Personal Password Policy

Description: Everyone who uses web-based services such as eBay, Amazon, and Yahoo, needs to authenticate their identity with passwords. Password quality is important since easily guessable passwords can be easily defeated. Leo and I recap a bit from last week's program, then discuss passwords. We suggest an approach that anyone can use to easily create unbreakable passwords.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-004.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-004-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 4 for September 8, 2005: Passwords. Steve Gibson is on the line, our security wizard, the king of security, the guy who coined the term "spyware," of course created ShieldsUP!, which has saved almost 40 million people from themselves.

Steve Gibson: We passed 38 million the other day.

Leo: It's amazing. It's amazing.

Steve: Use of the ShieldsUP!.

Leo: GRC.com, and the author of SpinRite, which is still, to this day, after over a decade, the best hard drive recovery and test solution out there. GRC.com.

Okay. Last week we did this thing on routers. And I don't know about you, but I got a ton of mail on this.

Steve: Well, I did, too; and in fact I want to bring up a few points that readers - or listeners, I guess - wrote back. One guy - who said I could use his name, so he probably wants me to mention him, his name is Jeff McDonald - made the point that, you know, you and I were talking toward the end about the hardware versus the software firewall issue. That is, if we have a NAT router out on the front line, is there really a need for software firewalls on the machines? And, you know, we were talking about the fact that software firewalls still allow you to do per-application control.

Well, Jeff made the point that, well, sure. But if you're going to have a network of computers, then if something nasty got into one computer, then in the same way that we were talking about the Zotob worm in our very first podcast where, you know, somebody brought it from the weekend home into the corporations and then it got loose within the corporations' Intranet, similarly you do want your individual machines protected, each of them behind the NAT router so that, if something nasty got into one of them, it wouldn't as easily spread through all the others.

Leo: Well, that's just a subset of the general issue about software routers, which is, if a beastie gets on your machine somehow, whether it's from somebody bringing a laptop in or you opening an attachment, you don't have a software firewall to protect you.

Steve: Right, right.

Leo: But on the other hand, if it is on your machine, it could turn off the software firewall; whereas, if the bad guy's on somebody else's machine on my network, at least my firewall will protect me.

Steve: Right. And of course, you know, that's always going to be the problem with a software firewall, that the software running in the same computer is vulnerable to anything that's in that computer.

Leo: Yeah.

Steve: Also, we talked about both the Tiny and the Kerio firewalls.

Leo: They're not going to be free much longer.

Steve: Well, exactly. Tiny has been purchased very recently, it turns out, by Computer Associates, you know, CAI. So that's probably going to go away. And it turns out that the Kerio Personal Firewall is still available, but their Server Firewall version is being discontinued at the end of this month, at the end of September 30. So...

Leo: Well, what do we do?

Steve: ...you know, it's really looking like free firewalls are beginning to become pretty scarce.

Leo: Does ZoneAlarm still have a free version?

Steve: ZoneAlarm still does. It suffers from sort of a kitchen sink syndrome. They're trying to be feature complete, that is, to keep up with Symantec, that's just, you know, a huge, bloated firewall. I mean, it does all kinds of things for people. And for many people it's the right solution because it does cookie management and pop-up blocking and all kinds of stuff. But I really like a trimmer sort of application-specific solution, that ZoneAlarm was in the old days.

Leo: Well, to respond to this correspondent's issue, even the Windows Firewall would be sufficient in that case.

Steve: That's really true. And in fact, someone also mentioned that the Windows Firewall in Service Pack 2 does alert the user if a program running in the system wants to create a listening port. That is, it doesn't tell you if it just wants to communicate outwards. But if it was like a trojan or a server or any kind that wants to set up a connection and open a port for listening, even the current Windows Firewall will tell you that that's going on. And you have to give it permission to do so. So that's a good thing.

Leo: So probably, for most people, if you've got a NAT router, turning on the Windows Firewall is adequate protection. Yes?

Steve: I think that that's true, except that you still wouldn't get the notification of some spyware that was phoning home. And that's probably a useful thing to do, even though the spyware could be aware of your firewall and circumvent it in order to get the message out, if it wanted to.

Leo: Right. You don't really have any assurance with a software firewall that you're not compromised.

Steve: Right.

Leo: It just may catch some compromises.

Steve: And then the last point I wanted to make from last week's podcast is an amazing number of people wanted me to talk about or mention SmoothWall, which is a sort of a prepackaged firewall, based on Linux, that includes Linux along with it. It's completely free. It's www.smoothwall.org is the website.

Leo: We have Patrick to thank for that because Patrick Norton was a big SmoothWall fan. Of course, you have to have a dedicated computer to run SmoothWall.

Steve: I was just going to say, it's sort of off on a different branch of our main topic, which was how you could just use either a single NAT router, or even two, in order to create various types of security configurations. But for someone who's more of a hardcore networking guy, who's got, you know, an older machine that is no longer really speedy enough to run Windows and do useful things, especially with, you know, today's media sizes and so forth, if you can stick a few more NIC cards into it, you could definitely take an older PC, give it one interface card for the WAN, one interface card for your LAN, and then a third interface card if you wanted to set up a true DMZ, a true sort of protected separate network, then SmoothWall is a terrific solution for that. You don't need to know Linux. It's got a web browser-based interface, I mean, it's got bells and whistles you can't even imagine. So for a higher end user, it's certainly the case that that would work.

Leo: It's funny, we really touched on a nerve there. I mean, I got so much mail. And it seems like people who for some reason were really offended when you say - when I say I don't recommend a software firewall, I recommend a NAT router instead, I don't want to offend anybody, but that's just my opinion. So, and you think that probably it's not a bad idea to run a software firewall.

Steve: Well, you know, you and I don't.

Leo: We don't.

Steve: But I'm also extremely careful and paying attention to what my machine is doing from moment to moment. But on the other hand, it is because I was beta-testing ZoneAlarm that I first discovered spyware.

Leo: But things have changed since then.

Steve: Yeah.

Leo: I mean, spyware is much more sophisticated than it used to be.

Steve: It is also the case that Microsoft is becoming clearly security conscious. And, as we know, Vista will offer an outbound-blocking, built-in firewall.

Leo: Right. Well, that'll be...

Steve: Which is probably going to end up being the recommendation, as long as they can bolt it down enough so that software isn't able to turn it off and get around it.

Leo: Right. So your recommendation now is what?

Steve: Certainly a NAT router continues to provide very good, I mean, like, perfect protection from external intrusion into the system. And I think that the Kerio Personal Firewall Version 4.2, which is the current one, the free version - not the Server Firewall, which is being discontinued at the end of the month, but the current Personal Firewall - I think that's the best solution for a nice, you know, not heavy, it's very small, it's one of those smaller firewalls around in terms of download size and just lightweightness, and it behaves itself very well.

Leo: And I'm just going to say that in my - because I've had so much experience with people installing ZoneAlarm and having problems, you know, anytime you put system-level software on your machine, you know, some percentage of machines are going to have compatibility issues, slowdowns, crashes, maybe even stop working. I'm just going to say, using that router, if you want a little more extra protection, turn on the Windows Firewall. If you're using XP Service Pack 2, that's a pretty darn good combination.

Steve: I really think that's the case, yes.

Leo: Yeah. All right. Now, let's move on to something that people don't pay enough attention to and probably should: passwords.

Steve: Right. Right. There was an interesting comment made by actually Microsoft's senior program manager for their security policies, a guy named Jesper Johannsen, at a conference a few months ago. He stood up in front of the room and said to everybody that the recommendations most corporations give their employees, if not, like, formal security policy, is wrong. Most companies are now telling their employees, do not write down your passwords because of the problem of, you know, people gone at lunchtime, and someone comes into your cubicle and sees your passwords written down on post-it notes.

Leo: Yeah. People leave their passwords on the monitor.

Steve: Well, of course the classic from so many movies is somebody turning the keyboard upside down, and there's the password written on the underside of the keyboard.

Leo: Why did he say that that was bad advice? That seems like good advice. Don't write it down.

Steve: Well, and what's interesting is that this got picked up, and then a real security guru, Bruce Schneier - who's, you know, counterpane.com, really understands security - is in complete agreement, that passwords should be written down. The point is that, if you don't allow people to write down passwords, they are forced to choose really dumb ones.

Leo: Because they can't remember anything better.

Steve: Because they can't - exactly. They can't remember a complex password which will not be in a dictionary. So if you - the idea is that corporations that are saying "Do not write down your passwords" are inherently forcing people to choose passwords that are easily guessable or prone to dictionary attack; that is to say, by refusing to allow people to write them down, they're having to choose bad passwords. And that's worse than writing them down. The point that Bruce makes, which I think is a very good one, is that, write down your passwords on a small piece of paper and put them where you put your other private pieces of paper, which is to say, in your wallet. He makes the point, and I think it's a good one, that people are already good about protecting written-down information that they know they need to keep private. So don't put it on a post-it note on your monitor, but stick it in your wallet.

Leo: That seems sensible.

Steve: You already don't want people to get your credit cards, and you probably have other private information in your wallet that you don't want people to have access to. And he makes a point that people

are good about protecting that kind of information.

Leo: Is it okay to use a software password wallet that is protected on your system? That's what I do.

Steve: Well, that's really where I wanted this conversation to go. I wanted you and me to sort of open up the topic during this podcast and get people to think about what they can do about passwords. Because normally what happens is, you know, I mean, first of all, anyone who's using Internet services is being confronted with the need to create or enter, you know, to be involved with passwords because to do online services, whether it's eBay or Amazon or whatever, you're having to authenticate yourself on a more or less continuous basis. Most people have never taken some time to create their own policy, their own personal password policy. They're on the web, they're doing something, and suddenly something says, okay, give me a password, create a password. And so, you know, they think of - they just do the first thing that comes to mind, whatever that might be. And so I wanted to take some time to discuss the issue of passwords and cause our listeners to sort of say, okay, wait a minute, this is an important thing. I'm going to, you know, take five minutes and figure out what I want to do about this, rather than continuing not to think about it and not to think that it's important. Because I think it arguably really is an important issue.

Leo: So create a personal password policy, and do it now while you've got the leisure to think about it. I'll tell you what I do. I try to create passwords that are both strong and memorable by using various mnemonics and devices. Let's start off by what is a good password, Steve?

Steve: Well, we know that strong passwords are things that are not in dictionaries. One of the most powerful attacks against passwords is the so-called "dictionary attack." And there are, like, 300MB dictionaries - I'm sorry, 30MB dictionaries that are floating around the 'Net that contain just about every word you can imagine.

Leo: So if you've got a real word, a pet name, a personal name, you're going to be cracked pretty quick.

Steve: Forget it. Exactly. It's like people who use their names in email get spam without ever having told anyone what their name is because their name is in every one of these spam lists. And so the spammers just use dictionaries to drive their spam sending. And so the same sort of approach can be used in cracking a password. You just simply guess what the password is from a list of all known feasible words. And it's amazing how often that's effective.

Leo: How about a nonsense word?

Steve: You absolutely don't want to just use a normal word or your name or your pet name or anything like that.

Leo: Right. How about a nonsense word? Is that acceptable?

Steve: Well, the best passwords are not easily guessable and not obvious. So, for example, a mixture of letters and numbers makes a good password.

Leo: Little punctuation salted in for good measure.

Steve: Or something, for example, maybe a word that you scramble up. One of the most interesting approaches for websites is to come up with sort of a personal hash of the domain name of the website. For example...

Leo: There's a dashboard widget that does this. It's kind of a neat...

Steve: Oh, okay.

Leo: So you have a standard password that you use on all sites, but you hash it with the domain name of the site.

Steve: Well, the problem is that that requires the use of some software.

Leo: Right.

Steve: And, for example, a software password wallet is also a nice approach. The problem is that it's not portable.

Leo: Right.

Steve: And so if you're ever at someone's - at a friend's house, or away from your desk...

Leo: Yeah.

Steve: And the other problem is, of course, that could be stolen, or somebody could - if someone got the master password for that...

Leo: Oh, boy.

Steve: ...then they unlock your password wallet, and they've got all your passwords. What I'm thinking of is imagine a simple algorithm that you can memorize which is a way of, like, mutating the domain where you're visiting in a way that is unique to you. For example, take every other letter from the domain name, or every third letter. Come up with a rule for capitalizing them. Swap some letters around. You know, just sort of make up your own algorithm - and you don't share with anybody else, and don't use anything that I've talked about on the show, of course - and use that to create a password. The beauty is that it'll be unique, it'll not be in a dictionary - unless you don't have a very good algorithm. But once you know what it is, you don't have to remember the password any longer because you can always regenerate it. And wherever you are, you can regenerate it. I mean, it might take a little bit of pencil-and-paper work, depending upon - or maybe it's something that you can sort of type in as you look at the domain name. So, like, you know, reverse the order of certain groups of letters. Change the capitalization in a special way. Maybe take the name and, like, mix in the year of your birth, alternating that with the letters. I mean, you can get creative. But the beauty is, it's your own - basically it's your own password-hashing algorithm that takes the domain, mixes something that's unique to you in, and maybe tack on a couple gibberish characters that that part you don't ever change, but the gibberish is completely made up, you know...

Leo: This is a good technique.

Steve: ...q7z, you know, w or something.

Leo: I like this. So if I'm on nytimes.com, I could, say, intermix my year of birth at every other letter, and then uppercase every third letter, so I'd have n1Y9 and so forth, and that would not be a guessable password.

Steve: Exactly. It's going to create a super-strong password. It's going to be an algorithm, I mean, okay. If two people on the planet had the same algorithm by chance, that's not a problem either.

Leo: No.

Steve: Because the chances are...

Leo: You don't know which two.

Steve: ...you know, because there are so many algorithms, that no one's going to be able to figure out what the algorithm is.

Leo: Right, right.

Steve: So if there was an "algorithm collision," as we would call it in cryptography, that doesn't weaken your use of your passwords; but it does create something that's portable, that - I mean, and you might want to write the rules down. You could imagine writing them down in your wallet in case you ever forget them, and nobody who looked at it would know what that was. They'd go, what the heck is this?

Leo: Especially if you did it a little cryptically, you know. "Alternate third letter with year of birth," I mean, nobody's going to think of that.

Steve: Exactly.

Leo: Now, before we wrap, let me ask you a question, Steve. How do you do your passwords?

Steve: [Laughing] I'm not as good as I should be. I have - always sitting next to me is a Palm Pilot, which is my address book and a list of all of that kind of stuff. It's just my master notepad. And I do have a huge number of passwords that I've used over time. So what'll happen is, if I'm away from my Palm Pilot, I'll have to hope that the website I'm using is patient as I'm running through all the possible passwords that it might be.

Leo: That's what I do, too. It's embarrassing. That's what I do, too.

Steve: [Laughing] Wait. Did I use this one here?

Leo: Yeah.

Steve: Did I use that one there?

Leo: Yeah.

Steve: Which one did I use?

Leo: I have a few what I consider high security passwords, some medium security passwords, and some low security passwords.

Steve: Ah, now, that's another very good point because it's certainly the case that not all things require the same level of protection.

Leo: Right. The New York Times I don't really care if my password's guessed.

Steve: Exactly. One thing you don't want to do, however, something that got me a while ago, I've been a victim of credit card fraud online twice.

Leo: Hmm.

Steve: And the most recent case was that my bank apparently used an online web form that allowed you to change your mailing address, which I think is a really bad thing for the bank to do in the first place.

Leo: Yes.

Steve: Because what happened was that somebody was ordering stuff shipped to Colorado, rather than Southern California. And my bank, you know, a red flag finally went up, they realized something strange was going on, my behavior pattern had changed. And mostly I was now in Colorado, apparently, which never happened.

Leo: Right.

Steve: The point is that, even though my password was different, the bank used mother's maiden name as authentication. Well, somewhere else, on a different site I had used it, not as my password, but as, like, a password reminder kind of thing. And the point is that there are places where it's a common security problem, it's called "repurposing." That is, I didn't use my mother's maiden name as a password; but I did use my mother's maiden name, knowing that it was my mother's maiden name, in order to have a password reminder on another site.

Leo: Right.

Steve: So any employee of that facility would have a list of all the mothers' maiden names of people.

Leo: Yes.

Steve: And if they then went to somewhere else that was actually using the mother's maiden name as the password, you know, you're cracked, basically.

Leo: It's not such a hard thing to find out somebody's mother's maiden name, either, so.

Steve: No. That's probably a good example of the worst possible thing you could use to protect yourself.

Leo: Well, and let's not forget Paris Hilton, who used her dog's name as her password reminder. And of course everybody knew her dog's name and figured that that would probably be what she'd use. So that's a bad choice.

So I think we want to get some feedback, don't we, from people on how they do this, what they recommend, and what works for them, maybe if they use some password software, that kind of thing? Should they go to your site?

Steve: I'm sure we will, and we can certainly start off next week's show by talking about the feedback we get from this.

Leo: That's great.

Steve: But more than anything the message would be, give this some time. Rather than always being in a hurry, needing to come up with a password quickly, take some time now, maybe invent your own cool little algorithm that takes any domain name and turns it into a password that you can use. And again, the beauty of that is, that way you're creating a different password every time, never using the same one twice on different domains, and you're able to recreate that without needing to memorize it.

Leo: I love it. It's your personal portable password policy from Mr. Steve Gibson. GRC.com is the website. Security Now!, it comes out every Thursday. If you want to subscribe, you can go directly to the feed, which is leo.am/podcasts/sn. You can also subscribe on iTunes, PodNova, Odeo, all the usual places. Or just go to GRC.com, where Steve makes available, not only the 64kbps version, but also a lo-fi version for those of you on the dial-up or who just want a smaller file size.

Steve: Oh, and also text and PDF text transcripts of the shows, also.

Leo: I love that. Are people downloading the transcripts?

Steve: Yes. And we're getting a lot of positive feedback. On your first TWiT in the Apple Store last week, I noticed that you did a poll, asking people if they like the 64kbps, if they like the 32kbps or less...

Leo: They all wanted the high quality.

Steve: For what it's worth, we're getting a lot of downloads of the more efficient...

Leo: Interesting.

Steve: ...you know, leaner 16kbps. So it's very popular also with people who are getting this over modem.

Leo: Well, we'll keep doing that. And really it's the content that counts. And that's why, of course, we offer it so many different ways.

Steve: Absolutely.

Leo: Steve, always a pleasure. I'll talk to you next Thursday.

Steve: Thanks, Leo. I look forward to it.

Leo: That's it for Episode 4 of Security Now! with Steve Gibson. Our thanks to AOL Radio at aolmusic.com for providing the bandwidth for Security Now!. If you'd like more information about the topics we discussed, or to give us feedback, visit GRC.com/securitynow.htm. You'll also find transcripts and low-fidelity versions of the same show there. To subscribe, visit the iTunes Music Store, the Podcasts section. Or just download a podcasting program like iPodder X and enter leo.am/podcasts/sn. Of course you can hear Security Now! on AOL Radio in the Podcasting Channel. I'm Leo Laporte. Thanks for joining us.