wanted to, you might feel more comfortable switching to your number two password that's already recorded on the CD-R throughout your network, so that you've essentially obsoleted that first one. You've removed it from being able to have any access to your network.

**Leo:** We were talking about that at the meet-up, something kind of related, which is this reverse - this cracking of the MD5 hashes. Somebody put out a CD or a disk, I guess it was a hard drive, with all of the reverse hashes, right, so you could do a reverse lookup?

**Steve:** Well, yeah. It's called a "precomputation attack." And we're seeing that both for MD5 and SHA1. The idea is that those are very secure hashes. They have been weakened a little bit through recent cryptanalysis. But they're still, you know, they're widespread, in extreme use everywhere. What's happened is, hard drives have gotten so big and so cheap. And of course the Internet has happened. What's going on is that people are precomputing the hashes. They're doing basically a brute force...

**Leo:** In reverse.

**Steve:** Well, they're doing a brute force use of the hash forward, and they're storing the value and its corresponding hash on a hard drive. Then what you do is you go to a website that's got this massive database of precomputed hashes. You give it the hash; it gives you the password. So it's not - it hasn't cracked the hash, it's just done them all.

**Leo:** That's pretty amazing.

**Steve:** Well, it's...

**Leo:** Once again, that's why a good, long, random passphrase or password is the best solution. Because they're not going to brute force something like that.

**Steve:** Exactly. It's going to be way down after the end of the life of the universe...

**Leo:** Before they get to it.

**Steve:** ...before they get to it. Now, also in a prior episode I mentioned the idea of creating a secure connection to webmail. That is, we were talking about, you know, SSL at the very beginning of our VPN conversion, how, if you're using an SSL connection to a remote server, your communications cannot be eavesdropped on.

**Leo:** That's how Yahoo! Mail works and a number of other clients. And you can even use a POP client that way if your ISP supports it.

**Steve:** Exactly. But in the case of webmail, some people were having some problems doing this with Google because it turns out that Google has a funky way of bouncing you from your log-on page, which is secure, to a non-secure session, once you've logged on. So I did a little poking around. And it turns out that, if you use the proper URL, among many ways of getting Google Mail - for example, if you use <https://mail.google.com> or <https://gmail.google.com>, then, for whatever reason, you'll get a secure connection when you're actually logging on, and it will bounce you to a continuing secure interaction with the server subsequently. But other ways of entering bounce you over to a non-secure connection. So if you use <https://mail.google.com> or <https://gmail.google.com>, it will see that you want a secure connection and leave you that way.

**Leo:** Good to know. All right. That's what you should bookmark and use that every time.

**Steve:** And in the last little bit of stuff that I have been meaning to say for weeks but keep forgetting...

**Leo:** You got your notes now.

**Steve:** I do, baby. I'm home. We've never told everybody who's listening to Security Now! that GRC runs, and has for years, an extremely useful set of security-related newsgroups. Our news server is [news.grc.com](http://news.grc.com). And if you - this is not a web-based forum. It's real, you know, Usenet-style news reading. But most web browsers, you know, IE and Opera and, I presume, Firefox, do have built-in Usenet newsreaders. So...

**Leo:** Actually, Firefox does not. But there are - well, it kind of does. It's got a funky way of doing it. But you can add an extension like Sage or Fizzle to give it that capability.

**Steve:** Okay. Well, I'm not a big fan of web-based forums because I've become addicted to, like, real Usenet-style news, where you've got lots of newsgroups; you've got well-threaded, very clearly threaded dialogues. You can see which postings you've read and so forth. My favorite client is free, and that's Gravity, the Gravity newsreader for Windows that people can find on the 'Net. And there are other ones.

**Leo:** Actually, I want to correct myself. I was talking about RSS. People use Thunderbird for newsgroup reading, as opposed to Mozilla, or Firefox.

**Steve:** Ah, okay.

**Leo:** Yeah. But you like Gravity. That's a good - I'll put a link in the show notes to that.

**Steve:** I like Gravity. Also, on our main navigation bar at [GRC.com](http://GRC.com), at the top of the home page or the bottom of every page, the far right link there is called Discussions. We have a page at [GRC.com/discussions.htm](http://GRC.com/discussions.htm). That will give people sort of some foundation in this. I have a step-by-step guide for setting up Internet Explorer, or I guess it's Outlook? Oh, yeah, I'm sorry, it's Outlook Express that is both email and has the...

**Leo:** Newsreader, yeah.

**Steve:** ...newsreader. So I take them through a step-by-step. We have a little bit of some fancy stuff going on for the way you log on, that I explain, because we have something that no other newsreader has, which is an ability to allow people to securely cancel their own messages. I create a hash of their username and password that they use for logging on so that they're able to securely delete their own postings, if they want to, without anybody else being able to. Anyway, there's a bunch of technology I've actually been working on for years for our own newsgroups. So I wanted to tell people. Among our listeners, I know from the feedback

we get, we've got real security junkies here. And there is a really super community of people who hang out on news.grc.com, my news server there. And in fact, the Discussions page does allow you to use a web reader, a web interface to just sort of browse around the newsgroups, if you weren't sure you wanted to go to all the trouble of setting up a newsreader and participating. You're not able to post from there, but you can browse around, look and see what the newsgroups are. Oh, and I just created a Security Now! newsgroup.

**Leo:** Great.

**Steve:** That is there, it's been there for a few days, and it'll be entertaining specific dialogue relating to whatever we're talking about on Security Now!.

**Leo:** So GRC.com/discussions.htm. You can read them online if you want to participate. We'll put a link to Gravity, Steve's favorite newsreader; but there are many, many choices, of course.

**Steve:** And if you've got Outlook Express with Windows, you've already got a newsreader built in.

**Leo:** That's cool.

**Steve:** Okay.

**Leo:** Hamachi. Let's finish up from last week because that was very popular.

**Steve:** Yes. Now, the good news is, a lot of people fell in love with this. Alex Pankratov, Hamachi's chief lead developer, the guy that I was talking to for several weeks before talking about this last week, sent me a link from this delicious server that shows all the people that are linking. And there was a phenomenal reaction to number of people who are interested in Hamachi following our talking about it last week. I've got one posting here that someone sent a few hours ago, who posted to our site saying, I do a lot of traveling and have always had issues with using the wireless connections at hotels. I was so happy to have heard about Hamachi that I had it installed and running before I finished listening to your podcast.

**Leo:** That's nice.

**Steve:** You are right. Hamachi rocks.

**Leo:** Very easy on Windows. A little more tricky, I did it on a Mac, but you have to download some additional software and do some configuration. But I started using it right away, and I love it.

**Steve:** Are you talking about Hamachi on the Mac?

**Leo:** Oh, I'm sorry. It's something else.

**Steve:** You're talking about OpenVPN.

**Leo:** Forget I mentioned that. I'll edit that out. So Hamachi is very cool. There is no Hamachi for the Mac, but that's coming.

**Steve:** So he said, you're right, Hamachi rocks. I'm leaving for Europe for a three-week vacation. And now, using Hamachi and an open source VNC, I have a way to securely connect to my home PC, transfer files,

browse the web, and check email.

**Leo:** Wow.

**Steve:** So there's an example of the good news. Now, there were some disappointed people, who, for example, are behind very restrictive corporate firewalls, or behind, like, ISP proxy servers. So it's important to say that, good as Hamachi is, there certainly are Hamachi-hostile environments where you're not going to be able to use Hamachi. Unfortunately, those people who were really excited by last week's podcast about Hamachi and downloaded the client, hoping that they would be able to immediately connect to their home machines, in some cases they were. In some cases they found that, for whatever reason, for example, their corporate firewall - I saw some posts where their corporate firewall allows traffic out through port 80 and 443...

**Leo:** And that's it.

**Steve:** ...only.

**Leo:** Geez.

**Steve:** You know, for example, DNS goes to the corporate DNS server.

**Leo:** Right.

**Steve:** SMTP and POP for transferring email, or in fact maybe IMAP, goes to, again, the corporate local mail server. And they have no access to anything other than ports 80 and 443 for browsing the web. So in that scenario, they're going to need a different tool. The good news is, we've got a different tool, which we will be talking about. So there were people for whom Hamachi was not, you know, the holy grail that we've been talking about.

**Leo:** Hey, if I were a corporate IT guy, I think blocking all ports but 80 and 443 sounds like a pretty darn good idea.

**Steve:** Oh, I agree.

**Leo:** To be honest with you, I would do that.

**Steve:** In fact, some people took exception, understandably, to my saying last week, hey, you know, you could run this at home and on your desktop in your company and get...

**Leo:** And they'd never know what you were doing.

**Steve:** ...and, well, and get access to your home. And of course the reciprocal works. From home you could get access into your corporate network. People were annoyed that I, as a security person or security-conscious person, was suggesting the use of this for accessing corporate networks remotely. And so your point is well taken, Leo. You would hope that a corporation already has dealt with this because, you know, it's been possible for a long time using all kinds of techniques.

**Leo:** And we're not advocating doing an end-around on your IT security because the next Zotob worm, if you're the vector that brings it into the corporation, they're not going to like you too much.

**Steve:** That'd be bad.

**Leo:** That'd be bad thing. One other note I got from a good friend and Perl wizard, Randal Schwartz, he's the author of "Learning Perl" and really a great guy, had a couple of questions for you. First of all, he said, Hamachi's not open source. How can we trust it?

**Steve:** Ah, well, that's a very good point. I mean, it's one of the things that made me anxious and continues to make me anxious. I'm going to end up probably over on OpenVPN, which is how we're going to wrap up this episode of Security Now!. But Hamachi is - I'm convinced that Alex has really designed this system exactly as he's told me he has. He's got years of experience with security, implementing IPSec tunnels, you know, classic VPN solutions. I couldn't feel any better about this than I do, short of doing a complete source audit and, you know, build verify and all that, which is just not practical. So it's certainly the case though that, well, I mean, you know, we're trusting Bill when we use Windows.

**Leo:** Right.

**Steve:** We're, you know...

**Leo:** But that's why a lot of people say use open source security software and only open source security software because you don't know what government backdoors are in there and so forth. Things like PGP, you know what's in there.

**Steve:** Well, that's certainly the case. And in fact, I think you made a comment, I don't remember if it was before the podcast or under your breath, that was like, you know, Alex Pankratov sounds like a Russian...

**Leo:** Who is this guy, KGB?

**Steve:** Exactly. Who are we - well, and in fact, it's why I went around and around with him to make sure, for example, that the asymmetric key pair generated by the client was never given at any point, was given to the server or left the client, so that it wasn't necessary for us to trust the Hamachi server. And, you know, I'm sure Alex has told me the truth, but I have no proof of it. So listeners should certainly be aware of that.

**Leo:** And he points out, and I'm sure we'll talk about it at some point, that the next version of OpenSSH 4.3 will add support for tunneling. Essentially you can set up an OpenVPN-type tunnel using SSH.

**Steve:** Well...

**Leo:** Which'll be nice.

**Steve:** It'll be nice; but again, we have to be careful with details because OpenVPN has done something very correct that Hamachi has also done very correct, which other solutions have not. And that is, because it's - I assume it's OpenSSH, so it's a TCP tunnel.

**Leo:** Right.

**Steve:** And we've talked before about the problems of tunneling TCP through TCP. Whereas Hamachi is UDP based, and OpenVPN in its default configuration is UDP based. And that's a better transport protocol because you don't have the problem of two reliability-guaranteeing protocols like TCP interacting with each other in a bad way.

**Leo:** And as you pointed out, that's one of the reasons people don't like VPNs. They seem slow and sluggish. It's because it's TCP over TCP.

**Steve:** Well, and the other problem is, yes, that TCP optimizes its packet size so that it doesn't fragment as it crosses the Internet. The problem is, if you encapsulate TCP in TCP, you're making a larger packet because you've got the already maximum-size TCP packet enclosed in another packet that has inherently made it bigger. So you often have fragmentation problems which can be very severe, meaning that every packet hits the first router that is not able to forward that overly large packet. It cracks it in half, and the Internet never reassembles those. So suddenly you've got twice as many packets, twice the opportunity for packet loss and retransmission, and twice the number of packets coming back in that then need to be reassembled. And some routers will not, because there has been a history of fragmentation attacks, different ways of using fragmented packets to get through firewalls. Because, for example, a firewall that doesn't have the whole packet can't really check it as thoroughly as it would like to, many firewalls drop fragments because fragments are not supposed to happen. So this is one way that VPNs can not only have low performance, but actually fail.

**Leo:** Good to know. All right.

**Steve:** Anyway. One last issue with Hamachi is relative to Remote Desktop. I was jumping up and down last week about how I was able to log on to my desktop remotely from home, from Toronto.

**Leo:** You showed us. It was so cool.

**Steve:** Yeah, exactly. I mean, and thankfully, Remote Desktop is a very efficient protocol. Hamachi has a problem, or I guess actually Remote Desktop has a problem, if the Hamachi client is running with the same user on your desktop that you are trying to log in as remotely. You get this "This user already logged on" sort of collision, apparently. Alex has responded to this. And over in the Hamachi forums there is discussion and the resolution of this problem. It turns out that, if you run Hamachi as a service, then it runs as the system process as opposed to on your desktop as the logged in user, and then you're able to log in remotely. So for all the people who have had problems getting Remote Desktop to work as easily as I did, I actually was running it as a system process, as a service. So it was logged in as the system and not as the user I was logging into it as.

**Leo:** Is that dangerous?

**Steve:** It's, no, you are...

**Leo:** It's got system...

**Steve:** You are trusting it because it has more privileges in your system.

**Leo:** Right. All right. We're all caught up; right? Any more?

**Steve:** The one last issue...

**Leo:** Okay.

**Steve:** ...with Hamachi is...

**Leo:** We may have to put OpenVPN off till next week. No, go ahead.

**Steve:** Well, but Hamachi's important.

**Leo:** It is.

**Steve:** And it's going to be one of our enduring solutions, I'm sure.

**Leo:** Oh, yeah.

**Steve:** Some people are using Hamachi on their own internal networks and have said, hey, I've got all my systems running with Hamachi. Do I need WPA anymore? Well, that's a really good question. If you were sure that you're using Hamachi for your filesharing and to link things together, I could argue that that really replaces the need for internal Wi-Fi encryption. Remember, however, that you do have the problem of people using your network and, you know, being able to mess with your systems. You still, even if you've got Hamachi interconnecting your systems, you still have your non-Hamachi'd IPs available.

So there's two problems. There's the problem of you using the non-Hamachi IP by mistake, if you weren't really careful; and the fact that all the non-Hamachi, the regular native IPs, are still available. So it's really not okay not to use WPA. I would not recommend it. However, one of the cool things about using Hamachi within your network, especially if you've adopted one of the multi NAT router approaches that we've talked about for isolating networks from one another, people who have done that in the past have written to me saying they've got problems because, like, filesharing and printer sharing breaks across routers. And that's the case because Windows normal filesharing broadcasts will not be moved across routers. Hamachi does forward broadcasts, and people have reported that, using Hamachi, now they've got their filesharing back, even in complex multi-router configurations.

**Leo:** And we also met a number of gamers who use Hamachi. This might, up to now, have been the most popular use of Hamachi, to turn LAN games into WAN games, which is very cool.

**Steve:** Right.

**Leo:** Yeah. We won't name the person who told us all about that.

**Steve:** Nope.

**Leo:** Because of his high-ranking security clearance.

**Steve:** In the military.

**Leo:** We won't - shhh, that's enough.

**Steve:** Oh, oops, okay.

**Leo:** But I think that's - actually, gamers were the first to really get the value of Hamachi, I think.

**Steve:** Yup.

**Leo:** All right. Shall we talk about our subject for the week, which is OpenVPN?

**Steve:** Not quite.

**Leo:** Oh, there's more?

**Steve:** There's one more.

**Leo:** One more thing.

**Steve:** I have to talk about iPig, the worst-named but very compelling-looking VPN solution I just started playing with yesterday. A number of users wrote to me about it. I tracked it down. It's [www.iopus.com](http://www.iopus.com). The trouble is, for some reason the guy who did this shows a picture of a silver hardware wireless router on the page for iPig. And several times I went there thinking, no, no, no, I'm not looking for a hardware solution. You know, I don't want an iPhantom-style thing. I'm looking for a client-and-server software package. Well, that's what this is. It's got nothing to do with hardware at all. So I'm not sure why he shows a hardware router on the page, leading people to think that, unfortunately, that's something to do with what his iPig software is.

**Leo:** Is it, like, a software version of a hardware router?

**Steve:** Okay. It is extremely cool. I ran his server - he has a free server and a free service. I ran his server on my system. I installed his client on my laptop. I then connected to my - oh, I also had to forward a port from my router through to the listening port on my server. So there is that aspect that anybody who's going to be running a server on their LAN needs to be aware of. Hamachi avoids that by doing outbound-directed NAT traversal. So that's not a problem. But anyone using OpenVPN or using iPig will need to open a port and forward a port through their router, also through their firewall, if they've got one, so that the program is able to answer incoming calls. I then, using this free client-and-server solution, I connected to my server. I ran Remote Desktop. I connected to my fileshares. I talked to other machines in my own private LAN and accessed the Internet back out through my Internet connection. I mean, it is the holy grail that we were looking for. Unfortunately, it's called iPig.

**Leo:** And it's not free. Or is it?

**Steve:** It is free.

**Leo:** It's free.

**Steve:** It's completely free. His server-side unit will allow you to define five accounts and presumably have five users simultaneously using it. I can't imagine why that's any practical limitation. He also has a free service. You can use his server with a five-gigabyte limit for an account. And - which is, I mean, would last you years if you were just using it for email. If you were trying to do something, you know, like using BitTorrent or something, that would be a problem. You would burn out that account before long. He's thinking about going to a paid service, like \$29.95 per year for hundreds of gigabytes, which solves that problem. So it's really an interesting solution. You use the free iPig - which I hate saying, but there it is - iPig client. You connect to his server. I mean, it's a simple download. You connect to his server, you've got encrypted access from any hotspot out to the Internet. And it's free. Or...

**Leo:** Well, is this better than OpenVPN or - I mean, PublicVPN or HotSpotVPN or one of the commercial services?

**Steve:** Well, okay. What he's doing is, he's redirecting. He runs a little driver in the client that redirects your traffic through the connection the client has made to your server. Then it goes out over the Internet. Now, the problem with this is that the traffic is going to be prone to proxying and NAT problems. Unless he's dealt with that. I've got a dialogue open with him now. His name is - he's a neat guy in Germany, they're based in Germany - Mathias Roth. I was concerned about the security aspect, so I opened a dialogue with him. We went back and forth actually this morning. And if anyone wants to go to the iPig forums, they'll see my posting and the thread between Mathias and myself, talking about exactly what the security protocol is.

Because I did some packet sniffing last night, and I saw that my username was in the clear, followed by a 256-bit token. And I was concerned that that might be the key. He uses 256-bit AES encryption, which is very strong. And over the course of the morning, going back and forth with him - he's gone to sleep now because he's in Germany, and we're going to continue our discussion when he wakes up in the morning, his time.

Anyway, he did everything correctly. His system is prone to the same kind of brute force security attack that WPA is, or any preshared key technology is. But it's very clean, it's very simple, and it looks fine to me. So you download his free iPig client. You connect to his server. You've got - wherever you are, hotspots, hotels, you name it - you've got up to five gigabytes per account of access. You would then have to delete the account and create a new one, and you've got five gig more. I'm hoping this works for him and that people will instead, once he offers a for-fee service, will consider using that.

The other cool thing is, using the same technology, anyone can download his free server, set it up in a Windows machine - ah. This is only Windows. So that's one difference from OpenVPN and Hamachi is, at the moment at least, it's only a Windows platform-based solution. So you'd run the iPig server on your system, change the default port - he defaults to 11888. The first thing I did was move it somewhere else because you would never want to be running any service like that on the manufacturer's default port so that, if some vulnerability was found at some future point in his server, you'd have people scanning the 'Net, looking to attack you and get into your system that way. So run it on a different port, forward that through your router, and you can connect to it just the same. And when you do, you have access to all your machines in our network, as well as access out to the Internet.

So it's a, I mean, it's a really interesting solution. I haven't spent nearly as much time with it as I have with Hamachi. And again, there is the question that I've raised, that he had to go to sleep so he hasn't answered yet, is what about protocols which are NAT router and proxy sensitive? For example, in the FTP protocol, several of the connection setups include your IP address and port number of your machine. Well, since this has been redirected through a different machine, those packets are no longer going to be correct. NAT routers that are aware of this, they will reach into - they'll see that you're doing FTP based on ports and looking at the protocol. They'll reach in and adjust those packets to reflect the fact that the IP has been changed. I don't know if he's doing that. It's a big job, if he is.

And there are other protocols, like SIP and the H., what is it, 363, the various teleconferencing protocols, that also embed ports and IPs in their packets. So it might be that this isn't a universal solution. But certainly for web browsing and mail and many other things, it's worth a try, and it's free, and the security looks fine as long as you go to my passwords page or just invent a really nasty long key. He's got everything else worked out well. So again, I think people should take a look at it.

**Leo:** Change the default port and use a nasty key.

**Steve:** Yup.

**Leo:** And we should say that, yeah, as bad as iPig is, at least it's an acronym for the iOpus Private Internet Gateway. So there's a reason for it. It's bad, but there's a reason for it.

**Steve:** And the logo has a pig's nose with a key hanging from it.

**Leo:** That might be worse than the name. But it's free, you know.

**Steve:** It's free, and it looks great. And I'm going to be working with Mathias in the future. I will get answers to these questions that I still have. I'll talk about it, I'm sure, next week and have an update for people. But it really looks like a very nice solution.

**Leo:** All right. Now, we're more than half an hour into the podcast, and we haven't really gotten to the meat of the matter. So let's do that now.

**Steve:** Well, the good news is, there is too much meat for us to get to on OpenVPN. OpenVPN is probably

what I'm going to end up using and what you're going to end up using.

**Leo:** It's the holy grail?

**Steve:** It is, for many reasons, the holy grail.

**Leo:** Yeah.

**Steve:** It's not client-free. We know no client-free solution exists. We tried that using, you know, Word and - or, I'm sorry, Word - using Windows, PPTP, IPSec, L2TP, all that acronym soup stuff. We realized that VPN NAT routers are good for talking to each other, but really not designed for talking to roaming hotspot users, and that those protocols tend to get blocked with a high degree of probability.

OpenVPN is an open source project located over at SourceForge. It uses a UDP tunnel, which is the best transport for moving tunneling protocol, if you're able to get UDP from your client to your server. It is multiplatform, running on Linux, on the BSDs, on Windows, on the Mac. So it's a beautiful multiplatform solution. The other cool thing is, thanks to its open nature, it's been ported many places. For example, an OpenVPN server is part of Monowall, which many people are already running on a little, you know, discarded PC running Linux, and they're using it as their firewall or gateway in their home network. So OpenVPN can be installed or turned on in Monowall, and you've got remote access to your internal LAN. It's also supported by the OpenWrt project, which means that people who are downloading different firmware for their Linksys and other routers will be able to essentially put an OpenVPN server in their little plastic retail box, and, again, access their network from remotely, much as we were hoping people would be able to in the holy grail.

And finally, there's a very nice service that you, Leo, and I have both been using now for a couple weeks, which is called HotSpotVPN. HotSpotVPN uses just the OpenVPN system, right out of the box. What they provide is about a \$10-a-month service where they provide the Internet connectivity for anyone using OpenVPN out on the road.

**Leo:** So OpenVPN requires you to run a server that your client can log into, but you can subscribe to services that run the server for you.

**Steve:** Yes. Very much like Hamachi, OpenVPN, when installed on your system, creates a virtual adapter. Now, that's important because that's the only clean way I've seen of solving this packet fragmentation problem. You're able to tell the adapter that its maximum segment size is smaller than what's truly the maximum segment size for the network, so that when TCP is setting its protocol up and generating packets, it'll be making smaller packets, which then the protocol encapsulates in its transport tunnel in order to send over the Internet. So you end up with - oh, and it's using UDP, so maximum VPN performance. I don't think anybody will see a slowdown using HotSpotVPN. I've certainly noticed none. So...

**Leo:** And I was using it, too, and I was actually very impressed by the performance. It seemed like it didn't slow it down at all, yeah, on my Mac.

**Steve:** Yes. And...

**Leo:** Very impressed.

**Steve:** And, for example, someone behind a corporate firewall that is allowing TCP 80 and TCP 443, they would be able to use OpenVPN to get to their machines at home because it would look just like - unless the corporate system was actually running a proxy, where it's accepting their true HTTP connections and then regenerating a request outbound, which certainly could be going on. But if it's just using port filtering, they'd be able to access their network from home. So it's a - what I like about it is it's a widely multifaceted solution. It's available cross-platform. It's available in many forms. And we have a reasonable-priced HotSpotVPN service that will allow road warriors to encrypt their connections out of the danger zone, out of the hotel and out of a Wi-Fi environment, out to the HotSpotVPN location. I believe he's got - I've spoken to

Glynn, who's the founder of the HotSpotVPN solution. He's got networks, I think, on both coasts. And he's considering putting another network perhaps in an international setting in order to continue to do some load balancing. But it's a very wide application domain.

The downside, and of course there is one, is it is anything but one click. Whereas Hamachi, if it works for you, is amazingly zero configuration. And even iPig, if it can work for you, will probably be a fantastic solution for people for whom that works. OpenVPN is a much more complex product. I would consider it the Swiss army knife of VPN solutions. You configure whether you want TCP or UDP protocol, what port you want to run on, and, I mean, well, that's just the beginning. I mean, it's...

**Leo:** I want to clarify something just so people understand that. The commercial providers like HotSpotVPN, they're providing the OpenVPN service. In fact, they make it pretty easy to configure. That's one of the reasons you pay them. But that's not, when you're talking about OpenVPN, you're talking about the free software that they use, which is more complicated to set up on your own.

**Steve:** Yes. And in fact, I don't want to scare people away from HotSpotVPN. I was very impressed.

**Leo:** That was easy. On Windows, that's just - you run an installer, and that's it.

**Steve:** I mean, literally. It installs exactly the same stuff as if you were to download it from SourceForge, except that they've done all the work of pre-preparing your asymmetric public key certificates. It's all part of the bundle. So you sign up for HotSpotVPN, you get a link in a return email, you click the link, download a package, install it on your machine, and you literally click an icon on your taskbar, and you're connected securely to their servers. It is that simple. They've done all of the work.

**Leo:** I installed it on a Windows machine and a Mac machine. It was very easy on Windows. Little more complicated on Mac because you need a second solution called Tunnelblick, and you have to configure that a little bit. What does it take to do OpenVPN yourself? What are the steps to do that?

**Steve:** Well, that's really what I'm not going to talk about today.

**Leo:** Because it's so complicated.

**Steve:** Well, yes. What I'm going to do is, you know, a lot of people have said, okay, enough already on the VPN topic. And in fact it doesn't make sense for me to try to explain in detail how to install OpenVPN oneself. I'm only going to be using all the online documentation. I'm going to put up on my show notes, for this Episode 19, a list of all the online available documents. So anyone who is intrepid and wants to go ahead and mess with OpenVPN, knowing that we vetted it enough to know that it really does work and really is a terrific solution, anyone who wants to is welcome to. What I'm going to do in the background now is I'm going to put together some - I'm going to distill all that into some simple, easy-to-use how-to guides.

**Leo:** That's kind of what's lacking in the OpenVPN documentation.

**Steve:** Yes. It really is. Well, the problem is, you know, these guys who developed it are all excited about all the bells and whistles they've got. I mean, there's all kinds of stuff, where if you drop your connection, you may come back with a different MAC address because the adapter assigns a MAC address on the fly. So you would have an old MAC address in the ARP table, but there's a command-line switch you can put in to automatically flush the ARP table when you reconnect...

**Leo:** I don't want to know. I don't want to know.

**Steve:** ...blah blah blah, right. So I'm going to work through all that nonsense. I'm going to figure out, okay, here is exactly what you have to do. Here's some scripts. Here's some guides. Here's some screenshots.

Follow these, you know, instructions, and you'll be set up with, like, the optimal configuration. And the good news is there is a really good optimal setting where you can connect into your system remotely with what's called a bridge, as opposed to a routed connection. The bridging connection essentially extends your local LAN Ethernet, including the Ethernet broadcasts, across the bridge to your machine. That means that all file and printer sharing works; non-TCP protocols work, like if you wanted to use NetBEUI if you were really security conscious, that would work through the bridge. And ARP traffic works. So, for example, you're able to participate on the LAN and automatically route back out to the Internet. So, I mean, it is, it's a high-configuration holy grail solution. I'm going to work to - and I want to make it clear that, at the time that we're recording this, Leo, these guides don't exist. But that's what I'm working on. I'm going to nail this stuff down for myself, and I will share everything I learn along the way and distill some simple how-to approaches that figure out exactly what to do to make it work.

**Leo:** So if you can do that, then OpenVPN would be your choice. Are there any drawbacks to OpenVPN? Besides the complexity of installing it and getting it running?

**Steve:** Let me think. You do have to have a static incoming port that will accept connections from known and unknown people.

**Leo:** Can you use DynDNS or some other solution if you don't have a static port?

**Steve:** Well, now, that's a static IP. I meant...

**Leo:** Oh, you mean a static port, I'm sorry, okay.

**Steve:** Right. And you absolutely...

**Leo:** But you just do that by opening up your firewall, port forwarding.

**Steve:** Well, but I'm just saying that, you know, Hamachi doesn't require you to have any static port forwarding through your router or your firewall. Any solution where you're running a server on your LAN, whether it's iPig's server or the OpenVPN server, it will absolutely require that you run a port forward through. Now, I don't think it's a problem because this thing is very well hardened. It's been scrutinized. It's open source. But again, you want to pick some wacky port that only you know so that it's unlikely to be found. Just, you know, a little obscurity doesn't hurt. You also would want to run a Dynamic DNS. And many of the contemporary routers now allow you to set up a DynDNS account, and they will maintain that for you.

**Leo:** That's the static IP we were talking about.

**Steve:** Exactly. So that if your ISP did change your router's IP, and you were away from home, you'd be screwed. You wouldn't have any idea what IP to use to connect to your home network. But if your router supports Dynamic DNS, or you run a client on your own machine which will do the same job, then you'll always have your own domain name, you know, bobshomenetwork.dyndns.org or whatever, which will always be pointing to your router's IP, making sure that you're able to access it remotely.

**Leo:** It's a lot better than trying to get your spouse to run ipconfig. Trust me.

**Steve:** Well, and you would also want that, if you were using the iPig solution - I encourage people to take a look at iOpus's iPig. It's badly named, but it really worked well for me in my brief run-through yesterday. And so far the security architecture looks very solid.

**Leo:** Details on how to use OpenVPN will be available on your site in the show notes.

**Steve:** Excruciating details.

**Leo:** Do you anticipate - you're not going to work on that through Christmas, are you?

**Steve:** That's all I'm doing.

**Leo:** Steve.

**Steve:** I'm working on Open - I'm rolling up my sleeves.

**Leo:** Steve. You're the kind of guy that goes to a Chinese restaurant on Christmas Day, aren't you.

**Steve:** I am. In fact, Sam Woo, my favorite place, is open 365 days a year - on Thanksgiving, on Christmas, on New Year's, you name it.

**Leo:** So if you're looking for help with Hamachi or OpenVPN, Christmas Day, we have a date at Sam Woo's. No, no. Don't - leave poor Steve alone. He'll be reading a little science fiction, I hope, and taking a break.

**Steve:** But I will be setting up a Linux machine from scratch and doing the Linux config...

**Leo:** Wait, wait, wait, wait, wait. You're going to set up a Linux machine?

**Steve:** Oh, I'm sorry, I meant FreeBSD.

**Leo:** Okay.

**Steve:** The newsgroup server that I talked about at the beginning of the show, news.grc.com? That's a FreeBSD UNIX machine. FreeBSD is my, you know, Linux/UNIX-style platform of choice.

**Leo:** I was getting faint for a moment there. I thought the world was coming to an end.

**Steve:** Oh, I do it all the time. I love FreeBSD.

**Leo:** Yeah. FreeBSD is great. And we Mac users know a little bit about BSD because that's what's underlying Darwin.

**Steve:** That's right.

**Leo:** Okay. Are we complete now? Do we have everything we need to know?

**Steve:** I think we're done.

**Leo:** VPNs have been covered. I so decree it.

**Steve:** Now, what we'll do is, we will touch on this. I mean, VPN...

**Leo:** It's not going away.

**Steve:** Exactly. VPN is a core topic for Security Now! and for us. You know, you and I roam around, we're telecommuters, we want security.

**Leo:** Oh, yeah.

**Steve:** So listeners don't need to worry that their questions that they've asked are never going to be answered...

**Leo:** No no no no. Yeah.

**Steve:** ...that we're never coming back here. I mean...

**Leo:** We live here. This is our - this is where we live.

**Steve:** Yes. I mean, VPN is a core technology. We're not going to drop it. As I learn more about iPig, as I learn more about OpenVPN and I'm posting things, we'll be touching on it. But we've got a whole bunch of cool stuff lined up for the beginning of next year and Security Now!. And of course next week we'll do our Q&A, and we'll talk about some more of users' questions.

**Leo:** Well, and I also see why we needed to do the early chapters to get to this part, because there is so much to understand about what's going on, the pros and cons, the negatives, the security risks. You have to understand that before you can even have a conversation about VPN. So that was well worth it.

**Steve:** Yes. And that was exactly our intent. And of course we're going to talk early on about security architecture, what is an asymmetric key, what is a symmetric key. And so one of the things that users need to be aware of is that we're deliberately creating a foundation here that will allow us to explain, once it's necessary, about OpenVPN certificates and how they work. It wouldn't make a lot of sense to talk about it now. But once we've really explained how this stuff works, it'll all come together.

**Leo:** If you want more information and that step-by-step on how to configure and run OpenVPN, [GRC.com/securitynow.htm](http://GRC.com/securitynow.htm). Those are the show notes. And some people are confused by the little icons. Click those little icons. They all do something. There's transcripts there. There's a 16KB version of the show which I know people love. I'm not sure why, but they love that low-quality, low-fidelity version.

**Steve:** Well, it's because the file size is so small.

**Leo:** It's such a small - I understand. I'm just giving them a hard time.

**Steve:** I know.

**Leo:** Because we work so hard on audio quality here. And for more information about all this stuff, Steve's the guy. And don't forget those newsgroups, the [GRC.com/discussions.htm](http://GRC.com/discussions.htm).

**Steve:** Oh, Leo, I mean, we've got hundreds of really good people who hang out there. And, you know, the Usenet-style newsreader is such a joy to use. I'm sure, you know, in the old days you've used it a lot.

**Leo:** I still use it. Oh, absolutely, yeah.

**Steve:** It's just a great way to have dialogues and conversations. And we do now have a Security Now! newsgroup on the GRC news server.

**Leo:** That's great. If you want to download the full version, of course, you can always get it at ThisWeekinTech.com. We do thank the folks at AOL Radio for broadcasting Security Now! on their podcast channel, and providing the bandwidth for the Security Now! downloads because there's a lot of downloads. And at some point we're going to try to put this all together in an anthology, maybe a CD. We've started to get requests from corporations who want to distribute them to employees and so forth. So we'll work on that, as well.

Next week, your questions, Steve's answers. Have a great and happy holiday, Steve.

**Steve:** Thanks. You too, Leo.

**Leo:** Thank you so much for all the work you've done on VPNs. This has been really fascinating. And it makes me feel good when I open up my HotSpotVPN to know that I'm safe now on the road.

**Steve:** That's what I'm using.

**Leo:** Yeah, it's just great. I'm Leo Laporte for Steve Gibson. We hope you have the best of holidays, and we'll see you next week on Security Now!.

Copyright (c) 2005 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details:  
<http://creativecommons.org/licenses/by-nc-sa/2.5/>