Open Wireless Access Points

Description: Leo and I examine the security and privacy considerations of using non-encrypted (i.e., "Open") wireless access points at home and in public locations. We discuss the various ways of protecting privacy when untrusted strangers can "sniff" the data traffic flowing to and from your online PC.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-010.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-010-lq.mp3

Leo Laporte: This is Security Now! Episode 10 for October 20, 2005: Open Wireless Access Points.

Steve Gibson is on the line, and we're ready to talk security. Steve, of course, the head honcho and maven at GRC.com, the creator of the great SpinRite file recovery and disk recovery program, which I still use and have used for years and love, and it's updated and great and better than ever. And of course ShieldsUP! and all of his free security products that you can download, like DCOMbobulator, Shoot The Messenger, UnPlug n' Pray - or is it UnPlug n' Play?

Steve Gibson: UnPlug n' Pray.

Leo: It is UnPlug n' Pray.

Steve: Because the idea is you want to run it and then pray that nothing else gets you.

Leo: Pray it works. And then of course the Security Now! podcast, which we're very pleased to say is getting a great response, I think a lot of interest. Everybody has to pay attention to security; and occasionally I'll see a message saying, well, I'm a Mac user, but I still listen. This stuff applies to Mac users, too.

Steve: Well, and in fact that's one of the things that, you know, we're trying to do with this, is there are some people who sort of just want to know what button to push. It's like, oh, don't confuse me with any theory. I just want to know what program to run, what button to push. But it's really more interesting, I think, to - I mean, certainly we do some of that, the way we did, for example, with RootkitRevealer, telling people who are using Windows to just get that off the Sysinternals site and run it. At the same time, it's much more valuable, I think, if we explain what this stuff is about. And, you know, I don't remember what the old adage was, something about, you know...

Leo: Give a man a fish, he'll eat for a day.

Steve: That's right.

Leo: Teach a man to fish, he'll know what equipment to buy.

Steve: Exactly, so...

Leo: Or something like that.

Steve: Well, what I think - no, I'm sure that's exactly the one that I was trying to think of.

Leo: Yes.

Steve: So the point is that, if we can explain essentially that, you know, the things that we know in our soul from having been dipped in all this technology for years and years, in a way that's accessible to people, then we're turning people into security, you know, gurus themselves, who, for example, won't want to know only what the best antivirus program is, but will be able to evaluate for themselves what the best one might be.

Leo: I think that's important. I think that, unfortunately, we do live in a world, certainly in the Windows side, where you have to be a security expert, unless you're lucky enough to be sitting behind a well-manned firewall at your office, and you don't use the stuff at home. I mean, everybody needs to have some security information.

Steve: Right.

Leo: It's just part of the deal. And if you're a Mac user, I think it's very important.

Well, the topic today impacts Mac users just as much as it impacts PC users. But before we get to today's topic, let's kind of wrap up this rootkit. Because we did learn some stuff since our last podcast.

Steve: Well, and in fact it was the day after you and I did the podcast in Toronto that we also did a show on Call for Help about the same topic, about rootkits. We ran RootkitRevealer on the various machines there. I don't think there was a single one that came out perfectly clean.

Leo: But a lot of it was false positives.

Steve: Well, that's exactly the point. For example, we discovered that Norton's secure-delete facility actually uses this same rootkit technology to hide deleted files from any programs in the operating system, much the same way we were talking about rootkit technology would be hiding malware. Of course, Norton's secure deletion system is not malicious at all. It's doing this in order to really securely save these deleted files until you want to bring them back.

Leo: So it's a legitimate use of rootkit technology.

Steve: Yes. And so, again, it's the perfect example of why it's worth spending some time on the theory behind the things we talk about because this would allow people, if people understood that what RootkitRevealer was doing was not revealing rootkits necessarily, but actually showing the difference between what's really on the system and what you're seeing - I mean, for example, you would have a sense that, okay, this is something that's hidden from me, not, you know - it's a false positive result from RootkitRevealer, not something that's necessarily malicious.

Leo: We also found that Kaspersky's Antivirus uses a rootkit to hide some of its processes.

Steve: Right.

Leo: And so we thought, oh, my God. We ran it on Andy's computer, and we were laughing because it was so loaded with stuff. And then we realized, oh, it's just Kaspersky. It's normal.

Steve: Right. There have been some people who have responded that they have found rootkits. They have found randomly named files and other confusing things. So it looks like it's very useful. But again, it certainly is the case that there are valid programs, non-malicious programs, that are also hiding things on behalf of the user as part of their function.

Leo: It just underscores your point. There's no such thing as pushbutton security. You really do kind of have to understand this stuff. You know, we have that bent, though, you and I. We like to understand it. We're interested. That's part of the fun of it for us. Not everybody wants to. But that's, I guess, just the way it is, at least...

Steve: Well, and I think that's what this program is about is explaining issues of security, oftentimes telling people, you know, what we recommend they do; but also, you know, a lot of why because, you know, why is what's really interesting, I think.

Leo: Let's change gears now, talk about our subject of the day, open wireless accent points, something everybody has to deal with, not only when they set up their own wireless network at home, but when you go to an Internet café, an airport, a hotel, and use their wireless.

Steve: Right. I think that, well, certainly we will be talking about issues of wireless security many times. You know, at some point we're going to talk about, you know, encryption and essentially non-open use of Wi-Fi. But I really wanted to spend some time to talk about open access points. For example, right now, where I'm sitting at home, I don't have wireless running. There are three open access points that my, you know, if I were running wireless, I'd have complete access to.

Leo: Your neighbors.

Steve: Those neighbors of mine have not secured their access points.

Leo: I walked downtown with NetStumbler running a couple of weeks ago, just to see. I walked through my small town. I live in a little community of about 50,000. And I would estimate about 60 percent - and apparently this is a pretty consistent figure nationwide - 60 percent of the access points I was able to see were unprotected.

Steve: Well, now, from prior conversations that we've had in TWiT, we know that a lot of people want their access point to be open. They sort of like the idea of creating a communal access to their broadband through their access point. So sometimes they're doing it deliberately.

Leo: I used to be that way. But as soon as I realized that people could see everything I'm doing, I kind of changed my tune.

Steve: Well, now, that's exactly the point. And that's really what I wanted to talk about is, if we step back a little bit, a wireless system is like an Internet hub, inasmuch as, you know, anybody who has access to - who is within range and has access to the radio signals is able to see all of the traffic going to and from. There are, you know, in Internet technology there's this notion of a hub versus a switch, where the difference is a switch actually looks at the data coming in and routes it back to or out to the destination where it's going to. So if one person is, like, sniffing all the traffic on their wire, they'll only see their traffic going to and from the switch because the switch sends other people's traffic down their connections; whereas with a hub, essentially you're rebroadcasting everything that the hub receives. Well, similarly, a wireless access point that is running open is working like a hub, inasmuch as anyone sniffing the traffic that they're able to receive sees everything coming and going. And because it's an open access point that is not encrypted, it's in the clear.

Leo: This is the nature of Ethernet. It's what they call a "collision-based network." Think of it as a big circle, a big ring, and all of the traffic goes around the ring everywhere until it finds its destination. But it's visible, meanwhile, to everybody on that ring.

Steve: Exactly. And in fact the original topology for Ethernet was a coax, a single coax cable, and you tied your cards into this coax.

Leo: Uh-huh, I remember that...

Steve: So the idea was that, if packets happened to be sent at the same time, they would collide. And they were listening themselves to the traffic, so they would see that they had collided because somebody else started transmitting at exactly the same time, so they would wait a random length of time. Chances are, then, that one or the other would retransmit in the clear.

Leo: So the upshot of this is that, when you're on a network like this, anybody else on the network can see what you're doing.

Steve: Well, yes. And in terms of what the person's doing, for example email, unless special actions and measures are taken, email is transmitted as pure raw text in the clear. So, for example, somebody running a packet sniffer, which are freely available for download on the Internet - Ethereal is my favorite packet sniffer - anyone sitting with a wireless machine running Ethereal will see all the traffic going to and from everyone's machine that is within range.

Leo: So they see raw data, though; but can they construct, you know, your emails, your passwords? Can they reconstruct that out of the raw packets?

Steve: Oh, absolutely. And in fact, tools like Ethereal will reconstruct dialogues because it's able to understand what the protocol is. It'll rebuild email messages. Much of the email log-on called POP is just in the clear. So you'll see usernames and passwords going out, you'll see mail that they're sending and mail that they're receiving. I mean, it really is completely insecure. So I think the real point that we want to drive home is that, sure, you may think that it's exactly the model that you had, Leo, where you were talking about initially running your access point open completely. It's great to think about sharing your bandwidth in a situation where you're not being billed per byte, you're just being billed a flat rate per month. That's like, hey, I'm not using my bandwidth, you know, I want to be a good citizen here and allow my neighbors to do so. But, I mean, it really is the case that, unless you take special measures, like running a VPN connection through, or running a secure tunnel to a remote proxy, I mean, it's very difficult to protect this by default in an open access point.

Leo: So the solution is to scramble your data. Now, it's scrambled when you go to your bank or you buy a book on Amazon.com because those are secure socket layers, and they're scrambling it. But it's not scrambled normally when you're downloading email or visiting a web page. So you said you can...

Steve: No, exactly.

Leo: You can protect it by scrambling it. And you mentioned VPN and other techniques.

Steve: Well, yeah. I had a person who wrote in asking, if they were on a secure site filling out a form, and they did not yet have the little lock showing, was it safe to submit that data. That's actually a really good point, that the way data is sent back to a web server is over, well, secure data is over this SSL connection, or as people see it in the URL, https, "S" being for secure, as opposed to just http://. The event of pushing the button and submitting the data will create a secure connection. So it's very likely that, if the web page is running securely, that is, even if it's not showing you the lock when it's displaying the form, submitting the form can still be done securely. However, unless you take a look at the source code of the web page, you're not going to be really sure that it's a secure submission. So most sites will take the time to, for example,

create the form on a secure page...

Leo: Right.

Steve: ...to show their users that they've got SSL technology and to give them the assumption that, when they actually submit the data, it's going to be secured.

Leo: And a late model browser - and you may have seen this warning, now you understand what it means - late model browsers will say, "Warning: You are submitting this data over an unencrypted connection." Most browsers will now warn you about that.

Steve: Right.

Leo: Just so that you don't think - well, I'll give you an example. I use SSL for my email. But in order to establish the SSL link, I have to send a password to log in. I presume that password is sent in the clear, unencrypted; right?

Steve: I would guess that that's probably going to be encrypted. If you're using SSL mail, you're probably connecting to a port other than the normal POP default port.

Leo: Ah, that's right. We're connecting over 443. So it's secure already.

Steve: Oh, okay. Exactly. So the idea is that, I mean, the beauty of SSL - and it's a very nice protocol that, again, we will be talking about in the future in some length because it involves this whole public key/private key business - the beauty is it establishes a secure encrypted tunnel, or connection, between the end points, prior to any user data passing through it. So that the connection is secured before the URL goes through requesting a page to be delivered over SSL, before your username and password goes through, I mean, it's extremely secure.

Leo: Now, when I set up my wireless network at home, I'm turning on WEP, or better yet, WPA. That's protecting me. Is that right?

Steve: Well, sort of. One of the things I want to talk about soon - maybe we can do it next week - is to follow on with this talk about, you know, open versus closed by talking about different types of closed or encrypted connections. Because it really matters what type of encryption you use.

Leo: Well, let's save that for a later date. But just at least say use WPA if you can.

Steve: Yes.

Leo: And...

Steve: Absolutely. If, as a result of us talking about this, people decide, hey, you know, I'm going to go to a little more trouble now - I think what happens is, oftentimes people, you know, bring their wireless gear home. They plug it in. They think, oh, well, you know, I'll worry about all that encryption stuff later. I just want to make sure this thing works and see if it goes. And, you know, they plug it in, they connect up, everything's working. And it's like, oh, well, I'll do that tomorrow, or next week, or whenever...

Leo: And I don't blame them because they...

Steve: ...and never get around to locking their access point down.

Leo: And it can be a real pain, you know, to do that, so I don't blame them. So, but assuming you're doing that at home, you would be safe; yes?

Steve: Doing what?

Leo: Turning on WPA encryption.

Steve: Yes, yes. If you are at home, well, basically any of the encryption - the original encryption, WEP, has been badly broken. And that's what I want to talk about when we specifically discuss this because it's really interesting how and why it's broken. But the successor, called WPA, was specifically designed so that it could be retrofitted in older gear that only used the WEP encryption. So WPA is extremely strong. I mean, it's industrial strength. You can use it anywhere. If your equipment only has WEP encryption, as all of the early equipment did, then that's certainly - that's, like, way better than nothing at all because it will encrypt the data. It's just that if somebody really wanted to get to it, they could. So if you only have a choice of WEP, that's certainly better than leaving your access point open completely.

Leo: But here's the problem. If I go to a coffee shop, or I go to the airport or a hotel, they don't turn on encryption. They have to leave them open so I can log in; right?

Steve: Well, that's exactly right. And again, it's really important to keep that in mind, that if you're using an open access point, you really need to think of it in terms of everyone in the coffee shop, for example, is clustered around behind you, looking at your screen. I mean, they're not actually looking at your screen electronically...

Leo: But they could.

Steve: ...but they're seeing the mail you're sending; they're seeing the mail you're receiving.

Leo: There's really two issues. We've talked about the privacy issue of people seeing your stream. What about the issue of people hacking into your computer? Aren't they able just to get access to your network by virtue of being able to glom onto that connection?

Steve: Well, I'm hoping that anyone who's concerned with security has taken the measure already of running a local personal firewall. This is another good reason why, even if you've got a NAT router at home that you know is going to be protecting you from external intrusion into your network, you still really want to be running a firewall on your machine.

Leo: If you ever leave your home network - you don't need it on a desktop. But if you ever leave your home network, you've got to have it on your laptop.

Steve: Yeah. And anybody using Windows XP Service Pack 2, and certainly anyone who's now running Windows XP should be; or maybe you prefer ZoneAlarm or, you know, Sygate or Norton or Outpost or Kerio or, you know, any of these many personal firewalls. You know, that's going to be there, carried around on your machine, and it's going to keep people from getting into it in any simple fashion, even though they are basically in a shared wireless mode.

Leo: Probably even just the built-in Windows Firewall would be sufficient in that case.

Steve: I think it really is absolutely sufficient in this instance.

Leo: And especially Service Pack 2, yeah. So what do you do when you go to a wireless access point? You can't force them to turn on WPA. How do you protect yourself?

Steve: There are really only a couple ways. If you were at an open wireless access point, accessing your corporate network, most likely you're in a mode where, in order to dial in or connect into a remote corporate network, you're going to be running over a VPN. A VPN is very much like SSL. It actually uses a different protocol, typically IPSec, which is IP Security, in order to establish an extremely strongly encrypted connection between your machine and the remote network. Essentially you're participating in that remote network, sort of extending your corporate network across the Internet, through the air, to your table in the coffee shop, and making your remotely connected machine very much secure, as if it were sitting inside of the corporate firewall on the corporate network.

Leo: Many of us, unfortunately, don't work at companies where we can do that. But there are alternatives, things you can do even if you don't have a corporate network.

Steve: Yes, exactly. The next step is to use some sort of a proxying service that is offering you a secure tunnel on purpose. You've mentioned the one that you have some appliance for.

Leo: Yeah. I use iPhantom. Now, you'd have to carry that around with you. I don't know how practical that is. But that does that because it establishes an SSL link with their servers.

Steve: Yes.

Leo: There's also companies...

Steve: Also Anonymizer.com.

Leo: Anonymizer does it. And that's...

Steve: And they explicitly offer exactly what we're talking about. An encrypted tunnel is what this is called, an encrypted tunneling service, where you would run some client software on your side. Basically you're using the wireless connection to get your machine on the Internet. Then you're creating an encrypted tunnel connection between your machine, client software running on your side, and this service, for example, the Anonymizer secure tunneling service, so that your traffic is encrypted through the air, across the Internet, to Anonymizer.com, where it is then decrypted in order to then transit from their location out over the Internet, just as you normally would if you were at home or in a corporate environment or wherever else. The point being that the vulnerable segment, where you're going over the air from your computer to the coffee shop or airport access point, that's encrypted. It's also encrypted all the way to where it gets to Anonymizer, so you're safe against, for example, employees at the access point who might be able to sniff your traffic, as well.

Leo: I want to mention two other products that do the same thing. One is very inexpensive, it's called HotSpotVPN. And it uses SSL, which is kind of nice because most of the time SSL ports are wide open. You don't have to talk to the coffee shop to say, hey, please pass my VPN traffic. Because not all routers will do that automatically. That's the...

Steve: That's true.

Leo: So since it's SSL, you can pretty much guarantee you'll be able to do that. If you pay for a year, it's fairly inexpensive. And then there's another one called PublicVPN.com. And same idea, you subscribe, and then you log into their servers, and they protect you. So there are choices. Do you think that's the way to go, I mean, if you're going to be in a coffee shop?

Steve: I really do think that's the way to go. It's, I mean, sure, it's not free, but you're getting some substantial benefit from the service. If you're a person who uses open access points, you really need to be aware that - well, and in fact, what's really interesting, Leo, is even if you were to use encryption, that is, if you were to use first-generation WEP encryption, typically everybody on the access point has the same key. So even if it's encrypted, if you're using WEP encryption, you still don't have any protection.

Leo: That's not good.

Steve: No, it's - no. WEP does have a configuration where you can use a per-user key. But due to the, you know, tremendous overhead of managing keys for individual users, almost no one does that.

Leo: Interesting.

Steve: Generally an access point has a single key. Everything connecting to it has the same key, and it encrypts it. But it means that, again, sniffing the traffic, it can trivially be decrypted if you're using WEP-style encryption, which is another reason WEP is really bad and WPA is a much better solution if you have a choice.

Leo: Now, I notice that Wi-Fi hotspot providers are becoming more aware of this. I know that T-Mobile now claims that it's offering some sort of - I'm not sure how they're doing it, so we'll have to look into it. But they provide some sort of security for users of T-Mobile hotspots. I'm sure Wayport, the other big provider, is going to start doing the same thing.

Steve: Yes.

Leo: Boingo has for a long time.

Steve: Certainly if the user was just surfing the Internet, they didn't care if anyone was, like, looking over their shoulder, seeing the pages that they were bringing up, saw the URLs they were clicking on, the music they were downloading, or whatever they were doing, you know, there are certainly scenarios where you really just don't care about eavesdroppers. But it is totally the case that, unless you're taking some measures on an open access point, eavesdropping is completely possible.

I'll mention one scenario for the home user that's useful because it's simple and free, and that is, if your access point is not part of your cable modem or your main router, but you've got a separate access point, like a freestanding little radio that you plug in to your router, if that's a switch as opposed to a hub, as most of these routers are, then your traffic on your wired network is not going to be seen by the wireless network. That switch gives you some isolation. And so there are ways that you could, if you really wanted to run an open wireless access point for your neighborhood, for example, there are ways that it could be done securely; but you really need to give it some thought.

Leo: Anything more to be said on this topic? I know there's a lot more to be said, but on this particular show, how about?

Steve: I think we've got this one covered. And next week let's talk about WEP versus WPA...

Leo: Absolutely.

Steve: ...and the different types of encryption of wireless because we've had a lot of questions from people about that.

Leo: For more information, of course, we've got the show notes, they're online, and we'll put links to all the websites and products we mentioned on the show notes at GRC.com/securitynow.htm, or on ThisWeekInTech.com, where I also post the show notes. By the way, I want to mention, if you use a podcast client like iPodder X or iPodder, the show notes are also visible in the RSS of the feed. So the information that we're talking about is part of what you get if you subscribe to the show. It's not visible in iTunes and some of the other aggregators, but it is visible in most of them. So that's another way to see where those links are and so forth. Look in the show description of your aggregator to see more.

And Steve keeps a pretty good page with lots of information and feedback, and there's always a conversation going on around it at his website, GRC.com/securitynow.htm. That's where you'll find the small versions of this show, the 16KB version for those people who want to play it back on portable devices or just don't want to spend the time downloading it. He also provides transcripts in a variety of formats for people who want to share this information with colleagues, friends, and family.

And I want to thank the folks at AOL's podcast network, AOL Radio at AOLmusic.com, for providing us with the bandwidth for Security Now!. It's a great pro bono service they offer that makes it possible for us to get this to you in the easiest possible way.

We'll be back next Thursday with more Security Now! with Steve Gibson. Thanks, Steve.

Steve: Thank you, Leo.

Leo: Have a great day. I'm Leo Laporte. Take care.