SECURITY NOW!

Transcript of Episode #11

Bad WiFi Security (WEP and MAC address filtering)

Description: Leo and I answer some questions arising from last week's episode, then plow into a detailed discussion of the lack of security value of MAC address filtering, the futility of disabling SSIDs for security, and the extremely poor security offered by the first-generation WEP encryption system.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-011.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-011-lq.mp3

Leo Laporte: This is Security Now! Episode 11 for October 27, 2005: WEP and MAC Address Filtering. Right?

Steve Gibson: Yeah.

Leo: Steve Gibson.

Steve: Yeah. Now, talking about wireless security is a huge issue for people. It's complicated. There's a lot of acronyms, you know, sort of an acronym soup area. And, sadly, the vendors of these wireless routers are doing really dumb things. I ran across some pages in one book that showed the default WEP keys that some routers have.

Leo: So they have keys that anybody who knew what they were doing could just crack right away.

Steve: I just - when I saw this, it was like, my god, these people are never going to learn.

Leo: Wow.

Steve: You know, it's like having, you know, default administrative name, or username and password. It's like, okay, that's just a bad idea. And so here they're, like, creating really good security, or what they hope is really good security, and then giving it default passwords.

Leo: Good lord.

Steve: Just amazing. But a whole ton of people posted to the Security Now! page all kinds of ideas and questions and things about our last week's topic, which was the idea of open access points. And there were a couple things that I thought we had covered that I guess we hadn't, that I want to. And many people were wondering about MAC address filtering.

Leo: Right.

Steve: But first of all, a question that we got several times was, what about the legal implications of leaving your access point open on purpose so that other people can use it? And I would have thought we would have talked about it. But if not, we certainly want to because, of course, that's the huge issue, is if your neighbors are using your access point, then anything they're doing which is illegal - and you might guess that maybe someone would tend to use somebody else's access point just specifically because of the inherent anonymity that they're going to get. But any traffic which is backtracked towards them is going to hit your IP address, that is, the IP of the open access point, and stop there. I mean, that's the public IP for the access point. And at that point, you know, it goes wireless, and there's no way to track it beyond there.

Leo: So even if you want to let people use - I mean, I think there's something to be said for being generous and letting people use your access point. You might want to think twice about it just because you'll be liable for what they do on it.

Steve: Well, it's do you know your neighbors? Or maybe it doesn't even matter if you know your neighbors. So, yes, I don't want to discourage people from being generous and sort of having this community spirit of, oh, you know, my bandwidth is a flat rate, I'm not paying per transfer, so I'd like to make it available. But again, as with so many things, as long as you know that, you know, the RIAA might come knocking at your door, I mean, and they are suing people; and that, you know, any kind of filesharing, any file downloads, anyone who's, like, tracking malicious activity will come to the IP of your router, which is the same as your access point, and stop at your location.

Leo: Certainly something to be aware of, although we're not legal experts; so the legality of it and so forth and what your liability is I would have to leave to a lawyer.

Steve: And, you know, we've talked on several previous TWiT episodes a few months ago that there have been some strange legal judgments made. Like someone got sued for using someone else's open access point.

Leo: Right, right.

Steve: Because he was doing it deliberately, they said, oh, well, that's an abuse of somebody else's computer network. It's like, oh, okay.

Leo: And we don't know yet what the upshot of that case will be. But, yeah, it's, you know, it's kind of murky right now, to be honest.

Steve: It's strange.

Leo: We don't, you know, they're all - the rules - nobody's really codified how this whole stuff works and who's liable for what, so I guess it makes sense. There's also the other issue, then, there's a real security issue of an open access point. Even if you're using SSL and encrypting everything you're doing, it still gives people access to your network; right?

Steve: Oh, well, it does, although the switch provides some protection. Now, a couple people who know a little bit more about the way Ethernet switching happens took issue with my saying that the fact that you had a switch on your access point was good because it meant that your wired network traffic would not be going out over the air. Well, that's completely true; but it turns out, and this is absolutely true, that there are ways to penetrate switches. And we'll talk about that here in a couple minutes when we talk about MAC address filtering. But it is the case that a switch can be breached. But, in general, it's also true that the wired traffic is not just being gratuitously broadcast all over the neighborhood, which is, you know, certainly something you want to be aware of.

Leo: So, but not all - most routers are not switches.

Steve: Actually, most routers are switches.

Leo: Oh, they are, okay.

Steve: Yeah. So, for example, a Linksys router will have a 4- or 8-port switch. And so the idea behind a switch is that traffic is being sent to the endpoint that it's destined to, not just broadcast...

Leo: Right.

Steve: ...out on all the wires or out over the air.

Leo: And that gives you some protection.

Steve: That gives you some protection unless somebody really wanted to work to penetrate that. I guess I ought to talk briefly about how that's done. There's something called "ARP spoofing." ARP stands for Address Resolution Protocol. The way Ethernet functions, Ethernet works on these things called "MAC addresses," which is sort of the address of the physical interface. Every Ethernet card has a unique 48-bit MAC address. 24 bits of that 48 bits - that is, half of the address, 24 bits - is assigned uniquely to each manufacturer. And then they have the other 24 bits - actually it's the least significant, the right-hand 24 bits - which is a serial number which they increment uniquely for every single device they create, the idea being that there is no provision on the Ethernet protocol for dealing with the collision of MAC addresses; that is, two adapters, both plugged into the same Ethernet, are going to have a problem if they've got the same MAC address.

Leo: Let me just kind of - a MAC address is a unique number assigned to your network card or all network interface cards, wireless adapters, wireless access points. Each have supposedly a unique MAC address.

Steve: Correct.

Leo: And is it guaranteed to be unique, or is it likely to be unique?

Steve: Well, it has to be unique for an Ethernet, for local segment of an Ethernet; that is, all of the adapters that can see each other on the Ethernet, it has to be a unique MAC address.

Leo: So that's how the packet knows where to go, or...

Steve: Exactly.

Leo: Yeah.

Steve: And, in fact, that's where this Address Resolution Protocol comes in. What happens is, typically the gateway machine, that machine that is on the connection between your local network, your LAN, and the WAN, or another chunk of LAN, when it gets a packet that's destined for inside, it sends something called an "ARP broadcast," basically saying, hey, who has this IP, that is, which adapter out there is handling traffic for this IP address. Because a MAC address and an IP address are very different. The IP address, as we've talked about many times, is the unique address for the Internet, which is different from the - sort of like the physical hardware address, which is the MAC address. So in response to this broadcast, which all adapters receive, one of them that has that IP assigned to it says, oh, that's me. So it answers the request, saying that my adapter is assigned to this IP. So at that point, anything listening has the - essentially begins to build up a map, gets information about which IPs are associated with which MAC addresses. So this is the way that a switch, then, learns on which wired connections, which MAC addresses are valid, and which IPs those are associated with. Okay, now, this all comes...

Leo: Okay. I'm trying to follow this. It's a little complicated, folks, and I - this is one of your black diamond Security Now! podcasts, for the experts here.

Steve: Well, there's all the details. Now, the question that so many people wrote in to ask about after last week was, many people said, you know, for whatever reason, I'm not using any encryption, I'm not using WEP, I'm not using WPA; but I do want security on my wireless network. So I've taken advantage of what's called "MAC address filtering." On my router, I'm able to give it a list of MAC addresses, that is, the physical adapter, like the wireless adapter, serial number that I want to allow to have use my access point. Is that secure?

Leo: Right.

Steve: And the answer is, not at all.

Leo: Now, but see, this is a surprise to me because pretty much every corporation does this - we did it at TechTV - the assumption being, well, by preventing nonregistered MAC addresses from logging in, we're secure.

Steve: Yup.

Leo: Why is it not...

Steve: Absolutely not secure. It's...

Leo: Why not? It seems like it would work.

Steve: It's what I was referring to when I said it's hard to believe that router manufacturers are offering something which is completely bypassable. But that's what's going on.

Leo: So I just want to mention one more time, so people understand, this is that setting, usually called "MAC address filtering," that most routers have. And what you do is you'll get the MAC address of all the different wireless cards that you want to allow to connect to your access point, and you'll enter them into a table. And if this filtering is turned on, only cards with that MAC address, in theory, will be able to log into your access point. It seems like the ultimate in security. It's an affirmative security policy, saying only these people can get in.

Steve: Yes, it is a feel-good...

Leo: You're really bumming me out here.

Steve: Well, okay.

Leo: So what happens? Do we spoof it? How do we crack that?

Steve: Yes, that's the problem, is that the MAC address is the front of every packet sent, says basically there's a - I'm going to this MAC address from this MAC address. Which means anyone with any sniffer software...

Leo: Ah.

Steve: ...instantly sees all the authorized MAC addresses for the wireless network.

Leo: Well, not all of them. All the active...

Steve: It's that...

Leo: All the active ones.

Steve: All the active ones.

Leo: So they watch traffic that's legitimate traffic. They capture even one packet, they've got the MAC address that they can spoof.

Steve: Yes. They have a valid MAC address which has been authorized and recognized by the access point, and they can simply use it. It's that bad.

Leo: You know what? That provides no security at all. So in other words, I'm a bad guy. I'm sitting outside of Big Bank, Incorporated. Big Bank, Incorporated believes in wireless, but believes in secure wireless, and says only these MAC addresses can connect. So I just capture one packet of somebody talking to their router. I say, oh, there's their MAC address. I put in - almost every program allows you to spoof MAC addresses. That's trivial. In fact, your router allows you to spoof its MAC address very often.

Steve: Well, in fact, many user interfaces allow you to specify...

Leo: What's your MAC address?

Steve: ...a MAC address for, you know, whatever reason. I mean, there's nothing at all special about a MAC address. It's just a 48-bit serial number. If...

Leo: Now, wait a minute, though. You said that only one device can have that MAC address. So I cannot get on while that other one is on still.

Steve: Well, actually you can.

Leo: Oh.

Steve: Because there's nothing to prevent two devices from using the same one. That is to say, it'll be little confusing for the other one...

Leo: Right.

Steve: ...which is receiving traffic that's bound for it. But that happens all the time. So if you adapt - or, sorry, adopt the MAC address of some other machine, then it'll go to the access point. The access point checks the MAC address against its list of authorized MAC addresses, sees that it's valid, and accepts the traffic from it.

Leo: Wow. So, okay.

Steve: So there are even - there are plenty of more advanced things that can be done, as well. There are ways to disassociate a remote machine from the access point using the wireless protocol. So, I mean, this is something that's been researched extensively. There are ways you can disconnect one machine and then connect yourself in.

Leo: So you could knock the other guy off.

Steve: But the short version of this is it provides zero protection. I mean, it would protect your access point from a neighbor casually connecting or maybe, as often happens, mistakenly connecting.

Leo: Right, right.

Steve: There was a true story that I heard - this is not an urban legend - from a security guy who went to one of his clients' homes who was complaining that something was wrong with his wireless connection. And when he looked, it had a Apple AirPort SSID. Well, this was a Windows guy. And he said, you know, I've got a Linksys wireless router here, not an Apple AirPort. So they unplugged his Linksys wireless router, and he stayed connected.

Leo: He's still on.

Steve: He was using, without knowing it, he was using his neighbor's wireless connection. So then they shut his system down and reconfigured things, turned it back on, and it's like, oh, now I'm connected correctly. But then they realized they forgot to plug his router back in. Now he was using somebody else's wireless access point. There were several of them within radio range. And his system was just grabbing whatever one came along. So, I mean, there are certainly cases where locking down and filtering MAC addresses would prevent casual misuse of your access point. And so I don't want to say it's completely useless. It will certainly prevent casual use. But it should never be confused with security. It is not security.

Leo: Well, it's similar to the SSID hiding that some people advocate, where you hide the name of your router so that people don't see it. But that's - in fact, it's almost identical to that because it hides it only from those who aren't using packet sniffers, but everybody else can see it just fine.

Steve: Exactly. Anyone who wanted access to your access point would still be able to get it without any trouble at all.

Leo: So we've eliminated the use of MAC address filtering, SSID hiding, and WEP encryption. It sounds like the only way to secure wireless networking is with WPA encryption.

Steve: Well, that's really true. And what I want to do is, for the balance of this second podcast about wireless, is I want to talk about WEP encryption because, again, it's so tantalizing, and it was the legacy encryption technology, which has been obsoleted. But because older equipment doesn't support the stronger WPA encryption, many people are using WEP encryption because that's all they've got, or it's there; or, you know, they've heard that it's not secure, but they've really never taken it very seriously.

Leo: Well, and this is also - this story is really a very good object lesson in how not to design a security protocol.

Steve: Well, what happened is really interesting.

Leo: Yeah.

Steve: It was designed by - the WEP, W-E-P, this original encryption was designed without consulting security people. It was a security protocol designed by engineers who had the best of intentions but weren't security people.

Leo: It's a security protocol that sounded like a good idea at the time.

Steve: Well, and, for example, it uses an extremely good cipher technology called RC4. That's an RSA proprietary cipher which is very good for encrypting as long as you use it correctly. And that's really the key. The foundation of WEP encryption, with this RC4 cipher, is extremely strong. But it was used in a very bad way. For example, an absolutely unbreakable encryption is something called the "one-time pad." With a one-time pad - and this was used by the U.S. military in early world wars and was never broken because it is unbreakable. And, you know, I don't say that casually. I mean, really, truly unbreakable, not like, oh, there aren't enough computer power, you know, it would take X billion billion years, no. Unbreakable. The idea is that you generate random numbers. And it's - now, that's super critical. The numbers have to be really truly random.

Leo: Now, that's hard for a computer to do, in fact.

Steve: Well, it's very hard. And, in fact, back in, you know, World War I, it was the bingo bowl approach, where they had a whole bunch of letters, A through Z, in a big ball that rolled around, and the cage spit one out, and they wrote this down on a pad of paper - which is why it's called a one-time pad - and then they put that ball back in, waited a minute, pulled the next one out. So they ended up with a pad of paper with letters A through Z, really, really, really random. Then they mixed the message that they wanted to send with this pad. And in the case of mixing, for example, you would take the letter you wanted to send, you would look at the first spot on the pad, and it would be A through Z. Well, that told you how far along in the alphabet to shift the letter you wanted to send sort of like forward. And so that would convert your letter A through Z to a different alphabetic letter A through Z, having sort of rotated it forward in the alphabet by the amount specified on the pad. Well, clearly that would create a completely scrambled message. What's amazing is, it's impossible to decrypt it. There is not enough information contained in that message...

Leo: Well, a short message. If you had a long message, eventually you'd see a pattern; right?

Steve: No. No.

Leo: Oh, because you keep reusing - you keep changing it.

Steve: Yes. Every...

Leo: You left out a key part.

Steve: You change for every single letter.

Leo: Ah ha.

Steve: For the second letter, you use the second position in your one-time pad.

Leo: Got it.

Steve: The third letter, the third position.

Leo: So there are no repeats.

Steve: And you never reuse your one-time pad ever, ever, ever. Now, it turns out that some of our foreign adversaries also had the idea of a one-time pad. They made the mistake of reusing it.

Leo: Right. And that's how you can crack it.

Steve: And that's all it took to break their encoding because reusing it and comparing these encrypted messages was, essentially, a huge mistake. But so the idea is, when you receive this message, if you have the same one-time pad - and that was the problem with this approach was that, once this was generated, then the recipient had to have an identical copy of this pad. But, for example, if you were a submarine operator, before you left port you'd get a whole suitcase full of these one-time pad sheets. And then that's what your decryption officer would use in order to decrypt these messages. And, once used, that pad was destroyed, and it would never be used again. That's an unbreakable cryptography. I mean, truly unbreakable.

Leo: Now, the reason - just as a side note, the reason computers are not good at random numbers is because they use an algorithm, which inevitably repeats.

Steve: Well, yes. Anything...

Leo: So they're called "pseudorandom numbers." They're not really random.

Steve: Yes, exactly. And, in fact, a computer just can't generate anything random. It's a deterministic math machine that is always going to go from one place to another. However...

Leo: There's not enough chaos.

Steve: Yes. And, in fact, at Sun Computer they have photocells aimed at lava lamps.

Leo: Which are random.

Steve: I'm not kidding.

Leo: They are chaotic.

Steve: They use lava lamps to generate cryptographically strong random numbers.

Leo: I love that.

Steve: Because it's just - it's like weather patterns. I mean, it is...

Leo: It's chaotic.

Steve: ...pure chaotic physics, and it is nondeterministic. Now, computers can do a very good job with generating random numbers. And that's what this RC4 algorithm does. It is an extremely good pseudorandom number generator. The idea is you give it a key, and that's the encryption key that WEP uses. And using that key it scrambles its initial condition in a pattern based on the key. From that point on it generates very good random numbers. Now, it then uses this stream of random numbers to, in the same way as a one-time pad, to encrypt any communication going between endpoints. The access point has the same key. It uses this string of random numbers to perform the encryption. And then the recipient has the same key. It's why it's called a "preshared key," or PSK. It uses the same key with its RC4 algorithm to generate an identical stream of these pseudorandom numbers, which it then essentially mixes again in order to restore the original message.

Well, it's a good idea except it was used badly. For example, there was, in the initial implementation, an access point would authenticate someone who wanted to connect with it by sending it a - it would just make up some message of any sort. And it would send it to somebody who wanted to connect. The endpoint that wanted to connect would use its key to encrypt that message - whatever it was, it could just be randomness - and send it back. The access point would then decrypt it and compare it with the message it sent. Okay, now, from an engineering standpoint that sounds like, you know, a secure thing because that was a way for the machine that wanted to connect to prove that it had the key, because only if it had the key would it be able to encrypt what the access point sent properly. So that when the access point decrypted it, it would compare properly to what was originally sent. What they forgot was that somebody sniffing would see the in-the-clear text go to the end that wanted to authenticate itself and would see the encrypted response. Well, since it had the in-the-clear text and the response, it had everything it needed to decrypt, basically to decrypt the encryption and determine trivially what the pseudorandom sequence was that the shared key was generating.

Leo: So in order to decrypt WEP, all you need is enough information.

Steve: Well, and in the case of this horrible authentication protocol - which, by the way, has since been removed because it was so bad - you literally just did what's called an "Exclusive OR," an "EXOR," of the encrypted message and the plain text, the unencrypted message. And what you got out was the stream of pseudorandom numbers that...

Leo: But how do you get the unencrypted message, though?

Steve: Because that's what the access point sent initially...

Leo: Oh, to say hello.

Steve: ...to tell the endpoint to encrypt.

Leo: Oh.

Steve: Was just amazingly dumb.

Leo: So you really only have to get a little data, and you can see the whole - you can get the key, and you're done.

Steve: Well, what that meant was that then, when the eavesdropper wanted to authenticate, he would say, "Hi there, authenticate me." Well, the access point would send a different test jumble to him. He didn't have to have the key because he already figured out what the pseudorandom stream was that resulted from the key. So he just used that to encrypt a message and sent it back, and it was a perfect match.

Leo: And so he's on.

Steve: And so he's on. Now, that's not the same as being able to communicate from there on. But it turns out that, I mean, that's typical of the mistakes that were made. WEP, the WEP technology, is so badly broken that, given about an hour, it's possible to crack it for sure. Sometimes you crack it sooner; sometimes it takes a little bit longer. There are newer attacks which are able to stimulate the access point to generate much more traffic than it normally would in order to get it to give more samples of its use of the key, which then, using any freely downloadable software - I mean, there's like 10 or 15 different WEP decryption packages now, and people are spitting them out just because it's sort of fun sport.

Leo: So if you're - why, you know, didn't these engineers realize the flaw here?

Steve: No.

Leo: And why not?

Steve: The other thing, for example, is - I mean, it's just - the more you read about this, and I've studied this extensively, it's like mistake after mistake after mistake. It turns out that, because they knew they couldn't use exactly the same key over and over and over because that would generate exactly the same pseudorandom sequence used for encryption, what they did was they said, okay, we're going to have a 24-bit counter on the front and 104-bit encryption code. That's where this 104 comes from. Some people have seen a 40-bit key...

Leo: Right.

Steve: ...or a 104-bit key. Well, if you add 24 to 40, you get 64, which is one of our favorite binary lengths. If you add 24 to 104, you get 128, which is another one of our nice, you know, binary lengths, 128 bits. That's where this 104 comes from, is it's 128 bits minus 24. So they put a counter on the front of the key, and every time a message is used, the access point sends the counter and then uses the rest of the 104 bits with the counter to encrypt the message. The problem is, it turns out that RC4 has weak keys, that is, some percentage of keys don't do a good job of prescrambling its initial state, so that it ends up not generating good random numbers. So every so often, just in the normal use of traffic going over WEP, you know, every access point, every WEP-based device will encrypt with a bad key. Since the receiver has to have that 24 bits to know which key was used, that's sent in the clear. So anything sniffing is able to say, oh, there's a bad key, because now bad keys are well known. So anyway, the bottom line is WEP is really, really, really badly broken.

Leo: And if they had just asked, any security expert would have immediately seen the problem and said no, you can't do it that way.

Steve: Oh, exactly. I mean, anyone who understood that RC4 was a good pseudorandom number generator, but you can't trust it in this application for many reasons. For example, if you just throw away the first 256 bytes that it generates, after a while it gets going, and it does a good job. But right off the bat, what it's spitting out is not very random.

Leo: Oh.

Steve: Well, it turns out that's the header of the packets. And headers have a very well-defined format. Which means knowing what the headers are is something, you know, any TCP or IP engineer has. So knowing what it is, you can subtract that from the encrypted message and get the random bytes back. I mean, it's just horrible.

Leo: So really now what we've learned is - and we knew this before - WEP doesn't work. Now we know why WEP doesn't work. That's one of the forms of encryption on wireless access points.

Steve: Well, it's the original encryption. In any system which supports wireless encryption, WEP will be there, and sort of maybe encouraged - people tend to use it because they may have an older laptop or an older wireless adapter that only supports WEP.

Leo: Right.

Steve: Now, there is - and we're going to talk about next week, you know, how to really lock down a wireless system. There is a free WPA client running around, and XP supports WPA. And...

Leo: As does OSX. So any modern operating system you'll be able to use WPA. And maybe a firmware upgrade on your router will make it support WPA.

Steve: Yes, that's very much - that's very often the case is that the original firmware - now, the good news is that WPA is extremely good because WEP was extremely bad.

Leo: We learned.

Steve: That is what happened, is WEP was so badly broken and was such an embarrassment to the 802.11 guys, the folks that were doing this, was that this time, for round two, serious security oversight was given.

Leo: Right, right.

Steve: And the new protocols, TKIP, which was deliberately designed to be retrofittable into older hardware. So with this background now, next week we're going to talk about what you do to really be secure with wireless, and how and why that really works in a very secure fashion.

Leo: And you can no longer live in a fool's paradise, thinking that you're secure because you've got WEP or MAC address filtering or SSID hiding. None of those do anything at all.

Steve: Yeah. MAC address filtering is good because it will prevent casual, inadvertent misuse of your network.

Leo: As will WEP.

Steve: Well, yes. And, in fact, you certainly, I mean, WEP is better than nothing. And also, if you change your WEP key often, it's normally the case, for example, it used to be that a busy access point would run through all of its keys in about seven hours. Now it turns out you can stimulate an access point to just pour these keys out and make it much more, you know, basically bring the average cracking time down to about an hour.

Leo: So we'd have to change our keys every hour to be safe?

Steve: Yeah, well, and the good news is that's what TKIP does.

Leo: Ah.

Steve: It's a Temporal Key Integrity Protocol that keeps the keys changing. And it never actually uses the master keys in the transfer of the packets. That's the other mistake that WEP made is this preshared key, this key that each endpoint has, is what's being used to do the encryption. So once you have that, you've got literally the keys to the kingdom.

Leo: Right.

Steve: With WPA, the keys are used to derive other keys, which are then used for encryption. It just - it's really so much better.

Leo: We'll save all this for next time. Maybe you'll explain to me WPA, WPA-PSK, WPA-TKIP, and all the other little acronyms. I have to say one thing: WPA is much easier to use than WEP because you don't have to do these long hexadecimal strings for your passkey. You can use regular passwords. So...

Steve: Right.

Leo: ...by itself, that's a good reason to shift.

Steve: And by the way, there are attacks. I'll just say, if we're moving people from WEP over to WPA, take the time when you're reconfiguring to come up with a really good, long passphrase because WPA is prone to dictionary attacks, which we've talked about before with passwords. So in the same way that you want to use a really good, strong password, meaning numbers and letters and things that are not in a dictionary, even WPA can be prone to dictionary-style attacks.

Leo: Steve Gibson, we've done it again, explaining the lack of security in wireless. And I think, you know, I have to say, every place I've gone, and I can think of some places, including TechTV, has used MAC address filtering. To learn that it's useless is just kind of a shocker for me, frankly.

Steve: And again, you know, as we've often said, a false sense of security...

Leo: No kidding.

Steve: ...is worse than none at all.

Leo: Yeah.

Steve: People thinking that MAC address filtering is going to really protect them and, like, be better than WEP, for example, is...

Leo: And it's a pain to implement because you have to figure out what your MAC address is and then take it to the, you know, priest, the guy who holds the keys, and say here it is, please, sir, may I have access, and it's doing nothing.

Steve: Nothing.

Leo: I love it. If you want to take this information to your boss or your IT supervisor and explain to him why what he's doing isn't making a hill of bean's difference, go to GRC.com/securitynow.htm, and all of this will be explained in detail. There's also a lo-fi, 16KB version of this for people who don't have the bandwidth or the space to store a larger file, as well as transcripts for those bosses who can't actually figure out how to listen to a podcast.

We want to thank Jamie Diamond, our high school sophomore, for our opening theme, and Mark Blasco for our closing theme. And of course the great folks at AOL Radio who broadcast Security Now! on their podcast channel, but also provide us the bandwidth for download at AOLmusic.com. We appreciate the support.

Steve Gibson, thanks for joining us. We'll talk next week about really, truly, for once and for all, locking down wireless access.

Steve: Absolutely.