SECURITY NOW!

Transcript of Episode #272

Firesheep

Description: After catching up with a very busy week of security-related news and events, Steve and Leo celebrate the game-changing creation and release of "Firesheep," an add-on for the Firefox web browser which makes online web session hijacking as easy as it could possibly be. This WILL change the world for the better.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-272.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-272-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 272, recorded October 27, 2010: Firesheep.

It's time for Security Now!, the show that covers your security online. And no man better prepared to do that, I think, than this man here, Steve Gibson. He is the guy in charge at GRC, the Gibson Research Corporation, GRC.com. He's the author of SpinRite, which is a fantastic hard drive utility, a must-have for anybody who has hard drives, but also of a host of free and useful security solutions at GRC.com. And he's been doing this show nigh on, well, we're on our sixth year, almost five-plus years now.

Steve Gibson: Well, I guess no one that you could get who's any better who you could get on short notice. So, yeah. I was available.

Leo: Short notice? We got you five years ago. Hey, Steve. How are you today?

Steve: Great, Leo. We were - I promised last week that we were going to finally, I was going to finally be able to unveil a passion of mine for the last 18 months, the Benchmark, the DNS Benchmark that I have been working on. And it got preempted, as things are wont to do on our podcast when something even more fun and sometimes fantastic comes along, as happened this week.

We need to talk about something which was a surprise to everybody at a security conference in San Diego this last Sunday, that took everyone by surprise, which is being downloaded at a frenetic pace. 300,000 copies of this little Firefox add-on was where the count was earlier this morning when I began putting my final notes together for this. Last time I looked it was at 322,000. So in the last couple hours another 22,000 copies have been downloaded.

This is going to - the reason I'm excited about it, the reason we're talking about it, the reason it's my favorite Firefox add-on ever, is that it's wild, and I think it will finally force change. We've talked so often, I mean, till we're blue in our virtual faces, about the problem with open WiFi and the lack of SSL security and what it means that logon credentials in the form of cookies are hijackable. Well, until now it's been arcane. It's been difficult to do. This thing, anyone can run, and it shows you everyone who's using social networking sites, Web 2.0 stuff, in the same hotspot where you are, and allows you to hijack their session, logging on as them with a single click.

Leo: Wow.

Steve: So, yeah, it's big.

Leo: Wow. That's amazing.

Steve: Yeah, we've got lots to say about it, lots of news and updates, and a great podcast today.

Leo: So let us start, I guess, with our security updates here.

Steve: Yeah. A couple things. Our listeners will probably - our listeners using Firefox may have noticed that their Firefox jumped up to 3.6.11, if they're on the 3.6 train, or 3.5.14. It's interesting, I thought we had announced, because they had announced, that they were going to stop moving 3.5 forward. But they keep doing that. I guess they just haven't had the migration over to 3.6 series that they were hoping for. So they have been continuing to fix 3.5 and moving that forward. This was fixing a bunch of vulnerabilities, 12 in total, five of which were rated critical, remote, that is to say, remote code execution vulnerability. And it affected Firefox, Thunderbird - both the 3.1 and the 3.0 train of Thunderbird - and SeaMonkey. So pretty much across the board that's been fixed.

Now, unfortunately just two days ago they, that is, the Mozilla folks were informed of a new zero-day vulnerability, which we don't often see in Firefox, in Firefox itself. Turns out that there's a mistake in Firefox's implementation of some aspects of JavaScript which were first seen being exploited on the Nobel Peace Prize website. So people just...

Leo: Whoa.

Steve: Yeah. Innocent Firefox users who visited the Nobel Peace Prize website were getting malware installed into their machines if they were using XP. The malware has been analyzed, and it looks like it's specific to the Firefox version. So it figures out what version your Firefox is. And this is because, when you go to the site, the bad guys have installed - probably using some CSS or cross-site scripting, XSS, something, some technology, maybe an SQL injection - they got their JavaScript onto the Nobel Peace Prize website. So when that JavaScript runs, it checks the version of Firefox and then uses that with some version-specific exploits which Mozilla is now aware of, but for which there is as yet, while we're recording this, no fix, to install code on your machine. But it also checks to make sure you're not using Vista or Windows 7, so it looks like it's XP specific.

Not much is known about it right now. The problem is both in 3.5 and 3.6, and actually in 4, the as-yet-unreleased beta of Firefox, although you can't get exploited under 4. What they're in the process of doing is fixing it very quickly. I imagine maybe by the time our listeners hear this there may be a 3.6.12 and 3.5.15. So my announcement of this just-updated Firefox may already be obsolete. Mozilla's own site says the only thing they know to suggest people do is, not surprisingly, either disable JavaScript or use NoScript to run without scripting by default. But again, had you gone to that site and needed scripting, then you would be in trouble if you turned it on.

Now, this is the only place it's been seen. I saw some other reporting saying it is being used at other sites. So, again, NoScript is your friend. Run without scripting if possible. Turn it on only for sites you trust. And with any luck this will get fixed very quickly. I mean, the Mozilla guys have known about it now for a couple days. They know where the problem is. They're fixing the code across their code base. So the 4 version of Firefox will get fixed even though it's not vulnerable to the same attack. So it'll get fixed as part of them fixing their major code base.

RealPlayer we haven't heard about for a long time...

Leo: Because nobody uses it.

Steve: Exactly. And I was going to say, my advice is much as it is with Shockwave, which is less needed. Unless you know, unless you really know you need RealPlayer, because your corporate media is only in .RM format or something, now is a great time to remove it, rather than updating it, unless you know you need it. They have released across-the-board patches for all of their various annoying versions of RealMedia. They've got corporate and executive versions and other stuff.

There are seven remote-code exploits which they patch with this. So you could either, if you know you need RealPlayer, definitely want to update yourself because here's the problem: Even if you're not using it, if you installed it four years ago, and you haven't clicked on any RealMedia since then, it's still in your system, and it can be invoked when you go to a malicious website through JavaScript, which is the method of entry here. So it's the kind of thing where, unless you really need it, it just represents a vulnerability which you don't need to have. So just go to Add/Remove Programs in Windows or over on your Mac, and just get rid of this thing because it's doing nothing for you if you're not actively using it except creating a vulnerability that you could well live without at this point. As you said, Leo, no one is using RealMedia anymore. If I see something that I really want, and it's .RM...

Leo: Which frequently happens with, like, older sites and stuff. And it drives me crazy.

Steve: Too bad. I'm not going to view that, whatever it is, because it's just not worth it. It's a bad viewer. And just a note that Google, very much under the radar as always, has continued to creep Chrome forward. They fixed some more things. We don't know what, but Google moved to v7.0.517.43. So fixing things as they do, with their sort of low-drama, low-disclosure, continuous self-repairing on-the-fly security updating.

Adobe is in the doghouse yet again with a...

Leo: It's hard to believe.

Steve: I know. It's a big surprise.

Leo: How could this happen?

Steve: I think we skipped them last week.

Leo: One week off.

Steve: They got one week off, exactly.

Leo: Geez, Louise.

Steve: They've got a zero-day vulnerability. And the good news is it's in Shockwave Player. Which, again, you probably can live without. Once upon a time, if you were a Windows user who looked under Add/Remove Programs, the naming, that is, the nomenclature they used for describing Flash and Shockwave was confusing. The good news is, they've simplified it. If you look under Add/Remove Programs, it'll just say - the one you want is, and probably can't live without - I mean, I can't live without it even on my iPad, unfortunately, I'm forced to - is Adobe Flash Player 10. That's what you'll see, Adobe Flash Player 10 plug-in and Adobe Flash Player 10 ActiveX or something. That's what you need.

Anything that now says Shockwave is vulnerable to a zero-day problem. There is no update for it. So if you have to have Shockwave, then running with NoScript, again, scripting is the way all of these things get invoked. So running with NoScript will provide you some protection until Adobe is able to catch up and fix it. You can go, if you want to see whether it's installed, go to adobe.com/shockwave/welcome. And that will - it'll show you what version you have, if it's installed, or try to give it to you if it's not. Don't accept it, if you don't have it installed. You'll just know if it doesn't show you what version you have that you're safe from it. And you can also just go to Add/Remove Programs.

And again, it's one of those things like it's falling into disuse. It's their sort of higher power authoring platform for really sort of heavyweight fancy stuff, sort of higher end above what Flash does. Flash is generally, of course, what everyone is using to a much greater degree. So again, very much like RealPlayer, Shockwave is aging and is falling into disuse. And obviously here it's representing problems because it's creating vulnerabilities which, unless you need to have it installed, just get rid of it.

Leo: You know what's funny, the new Apple little - the MacBook Airs, for the first time ever on a Mac, don't come with Flash. And really the reason is probably just that, if they build it in, it'll be an old version. And since there's so many updates these days they figure, well, if you need it, you'll just install it. Some people are interpreting it as a backhanded slap at Adobe.

Steve: Or maybe a forehanded slap. I mean...

Leo: Well, but I also understand, okay, so they ship it with Flash on it. Tomorrow Flash could - there could be a big security flaw, and it could be updated. So wouldn't it be better just to let people install - and they do the same thing with Java, by the way, there's no Java installed on it - let people install it, the most up-to-date version? I haven't installed it yet.

Steve: Well, and I was just going to mention that, speaking of Java, one of my notes here in news is that Apple has formally said they're going to stop independently supporting and providing Java in the future.

Leo: Right. They used to do their own JVM. And so they're going to let Sun do it. And why not?

Steve: Exactly.

Leo: Why take responsibility, especially now that there have been problems?

Steve: Well, and they're going a little further. They're saying that they're going to reject any apps written in Java in the future.

Leo: Oh. See, this bothers me.

Steve: Yeah, on their app store, if it's - this is going along with their same on the iPhone issue. Remember Adobe tried to do the whole cross-platform app development thing; and Apple said, no, no, no, you've got to develop using our tools, not some third-party interpreter thing. Their argument is that such apps that try to be cross-platform don't take advantage of specific features on that platform. So Jobs is taking a very hard line on this. And this is very much along the same lines. Java itself falls under that same umbrella of being an interpreter. And Apple is saying, no, we're not going to allow people to do less than really good apps, by their definition. So, yes, so Java will not in the future be supported. I guess, what, 10.7 will have it, but not the future? Or does 10.7 not have it?

Leo: I would guess it's not - because 10.7 is not out until next summer. So I would guess it's 10.7. But it doesn't come on these new Macs, either. But that doesn't mean you don't get Java. It means you could just install it yourself from Sun.

Steve: Right. And what typically happens is you will install an application which was written in Java. And so its installer will drag Java along behind it in order to create the platform that it needs for running. I mean, no one just goes and gets it because they have nothing better to do that day.

Leo: Actually, I went and got it, and that's because I wanted to do development for Android, which requires not only the JVM, but also the SDK.

Steve: But this is you, Leo.

Leo: That's me. That's a little unusual, I agree, yeah.

Steve: Okay. So Wall Street Journal has for some time now been doing a series under the umbrella title, "What They Know."

Leo: Oh [sighing]. Okay, go ahead. I just had to breathe a sigh [sighing]. You've got to remember, they own - they're owned by News Corp., which owns MySpace. And they never disclaim that. I wish they would.

Steve: Yeah. It's funny because they did mention in one of these stories that The New York Times owned one of the properties that was being hit upon here. So in the latest story on tracking, the Wall Street story begins: "In the weeks before the New Hampshire primary last month, Linda Twombly of Nashua [New Hampshire] said she was peppered with online ads for Republican Senate-hopeful Jim Bender. It was no accident. An online tracking company called RapLeaf, Inc. had correctly identified her as a conservative who is interested in Republican politics, has an interest in the Bible, and contributes to political and environmental causes. Mrs. Twombly's profile is part of RapLeaf's rich trove of data, garnered from a variety of sources, and which both political parties have tapped [in the past]. RapLeaf knows even more about Mrs. Twombly and millions of other Americans [including] their real names and email addresses."

Leo: And where does it get this information?

Steve: Uh-huh. It turns out that they do deals with companies which use email addresses as part of their sign-on, logon user IDs. So when you sign onto one of these sites, RapLeaf - and it's funny, I've been thinking of them as RapeLeaf, and I have to keep reminding myself, Rap, Steve, Rap.

Leo: It might be appropriate, yeah.

Steve: Yeah. RapLeaf has a deal with them where they will disclose through a back channel connection your email address and the cookies that you're using with that site, whereupon RapLeaf installs their own tracking cookies that are synchronized, and now they have your email address. They also, of course, have what other personal information that site has about you, including perhaps your real name, if you identified yourself at some point to that site. So they are, I mean, this is what we knew was going on. We've talked about it before. It's finally getting some top-of-the-fold press now, which is I think all for the best because people have to understand what's going on.

Leo: But the thing to underscore is in almost, in fact, as far as I know, in every case this is material that they've publicly volunteered; and, for instance, a lot of this is gleaned from Facebook, which is why I brought up MySpace. It's from stuff that's public on Facebook. So...

Steve: Well, although what it turns out is, and this was another story under the same umbrella, it turns out that the top 10 Facebook apps, even against the privacy settings that the user has set, a user on Facebook who is using maximum privacy everywhere, the top 10 Facebook apps - unfortunately, Leo, Farmville is among them - is sending...

Leo: Don't look at me, I don't play Farmville.

Steve: Oh, I thought...

Leo: No, I gave up Farmville literally a year ago. It was driving me crazy.

Steve: What was that thing you played?

Leo: I play We Rule. That's not Facebook and Farmville. That's a standalone app on the iPad.

Steve: Okay, but what was the thing you were playing, went nuts over with the iPad?

Leo: Yeah, that's We Rule. I don't play Farmville.

Steve: Oh, okay.

Leo: In fact, I don't actually use apps on Facebook for this reason. But the point is, and I think the Journal actually was disingenuous on this, they did, against Facebook's own policy, reveal the userID in some cases.

Steve: Correct.

Leo: Which can then be tracked to the user. But only information that is public, that is set to "public," can then be viewed. So this isn't information that isn't already available to anybody who just goes and searches for you on Facebook.

Steve: Okay.

Leo: That's the point.

Steve: So using your userID, you're able to get the person's Facebook name.

Leo: Right, which you could find by a search, as well.

Steve: But even - and also their friends? Because...

Leo: No, that is something that is leaked by apps, and that I think is a big problem. And I don't think that's against the rules. I think that that's something that apps do do, all the time.

Steve: Okay. So RapLeaf declined to disclose who they're working with, citing NDAs.

Leo: Guarantee you it's Facebook.

Steve: Exactly. Nondisclosures. But The Wall Street Journal found sites installing RapLeaf cookies, including About.com, Pingg.com, TwitPic and Plixi and Flixster, Tester-Rewards. And then both apps on Facebook and MySpace are hosting RapLeaf cookies, essentially performing this kind of aggregation. And to give our listeners a sense for what this means, The Wall Street Journal reported, saying:

"The Journal decoded RapLeaf's information on [some random guy named] Gordon McCormack, Jr., a 52-year-old who lives in Ashland, New Hampshire. RapLeaf correctly identified Mr. McCormack's income range, [the] number of cars [he owns], his interests in gardening and the Beatles, and his interest in playing the online game Mafia Wars, among other topics. Mr. McCormack says he plays Mafia Wars almost every day before going to bed. RapLeaf also identified Mr. McCormack as someone with an interest in online personals. He says he isn't currently [doing] online dating, but might have a couple of profiles 'lurking out on the Internet.'"

Leo: All right, okay.

Steve: "When Mrs. Twombly, a New Hampshire Republican, registered at Pingg.com using her email address, RapLeaf matched her to dozens of 'segments' [as they call them], according to a Journal analysis of the computer code transmitted while she was on the site. The Journal was able to decode 26 of the segments, including her income range and age range and the fact that she is interested in the Bible and in cooking, crafts, rural farming, and wildlife. Mrs. Twombly says all the decoded segments describe her accurately. In Mrs. Twombly's case, RapLeaf transmitted data about her to at least 23 [other] data and advertising companies after she logged onto Pingg, according to the analysis of the computer code. Twenty-two companies, including Google's Invite Media, confirmed receiving data from RapLeaf. RapLeaf declined to comment on its relationships with the companies." And then I did a little poking around RapLeaf. And of course there is an opt-out page. You have to create an account with them.

Leo: Oh, great, and give them all the information, yeah, okay.

Steve: And give them your information, including your email address, in order to opt out. And it's like, okay, this seems annoying. And due to all the attention that this company has received, thanks to The Wall Street Journal's analysis, there's a link on the front page, not surprisingly, www.rapleaf.com, to a blog posting from their CEO that starts out: "There has been a lot of press recently about RapLeaf's efforts to personalize experiences for consumers. The following are some thoughts by RapLeaf's CEO, Auren Hoffman." Anyway, I loved the - and they're big on, well, we're trying to personalize your web experience.

Leo: Yeah, here's the value, right.

Steve: Yeah, and here's all the money we're making by helping you doing that.

Leo: A couple of things we should point out. First of all, this kind of information, I remember doing a radio show with a company, I can't remember its name, 20 years ago, where if I gave you my zip code, they'd know what magazines I subscribed to, what car, because...

Steve: Yeah, probably DoubleClick, Leo.

Leo: Yeah, a lot of this - well, no. It was pre-Internet.

Steve: Pre-Internet.

Leo: Yeah, a lot of this stuff has been available and known to marketers for decades, literally for decades. The other side of this is, I guarantee you this guy, for instance, all of this stuff is public stuff that he's put publicly on the Internet.

Steve: Right.

Leo: So I guess it's a good word of warning to us, if you don't want people to know this stuff, they are collecting it. I'm not sure that they're doing it in a nefarious way.

They're just - they're using databases to aggregate information that we're putting out there.

Steve: Yeah. And so the takeaway, in the case of Mrs. Twombly, she was unhappy when she found out what was being done, and started blocking cookies, and commented that some sites didn't work as well as they used to. But she was unnerved.

Leo: It ain't cookies, lady. It's your - if you have a Facebook profile that reveals all this stuff, well, you shouldn't be surprised that somebody else knows it. Anyway...

Steve: Yup.

Leo: Anyway. Sorry.

Steve: SANS, the very good, the excellent cybersecurity outfit, in their most recent newsletter they had a quote from a recent RSA Europe conference where our Homeland Security secretary Michael Chertoff said something that I found a little bit disturbing, I wanted to share with our listeners. Quoting from the SANS newsletter:

"At the recent RSA Europe conference held in London, former U.S. Homeland Security Secretary Michael Chertoff has called on countries to develop doctrines to deal with cyber warfare in the same way Cold War doctrines were developed for nuclear conflict. He told delegates at the conference that over 100 countries are now actively involved in cyber espionage and cyber attacks, and that clear rules of engagement need to be defined.

"While stating that countries should be able to respond to cyber attacks 'with overwhelming force,' he added countries need not 'respond to virtual attacks with real attacks, but I do think it's important to define when and how it might be appropriate to respond. Everyone needs to understand the rules of the game.' Acknowledging that attribution of attacks is difficult, Mr. Chertoff posited that countries that are victims of persistent attacks against their critical infrastructure should be permitted to incapacitate the platform used as the source of the attack, regardless of who is controlling the attack." Which really makes me uncomfortable, Leo.

Leo: Yeah, I'm with you.

Steve: Yeah. So he's saying that Internet attribution is a problem, which we understand, that is to say, the fact that attacks are coming from IP addresses in China, as we well know on this podcast, in no way means that this has anything to do with China, only that a whole bunch of their machines have had zombies installed unwittingly, and that those machines are being used as the attack platform.

Leo: So they should be able to take them out with a Predator drone?

Steve: And Chertoff is saying at some point this stuff does need to cross from the virtual world into the real world.

Leo: This is saber-rattling. I don't know if this is...

Steve: I know. Just disturbing, that there's this - and I have to say, though, I saw another note that the U.K. was finally beginning to allocate serious money for cyber warfare, cyber defense initiatives. The feeling in general is, I mean, and I still feel like I'm a little caught up in a little bit of a sci-fi world here; but, I mean, it's becoming very real as we talk about, for example, trojans that are able to infiltrate nuclear reactor sites. It's really clear that, I mean, look at all the trouble people have keeping this stuff off their own computers. And we know that the government is no better at it than individual end users.

Leo: Right, right.

Steve: I mean, there really is penetration being made into sensitive networks.

Leo: I mean, you have to think, if they're going to start taking out these computers, that they're going to take out a lot of innocent people.

Steve: Yeah, that's frightening.

Leo: People who are just zombied without their knowledge.

Steve: And France has passed and begun to enforce their newest anti-piracy law. The acronym is HAPOPI, and they've hired a third-party company in order to enforce this because they're not the enforcers themselves. The law is now in place that provides for enforcement. So a third-party company has been hired to monitor popular downloading sites like eMule and BitTorrent, to capture the IPs of the users of the sites, to send those - and we're talking 125,000 a day is what they're ramping up to - send the captured IPs to the relevant ISPs to obtain the email addresses of the people who currently have those IPs and send them a first warning email which reads: "Warning, your Internet connection has been used to commit acts, recognized by police authorities, which could be regarded as in breach of the law."

So the first email reminds users that they're legally responsible, regardless of who actually downloaded the film or song onto their machine. And if there's another infraction within six months, offenders will receive a registered letter warning them to stop downloading. Then a third offense can lead to legal proceedings and a one-year Internet connection blackout. So France is the first big country to actively adopt a law and start enforcing it. And a lot of other countries are watching to see how this goes.

Leo: Yeah, and a lot of other countries are considering a similar law, so that's scary.

Steve: Yeah, exactly. I had a friend, for errata, who suggested - he was using Safari's private browsing. And he sort of assumed that, when he turned on private browsing, he would suddenly go anonymous.

Leo: No.

Steve: What he realized - exactly. What he realized was that what it meant was that, while in private browsing, nothing that happened during that session of private browsing would be sticky. Nothing would be, for example, written to disk. But going into private browsing didn't immediately anonymize you from your non-private browsing session. In fact, you brought all your cookies with you that you would have had before browsing. It's just that anything that happened during that time was not saved. And he said, "You know, Steve, it might be worth pointing that out to people who assumed that they were anonymous while using private browsing." I thought, yeah, that's a really good point. Ought to mention that.

And then also in errata, we were talking about IP space depletion as probably being next year's recurring theme and news. Ars Technica carried an interesting story where they mentioned that one of the major /8 networks, in this case the 45 network, meaning all 16-plus million IPs beginning with 45-dot, so 45.anything, they were previously all allocated to Interop. And Interop gave back to ARIN 99 percent of them...

Leo: Oh, good.

Steve: ...just now.

Leo: Just as we were asking, couldn't they just ask for these back?

Steve: Yes. And so it was - so there is no provision for ARIN to, like, force unused IPs back. Apparently, behind the scenes, ARIN is going around to people who have huge allocations from the original allocation of the first digit of the IP, and saying, hey, you know, you're not really using all 16 million of those, and...

Leo: Give us a few back, just a few.

Steve: ...we'd really like to have some. Now, there was an interesting chart, I provided the link to you in our notes, Leo.

http://arstechnica.com/business/news/2010/10/embargoed-interop-gives-back-a-months-worth-

of-ipv4-addresses.ars

On that page is a really nice map which shows the allocated networks, and those which are still not allocated. So the free ones are 5, 23, 37, 39, 100, 102, 103, 104, 105, 106...

Leo: It looks like a bingo chart.

Steve: It does. 179 and 185.

Leo: And then there's a bunch of unusable ones, 127 and 224 and up.

Steve: Yup, 224 and up.

Leo: And of course 10-dot, yeah.

Steve: And of course 10 is unusable, that's the whole 10-dot RFC 1918 reserve network. And interestingly, despite Interop, I mean, Interop doing this was very nice. What it bought us was one month. So giving back 99 percent of a full /8 network bought us a month. So we're in trouble.

Leo: So there you go.

Steve: Yeah.

Leo: Wow.

Steve: Yeah. And I have a very short note from a happy user of SpinRite that I wanted to share, Dianne Dunnett, who wrote - and just very quickly, she said - she called it "GRC Post Sales Statement." She said, "GRC, I've used my copy of SpinRite 6 to correct two of my home computers, one that would not load into Windows after the Windows scrolling bar screen" - whatever she meant by that, "after the Windows scrolling bar screen" - and then she said, "and the other with a Windows registry hive error that kept it from booting. SpinRite has without a doubt saved my bacon."

Leo: That's great.

Steve: "Thanks so much."

Leo: That's great. Yeah, those hive errors are horrible.

Steve: Oh, boy, yes. I've had 'em, and you've had 'em.

Leo: Yeah. Well, it's just this opaque binary blob that you can't fix. So obviously there was a bad sector somewhere in that blob, and SpinRite was able to recover the sector, which is just great, yeah. All right. Let's talk about Firesheep.

Steve: Okay. So this last Sunday, on the 24th of October, the ToorCon 12 Annual Security Conference occurred, from Friday through Sunday. And there were a number of presentations, as there are at these security conferences. I got a kick out of two of them, that our friend Samy Kamkar - who is of course notorious for his creation of the Evercookie. I love the title of his. I didn't bother to go dig into what it was. But the title was "How I Met Your Girlfriend."

Leo: Okay. Sounds like a sitcom.

Steve: Exactly, I just - I got a kick out of the title of his, "How I Met Your Girlfriend." And you can imagine at a security conference it's something you didn't do right...

Leo: Gets your attention, yeah.

Steve: ...that gave him access to her. And then Julia Wolf had my favorite presentation title. It was, all caps with underscores, OMG_WTF_PDF.

Leo: Say no more.

Steve: Say no more.

Leo: Say no more.

Steve: OMG_WTF_PDF.

Leo: I love it.

Steve: But at noon on Sunday, the last day of the conference, Eric Butler and Ian Gallagher, both security guys who operate out of Seattle, Washington, delivered their presentation which pretty much brought the house down. It was titled "Hey Web 2.0: Start protecting user privacy instead of pretending to." And the description of their presentation online is worth sharing. This is what they wrote ahead of time. It says:

"Despite growing public concern over web privacy, especially within social networking sites, companies including Facebook, Twitter, and even Google all fail to protect users against session hijacking attacks. These attacks are nothing: Session hijacking is one of the oldest, simplest, and most widely known attacks against the web. An interested attacker can view your private Facebook photos, broadcast Tweets as you, see your web history, and anything else you can do while logged in to your own online accounts.

"We're bringing up this tired issue to remind people of the risks they face, especially when on open WiFi networks, and to remind companies that they have a responsibility to protect their users. To drive this point home, we are releasing an open source tool at ToorCon 12 which shows you a 'buddy list' of people's online accounts being used around you, and lets you simply double-click to hijack them."

Leo: Okay.

Steve: This is fantastic, Leo.

Leo: You think this is good?

Steve: Oh, this is the best thing that ever happened. This is, I mean, if I had a different security profile than I do, this is what I would write. I can't write it, but I can cheer it. This is great because this is finally going to really put, I mean, this is what it takes to force change. We're never going to move from IPv4 to IPv6 until we run out of IPs. We're never going to get online Web 2.0 sites to just switch over to SSL exclusively until they have to. And this makes them do it.

Leo: You know, when I used to go on - I still do, I go on geek cruises with a guy named Randal Schwartz, you know Randal, he's a programmer, does our This Week in Open Source, FLOSS. And he's also a hacker, from years gone by. And we got him to stop doing this. But it was the same thing, it was very effective. I'll never forget, the first time I went on a cruise with him, he came up to me and gave me a piece of paper. He said, "Is this your email password?" I said, "What?" He said, "You're sending it in the clear every time you're on the ship's WiFi. Just thought you should know." Same idea; right?

Steve: Well, yes. And look at the trouble Google got themselves into by capturing unencrypted WiFi. I mean, just driving around. They weren't even doing anything with it. Okay. So to frame this a little better, ConsumerAffairs.com today wrote:

"Computer security specialists have issued a warning about Firesheep, a new downloadable add-on to the Firefox browser. If the person in a coffee shop with you has it, they can see exactly what you're doing online.

"The feature was reportedly created by a Seattle software developer, whose purpose was to demonstrate how vulnerable unsecured networks are. Unfortunately, he's unleashed a tool that can turn a computer amateur into an accomplished hacker. With Firesheep, a computer user can log onto a public network, in an airport or coffee shop, and get a list of all the computers that happen to be connected to the network at that moment. Simply by double-clicking on one of the names...."

I mean, and this thing, it shows you a list of all the users on your WiFi hotspot, the social networks they're using, and their pictures, which it goes and retrieves from their Facebook page and MySpace and anything else, Twitter for example, and literally you browse them. You click this - and I'm going to explain how in detail in a second. But you are then them. You're logged on as them to their Facebook page, to their MySpace domain, to their Twitter account, able to do anything they are. This is chaos, Leo. This is fantastic.

Leo: You're sounding like a black hat. What's amazing is how easy it is to use. I mean, you have this extension installed, and you just see the list.

Steve: That's the point. I mean, yes, you could be a Linux user with Cain and Abel, and you could type a bunch of arcane crypto commands and see this stuff going on. I mean, I've done that. I mean, it's possible. But this is game changer because of how easy this makes it. Now, when I went there this morning there were 300,724 downloads. Can you click the link now?

Leo: Holy cow. Wow. Yeah, let me go back to it and see how many there are now. This is at GitHub. It's not, by the way, an official Firefox extension.

Steve: Correct.

Leo: He does not offer it through Firefox. They'd probably block it. 325,985 downloads.

Steve: Okay. So since this morning another 25,000 downloads. Mozilla is on record as saying of this extension that, well, this is not a Firefox vulnerability.

Leo: Right. Any browser could do this; right?

Steve: Yes. And in fact the cat's out of the bag now. If Firefox were to block it, it's trivial to create a standalone application that will do this. And I'm sure we're going to see one shortly. There's just no doubt about it.

Leo: Now, this works because these passwords are being sent in the clear.

Steve: Well, not - no, no.

Leo: No?

Steve: No. And that's what session hijacking is. We'll talk about it in one second.

Leo: Whoa.

Steve: So just to finish the Consumer Affairs story, they said, "Simply by double-clicking on one of the names, the Firesheep user can access whatever that computer user is doing online. If they are updating their Facebook account, the Firesheep user is also logged in. Firesheep works by intercepting Internet cookies, which websites place on your computer when you visit so they will recognize you when you return. Professional hackers have had that tool in their arsenal for years. Now, thanks to Firesheep, anybody that has downloaded the add-on can do it," too.

And so here's the deal. On all these sites they switch you to SSL to log you in. But then they give your browser an unsecure cookie, take you back out of SSL just because they can. They don't have to, but they do. And now that cookie is the way your session is authenticated. That is the only way you're identified. So anybody sniffing your unencrypted traffic, which all traffic is at an open WiFi hotspot, has always, has long been able to use that cookie, pick up that cookie which is sent with every request your browser makes. That's the way - that's your entire session state is that cookie, just some random gobbledy-gook, doesn't matter what it is.

All a third party has to do is use that cookie, and they are indistinguishable from you at that location. And even your IPs are the same because you're all being NAT'd through a single IP out onto the Internet. So you look just like the person sitting next to you at Starbucks. So currently supported is Amazon, Basecamp, bit.ly, eNom, Facebook, Foursquare, GitHub, Google, Hacker News, Harvest, The New York Times, Pivotal Tracker, Twitter, ToorCon, Evernote, Dropbox, Windows Live, Cisco...

Leo: Crap, all the stuff I use.

Steve: ...Slicehost, Gowalla, and Flickr. And coming soon is Yahoo!, eBay, LinkedIn, Digg, Reddit, Wikipedia, Blogger, GoDaddy, Posterous, Tumblr, Netflix, YouTube, Slashdot, MobileMe, PayPal, Salesforce, Craigslist, MySpace, Match, and AOL.

Leo: This is terrible.

Steve: It's fantastic.

Leo: Holy cow. I mean - okay, okay. Proceed.

Steve: First of all...

Leo: I'm terrified.

Steve: There's, okay, some of this is a bit of an exaggeration. For example, PayPal is on the "coming soon." But PayPal never has you in the clear. I don't think even using SSL Strip, which would remove the HTTPSes from the links, I don't think PayPal will function. And we know that PayPal is an early adopter of STS, the Strict Transport Security protocol which, for example, Mozilla is supporting. And what Mozilla, in Mozilla's formal comments about this add-on, they said, well, this is not a mistake in Firefox. This is because sites are not using SSL to transact session state in cookies.

If we turn the clock back a few years, you may remember that at one point I was needing to allow my employees, Greg and Sue, to roam away from home where I had them locked down for secure access to GRC. I wanted them to be able to roam around. And what I used was a feature that browsers have always had, where cookies can be tagged as SSL-only, so that when a cookie is given to the browser, there's a flag that's just called "secure equals," and you say secure equals [indiscernible] yes or something. And so the browser tags it. It will never send it out unless the session is secure.

So part of my means for - Sue, for example, could be using an open WiFi hotspot. First of all, GRC enforces SSL for these things, and never accepts a non-SSL connection. But even so, the cookies that we use for maintaining state are tagged as SSL-only. But if anything, for example, if Strip SSL were used to strip that out, even though at my server side I refuse to accept a non-SSL connection, so even Strip SSL wouldn't work, the browser at that location would never divulge the session state over a non-SSL connection.

So it is entirely possible, it's not rocket science, just to force SSL. It's just all of these sites are not doing it. They're switching people back over. And I'm excited about this, obviously, because this is going to create major ripples. I mean, the idea that, I mean, there will be a half a million of these things downloaded by tomorrow. This thing is going to take off like wildfire. People are going to experiment with it. They're going to load it into Firefox, go to Starbucks, and say, wow, it works. I mean, maybe mischief is going to be created by this. I imagine some will be. I mean, I would never, ever touch anyone's web, Facebook site settings or anything. Unfortunately not everyone are you and me, Leo.

And immediately people like Amazon, I mean, Amazon is guilty, too, of taking us back out of SSL for - we've discussed this before with Amazon. Important transactions are back to SSL. In fact, just like last month I was talking to Mark Thompson about this. He's working on a project, and we were talking about security, and he had looked closely at what Amazon does and mentioned to me that they were - that Amazon took you back out of SSL, and it was only for things that mattered.

And I said, "Mark, listen to me. Absolutely without equivocation never accept a non-SSL connection. There is no reason in this day and age not to always be using SSL." He's doing something where there will be sensitive information. And I said, just from day one never make this mistake. Always be SSL all the time for the kind of stuff he's doing. I think I made the point with him so that that's the way his system will be designed. These other companies are just going to have to make the change. I mean, and we're talking within days. This is, I mean, this is huge. And this represents a major, major positive lesson. Now that this exists...

Leo: It's called a spanking.

Steve: I mean, this is really - this is really big.

Leo: All right, let's get back to Security Now!. Steve Gibson has been telling us about a Firefox extension. It's on GitHub, it's not on the official extensions page; but if you search for Firesheep you'll find it right away.

Steve: Yup, if you just Google "Firesheep," you'll find it on GitHub and a bunch of stories about it.

Leo: You said not to install it. You told me not to install it.

Steve: I'm going to install it.

Leo: It's a little buggy?

Steve: Yes. It is raw. It's 0.1. It's the code that they released at the show on Sunday. They're in the process, it's right now supported for Windows and Mac. For Windows you need to install the WinPcap sniffing library, thanks to me, actually, because Windows doesn't have raw sockets, which is what WinPcap provides.

Leo: Oh, how interesting.

Steve: Uh-huh. But...

Leo: You don't need to do that on the Mac; huh?

Steve: Correct. The Mac does support standard UNIX raw sockets.

Leo: Oh, interesting.

Steve: And so it's able to sniff. I saw a note from the developer that he's got it running under Linux, so he's in the process of getting it up under Linux.

Leo: So if my understanding is correct - let me just, to recap, people are tuning in or whatever - you install this extension. You go anywhere where there's an open access point, anywhere, a coffee shop, Starbucks, whatever, and it will show you on the left...

Steve: Or driving down the street, Leo, also.

Leo: Yeah, actually, there's a lot of open access points all around the street. So it will show you, on the left, a bar opens up, and it will show you other people sharing that open access spot with you, and what they're logged into.

Steve: Yes. The idea is, it's sniffing the traffic, just the way Google did when they were roaming around doing their mapping. It sniffs all the traffic that's available on the WiFi at that access point. It looks at the transactions. It sees www.facebook.com, twitter.com, amazon.com, New York Times, Foursquare, and so forth. It has a little bit of JavaScript which tells it how to interpret those specific sites that it knows about, and it has a separate file of handlers which is growing now as it's becoming more able to deal with additional sites. And so what it does is it starts populating like a list, like a sidebar, of all the things that people are doing on that WiFi hotspot, their name, it goes and shows you their photo. So you can sort of turn around and go, oh, yeah, there he is over there on the side.

Leo: Ay, ay, ay.

Steve: And so...

Leo: So it pulls these photos from Twitter or Facebook or Flickr or wherever the profile photos exist.

Steve: Right, because it knows everything about them. It's able to log in as them, get that information. And then you simply, if you want to impersonate them, literally hijack their session, you just double-click on it, and you're logged in as them, on their Facebook page.

Leo: And it does that because it doesn't give you the password, it's not that the password is out in the clear, but the cookie, the authenticating cookie is sent in the clear. And so you have the cookie. You just say "I'm them."

Steve: Correct. Now, okay. The thing that Starbucks could do to fix this immediately, I mean, and it would be wonderful if they did, is simply to bring up WPA encryption with the password "Starbucks." It doesn't have to be unknown. We don't have to have per-user passwords or anything.

Leo: Oh, interesting.

Steve: We already discussed how WPA provides inter-client isolation. We discussed this a couple months ago under a different context. So right now you walk into Starbucks, and you're online. They're unencrypted, and they're open.

Leo: So use WPA. You can tell everybody the password, including somebody running Firesheep, doesn't matter.

Steve: Yes.

Leo: Oh, that's a simple fix.

Steve: So it's a huge fix. And it's the kind of thing that Starbucks, that is mentioned in these articles over and over. And I keep saying their name because I'm at Starbucks all the time. I would love them to bring up WPA encryption across all of their newly free WiFi, and just let people know, I mean, everyone would know, as soon as you try to log on, it'll say, what's your password? Just type in "Starbucks."

Leo: Put a sign over the counter.

Steve: And the problem is solved, completely solved, period, because...

Leo: So if you're - I'm going to go over to my local coffee shop. My friends over at the bakery over here have - in fact everybody in town now has WiFi, open WiFi. And just say, this is all you have to do, please do this. Use the name of the establishment as the password, and it would fix it.

Steve: Well, and in fact, Leo, have this installed on your Mac, walk over there, show them that right now...

Leo: Oh, that's a good idea.

Steve: ...all the users that are using it are exposed because they're using their WiFi, and tell them it's this easy to fix it.

Leo: Now, if I logged in as somebody using the cookie, let's say I got into their Facebook account, could I just change their password?

Steve: Absolutely. You're them. I mean, we're talking - this is havoc. This is chaos.

Leo: Wow. Now, some sites would say, well, what's your original password, and would need that.

Steve: Ah, good point, yes.

Leo: So you hope that they do things like that.

Steve: Yes.

Leo: Good lord. But even if they can't change your password, they can read everything as if they're you.

Steve: They could change your photos. They could change your privacy settings, drop all your privacy to zero.

Leo: Oh, this is horrible.

Steve: It's horrible.

Leo: We're going to see people using this like crazy.

Steve: I know. I mean, what's the download count now?

Leo: It's like the count and the amount. Let me go back. Let me see. Downloads, it was 325,985. I think thanks to this show alone you probably - 327,940. Another 2,000 people have downloaded it just since we looked last time.

Steve: Yeah, it's going to go exponential, Leo.

Leo: Ay, ay, ay, ay, ay.

Steve: Yeah. And again, this is just the first. Now that this concept is out, we're going to see it go like crazy. And so, okay, so the thing that - the remediation for the wireless access providers simply bring up encryption, finally. Again, it doesn't have to be a secret password, just Starbucks can make it "Starbucks." And that solves the problem. However, the providers of these services, the Facebook, the Twitter, the MySpace and so forth, they can't rely on that. They have to simply enforce SSL, just like Google did. While you were reading that last sponsorship spot, I went over to docs.google.com, which I had just been using to prepare the docs for this, and tried to remove the "S" from HTTP, and it bounced me, it redirected me right back over to HTTPS, forcing me to have a secure connection while I was doing these things. So Google is enforcing it. There's no reason everyone isn't.

Leo: Yeah. Nowadays machines are - even these Netbooks are fast enough to do SSL full-time.

Steve: Actually there's never been a question. Remember that, I mean, and I've already seen this by people who aren't up to speed on encryption. SSL used to be expensive back with HTTP 1.0, when browsers were dropping and reestablishing connections. Now browsers are maintaining those persistent connections to web servers. The only expense is during the public key negotiation at the beginning of a transaction. And SSL now caches credentials. So even browsers that drop connections and reconnect, you're able to use a cached credential. The overhead is negligible because of other advances that have been made in the protocols. So it's not expensive for the end user, and it's not even expensive for the aggregation of all those connections at the server. There's just no reason not to do it.

Leo: Wow, very interesting.

Steve: And this is - I'm sure we'll have some news next week because this thing is just making everybody go nuts.

Leo: Well, yeah. I mean, if you were malicious, you're going to go out there, and I'm just thinking, I mean, I'll probably use - I'm using an open access point right now. I mean, holy cow. We're going to lock down our access points here at the studio.

Steve: Yup. Just use a simple - all you have is a simple password because, as we discussed, WPA does enforce inter-client isolation. Individual clients negotiate their own private keys with the access point, even though they're using a common password. The password gets them in, but then their sessions are individually isolated. So that provides you protection against this kind of passive eavesdropping. So it's trivial for Starbucks to fix the problem, and it'd be great if they did.

Leo: Yeah. Let's hope they do.

Steve: And in the meantime, Firesheep, Firefox add-on, have fun. Don't be bad with it. Don't be bad.

Leo: Don't be bad.

Steve: But just have fun because this is...

Leo: And [indiscernible], don't be bad. I wonder how many people in the TWiT Cottage have already downloaded this. Wow. Steve Gibson is at GRC.com. That's his website. That's a place you can go to get - you can, the DNS Benchmark is out, in beta, and I'm presuming we'll talk about it.

Steve: Oh, and no, it's out of beta. It's at v1.2. I did want to mention to our listeners - thank you for reminding me, Leo. It's linked from the main menu. It's on our freeware page. I took it public for this podcast before this...

Leo: Oh, good.

Steve: ...before Firesheep happened. And it's like, oh, shoot, now we've got to wait two weeks. But this would be good because our listeners ought to grab it, take a look at it, familiarize themselves with it. Frankly, I think you'll be blown away with what I did in 162K of code. And I'm going to...

Leo: That's amazing.

Steve: In two weeks we will talk about all the technology that's underneath the covers there and what it does and how it works.

Leo: Truly amazing. That's GRC.com. That's where Steve lives, Gibson Research Corporation. It's also where ShieldsUP! is and a whole bunch of other free useful utilities for security. And of course one paid utility that you must have, Steve's bread and butter. It's called SpinRite, the world's best hard drive recovery and maintenance utility. And you should be using it if you've got hard drives. Not on solid state, but on spinning drives, absolutely should be using it.

Steve: Yup.

Leo: And when you go there you can also visit the show notes; the 16KB as well as 64KB versions Steve hosts. He has small versions for people with bandwidth limitations. He also has a complete transcription of every show, which is great. That's all GRC.com. And if you have a question for next week's show, because we usually do a Q&A show every odd episode, GRC.com/feedback to ask that question. If you heard something today or on any show that you want to know more about, that's a good time to do that. GRC.com/feedback.

You can watch us do the show every Wednesday at 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1800 UTC at live.twit.tv. And join us in the chatroom at irc.twit.tv, always fun. But of course most people listen after the fact, at your convenience, just by downloading the show, TWiT.tv/sn for Security Now!. TWiT.tv/sn has a list of all the different RSS feeds, the iTunes, the Zune, and all of that, so you can get it that way.

Steve: It's at five downloads per second right now.

Leo: Holy geez.

Steve: 328,556.

Leo: I love this idea. I'm going to put it on the little Air, bring it over to my local coffee shop, good friends of mine, and say, you know, you might want to turn on WPA.

Steve: Yeah, and then just put up a little sign, "Here's our password." Because, I mean, it's so easy to do. As we know, when you go to - there's an Italian restaurant that I go to, and they're encrypted. And so the first time I walked in with my iPad, I said, oh, I can't remember what's your password. I think it was, like, "realgoodeats" or something like that.

Leo: That's great.

Steve: And it's just, they tell everybody, and that way they're not exposing their own customers to this kind of liability. So it doesn't have to be secret.

Leo: Realgoodeats, I like that. Thank you, Steve. We'll see you next week...

Steve: Thanks, Leo.

Leo: ...on Security Now!.