SECURITY NOW!

Transcript of Episode #329

BrowserID

Description: After catching up with the week's news, Steve and Leo examine the operation of Mozilla's solution to the need for secure, reliable and easy-to-use establishment of online Internet identity known as: BrowserID. They also compare it with all of the other existing technologies and solutions we've discussed before.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-329.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-329-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 329, recorded November 30th, 2011: BrowserID.

It's time for Security Now!, the show that protects you online, your online privacy, your security, and of course talks a little bit about science fiction and eReaders on the side. That's because of this guy here, this guy, Mr. Steve Gibson, the host of the hour.

Steve Gibson: Speaking of which, I did hear an interesting suggestion. Actually someone tweeted that maybe an interesting idea for our special holiday show would be just to do a whole episode on science fiction.

Leo: I like it.

Steve: Yeah, I mean, sort of go back over the recommendations, remind everybody of the stuff that we've found, and talk about the authors and just do a sci-fi show.

Leo: That's a great idea. We'd have to do a special recording time. We could figure that out.

Steve: Yeah, you and I would just find some time, and I'd lay out - do my regular production and plan it out and figure out what we would talk about.

Leo: Okay. Let's coordinate. I don't know if they've already started the "best of" yet. But if they haven't, then I think that's a great idea.

Steve: So we have a fallback in case there isn't enough "best of" ideas.

Leo: Right.

Steve: And I think this show's a little tough to do that with.

Leo: Yeah, I agree with you.

Steve: So I was thinking, maybe just something that our listeners would find - and there seems to be a strong interest in sci-fi among our listeners. So anyway, we'll see what people think about that.

Leo: And it's not like you'll lose anything. It would have been a dead spot anyway for the holiday, so no big deal.

Steve: Yeah, precisely.

Leo: Today we talk about...

Steve: Mozilla's attempt to solve the Internet identity crisis. As we know, identity is the big need we have. We talk about passwords and logins and LastPass and YubiKeys and VeriSign and tokens and footballs and, I mean, this is just an ongoing issue. And Mozilla has weighed in. There is a technology for secure verification of an individual's email address. And what I like about what they're calling "BrowserID" is that it is able to use, in a secure fashion, email addresses that people have. So today we're going to catch up, as always at the top of the show, with what news has transpired in the last week, and then plow into how email addresses can be used rather than other things, but then also compare this with everything else we've looked at to sort of put it in context. And I like it because it's very simple to use, and they've managed to make it secure. So that's our topic for this week. I think it's going to be good and interesting. And, who knows? It might succeed.

Leo: [Laughing] I like your vote of confidence. "It might even work." Well, we're going to try it because they've created a demo site. I'll be the guinea pig, and we'll give it a try. I think we established - we started the process ahead of time, cooking show style, and we'll see if it all works by...

Steve: Right. When the eggs are scrambled...

Leo: We'll see how it tastes. Steve, let us get to work, you and me.

Steve: So I just thought I would follow up on the wacky Illinois water pump SCADA failure issue. Remember that one of the things I talked about, I sort of - we finished debunking it, well, we started and finished debunking it last week. I had not mentioned it for a couple weeks because it just seemed a little sketchy to me. But one of the things that lent it some credibility seemed to be very definite teasers, like the fact that there was a Russian IP address that had been caught in some of the logs, which everyone jumped on and said, oh, it's been - this was hacked from Russia. Well, it turns out that a legitimate contractor working for the water utility district was traveling in Russia.

Leo: Oh, please.

Steve: And had legitimate access to the network. And that's where the Russian IP came from.

Leo: That's really kind of annoying.

Steve: So we'll just - we'll be a little calmer next time and wait for the facts...

Leo: Well, it's not us.

Steve: No, but the industry has learned a lesson because the industry just jumped all over this.

Leo: Well, who was the guy? Where did this original report come from? Because that's who...

Steve: It came from a blogger who had some contact with the water district. But then also one of the administrators said, either on radio or television the day after, that there was - that this had happened, that it looked to them like there had been a penetration, and that the failure of this water pump was a consequence of the fact that the SCADA system was under control of some remote entity that's hostile.

Leo: So annoying.

Steve: So it's like, okay.

Leo: So annoying. Well, there you go.

Steve: Now, I didn't remember whether I had said before that Windows 8 Windows

Update was going to acquire some welcome features. Because one of the annoying things about Windows, and I hear people talking about this all the time, is they'll wake up their machine in the morning and see that it has rebooted itself, which is sometimes annoying. So what Microsoft is going to explicitly do, starting with Windows 8, and apparently not change this behavior in prior versions - and I don't know why they wouldn't, but maybe when they release 8 they will back port this to earlier versions, although that's not what I understand.

But Windows 8, they will deliberately consolidate any changes that will require a reboot and consolidate those so that a single restart will be required, and not multiples. And they will in any event provide a, depending upon the user's configuration - because this is sometimes a system by system determinant, whether or not a given machine needs to be restarted. So Windows will determine that and then give the user a three-day warning prior to a restart event. So they can say, okay, just - I've saved all of my data. Go ahead and do it now. In any event, there'll be - it'll be much less inconvenient than having Windows just decide at 3:00 a.m. that it's going to restart.

Leo: It doesn't warn you? I always thought it kind of let you know, at least. It doesn't even do that?

Steve: No. Typically people just realize, like, their system looks strange, and they go, wait a minute.

Leo: Something happened.

Steve: What's happened? It's like, oh, my god, it restarted. So, yeah.

Leo: I was in the middle of a very important project the other day, and Windows - it didn't reboot. But it, like, took me out of the - I was playing a videogame, okay?

Steve: Okay.

Leo: I was killing trolls.

Steve: Leo, it was important for you.

Leo: It was.

Steve: Yes.

Leo: I'm in the middle of killing trolls, and all of a sudden, whishhht. And then Windows says, hey, we've got to - you want to update now? It's like, no.

Steve: Yeah. Yeah, I always...

Leo: That's really not good behavior, I don't think.

Steve: It's annoying when you're telling it, just hold off a minute, let me finish what I'm doing because I've got all this stuff going on, and I don't want to do it right now. And then it keeps popping up and saying, hey, don't forget, it's time. And you're just, yeah, yeah, I know.

Leo: I understand the need to get people to update. I do understand that. But, you know, come on.

Steve: Yeah. So Bruce Schneier, our great friend and cryptographer...

Leo: Love him.

Steve: ...in his recent blog quoted a Juniper Networks blog that had a couple interesting stats that I wanted to share. And the title of Bruce's blog entry was "Android Malware. The Android platform is where the malware action is." And so the Juniper Networks blog poses the question, or asks itself rhetorically, what happens when anyone can develop and publish an application to the Android market? The answer is a 472 percent increase in Android malware samples since July of this year.

Leo: Now, does that mean 472 malware applications on the market?

Steve: Yes.

Leo: Wow.

Steve: They said, "These days it seems all you need is a developer account that is relatively easy to anonymize, pay $25, and you can post your applications.... In addition to an increase in the volume, the attackers continue to become more sophisticated in the malware they write. For instance, in the early spring, we began seeing Android malware that was capable of leveraging one of several platform vulnerabilities that allowed malware to gain root access on the device, in the background, and then install additional packages to the device to extend the functionality of the malware. Today, just about every piece of malware that is released contains this capability, simply because the vulnerabilities remain prevalent in nearly 90 percent of Android devices being carried around...."

So that's, yes, that's what the hackers are having fun doing. They're saying, hey, let's, I mean, they're curious and interested in wanting to develop for the latest things. And Android is interesting and fun, and they've got Android phones, or tablets, or whatever device. So that's what they're doing, is it's got sort of where it's caught their attention.

Leo: Now, we shouldn't, I mean, there's underneath that statement, I just want to be clear, there's the implication that somehow, because the Apple Store is more regulated, it's less vulnerable.

Steve: It is.

Leo: And, well, yeah, except that...

Steve: Not perfect, but...

Leo: Far from perfect. Far from perfect. And I'll give you two examples. Charlie what's-his-name.

Steve: Miller.

Leo: Miller. Posted, wrote example code and posted it, and Apple approved it. And then their response to that was to kick Charlie Miller out of the developers program.

Steve: Yes. Unfortunately, they reacted in a way that I think was inappropriate. He was a security researcher. He notified them months in advance that he had found something that they should fix. And...

Leo: And I'll give you another example. Yesterday Apple approved a program that explicitly said it was designed to do tethering of the iPhone around the carrier's objection. Apple approved it. Then when people started writing articles, even though it said "Tether," it was the name of the program, by the way, Apple approved it, and then pulled it after a number of articles were written about it. So I really don't - I think that's very clear evidence, two pieces, and I'm sure there's more, that Apple is not paying the kind of attention to the stuff that it's approving that you would expect.

Steve: Yeah, I don't think that they...

Leo: They can't.

Steve: I don't think that they can, yeah.

Leo: They can't. There's too much. So I don't think there's 246 pieces of malware in the Apple Store, but I don't think there's no malware. I don't think that that means there's no malware. I think the good news on both Android and iPhone, the thing that I would say is important is, A, they all have kill switches. So when malware is found it can be deleted immediately from your phone. They can reach into your phone and take it. And the second thing is I think that they are taking a little care in designing these mobile platforms with sandboxing and so forth, Apple perhaps more so than Android. But I think that that is going to make these less attractive in the long run because it's just not as easy.

Steve: Yes, and I think we're in the early days. And as this quote indicated, they are taking advantages of known problems which still exist. So it's the typical malware-antimalware, cat-and-mouse game, where these platforms need to be updated in order to close some of these holes. The takeaway is very similar, though, to the takeaway with today's drive-by phishing and email and link-clicking. We tell people, do not click on links, no matter how tasty-looking they are, in unsolicited email that you receive. That's the way most systems, most desktop systems are getting infected. And so I would say, fun as it is to run every application which presents itself as "run me, run me" on your Android phone, you just don't want to do that. I would say be careful.

Leo: Well, that's for sure true. And...

Steve: Be careful about what you run and what you...

Leo: There's even a greater risk on Android because they have a checkbox in the preferences that says, "Is it okay to install apps from third-party, not just the marketplace?" And while they do warn you, and when you check it, it says, "Now, you understand this is risky," most people do turn it on because there's a lot of great stuff you can get at third-party sources. You'd have to jailbreak an iPhone to do that.

Steve: Yeah. So again, the takeaway is, I mean, sure, if you've got a platform that is your toy, and you don't have information there, you're not using it for anything serious, you want to just mess with it, then fine. Load everything you want to. But if you're a serious user, you've got contacts and address books and you do go to sensitive sites, you use this as your multipurpose platform, then today's equivalent risk to clicking on links in unsolicited email over in, not only Android, but also the iOS platform, is apps. Those are the things you need to be careful about. And so don't just go running around being promiscuous and loading everything you can get your hands on because it is a magnet for malicious activity. And so that's really the takeaway that I wanted to offer. And that is what Bruce was - that's the point that Bruce was making.

Leo: Right. It's not, by the way, 472 apps, I misspoke, it was a 472 percent increase.

Steve: Correct.

Leo: Which is a weird number. I'd like to know what the number of apps is. Because if it's four apps, that means there's 17. If there's one app, it means there's five. I mean, what is that number?

Steve: That's a very good point, yes. Although...

Leo: I hate it when they do that. And, you know, it's always malware companies that do that because they want to scare the hell out of you. I don't know if Juniper Networks sells any malware, but - they do, okay. So consider the source.

Steve: Yeah, yeah. Which doesn't mean it's wrong. And the takeaway is...

Leo: No. But that's interesting to give a percentage, not a number. Right?

Steve: Okay.

Leo: I think. It's very interesting. I'd like to know the number.

Steve: Okay. Everybody, just be careful with the apps you load.

Leo: Yes. No, no, the message is absolutely valid. I just don't want people to get terrified because there's a 472 percent increase.

Steve: So Brian Krebs, our illustrious security blogger, has noted in a recent blog that I thought was interesting - I wanted to remind people about Java because he noted that a new exploit that takes advantage of a recently patched, critical security flaw in Java is making the rounds in the criminal underground. Which is what Brian really does, he does a great job of keeping an eye on what's going on among all of the exploit forums on the 'Net. And he says this exploit which appears to work against all but the latest versions of Java is being folded into automated attack tools. And that's what I find really significant. He said the exploit attacks a vulnerability that exists in Oracle Java, the JDK and the Runtime 7 and 6 Update 27 and earlier. So it's only the latest one, Update 29, and Java 7, which is still not quite released yet, Update 1, that are secure.

So I'll remind our listeners, you can just go to Java.com, and that's the site where this can be found, just Java.com. And there's a link that is "Do I have Java?" which I like because it's not going to install the latest version if you don't have it. It checks to see whether you have it, and then you can check to see whether you've got the latest version. So what's happening is this critical security flaw, by having it moving into the automated attack tools, it then gets just incorporated sort of automatically into all of these things that the bad guys are using for getting into our machines. And that's where we begin to see the prevalence of its usage increase. So just further reason to make sure, if you've got Java installed on your machine, that it is Update 29 or - that is, Java 6 Update 29 or Java 7 Update 1.

And that reminded me that we hadn't talked about Firesheep for a while. And so I thought, because that was the classic, super simple, you don't need to know anything about computers in order to acquire access through impersonation, for example, in an open WiFi environment, anybody's online sessions that are not being secured by SSL connections. So I just jumped over, and we are now at 1,980,000 downloads of Firesheep. So it was a little over a year ago that we talked about Firesheep. It was released on October 24th of 2010. So here we are toward the end of November, about a month and a year later, and it's almost at 2 million downloads. So, and remember, that's the thing, you just download it, and you go to an open WiFi, it runs for - it is an add-on to Firefox. And as you sit there in an open WiFi environment...

Leo: It's an amazing thing, yeah.

Steve: ...you start seeing people's faces popping in over on the left-hand bar.

Leo: I had it on my laptop for a long time. I finally took it off because I was just embarrassed that it was even running. I was afraid I'd get caught, to be honest.

Steve: Yeah, well, I mean, and it's freaky. You just open it, and then it's like, oh, yeah, there's that guy sitting over there.

Leo: It's just creepy, yeah.

Steve: Oh, and then - and there she is. And they're doing things with Yahoo!, like there's a lot of uses of Yahoo!, and a lot of Facebook, also. And...

Leo: Although I bet you that's better now that they're using HTTPS.

Steve: Yes, yes. And that's the key, is as these services have been moving to persistent HTTPS, largely inspired by now the year-old Firesheep, this is no longer as effective as it once was. But...

Leo: That would go in a "best of" except that it was a year ago. And you were so happy about Firesheep.

Steve: I was giddy.

Leo: You were giddy. And I was going, Steve? Really? Giddy? It sounds like a hacker tool. And you were absolutely right because you said, well, this is going to force the issue of HTTPS everywhere. And I think that you were absolutely right. And now Facebook does it, Twitter does it, Google does it. I think that's exactly - that was the impact.

Steve: Brian also - Brian Krebs - also blogged something that I thought was very interesting. And I think he coined the term "malvertising."

Leo: [Laughing] He's the only one to take credit for it, anyway.

Steve: He detected attempted malvertising on his own site.

Leo: Wow.

Steve: He was in an exclusive underground hacker forum, where he found some discussion among these hackers about buying ads on his site which were going to be deliberately infected with malware. And so he blogged, he said, "Members of an exclusive underground hacker forum recently sought to plant malware on KrebsOnSecurity.com..."

Leo: Guess they didn't know Brian was a member of the exclusive hacker forum.

Steve: Exactly, "...by paying to run tainted advertisements through the site's advertising network, which was Federated Media. The attack was unsuccessful, thanks to a variety of safeguards, but it highlights the challenges that many organizations face in combating the growing scourge of 'malvertising.'" So now we have malvertising.

Leo: [Laughing] It's interesting, though. It is an issue. And in fact we've see it before. It happened on MySpace all the time because people don't vet the advertising. They have automated systems that allow you to buy that advertising.

Steve: Yup. It's just, I mean, it is scary. It's a way that bad guys could say we want to target a specific site that has access to the kinds of viewers that they want.

I also wanted to bring to our listeners' attention that Yubico is having a holiday discount. Normally the YubiKeys are $25 each. For the holidays, I think through the end of the year, they have a 10-pack for $99.

Leo: Ten for - wow. That's a good deal.

Steve: Yes. So you get five white YubiKeys and five black YubiKeys, 10 for $99. I tweeted this, and I had some responses from people saying, hey, thanks. They're going to give them as Christmas presents since that brings the price down to $10 for a YubiKey. So you can give secure authentication for Christmas.

And there was a story about HP printers which I had on my list of things to get to, but I got so sucked into figuring out exactly how BrowserID was working that I didn't have a chance to go back and nail the story down. And maybe you heard about it, Leo. Somehow there's an Internet vulnerability on HP firmware which allows bad guys to change the firmware and shut down your printer over the Internet. So anyway...

Leo: Good lord.

Steve: I will track it down. Tom and I - Tom probably covered it on his daily news because I got a...

Leo: On TNT every weekend.

Steve: There was a lot of coverage on TNT. But anyway, I will, between now and next week, make time to follow up and figure out what that's all about. So everybody can stop sending me notes in Twitter because I've been getting a lot of notices about it. So I do, I wanted to let everyone know I know about it. I just haven't had a chance to nail it down.

Also, everyone knows from our talking about ultracapacitors that I'm interested in capacitors and transportation. So there was an interesting blurb about Mazda putting large capacitors in their next-year model cars, their 2012 cars. And they use the term "double layer capacitor" without ever explaining what it is. But it's clearly a very large capacitor. And so what they've done is clever. When the driver takes their foot off the accelerator, an alternator is engaged as part of the braking system to charge a large capacitor.

Now, an alternator will generate a varying voltage, so it could be much greater than the car's normal 12v DC operating voltage, which is just fine because you'd like to charge the capacitor to as high a voltage as possible. And then what's clever about this is it doesn't attempt to use the energy in the capacitor for automotive, that is, for motive force. That is, it doesn't turn the alternator into a motor and, like, dump the capacitor back into the drive train. So it's not trying to capture the momentum and then reinject it. Instead, it simply uses the charge in the capacitor for the car's electrical system, which I thought was kind of clever because you...

Leo: Oh, instead of the car battery.

Steve: Well, exactly. So it, well, actually the battery is there to, like, start the car. But normally it's the car's normal alternator is used to power all of the stuff going on in the car - the entertainment system, the multiple computers that we have, and anything else. Well, it turns out that that provides - all of the electrical demands on a contemporary car are enough that it substantially affects the car's gas mileage.

Leo: Oh, yeah. Absolutely, yeah.

Steve: And we know, for example, that, like, when you turn on the air compressor - now, that's both the compressor, but also the mechanical drag that the compressor has on the car. But the alternator itself, that normally runs the car's systems, is lowering the mileage. So Mazda has found that, if they use an alternator for braking and capture that energy in the capacitor, and then they use a DC-to-DC step-down converter to, like, step down whatever, essentially a voltage regulator, but an efficient one, to bleed that capacitor that stored the momentum during braking, to bleed that as 12v DC into the car's electrical system. That lightens the load on the alternator, which would otherwise be doing that, and substantially improves gas mileage. So, very cool.

Leo: Oh, cool. So it's not a hybrid. It's not an electric car. But by being more efficient in terms of its electrical system, you're more efficient with fuel.

Steve: Yeah. I mean, one of the things that you cringe about is we all have disc brakes on our car.

Leo: Right, and that's wasted energy, yeah.

Steve: Absolutely. They're heating up. They're smoking. They're just big clamps that just clamp down on this spinning disc and dissipate your energy in heat. And so it's like, wait a minute, that's really dumb because we burned all this gas, or maybe electricity, getting ourselves going. Then we throw it away in our disc brakes. So instead, let's electronically brake the car and capture that energy. Well, sometimes they capture it and then try to use it for automotive force. Here they're just using it for electricity, which ends up - and again, the reason that's neat is that all of these conversions are lossy. So it's a lossy process in the alternator to convert the mechanical momentum into electricity. It's lossy again to convert the electricity back into mechanical momentum in a motor to reaccelerate the car. So by saying, wait a minute, we're not going to accept that second phase of loss, we're going to use the electricity for electricity because we need that in the car, too, and that'll improve our mileage. I thought that just very clever.

Leo: You know, it's an interesting issue on electric cars is that modern gas engines generate so much heat that you can heat the car easily. You've got plenty of spare heat. But an electric engine they actually have to drain the batteries to heat the car. So these newer electric cars, they have to do all sorts of interesting things to get them heated without depleting the battery.

Steve: Ah, and heating is a very energy-consuming process.

Leo: Exactly. So most of them have got, for instance, seat heaters, which is a much more efficient way to heat you up.

Steve: Okay, I'm not - I'm going to skip all the jokes...

Leo: You've got a warm bottom, exactly. But you know what, it's not so bad. I like it.

Steve: So we have enjoyed over the last, it's been a while, tracking those intrepid little rovers around Mars, Spirit and Opportunity. We talked about it many times because those little suckers, a storm would come along and coat their little solar cells with dust, and then they'd stop for a while. But then the dust would get blown off, and they'd wake up, and everyone at JPL would pop some more champagne corks, and those little suckers just kept on going, roaming all over the place. So I wanted to note that the mega-rover was launched on Saturday by an unmanned Atlas V rocket, and it's now making an 8.5-month, 354 - wait, 354 miles? That can't be right.

Leo: Thousand, maybe? 354,000 miles? 354 million miles? Maybe million miles.

Steve: 354 times 10 to the question mark.

Leo: Yes.

Steve: But it's making a long trip to Mars. So it will be...

Leo: So definitely more than 340,000. Must be 354 million.

Steve: Got to be million.

Leo: Yeah, because it's - yeah. That's right.

Steve: Yeah, it's Mars. It's out there.

Leo: It's a long way, yeah.

Steve: So, and it's on its way. And so 8.5 months from now I'm sure this podcast will note its arrival. Now, remember that the way the two cute little rovers, Spirit and Opportunity, landed was that they inflated a bunch of balloons, and they were sort of in the middle of this big balloon thing that they just dropped on, I mean, there were some parachutes that brought it down close. Then basically it just sort of dropped it on Mars, and it bounced around and rolled for a while, and then the balloons deflated in a very clever system, which then got this whole balloon thing out of the way.

Well, this sucker, okay, this is - this weighs a ton, this new mega-rover. It's called the "MSL," the Mars Science Laboratory. And its name, in the same spirit of having Spirit and Opportunity, this one is called "Curiosity." So this is the Curiosity rover. It's a $2.5 billion mission. It weighs a ton. It's the size of a car. It is nuclear powered. It contains 10.6 pounds of radioactive plutonium for power.

Leo: That's a lot.

Steve: Yeah. So it's 10 feet long by 9 feet wide, although it's also, I mean, like, if you measured it, it's got that sort of articulated design where it's got wheels out at the end of little arms. It has a 10-foot arm with a jackhammer on the end, a 10-foot mast sticking straight up that has HD and laser cameras, and they said it's only supposed to, like, wander off around 10 miles or so. But they're dropping it using a new technology which everyone's holding their breath about. You can't drop this thing that weighs a ton using balloons. So they have a new approach for getting it down on Mars that involves some sort of a hooking system. I haven't - I didn't ever see any videos about it. We'll be talking about that 8.5 months from now.

So with any luck, it will be successful. Many missions to Mars fail. The JPL guys regard Mars as sort of the Bermuda Triangle of projects. In fact, I think Russia just screwed up and got - oh, it was in Earth orbit. They were trying to get to Mars, and whatever it is they were doing wouldn't leave Earth orbit. So it's like, whoops. Mars claimed another victim sort of indirectly. So I think that'll be fun, to keep an eye on Curiosity as it lands on the Red Planet.

Leo: It's going to be kind of neat. It looks like a flying saucer, by the way. Have you seen it?

Steve: Oh, no kidding.

Leo: Well, it's a ball. But it's, yeah, it definitely, if I - or ball-ish. If I were - this is kind of a UFO-looking device. I'm just looking at some video of it.

Steve: Well, if there are any Martians that are...

Leo: The Martians are going to say, "What the hell?"

Steve: They're going to go, "Wait a minute, that's a flying saucer. You're right."

Leo: It's true, there are other people out there.

Steve: Exactly. It's coming in the wrong direction, though, because those flying saucers were supposed to be from Mars, not going to Mars.

Leo: It is the strangest design for landing that I've ever seen. It's very intriguing. This is cool.

Steve: Yeah. Well, 8.5 months we will be tracking Curiosity.

Leo: I just love the ingenuity that's involved in all of this.

Steve: Oh, gosh, yes.

Leo: Yeah. So basically there's three parts to it. There's the flying saucer part. Then there will be a craft that will eject from the flying saucer. And then it will drop the rover via wires as it reenters. It's very interesting. Then it flies off.

Steve: So maybe - because I heard something about hooks. So maybe it's a skyhook technology.

Leo: It's like a skyhook, exactly.

Steve: So it's staying up in orbit and then lowering this thing down.

Leo: Well, it comes in. It does make an entry and has retrofire to keep it from crash landing. But once it gets close enough to the surface it drops the rover down via wires and then flies off. It's very interesting. So I guess they did - the last time, remember, they tried the bouncing ball. Remember they had it...

Steve: That was how Spirit and Opportunity landed.

Leo: Yeah, boing, boing, boing. This is something completely different. I just love the ingenuity. I think it's fascinating.

Steve: Well, speaking of ingenuity, I got a nice note from Samuel Gordon-Stewart. He said, "Steve and staff: SpinRite just saved me." Now, this is an interesting one. I don't know if I've talked about this, certainly not for a long time. He says, "I have an old DOS application which for years I've been running off my hard drive. I only need to use it occasionally. And when I went to use it today, I discovered that I'd accidentally deleted it, probably in my recent cleanout of files I supposedly didn't need. Clearly I did. So I whipped out the floppy disk which has the application and related files on it. I went to copy it to the hard drive and nearly had a heart attack when it would no longer copy. Windows couldn't read the main executable. I took this as an opportunity to do something I've been meaning to do for a while. I bought SpinRite."

Leo: Yay.

Steve: "I let it loose on the floppy disk. It went a few minutes working, then dropped into DynaStat in various places. When I got back into Windows, I was able to copy the disk to the hard drive. I don't think it's possible to get a replacement copy for this DOS application that I'm using these days, so the $89 I spent on SpinRite bought me enough time to get the files one last time off the diskette, and saved me an awful lot of trouble. Thanks, Steve. SpinRite is fantastic. Regards, Samuel Gordon-Stewart in Canberra."

Leo: Yay. Yay.

Steve: So anyway, I want to remind people - not that many people use floppies any longer, I realize that. But it does a great job of recovering contents of diskettes, which are often, after a long time, no longer readable.

Leo: Stale. I never thought of it for that.

Steve: Yeah.

Leo: Intriguing. All right. BrowserID. I'm ready for some free beer, Steve.

Steve: So, now, that sounds like a little bit of a non sequitur...

Leo: He'll explain. He'll explain.

Steve: ...to those who weren't listening before we began recording. We have a couple things, some fun takeaways for our listeners, some places to go, some things to do. We've talked about identity and authentication often on this podcast because, as everyone knows, I think it's, like, THE big problem we need to solve: How do the services that we want to use on the Internet know that we are who we say we are? We talked about VeriSign, the PayPal football, of course YubiKey I just talked about again, a one-time password system. I've spent a lot of time developing my own Perfect Paper Passwords, and of course now the Off The Grid paper-based crypto system. We've talked about OpenID and OpenAuth. LastPass, of course, is still the system that I'm using largely.

Well, there's another entry into the game that's only a few months old and was recently launched by the Mozilla folks, the people of course who famously brought us the Firefox browser and some email clients and so forth. And this is called - they call it BrowserID. The thing that I like about this is that it is 100 percent open source. It's open everything, nonproprietary. It is cross-browser. It is incredibly easy, not only for the user to use, but for a website to decide they want to support, that is, in order - if they wish to allow users to authenticate to them, to log in with a verifiable identity.

They could create their own - create an account with us, what's your username, what's your email address. We'll send you email. Click on the link to confirm your email. What's your password? And that's what all websites traditionally have been doing. We end up, of course, with this problem that we're having to create identities, often with an email address, often with a password, individually for all these websites. How much nicer would it be if there was some central means for doing this?

So we're beginning to see this. I'm happy, for example - although I'm unhappy, as we've talked about often, with PayPal, I'm happy every time I go somewhere and I see PayPal as an option in order to purchase something because it's like, oh, yay, I don't have to give this site that I may not trust my purchasing information. They'll use PayPal as my purchasing provider. So that's a benefit for me.

Similarly, we're now seeing sites that are saying you can log in using your Facebook identity, log in using Google or using Twitter or Facebook. Well, now, in that instance, they're using OpenID or OpenAuth in order to use the fact that some other service knows who you are. And we have talked about that extensively. We've covered those technologies before.

So what the Mozilla guys decided was, okay, let's see what's the simplest thing we can use? And they thought about it and decided, well, that's our email address. The email address is something all of us have at least one of, many cases multiple of. And in fact, it is the thing that we are constantly proving we have control of because that's the way we do password recovery. If you lose your password, then email me a link that I can use in order to recover it. The point is, control of our email address is already the lowest common denominator. That's what everything else falls back to if all else fails, if we forget our credentials, if we don't remember what our username was or our password. It's like, okay, well, send it to my email account. And it's because I uniquely have control of that, that's like the, well, I already said it, the lowest common denominator.

So the Mozilla guys said, okay, let's stop there. Let's not go any further. Let's use that which we already have as the means for identifying users. So, Leo, before we began recording, I asked you to go to a demo site which these guys have set up, sort of tongue-in-cheek, but it's a nice example of how this works. And it is MyFavoriteBeer.org. So I would encourage our listeners to do this, too, anyone who's interested about this. I played the game. I did this. And I have to say I was surprised, when I understood what was going on behind the scenes, which I will be describing in a minute, but how transparent this was, how easy this was to do.

So go to MyFavoriteBeer.org, and it's a site, sort of like a sample site, like any site could be, that has decided to support the Mozilla BrowserID system. And when you bring up MyFavoriteBeer.org, up in the upper right is just a little icon that says "Sign in." If you do that, you're presented with a dialogue asking for an email address which you want to use as your identity. Part of the system is that you can use as many email addresses as you have chosen to set up, one or multiple. If the browser knows that you have authenticated more than one email address, then it'll give you a list of them, and you can decide which identity, that is, email identity, you choose to use, that is, you choose to present as your login for that site.

So what happens with MyFavoriteBeer.org is, if you haven't yet created a BrowserID identity, and you typically wouldn't have by then, you would give it an email address that you control and submit that. It would explain that it is going to send that address a link which you need to click in order to prove your ownership of that email account. So that's the typical email account authentication loop that we're all familiar with doing whenever we're needing to prove we own, we have ownership of this email address.

So then you check your email client. It will have emailed you a link, which you click, and that confirms your ownership. And of course the link's got some crypto gobbledy-gook in it, just a big UUID-style token which is used one time because only you, who controls that email address, would be able to know what that token is and then click on the link in order to authenticate.

So the act of doing that works with JavaScript that's running in your browser and with asymmetric keys. The browser generates a public and private key, given the fact that it has gotten verification that you own this email address. And using HTML5 local private storage, it's able to maintain that. Essentially your browser then stores this private key and the email address that has been associated. There are a number of ways that the public key can be stored. For example, there is BrowserID.org is a facility that will maintain, on behalf of users, their email address and public keys that allow other sites to query them for the public key.

So the browser maintains a set of email addresses and the private key. And the browser creates this asymmetric key pair which is then authenticated through this email loop in order to create certificates, which it keeps. Then, if you want to log into a website that supports BrowserID, the website will just show you a little login and typically say you could use BrowserID in order to log into me, much like this MyFavoriteBeer.org site does. And you're simply presented with, when you click the login, a list of any email addresses which your browser has had confirmed for it, and you log in. It's that simple. So you are spared from the per site login problems. You have authenticated that you control the email address.

Now, the website that you're logging into can essentially make a query to the site that contains the public key that matches in order to verify your certificate. So there is a trusted third party which can - and there can be as many of them as you like. You can choose who you want to use to store your credentials. You could store them yourself. And in fact it is possible for email systems themselves to support this BrowserID protocol. That is, as part of this trusted email technology, there is a facility where you would not need a third party at all, that is, the actual email service can provide this certificate signing and storage and verify email ownership to third parties.

So essentially that's the way the system works is, I mean, it's almost spooky how simple this is, yet the Mozilla guys have come up with a simple way of binding an email address to a private key which the browser holds. And then any website that you want to authenticate to is able to receive that certificate, essentially, from your browser, which asserts that you are who you are, that is, that you have proven your ownership of this email identity. It then queries the trusted third party that you have associated with that to get your public key, which it uses to verify the signature, and that's all there is to it. So it ends up being very easy to use.

So let's stand back a bit and look at this compared to the other guys, that is, the other technologies that we've talked about. We've talked about VeriSign, which is a proprietary system where they do have both software and hardware tokens. The software tokens, for example, running in a smartphone are no charge to the user. The hardware tokens, like the football or the credit card are not free, so you have to buy them once. But then using them is no charge to the user, although it is very expensive to actually use the system. That is, anyone who supports the VeriSign authentication is paying a substantial cost per authentication. So that's VeriSign's proprietary model for making money on their VIP, their VeriSign Identity Provider technology.

YubiKey, of course, is a favorite of ours. There you purchase the one-time password hardware, which is the little USB key token. You buy that once, and you own it, and they provide free authentication forever. So you get multifactor authentication. You get zero per use cost. Anyone who wants to support it is able to accept a YubiKey login and then use the YubiKey server infrastructure in order to provide the multifactor authentication on the fly. It is supported by other authenticators. For example, LastPass is able to use the YubiKey. And didn't I remember that Gmail started using it? Google now...

Leo: They have a second-factor authentication.

Steve: Oh, no, wait, they have their own.

Leo: They have their own. They have that Authenticator, the Google Authenticator.

Steve: Right, right. So they have their own.

Leo: Which actually, I mean, as much as I love the YubiKey, the idea of having it in my cell phone is so much easier.

Steve: Yes. Yes. And then there's OpenID and OpenAuth, which is gaining traction pretty rapidly.

Leo: Good, because it's a good system.

Steve: It really is a good system. Version 2 of OpenID is secure. It solved a problem that v1 had. And we're seeing more and more people saying, oh, you can, if you want to, log in using your Facebook identity or using your Twitter identity or using your Google identity. So those services - Twitter, Facebook, Google, and many others - are identity providers that allow you to, essentially, your browser bounces, behind the scenes, bounces an authentication off of them. And if you're logged in with them currently, it's transparent. You may need to log in on the fly. If you're not already logged in with them, then they'll confirm your authentication with them and then provide that back to the site that you're wanting to log in on. So that's got broad and growing support.

There's a little privacy concern inasmuch as that, like, they know, "they" serving as your authentication provider, know the sites that you're visiting because you are bouncing - that site is making a query of them, and then they're providing the authentication information back. So there is a little bit of that, although in the BrowserID model that I mentioned, by default there is that also. That is, the site that you're logging into with BrowserID is pinging your trusted third party in order to get your public key for verification.

It is possible to avoid that, and that is to have - and the way that's done is that you can have your browser contain that authentication with, for example, a time limit where you can say this is good for a week of no additional authentication use. It then has that signed with a time limit. And so the public key of the authenticator is used to verify the signature, rather than the individual's public key. So then you're not - the site you're logging into isn't querying for your credentials, they're just querying for the authenticator's signature, very much the way our public key system works now, where you're just getting the private key of the certificate authority and verifying that it signed the identity certificate.

And so of course in addition we have LastPass. So LastPass is cross-browser. It gives us cloud synching, so our instances of LastPass running on all of our various devices uses the 'Net and the cloud for keeping all of itself synched. The advantage it has, of course, is that it requires no support at all from websites. That is, everything is centralized in the browser. We're able to use different complex usernames and passwords for every site. It's kept cryptographically stored in the browser with no per site support required. So in that sense it's universal today. I lost my train of thought.

Leo: But I'm just glad that it's not Mozilla.org only. I do wish, I mean, how does it integrate with OpenID? Is it a completely separate system? Because, I mean, that's what bugs me. We have an open standard, if everybody would just get behind it. Is this better in some way?

Steve: Yeah. So I think what's going to happen is that we will end up with a smorgasbord of solutions for a while.

Leo: Yeah. That's no good.

Steve: Well, the Mozilla guys are going to end up tossing their hat in the ring, too. They will be building it into Firefox. And there is a video that we really should take a look at. I don't think it makes sense because we have largely an audio listenership here...

Leo: I could just show it in the background.

Steve: It's on YouTube. And if you search YouTube for "BrowserID," it's a beautiful example of this system working. And it makes a compelling case for once this is integrated into our browser, because after all the browser is the client that we're using as our interface to all these services. For example, they will be, Mozilla will be building this into the so-called "the chrome," that is, all of the user interface of the browser. The user's identity as their email address will show to the left of the URL, sort of in front of the URL...

Leo: If you're using a supporting browser.

Steve: If you're, well, yeah. Well, in Firefox it'll be built in. Now, again, this is all open source. Any browsers who wanted to could support it. You don't need - it runs, it's able to run just using JavaScript. So, for example, right now it runs on Safari and Chrome and IE and Firefox everywhere. That is, the existing BrowserID does. But it can be integrated more deeply into the browser to give you a more seamless experience. And you can, if you want to, you can establish your credentials once with your browser; and then, as you go to other sites that want you to log in which support BrowserID, it could be made transparent.

So, and again, you need to fit this with the use case. For example, I'm the only one using my machine. I'm the only one using my various laptops. So, and I have those secured. So once I'm using them, I'm happy with my identity being authenticated painlessly. There are other people who do want, like, to use their YubiKey every single time they log in, or they want to reauthenticate to LastPass in order to allow LastPass to securely log them into other sites. So I believe, based on what I've seen, this has a good chance of gaining some traction. But as you said, Leo, there's already some alternatives.

Leo: Yeah. We support a number of choices. And unfortunately, the marketplace is supporting Facebook Connect, which is the least good choice here. But every website in the world now, including ours, I hate to say it, because of user demand, will allow you to authenticate with Facebook Connect.

Steve: Yeah. So probably it would be better if more options were made available. And maybe that's what'll happen. For example, if BrowserID being pushed by Mozilla is picked up, I don't know if it would be competing with what Google is doing. It would be great if, for example, if Chrome were to build this in, too. I have sort of seen some Google and Mozilla - the sense that they're working together, which is a nice thing to see. So...

Leo: I just think OpenID is there. It's open. We support it. Maybe not a whole lot of sites support it, but we support it. And I just - I think that's the one that we should choose.

Steve: Well, okay. What you need, though, in order to use OpenID, is you need to be known to some other service.

Leo: Oh, that's a - yeah. That's a good point. And so this doesn't need that.

Steve: No. This doesn't.

Leo: See, that is a good point. You store the authentication credentials on your own system.

Steve: Correct.

Leo: Yeah. That is a good point. That's the one - you have to use an OpenID provider. I mean, I use my own website because I have a website. But if you don't have your own website, you have to use an OpenID provider.

Steve: Right.

Leo: That is a disadvantage. You're right.

Steve: So it'll be interesting to see what this does. I wanted to mention it because it's got the Mozilla guys behind it. Firefox is pushing it. What I could see, again, is that sophisticated users end up with a hybrid. That is, maybe if people are using Firefox or even Chrome, because it is compatible, Firefox is going to be very friendly with BrowserID. And it's so simple to set this up. You verify that you control this email address, and basically you're done. Then, if sites begin supporting browser ID, that will then start to pull it. And I wouldn't have a problem at all if it ended up winning in the long term, that is, if Facebook Connect was sort of an interim solution, but something that just sort of was even easier to use, and secure, and more private because, as you may have heard, Leo, Facebook is now getting a lot of privacy auditing scrutiny over concerns that they're not doing as good a job as they should with the privacy of their users. The advantage they have, of course, is such a massive user base.

Leo: Well, yeah. And regardless of how you feel about whether Facebook protects us or not, no private company - Microsoft, Facebook, or Google - should manage this. It's got to be an open and nonproprietary solution.

Steve: Agnostic and nonproprietary, exactly.

Leo: So, I mean, at least Mozilla's an open source foundation and all of that stuff. They're not a not-for-profit. I mean, they're highly profitable. But I trust them a lot more than I trust Facebook. Maybe there's a way for OpenID to work with BrowserID, and then that would be a good standard I would support. I guess, I mean, I support this. This is good. You're right. We need - at least we need a number of choices until one determines - becomes the standard.

Steve: Right. And that's what I think will happen. I think we'll, I mean, Firefox has - I mean, even though a lot of us have moved to Chrome, Firefox is still my primary browser. It's got a strong following. If sites begin to support BrowserID, I mean, it is so easy to use and just so transparent, while being secure, that that could give it some traction. I mean, we're still at the early days here. Anyway, I wanted to put it on the map of our listeners. I have no doubt we'll be talking about it in the future. Maybe it'll just end up being something that dies and never goes any further. But the Mozilla guys are excited about it. I like the fact that it is very straightforward. It uses simple, well understood crypto. It's open and standards-based and gives us, when it's in place, it gives us a very simple-to-use solution. And it's trivial to have it in place.

Leo: Right. I like that. I like that. The problem is I don't use Mozilla. Is there a Chrome plug-in I can use?

Steve: You don't even need to. You just did it, Leo.

Leo: I did do it. I have it. I'm done.

Steve: Yeah. Now, if you were log out of MyFavoriteBeer.org and then log back in, I mean, then go back to MyFavoriteBeer.org, you can log in using BrowserID.

Leo: I am on Chrome. You're right. It says, "Sign in using Leoville.com." I sign in, and now I'm here.

Steve: That's all there is to it.

Leo: And it even got my picture. I don't know where it got that.

Steve: You did a full secure cryptographic login. I mean, it is shockingly nice. And I would love our listeners to put "BrowserID" into YouTube and look at the demo. The demo from these guys makes it - it gives you a good sense, better than I can in an audio podcast, just for how seamless and transparent this ends up being. I mean, what you did, Leo, is all there is to it. And that's now persistent and sticky, and you can log out and log back in just that easily.

Leo: Good.

Steve: It really does work.

Leo: You, as always, turn us on to the most interesting, and not merely interesting, but important stuff. And I thank you for doing that, Steve.

Steve: Well, we'll see what happens with this. Again, we're in the Wild West. Lots of competing authentication approaches. We're covering them and keeping our listeners current with them. And we'll track them as they evolve.

Leo: This has been going on for so long, I mean, I go back to Microsoft doing this with their Passport single sign-on.

Steve: Right. [Buzzer sound]

Leo: I still, well, you know what's funny, when I log onto Live.com, that's what I use. It's the same address and password I've had for how many - I shouldn't say that. I should probably change the password now. But, I mean, I've been using that for all this time. And for a while it was useful because Microsoft owned Expedia, so I used that. Now they've got - they've weaned me off of it. They won't accept it anymore. And so more and more that's what's going to happen with anybody who has these old systems. Single sign-on is an issue, and I think we need it, and we need a secure system. And I think this, you know, this is a contender. I'll give you that.

Steve: Yeah. I mean, what I like - we have LastPass now because it requires no support from the service that you're logging onto. It puts it all over on the browser side. But over time I think what we're going to see is we're going to see - and this is what the stats have shown. For example, blogging, like sites that require you to log in in order to post a comment, if they give you the option of logging in using your Facebook Connect or using other accounts, I wouldn't be at all surprised if they add BrowserID to that because it is also simple for them to add this to their own site.

I mean, the Mozilla guys have done a fabulous job, both on the user experience side and on the so-called "relying party side," on the side of the relying party that wants to rely on the authentication. They've made it incredibly easy to add this. So what has been seen is that, when you make it easy to log into these, like, throwaway logins, not having to create an account, you just, oh, login using Facebook, more people post. More people get involved. And so it behooves sites to make it easy to log in without having to create accounts for that site. And so that's one of the ways that these alternative single sign-on systems will gain traction.

Leo: Yeah, yeah. I'm with you. Steve does this show, we do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, 1900 UTC, at TWiT.tv. I won't be here next week. Tom Merritt will be filling in as a...

Steve: We'll do a...

Leo: Yeah, we'll...

Steve: I was going to say, we'll do a Q&A with Tom next week.

Leo: Yeah. Sarah and I will be in Paris for TWiT in Paris for LeWeb. That's going to be a lot of fun.

Steve: TWiT in Paris.

Leo: TWiT in Paris. Tom and Iyaz and others will hold down the fort for us while we're gone. And we will be broadcasting, I should mention, 6:00 a.m. to 10:00 a.m. Pacific time, something like that, maybe 5:00 a.m. And then we'll rebroadcast those. We'll package them up and put them out as specials. But there are so many big names who are going to be at this event: Phil Libin from Evernote, Kevin Rose will be there, Dave Morin of Path, there's so many interesting people. We're going to interview them all, and you'll get a chance to see them. So there's a chance - it's funny. We're going to Paris to meet the biggest names in U.S. entrepreneurship. You'll get to see those interviews on TWiT next week.

Let's see. What else should I tell you? Oh, I've conferred with Eileen. She likes the idea of a sci-fi special.

Steve: Yay.

Leo: It's going to be a scheduling issue because then I come back from Paris, and then I leave on the 20th for Christmas vacation. So we'll figure this out. I won't be here on the 21st for our show, either. Tom will be doing that, as well.

Steve: Okay.

Leo: But Tom would be good for a sci-fi special because you know he does Sword and Laser. He does a sci-fi podcast. So he's an expert on all this stuff. But if we can work it out, I want to be here. If we can, we'll do it with you and me. Otherwise it'll be you and Tom.

Steve: Yeah. And you and I have such a history of discussing all of the things that we've found, and you know Hamilton so well and so forth.

Leo: Right. We'll figure it out. Tom might bring something to the table, though. He's always good for this stuff. What else can I tell you? GRC.com's the place to go to find Steve's software, SpinRite, the world's best hard drive recovery and maintenance utility. You've got to have SpinRite. But you should also check out all his free stuff there. Somebody was asking how it goes with - which project was it?

Was it - Off The Grid, I think it was. That's done; right?

Steve: Yeah. In fact, I finished the final printing page yesterday, and I removed the "This page is under construction" or whatever it was that I had said up at the top. That's gone now. The Off The Grid printing is absolutely finalized. I need to get - it's still not linked into the main menu, so you have to go to GRC.com/offthegrid in order to find it. You can't get there through the menu because I want to - I need to now just finish up the rest of the web pages, all the documentation. But it's completely wrapped up, so I'm really pleased with that.

Leo: Yay.

Steve: Yay.

Leo: Yay. When you go there, you'll also find a feedback form so that you can ask questions for next week's episode, GRC.com/feedback; 16Kb versions of the show for the audio bandwidth-impaired; full transcriptions, too, that's even more compact if you just want to read the transcription. Steve makes both of those available. We've got audio and video available at TWiT.tv. Thank you, Steve. Great show. Really interesting stuff, I thought.

Steve: Yeah. This is important. Someday we'll look back on this and think, wow, that's the way they used to do things? That's so strange.

Leo: [Geezer voice] In those days - you know, now I just put my nose against the screen, and it knows it's me. Okay, thanks, Tom.

Steve: Thanks, Leo.

Leo: Tom. Thanks, Steve. Tom will be here next week. And have a great week. And we'll see you next time on Security Now!.