SECURITY NOW!

Transcript of Episode #89

Even More Badly Broken WEP

Description: Steve and Leo review the operation of wireless network security and discuss in detail the operation of the latest attack on the increasingly insecure WEP encryption system. This new technique allows any WEP-protected WiFi network's secret cryptographic key to be discovered in less than 60 seconds.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-089.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-089-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 89 for April 26, 2007: WEP Insecurity.

Time to gather together to talk about security, something very important today in computing and the Internet. And of course there is no one I'd rather talk to about security than my trusted friend, Steve Gibson of GRC.com, the man who's done more to secure individuals, I think, than anybody else. Have you hit 50 million yet on ShieldsUP?

Steve Gibson: I just looked at it this morning, as a matter of fact, Leo. We're at 49.2 million uses of ShieldsUP. So, yes, we're approaching – that's going to be really neat, to actually cross the 50 million uses of ShieldsUP boundary.

Leo: And as Steve will say, but I want to reiterate this, that if you hit it, like, three times in the same hour, that's one. That counts as one. Steve's talking about these are kind of unique hits at way different times and so forth. This is people who are actually using it. And it's really amazing. 50 million.

Steve: It's actually, it's a good count because I keep track of in a list the IPs of the most recent 4,000 – actually, you know, 4K of course, 4096, being a programmer. And if the same IP is still in the list, I move it to the front of the list and don't count it again. So, and with about 25,000 people per day, you know, so it's going to last maybe four hours. And so if someone comes back after that length of time, I think it's reasonable to count them again.

Leo: That’s a new test. Yeah, they’ve done something, and they’ve changed their system, and they’re trying it again.

Steve: Right. But if they’re poking around at the site, I only count them once. So, you know, I’m really happy with that number. And in fact someone in the U.K. just yesterday, I got a link, I saw it posted in our newsgroups, has done a – he’s like an IT guy with one of the major U.K. magazines – did a user’s guide to ShieldsUP because he was tired of answering the same questions over and over and over.

Leo: Hey, that’s handy.

Steve: So, yeah, it’s very nice.

Leo: Although I have to say the online help in ShieldsUP is so good that I almost always refer people, I just say, hey, read – once you get your results, read what Steve says about it because it’s everything you’d ever want to know about port checking and all that stuff.

Steve: Right.

Leo: I mean, it’s all in there. Do we have any errata, addendum, something...

Steve: No, we don’t have any errata. We did a Q&A last week, so I didn’t have any errata from that. But I do have a really fun testimonial that refers to the testimonials that we’ve received in the past from SpinRite from a Security Now! listener that I want to share with people because this is the kind of story that really makes me feel neat about SpinRite.

Leo: You get these stories every day, it seems like.

Steve: Well, yeah. Yes.

Leo: That’s kind of neat. I mean, that’s really neat. It must make you feel good.

Steve: I have lots of them. And it is neat. This is from a guy named Duncan Smith, who is one of our listeners. And he says, “Dear Steve and all at GRC, I’ve listened to so many of these testimonials on Security Now! and now have reason to join the ranks of ecstatic customers with yet another ‘SpinRite saves the day’ story. My mother” – and I think he must be English from some of the idioms he uses. You’ll hear this in what he says. “My mother retired several years ago and enrolled in part-time classes for a horticultural degree. For the past six years she’s been working away, and for the last nine months has been undertaking her final dissertation. To celebrate the recent completion (but not submission)” – uh-oh – “of the dissertation...”

Leo: Uh-oh is right.

Steve: Nine months of work on her dissertation. You know where this is going. So he says, “To celebrate the recent completion of the dissertation and my father's recent retirement, they embarked on an eight-week trip of a lifetime to New Zealand. Last night I got the dreaded phone call. Her PC was stuck in a never-ending loop of restarts, never making it into Windows. The hard drive was also making 'unusual noises,' and her local PC store, as well as a computer-savvy neighbor, had suggested the hard drive was beyond repair and all was lost. She had no backup, and the PC contained all her degree work and all their digital pictures from that holiday and several years of other holidays.

Leo: As if the thesis weren't enough.

Steve: Yeah, it's all the photos. So...

Leo: You know, it still gets me that people are not backing up, just drives me crazy.

Steve: It's just, you know, it's because, of course, you know, I've lived with SpinRite and these kinds of problems and solutions now for, I think, like, 19 years, 20 years. It's just that the computer works today, and they turn it on tomorrow, and it works. And they figure, well, it'll work day after tomorrow. I mean, it's just, you know, it lulls, it truly lulls into sort of a false sense of security. And the other thing is, I think, when the computer is new, it contains nothing of value that isn't obviously immediately replaceable. And over time that value that it stores grows slowly. And so there's never really an event where it's like, oh, now I really need to start backing up. It just creeps up on you, and suddenly...

Leo: There's no warning. There's no warning.

Steve: Yeah. Anyway, so he finishes, he says, "I've been considering purchasing SpinRite for a while, so I had no hesitation in grabbing a copy before driving over to get the PC. Setting it off, I went to bed, hoping the testimonials I have heard were as trustworthy as the advice you give on Security Now!. I awoke this morning to find SpinRite had finished its business, restarted the PC, and it booted first time. One hour later, all documents were backed up, and I am seriously in my parents' good books," as he puts it.

Leo: If God or Steve Gibson gives you a second chance, take it.

Steve: So he said, "I'm seriously in my parents' good books. Perfect timing, as I have a house move coming up, and my wife and I need some extra babysitting for my daughter."

Leo: Now there's a testimonial.

Steve: And he said, "Many thanks for the great product and for all the work you put into Security Now!."

Leo: That's the headline.

Steve: Signed Duncan Smith.

Leo: "SpinRite Gives You Babysitting Time." That's the headline. I like it. I like it. That's hysterical. You know, it reminded me with a chill kind of what happened to my wife on her master's thesis. She didn't have Security Now!. It was lost...

Steve: She didn't have SpinRite.

Leo: I mean SpinRite. She didn't have Security Now! either; but she didn't have SpinRite, which is more to the point. It was lost, and she actually had to take that whole year over again. So it can go really badly.

Steve: Oh, no kidding?

Leo: Yeah.

Steve: Wow.

Leo: Yeah. She got an incomplete for that and had to do it all over again. Ooh, I know, it sends a chill just thinking about it. She did it. She got her degree, and she got her license. But boy, I mean, that's – talk about dedication after that. Which is maybe why she never uses computers now, come to think of it.

Steve: Exactly. Exactly. Well, and it takes one event like that, and then you...

Leo: Then you back up.

Steve: You realize, okay, I really have to do backups, yeah.

Leo: Yeah. All right. Let's talk about...

Steve: You wanted to talk about eBooks a little bit; right?

Leo: Well, you know, it's funny, we've become the eBook guys, haven't we.

Steve: I've been an eBook guy for a long time.

Leo: And I could never go with it because you were reading them on these little tiny Palms.

Steve: Right.

Leo: So you and I both bought a Sony eReader, and we've been spending a lot of time talking about it. Don't worry, folks, we're going to get right to WEP in a second. But we've been getting a lot of great email from people suggesting other places to get free eBooks, websites and so forth. There really is, even for the Sony, there's a lot of choices out there. So I'm very pleased.

Steve: Yeah. And I did want to mention your reaction so far to "Gibraltar Earth."

Leo: Oh, I love it. You know, I'm always a little nervous when I read stuff that hasn't gone through a regular publisher and isn't on the bookstands and stuff. And I don't know why. I shouldn't be. This is great. This is great. And Michael McCollum deserves all praise. I can't wait to read – I bought the Antares Trilogy and the second, "Gibraltar Sun." Got halfway through "Gibraltar Earth," it's fascinating. I can see where it's going, too. It's exciting.

Steve: Well, and "Sun" is, yes, "Sun" is the second in that trilogy.

Leo: Oh, it's a trilogy. Oh, good.

Steve: Actually, yes. I finished book two, and I wrote to Michael. And I said, you know, you have built such a cool universe, please don't be in a hurry to finish it. I mean, I'd like him to have two more books. But he's like, uh, I don't know if I've got two more books...

Leo: That's kind of how I felt about "Fallen Dragon" was don't, you know, gosh, you've created something here. And we all want to go back there, so don't stop.

Steve: And all I can say, Leo, is you have so much good reading ahead of you.

Leo: Oh, good. And, you know, this is now – so I've read over a thousand pages on the Sony eBook Reader, and I'm very comfortable with it now. One thing, though, I've only had – it's only gone down through the charges twice, which is more, you know, faster than it said it would, I have to say.

Steve: Have you listened to any music?

Leo: No, it's just reading. And it's not charging. I'm thinking maybe the first time it didn't fully charge because it's – I don't know if there's something wrong with my charger, but it doesn't seem to be – I'm going to leave it overnight tonight and see what happens. But it doesn't seem to be charging up. Have you had trouble with the charger?

Steve: Yes, I...

Leo: The red light's coming on.

Steve: Yes, I've had the same experience. Again, this is, you know, first generation. And this is unusual for Sony to have a problem like this. But what I noticed is I'll plug the book into its charger, red light comes on, red light goes off.

Leo: Yes.

Steve: It's still not charged.

Leo: Right, that's what happened.

Steve: And if you just do it again, it, like, kicks it a little bit more.

Leo: Okay, all right. It's good to know, yeah. Although I've been reading with one bar for, like, five days now. I mean, you know. So maybe that's why I had to charge it again is that I didn't really fully charge it the second time around. That's probably what happened.

Steve: I think you probably – yes, exactly, is it probably didn't work. Now, it happens from an electrochemical standpoint that lithium ion batteries are a little tricky to charge because the charge stop point is set by the terminal voltage on the battery. And that can be tricky to get right. That is, it's possible for it to, like, get a little false trip now...

Leo: That's probably what's happening, huh.

Steve: Yeah. Obviously this is a problem everybody else has solved. And who knows, maybe it's because it's got Linux in there, and it's missed an interrupt or something. But it's certainly the case that if you try a couple times, you'll end up getting a charge.

Leo: Okay, yeah. I have to say the ability to carry it with me everywhere at such a small package and have so many books in there is really, really great.

Steve: Yeah, I love it.

Leo: And thanks to Michael McCollum for going to the extra effort to make it work on the Sony Reader. Thank you, Michael. I appreciate it. It's really great. Highly recommended. Scifi-az.com.

Steve: And for what it's worth I've had other feedback from people who are similarly loving his books.

Leo: Is he published? Does he have other novels that are published? Are these published? Or is he all self-published?

Steve: Well, he's got a publisher. For a long time he was using a regular publishing channel. But he ended up getting the rights back, I don't know if they expired or whatever. But he literally now, I mean, you can buy his books in paperback. And he's got a complete printing system, a whole binding system. So the books that you buy from him, he has printed. And I think, as far as I know, they are professionally, you know, put together. So it's cool because he's getting a hundred percent of the revenue from that, less the direct cost of printing books, which, you know...

Leo: Right. And even more from the eBooks.

Steve: Exactly.

Leo: And he deserves it. They're really good books.

Steve: I can't wait for the third, or fourth, maybe, in the Gibraltar series. And I can't tell you, Leo, I mean, the Antares stuff is even better, I think.

Leo: Oh, really. Oh, I can't wait. I think the other – we'll say one more thing, and then, honest, we're going to talk about security. What's exciting about this is these readers make it possible for anybody to be an author because the cost of publishing is so low. And if, as these readers proliferate, as I hope they will, you'll have a large universe of readers for virtually no cost, the cost of bandwidth alone.

Steve: Exactly. And of course the Internet is the other enabling factor. It's going to be cool.

Leo: It's exciting. I love these times, I must say. Now, the Internet is also a scary, dark, forbidding place, with evil men desperate to get into your system. No, not really. But anyway, sometimes it helps to think of it that way in terms of security, and that's what's going on with WEP right now. Fill us in on this here.

Steve: Well, we haven't talked about WEP for a long time. Back on Episode 11, which was, what, 78 episodes ago, back in October of '05 was our coverage of – the actual title was "Bad WiFi Security." And that was really the last time, although we've mentioned it in passing many times since, but it was the last time we really gave strong coverage to the problems with the original encryption for WiFi, which was called WEP, which is an acronym, WEP, which stands for Wired Equivalent Privacy. And the goal of WEP was, and the reason they named it Wired Equivalent Privacy, was they wanted to create a level of privacy for radio WiFi that they felt was as strong as if the communication was wired, as if it was wired equivalent.

Well, they really fell far short of that. And a couple weeks ago a new group, three German guys at a technical university in Germany, published a paper where they demonstrated how they had figured out that they could crack WEP, that is to say, determine the encryption key being used in under a minute.

Leo: Whoa, that's not good. How long did it take before?

Steve: Well, it took much longer. In fact, it took on the order of five million packets captured...

Leo: That was the key, you had to have a certain amount of data before you could crack it.

Steve: Exactly. These guys have brought that down to about 40,000 packets from five million.

Leo: Two orders of magnitude, that's quite a bit faster.

Steve: It's a huge gain. So, now, this is still significant. You know, people might be saying, uh, yeah, but, you know, we all have WPA now so who cares. Well, the fact is that the demographics show that no encryption is being used on 25 percent of wireless networks; WEP is still in use in half of wireless networks; and the good, virtually uncrackable WPA encryption is only in use in about a quarter of wireless networks. Which is to say that the fact is, 75 percent of wireless networks today either have no encryption or WEP encryption. And only 25 percent are essentially uncrackable. And as we've said many times, those WPA networks, that is to say, WiFi Protected Access networks, they are only as good as the quality of the password because their weakness is brute-force cracking of the password. WEP's weakness is far more extreme. So to paint the picture, what this means, for example, is if you were using a hotspot where you were using WEP encryption, as many do because it's – because it was the original encryption built into WiFi, you always have WEP.

Leo: It's kind of the default, the fallback, the last resort.

Steve: Exactly. And in many cases, it's what is, like, first on the menu. It's the one that the system will choose for you. I mean, and a perfect example of this, Leo, is back when we were originally telling people, please please please do not use WEP, use WPA, we got a lot of email from people saying, I would love to use WPA, but my, you know, my wazzagazza doesn't support it. Or, you know, my TiVo won't support it, or my this or that. I mean, there were, like, all these problems with people trying to use WPA. I mean, there are even people who have now dual WiFi, one with WPA and one with WEP, where like they use WEP with their TiVo because they really don't need encryption, but they'd like to keep their neighbors from using their WiFi, and so you could argue that WEP – well, actually, until a couple weeks ago, WEP was probably good enough for keeping your neighbors off of your network. Now it really isn't any longer.

Leo: Well, is this fairly easy to do? I mean, is it just a program you download off the Internet and it does it, or do you...

Steve: Yes.

Leo: Oh, boy.

Steve: Proof-of-concept code is now posted on the Internet.

Leo: Which means it'll be in Cain & Abel or one of these tools any minute now.

Steve: Yes. Well, it is in the Aircrack suite, which...

Leo: Oh, okay. Well, that was fast.

Steve: Exactly, it took no time. And the reason this is significant is it's one thing to say, yes, I can get into WEP with five million packets. Well, five million packets, that's a lot of packets.

Leo: You have to sit out on the curb a long time, and you'll be noticed.

Steve: You need to bring your sleeping bag if you're going to do that. Here it's 40,000.

Leo: It's a thousand times faster. I mean...

Steve: No, 40,000 packets you could say, okay, well, that's still a lot of traffic. Well, let's walk through how this is done because what I love about this and about talking about this specifically is that it brings out many of the foundations we've laid before about the way crypto stuff works. In the first case you need lots of packets. And you need not only lots of packets, but you need packets that you know something about. Well, the way that Ethernet is glued together is with what's called ARP, the Address Resolution Protocol. And what ARP does – and we've discussed this in the past, so if anyone wants to go back and listen to an episode all about ARP, in fact where we talked about how ARP can be abused in order to create man-in-the-middle attacks – it's one of the reasons, for example, in a hotel setting you do not just want to plug yourself into the hotel network because it's trivial for someone to intercept your traffic due to ARP spoofing.

Anyway, the way ARP functions is anybody on the Ethernet sends out a broadcast to the entire network saying I need the MAC address associated with this IP. What ARP does, and the reason it's called Address Resolution Protocol, it resolves the relationship between IP addresses and MAC addresses on an Ethernet LAN. All Ethernet LAN endpoints, that is, all NICs, Network Interface Cards, they actually are addressable by their MAC address because the IP protocol is just one of many protocols that they could support. You could be Token Ring, you could be any of a number, for example, IPX, SPX, the old Novell protocol, all these things run on Ethernet. So the IP protocol needs a way to figure out which adapter card on the Ethernet we want to send our data to.

So a station, whether you're wired or wireless, will broadcast to everybody, who's the MAC address for this IP, for example, the gateway IP, in order to send the traffic to the gateway in order for it to get routed out of the LAN onto the Internet. Everybody receives this request. And the one proper, presuming there's no ARP spoofing going on, the one proper adapter that has that IP responds, saying I'm the guy with this MAC address. Okay. So all you have to do in order to generate a lot of packets is broadcast this request all the time, and you'll get a whole bunch of responses.

Leo: Ah. So you can stimulate it, in effect.

Steve: Exactly. You can tickle the network in order to cause it to – just like, you know, flood it with this data. Now, what's very cool about ARP – well, cool except that this is huge leverage for the attackers – is that the first 12 bytes is never – it never changes. The first 12 bytes of an ARP request happen to be AAAA, 03, then 000, then a 08 and 06, a 0, 01, 08, 00, 06, 04, 0001. Those are the first 12 bytes of an ARP request. The ARP reply has exactly the same bytes except the very last byte is a 02, which actually is the flag saying I'm a request or I'm a reply.

So now what we’ve got is we are able to watch ARP traffic on the network. And in fact, one of the many things broken about WEP is that there’s no what’s called replay attack – I was blanking there for a second. There’s no replay prohibition, meaning that you can – we’re just listening to the network. Now, we can’t inject a packet because we don’t know the encryption key. So what we’re able to do is we’re able to see packets that other people are generating, and they will occasionally generate ARP packets because this is something that – essentially ARP times out, and then you need to renew your knowledge. So when we see an ARP packet, we can capture it and then send as many more of that packet as we want in order to generate responses. So we’re using the same packet we saw once, and WEP doesn’t prevent you from doing what’s called a “replay attack,” which is to say replaying the same packet over and over and having it validated. WPA, the good encryption, never allows the reuse of an entire packet. So it has replay prevention, attack prevention; WEP does not. So we capture an ARP packet, and we’re able to identify it by length and send it back into the network in order to generate lots of traffic.

Okay. So now we have a whole bunch of these packets. Well, if we remember the way WPA works – I’m sorry, not WPA, that’s the good encryption. WEP, the bad encryption, WEP, the way it works is it uses a pseudorandom number generator, an encryption system, a pseudorandom stream generator called RC4. RC4 is initialized with an encryption key. Typically it’s either 64 bits or 128. 128 is the large size key, obviously, and provides substantially more protection than the 64-bit key. So 128 is what this attack is cracking, and certainly that’s what anybody who didn’t have some real reason to have weak security, you know, if you’re using WEP at all, you would certainly expect it to be cranked up all the way.

So this 128-bit key is broken into two pieces. There’s a 24-bit sort of front piece and a 104-bit back piece, so 24 plus 104 and you get 128, which is where the total key length comes from. Well, this 24-bit front piece is called the “initialization vector,” or IV for short. What happens is most adapters just use a counter to count this initialization vector upwards. Thus you have a counter on the front of the other 104 bits that are not changing, giving you an always-changing 128-bit key. Unfortunately, only the front of it changes, not the whole thing.

So what happens is, the way RC4 functions is this 128-bit key is used to generate a pseudorandom stream of bytes. Those bytes are XORed with the data. And we talked about XOR back when we were talking in detail about encryption and decryption. The idea is, if you have a string of randomness, and you XOR your so-called plain text, or unencrypted data, with this randomness, what you get back out is random. And if you are truly XORing with randomness, and this is what’s so cool about this, is there’s no way to decrypt that. If you mix plain text with something truly random, what you get back is as random as the original random stuff, even though it’s been modified by the unencrypted data, by the plain text. And what’s neat about XOR is that it’s easily reversible. That is, you re-XOR the encrypted text with the same randomness, and what falls out is the so-called plain text, that is, it decrypts.

Well, that’s cool, except it’s a problem if you ever use the same random data twice. That is, if what you’re XORing with is not totally random, not truly high-quality random data, then you’ve got problems. And this is the main weakness with the Wired Equivalent Privacy approach. Since we know the first 12 bytes of our ARP packets, all we have to do is XOR those first 12 bytes that we see in the air passing by on WiFi. We XOR that encrypted data with what we know is the first 12 bytes of an ARP request or reply. And what we get back is the first 12 bytes of pseudorandom data.

Leo: Oops.

Steve: Yes. Yes. Yes. And so as we get all these packets, we take the packet, XOR the first 12 bytes, and we capture the first 12 bytes of pseudorandom data for that corresponding key. Now, in the front of the packet is this IV, the initialization vector, is the unencrypted 24 bits that is changing each time. That has to be unencrypted and on the front of the packet because the receiver has to have that in order to add it to the secret 104 bits in order to make the 128-bit key in order to generate the same pseudorandom stream of data from the RC4 cipher in order to XOR the packet's contents.

So we're able to stimulate the network to flood us with ARP replies. We capture the packets, XOR the first 12 bytes, and save the 24-bit IV and the first 12 bytes that we know is generated by the RC4 algorithm. Now, all of that's been done before. The prior approach for cracking this, the thing that needed the five million packets, it was an approach where it required that many because it was error-prone. It also required that you were only able to essentially crack the key from the first byte, then the second byte, then the third byte. That is to say, in byte sequence. And if you made any mistakes in guessing, because these are all sort of statistical processes, if you made a mistake in guessing, and you realized, wait a minute, this doesn't seem to be working, you have to completely backtrack and essentially start over again.

What these guys did in the paper that they published a couple weeks ago was they used a different approach, sort of based on the first one, but using a different style of statistical checking which allows them to determine individual bytes of the key with no reliance upon previous bytes. And that gives them this tremendous gain factor. In cases where they're not able to absolutely determine what a byte of the key is, they're able to at least determine what it probably is. That is, they may have, for example, five or 10 or even 20 bytes. But that's much better than 256 because of course there are 256 possible combinations of a single byte. So in the worst case what they've done is they've hugely narrowed the number of possible bytes that an individual byte of the key might be, and RC4 is so fast that they can then test all the keys that are possible, even if they can't determine exactly what the key is, in order to verify that they've got the right byte determined.

Leo: So it's a smaller set. It's doable.

Steve: Exactly. It hugely reduces the set because, you know, if you had 256 times 256 times 256 times 256 for, like, for four bytes, that's a huge number. Well, it's four billion, much bigger than 10 times 10 times 10 times 10, which is just 10,000. So it turns out that the speed of RC4 that makes it possible to test guesses so quickly, leveraged with this algorithm that they've come up with that allows them to determine the individual, like the most probable byte, and then second and third and fourth and fifth and sixth probable bytes for each byte in the key, that gives them their leverage. The result of this is that they are able to collect 40,000 packets by stimulating a typical WiFi network in about 53 seconds. Then, in less than three seconds on a medium-speed ThinkPad – they used a 1.7 GHz Pentium M ThinkPad – in less than three seconds they can process the data they collected. And so that brings them to about 56 seconds, and they have a 50 percent chance of having cracked the key in under a minute. If they give themselves two minutes, then their probability increases to 98 percent. So the reason this is significant is that this is going to change – this changes the calculus. As we were saying before, needing five million packets means you have to have a motivation for cracking the network.

Leo: Right. Well, and I would tell people, use WPA; but, if you can't, it's okay to use WEP because it's enough of a barrier to eliminate all but the most determined hacker. Well, that's no longer true.

Steve: Right. In fact, it's almost faster to do this than it is to enter the WEP key for a network that you know. It's like, oh, I'll just turn on...

Leo: If you can't guess the WEP key, just crack it. Can't remember it.

Steve: You know, you type it in wrong. It's like this is faster than dealing with correcting a typo or, like, going into your router configuration or your computer. It's like, forget it, just crack it, it takes a minute now.

Leo: I'm sure there are videos on the 'Net already showing how to use Aircrack to crack WEP in less than a minute.

Steve: Well, and as you might imagine, this news got a lot of attention because, I mean, it really does change the calculus. You could now just open your laptop, run your cracker, and you could imagine that within a month there will be turnkey tools. It's like, don't even bother filling out the WEP form anymore, just crack the key because it only takes 60 seconds.

Leo: Well, I would never do this, but I have to say it's kind of tempting because many is the time I've had access points I could have used if I only knew the WEP key. And, you know, I mean, if you can't get online any other way, I'm sure there are people not as ethical as you and I who would do that.

Steve: Well, from time to time we've made Security Now! predictions, Leo. And a Security Now! prediction would be that in short order we're going to see some tools that are turnkey, easy for anyone to use. And, I mean, it really does change the calculus. So the takeaway message from this is that, if you're using WiFi, and it's not WPA encrypted, you either, A, don't want to use that WiFi network; or you want to make sure that you're providing your own encryption. You're using a VPN, or you're using HTTPS so that essentially your traffic is running through an independent layer of encryption, a so-called, you know, we've talked about tunneling a lot. So, for example, if you're using Gmail, make sure you're https://mail.google.com or Yahoo! or whatever. You want to make sure that you're providing your own encryption because you really, unless you're using WPA, that is, unless the network that you're hooked to is using WPA, WEP just no longer provides virtually any protection.

Leo: In other words, treat a WEP access point as an open access point.

Steve: Yes. There's virtually no difference.

Leo: All right, Steve Gibson. You know, I'm really glad you covered this because it's been all over the place. And as always, I think it's great to get the actual facts. Also I should point out that people talk about WPA being cracked, and it's not the same, is it.

Steve: No, no. In fact, as we said before, WPA, the only known crack for it, because this was designed by real security guys – as we said back in Episode 11, the original encryption, WEP encryption, was designed by engineers. And they had the best of intentions, but it's just embarrassingly riddled with problems. WPA was really designed by crypto people. The one attack – and this is not WPA's fault at all, there's literally nothing you could do about it – the one attack is the so-called brute force attack, where you capture some packets on the network, and then you start using virtually every possible decryption key. Of course you don't want to just start, unless you really have to, with A and then B and then C and then AA and BB and, I mean, you know, AB, AC, and so forth. What you'll do is you'll use a dictionary attack, trying combinations of common words, hoping that the user did something like that. So the only real way to hack into, as far as we know, WPA is by using a brute force attack.

So what you want is a really unguessable password for WPA, something unlikely to be, you know, in anyone's dictionary, just all kinds of random stuff. And of course that's why I created the passwords page of GRC. If you go to GRC.com/passwords, I give you, over a secured encrypted connection, a bunch of raw material. You can use it as is; you can grab some, refresh the page a few times, and then cut and paste to put your own together if you're not comfortable using one that actually came from our server. And the technology that I developed for that guarantees we will never issue the same one twice. So it's impossible for anyone to get that. In fact, I use one directly from that page. And, you know, it's in a little file on a USB dongle that I carry around whenever I want to put another system on my own network because, lord knows, I mean, this thing is just literally gibberish. And I kind of recognize it visually now, but I don't know what it is.

Leo: If you don't know what it is, I think it's pretty hard to guess. If you can't remember it. All right, Steve, we're going to wrap it up. We'll be back next week with more security for you. We encourage you to patronize our fine sponsors. They keep this show afloat, and we thank them for supporting the show. It's really nice to get your emails, to get your donations, and to get the support of sponsors, too. It really makes this all happen. And we thank you all for being so great. What a great audience we've built for this show.

And of course you can catch Steve every week on my radio show because he does a little mini Security Now! on the radio show. So we're trying to get the word out to an even larger audience. And that's on the Premiere Radio Networks on XM Satellite 152, Saturdays and Sundays. You're on at different times, so I don't know what time to say. I just rotate you around so everybody gets to hear.

Steve: Cool.

Leo: Thanks, Steve. We'll talk again...

Copyright (c) 2006 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/