Ali Baba's Cave ... and Zero-Knowledge Interactive Proofs

Description: After catching up with an eventful week of security news, Steve and Leo explore a variant of the story of "Ali Baba's Cave" as a means for clearly explaining the operation and requirements of cryptographic Zero-Knowledge Interactive Proofs.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-363.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-363-lq.mp3

SHOW TEASE: It's time for Security Now! with Steve Gibson. I got an email yesterday from Dropbox saying "We have changed your password." What's going on at Dropbox? Steve will talk about it. Plus a bedtime story, all about Ali Baba's Cave and Zero Knowledge. It's all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 363, recorded August 1st, 2012: Ali Baba's Cave.

It's time for Security Now!. Get ready. We're going to protect your security and privacy online with this guy right here, the Explainer in Chief, Mr. Steve Gibson of GRC.com, the Gibson Research Corporation. You've probably heard the name. Steve's been around the industry for years, going back to the first Apple II Light Pen, which he created. He also wrote great columns. What was the name of your InfoWorld column? Was it InfoWorld?

Steve Gibson: It was Tech Talk.

Leo: Tech Talk. I miss that.

Steve: The original concept, the name I had was Behind the Screens, which I kind of thought was fun.

Leo: Yeah, I like that.

Steve: But CompuServe, of all people - that sort of dates us - CompuServe claimed that they contacted the InfoWorld publishers and said, "We have a trademark on 'Behind the

Screens.' We'd like you not to use it."

Leo: See, this has been going on since years ago, folks.

Steve: Yeah.

Leo: Nothing new. Well, I like it. And did you - I know you were thinking at one point of making an eBook, compiling all of those. Did you ever do that?

Steve: Never "e." I did republish the first - I had co-publication rights from the beginning with InfoWorld. That was my deal is that I just wanted to be able to do something with them in the future, which always seems to be my approach. And so I did publish "A Passion for Technology," was the name of the series.

Leo: That's right, yeah.

Steve: Yeah, it was five books that were the first five of the eight years that I did it. And I went back and added more, of course. I added diagrams because they were just, for a weekly column, they didn't have the budget or the personnel or whatever to create diagrams for publication. So there are often times where a picture really helped the explanation. And so I added graphics to almost every one of the columns to also give people something they hadn't had before. And it was all printed on acid-free, archival-grade, museum-grade paper. We made a couple tens of thousands of sets and sold them for years. And somewhere I have them.

Leo: I was going to say, can you still get them?

Steve: I mean, the books are out of print, but I do have all of that text.

Leo: eBook.

Steve: It was - are you ready for this? - Ventura Publisher was the publication program that I used for doing the computer-to-print. And that's around somewhere. So I have thought it would be really neat to get them all up on the website. I wouldn't sell them. I'd just make them available.

Leo: Maybe an eBook. The real problem's going to be getting that out of Ventura. It's a technical issue.

Steve: Oh, it's a challenge, Leo. I want it.

Leo: You might have to write some code.

Steve: Gives me something to do.

Leo: All right. What are we talking - I see the name of the show on the screen: Ali Baba's Cave. What are we doing today?

Steve: Well, I promised everyone I would give them something to think about. And we have touched on, several times, we've touched on the terminology and some of the concepts underlying some cryptographic concepts known as "zero-knowledge interactive proofs." A zero-knowledge interactive proof is something that fascinates cryptographers. And in fact it's recently become of greater interest because of this approaching threat of quantum computing. The idea is you want to - we have two people. In traditional crypto parlance, we have Alice and Bob, A and B. And sometimes C, we have Carol. We bring Carol in. But those are the names all the cryptographers universally use to describe interactions between people who are exchanging secrets or needing to agree on cryptographically secure tokens and so forth. We have Alice, Bob, and Carol. And then I think it's Doug or Dave.

Anyway, in the case of zero-knowledge interactive proofs, we have Peggy and Victor are the standard players. Peggy is the prover, and Victor is the verifier. And the idea is Peggy wants to prove that she has knowledge of something without giving any of it away. So she wants to prove to Victor, the verifier - Victor is the verifier. She wants to prove something without divulging any of its content. So there's the traditional Ali Baba and the 40 Thieves myth, but there's a variation of it which can be used to explain these concepts. So that's what we're going to do today is we're going to explore Ali Baba's cave.

Leo: Wow. So this is one that you really want to put your thinking caps on for because we're going to involve your mind. No passive listening on this one.

Steve: Yeah. What's happened is, because this has become important, the concept of zero-knowledge interactive proofs has been formalized. And when academic people formalize stuff, they create very clear, careful definitions. And the trickiest thing is the definition of what it means to have zero knowledge communicated. And the end of the story that I'm going to tell...

Leo: I love this.

Steve: ...is about that.

Leo: This is great. This is great.

Steve: Yeah. This is going to be fun.

Leo: This is the thing I think people love most about this show is the fact that this is a smart show. You really learn something out of this show. I love it. I can't wait. Well, let me take...

Steve: Now, speaking - oh.

Leo: Go ahead.

Steve: There are some people who have not learned something.

Leo: And we'll find out.

Steve: Dropbox and, let's see, Dropbox and Tesco. It's a large supermarket chain.

Leo: Okay. Because I got an email from Dropbox which I forwarded to you.

Steve: Yup, and you were not alone. So we will talk about that in a moment.

Leo: I was very curious. I'm so glad you're going to cover this because I was trying to figure out, why are they saying this? Anyway, we'll talk about that in a second. So what's the Dropbox deal? I'm dying to know. I got an email, in fact I could show this, from Dropbox, that said "Change your password." But they did something that kind of puzzled me.

Steve: Well, okay. So we discussed on the podcast a couple weeks ago that there was something going on because Dropbox users who have control of their email accounts and are able to create aliases for themselves whenever they need to, they were receiving spam on email accounts that they had specifically created for their Dropbox accounts and for no other purpose.

Leo: Right.

Steve: Which led us to believe that there had been some problem at Dropbox which Dropbox was not talking about. So just yesterday, on July 31st, there was finally a posting on the Dropbox blog. It reads:

"A couple of weeks ago we started getting emails from some users about spam they were receiving at email addresses used only for Dropbox. We've been working hard to get to the bottom of this and want to give you an update.

"Our investigation found that usernames and passwords recently stolen from other websites were being used to sign in to a small number of Dropbox accounts. We've contacted these users and have helped them protect their accounts. A stolen password" -

here it gets interesting. "A stolen password was also used to access an employee Dropbox account containing a project document with user email addresses." So it wasn't just externally stolen account information that was being reused, but one of those happened to be an employee. Meaning that an employee of Dropbox...

Leo: Was compromised.

Steve: Yes, was compromised by reusing the same password that he used for his own Dropbox, Dropbox account as he used somewhere else. So they say: "We believe this improper access is what led to the spam. We're sorry about this and have put additional controls in place to help make sure it doesn't happen again. Keeping Dropbox secure is at the heart of what we do, and we're taking steps to improve the safety of your Dropbox even if your password is stolen, including: two-factor authentication, a way to optionally require two proofs of identity (such as your password and a temporary code sent to your phone) when signing in." And they said "coming in a few weeks." Also, "New automated mechanisms to identify suspicious activity. We'll continue to add more of these over time." And, "A new page that lets you examine all active logins to your account." And, finally, "In some cases, we may require you to change your password, for example, if it's commonly used or has not been changed in a long time."

Leo: Okay. That's BS.

Steve: I know.

Leo: I'm going to call BS on this...

Steve: I know.

Leo: ...because I have to, I use a unique generated password for Dropbox that's not used anywhere else. It's a very strong password, and they have changed it on me, at great annoyance to me because we use this for our corporate account. I have to go all over the place and change it in many locations. This is proactively keeping me safe. You idiots.

Steve: What would be interesting to know whether...

Leo: They must have been compromised.

Steve: ...or how widespread this is because what they may actually...

Leo: I think they changed everybody's passwords.

Steve: Right.

Leo: And that tells me they got compromised in a much more serious way than they're acknowledging.

Steve: Right. I'm afraid...

Leo: Right?

Steve: ...that, reading between the lines, that's what I would have to assume.

Leo: Why change my password, a good, strong, unique password, why change all these people's passwords if the only issue is a few people used the same password on multiple sites and they were hacked, or you've got your email address leaked out by our employee was hacked. Neither of those justify changing everybody's password. Certainly not mine.

Steve: Well, I was going to say, neither of those explain why you received that email because...

Leo: Well, now, Bear is saying he didn't get that email. Many people in the chatroom are saying that they did not get that. So it wasn't for everybody. All right. I thought it was for everybody. But then I'm wondering why it's for me. Maybe because I haven't changed the password in a year? I don't know. But it's a strong password. Believe me, if you saw this password - I looked at it. It was generated, I'm not sure if it was generated by 1Password, or it probably was generated by LastPass. It's 12 characters, random numbers, letters, special characters. There's no way it's not a strong password.

Steve: Well, and in following up on this, I, when I went to Dropbox, LastPass jumped in and logged me on. And I did not receive any email from them. But I also tend to obsolete my email addresses occasionally. And so I thought, well, okay, maybe they tried to send me something, but it bounced. So I still have an email address, and LastPass knows how to log me in. But it's not a current email. But it sounds like, from what you're saying, that that many people are getting this, but not everybody is getting it.

Leo: So even if they leaked my email address, that didn't mean they leaked the password. So I just have to think there's more than they're admitting here. Or they're being, I think, overly, well, you tell me. You're the security expert. If I haven't changed my password in a year, but it is a strong password, is there - we've had this discussion.

Steve: Yeah. I just - I don't buy this notion that a really, really good password should be forced to be changed. Well, okay. Right. I interrupted myself. I don't think - I don't buy the idea that there's any benefit at all to be gained from periodically being forced to change a really good, strong password. I don't see it. The only reason would be if, in the background, somebody is persistently trying to crack it and doing a brute-force attack,

and someday they're going to get there. But then you could say, okay, the only benefit of changing it would be if I changed it to something that they had already tried so that this brute-forcer wasn't going to still stumble upon the new one. I mean, there's no benefit.

Leo: In my opinion, the only reason that you could reasonably say, "Change your password, Leo," is if they knew or thought or suspected or were worried that my password had been compromised, which means that they have in some way been compromised and have not yet copped to it. That's the only thing I can understand. Because with a service like a Dropbox, it's a real hardship because it's not just one machine.

Steve: Right.

Leo: It's all over the place. I'm going to have failures, intermittent failures in all sorts of places that I don't even know about because this is our company account. There's nothing personal on here. It's completely stuff we share with each other. But I have it on I don't know how many machines. It's just driving me crazy. It's just unacceptable, I think.

Steve: Well, they're big. And they've made mistakes in the past. We talked about, remember, when due to a problem they had about a year ago, you could use any logon you wanted in order to access someone's account. It wasn't checking the password at all. You could just type "noodles" in as your password, and you'd get in. So it's like, whoops, not good.

Leo: I think they're not being candid here. And we're not alone, by the way.

Steve: Well, I did quote here, I caught the top four, the first four, or three, rather, responses to that blog posting. Someone posting as tekwarrior said, "You should start improving security by getting rid of email addresses as usernames." Kellic wrote, "Please use Google Authenticator so I'm not installing yet another dang app on my phone for this. LastPass already uses Google Authenticator, and it's slick." And then an anonymous poster said, "Agreed. Was thinking the same thing. I don't use Dropbox now because of the security issues, but I may give it a second glance. It would be nice if it was integrated with Google Authenticator."

Leo: I resent the idea that what they're really saying is, "Oh, Leo, you are probably one of those people that use the same password on multiple services, so we're going to make you reset your password." I resent that because I don't. And I had a strong password for Dropbox. I just really resent that.

Steve: And it's a true inconvenience that they have reset the password on your account.

Leo: It's really, really, well, we're going to move off Dropbox.

Steve: Well, then something else really bizarre happened. I got a tweet from someone called @Tinzien, who tweeted to @dropbox, @dropbox_support, and to me, @SGgrc. And he said, "Dropbox.com is showing a very weird and expired certificate when trying to visit the site." And I attached it to the email that I sent you, although you probably haven't seen the email. I know that some of your guys did receive it because they knew what the title of this podcast was. But so I have the JPEG of the Dropbox cert, which I captured. It was for www.kitchensink.n0t with a numeric "0," n0t.

Leo: What?

Steve: So kitchensink.n0t. And in the URL he did not mistype it. It's www.dropbox.com. And the certificate came up, and it was for kitchensink.n0t.

Leo: That doesn't sound right.

Steve: And then - I know. And then I logged into Dropbox, over SSL, of course, checked what the certificate was today. And I noted that it was not valid after 01/29/2014, which is some integer number of months later than last night. So it sounds like something strange happened. Maybe some funky certificate got served, or who knows what's going on. But just another data point. Dropbox, you were talking about moving away from them. And as far as I...

Leo: What is the n0t TLD? There's no n0t TLD.

Steve: I know.

Leo: This is, you know what, this is - they were hacked. That can't possibly - how could you even get a certificate for a nonexistent TLD?

Steve: Well, that certificate is self-signed.

Leo: So it's self-signed. On, it's bogus.

Steve: Yeah. So someone hacked it themselves and signed it.

Leo: Got it. Could be somebody at Dropbox.

Steve: Yes. It could be just like an internal working certificate that somehow got put up on their servers by mistake, or they were changing certificates...

Leo: I am less and less impressed with Dropbox. How could you fumble this so

badly, dudes?

Steve: Well, and remember, too, as far as we know they're not doing any pre-egress encryption. So they encrypt, I'm sure, for transit. But as I remember from our last look at them, they're subject to subpoena. So it's like, eh, I'm not putting my stuff there without having it encrypted first.

Leo: Oh, wait a minute. Now, this is interesting. One of the chatters has sent me a Google search for kitchensink.n0t. It's apparently - it was used in a Gmail hack attack? This goes back to 2008. Kitchensink.n0t is interesting. What is it? Wow. 105 million results for it.

Steve: Whoo.

Leo: And going back many years. I don't have time to do the research, but that's interesting. What is it? Wow. It's not something, well, I would have just said, oh, they're just using something random they made up.

Steve: Clearly not, yeah.

Leo: Clearly not.

Steve: So maybe there was some sort of an intercept of this one tweeter's posting.

Leo: Could just be him, yeah.

Steve: Yes. And somehow he got to a bogus Dropbox server with a self-signed cert. But any browser is going to notify him that this is not valid, and that's what happened is that Firefox had a fit when it got the certificate and said...

Leo: Yeah, but don't you find it interesting that the same domain was used in a Gmail man-in-the-middle attack?

Steve: Yeah, it is interesting, yup.

Leo: Well, so there are many. And if you want an alternative to Dropbox, we have a whole host of good TNO, Trust No One, choices. Steve did a whole episode on other choices out there. And I'm going to be relistening to that episode and picking somebody new because I'm not using them anymore. I'm infuriated. Why should I have to change my password?

Steve: Well, on that note, a number of tweeters commented that there was some strange behavior, well, unwelcome, from Microsoft's newly released Outlook.com. And I went over to Outlook.com to poke around see what was going on there. I guess it's a Gmail clone. I'm sure you know all about it, Leo. I've not spent any time there.

Leo: What is the name again?

Steve: Outlook.com.

Leo: Oh, yes, the new Microsoft Hotmail.

Steve: Exactly.

Leo: Yeah. In fact, I immediately - Dan in our chatroom said, quick, get your name. And I did. I immediately got LeoLaporte@outlook.com because that's important, to preserve that.

Steve: Absolutely. Anyway...

Leo: It's nice.

Steve: What people were tweeting was that it has a 16-character password maximum.

Leo: Oh.

Steve: So here they are. And someone sent me a screenshot showing the error message they received. And Microsoft's - this new Outlook.com says, "You are apparently using a password longer than 16 characters. 16 characters is our maximum. Please use only the first 16 characters of your longer password.

Leo: That is a long password, though; right? I mean, come on. 16 should be enough.

Steve: Yeah, but we know that it ought to be - we don't care how long it is.

Leo: Shouldn't be limited at all, yeah.

Steve: Yeah. It ought to be use what you want, and good luck to you.

Leo: Do you think they have some sort of like a fixed-length field in their password database?

Steve: Well, that's the concern is that they're not, I mean, if you hash, then it doesn't matter how long it is.

Leo: Right. That's a bad idea. It means they're not hashing; right?

Steve: Only if you're not hashing...

Leo: Oh, boy.

Steve: ...that you care about the input length.

Leo: Oh, boy.

Steve: Yeah. Meanwhile, Tesco is in the U.K.

Leo: Oh, here, by the way, just an update on that. Apparently the team did a "I am the creator of Outlook.com, ask me anything"; and they said, "We are aware of this problem, and we are going to adjust it."

Steve: Yeah, we'll make it 32. That ought to be long enough.

Leo: But you know what, what that shows is how smart the community has become. Why can't I have more 16 characters for a password? That limitation has always existed, probably goes back to Hotmail days. "We're looking into fixing it," says Martin. Hmm. Oh, so interesting. So Hotmail has been accepting longer passwords but truncating it. Oh, that's really bad. So that's interesting. So they are aware of it, apparently, and planning to fix it. Interesting.

Steve: God, you know? And what's amazing...

Leo: Well, it's legacy. It's legacy code. That's the real problem.

Steve: This is just not hard to fix. It's like it's Romper Room. Anyway, Tesco...

Leo: In fact, somebody asked - I love this. They're so smart. Recursion asks, "Why is there even a limit? The password should be salted and hashed. How can you not

process a password of arbitrary length?"

Steve: Well, and that brings us nicely into our next story. A security researcher named Troy Hunt - whose current blog posting is just www.troyhunt.com, so if you can go there, you can bring up his current posting. And I saw some Twitter traffic about this, and this has hit the U.K. news, naturally. The Register.co.uk picked up on it. Tesco is, Troy explains, a major, I guess THE major supermarket chain in the U.K., like Coles is in Australia and like Safeway is here in the U.S. And so Troy tweeted that - Troy explained that he had seen a rumor and then confirmed, because he's now in Australia but used to be in the U.K. and so had a Tesco web store account, that he asked them for his password, which he forgot, and they mailed it to him.

Leo: Wait a minute, physically mailed it to him?

Steve: Just - no.

Leo: Emailed it to him.

Steve: Sorry, emailed it to him in the clear, "This is your password."

Leo: Here's your password, dude.

Steve: Here you go. Now...

Leo: I should point out we get a lot of heat because TWiT.tv has, for historic reasons, there's no reason to log into it, but it has a login because it shouldn't be exposed, but it is exposed. And if you forget your password, we will email it to you in the clear. But there's nothing there.

Steve: Right. So there's no value.

Leo: There's no value to it. So it has no - there's nothing you can do with your password. So don't get mad at me.

Steve: So he asked them, because Tesco has an active Twitter account, and they responded: "Passwords are stored in a secure way. They're only copied into plaintext when pasted automatically into a password reminder mail." [Buzzer sound] So, oh, goodness. So Graham Cluley, who is the Senior Security Consultant at Sophos, responding to this, wrote: "It does look as though Tesco is not following industry best practice. Any company that can email you your password is doing something wrong." And Tesco has not replied.

And then TechWeekEurope picked up, and they reported - this is today they reported: "A

dangerous flaw has been found on the Tesco website, placing the company's online customers at risk, TechWeekEurope has learned, just a day after the supermarket chain was lambasted for weak security practices." Their story goes on: "Yesterday, security researcher Troy Hunt had exposed problems with Tesco security, including the fact that it appeared to be storing customer passwords in plaintext without proper salting and hashing."

Well, they may be encrypting them and then decrypting them to send, but that's not good either because, if their password database is captured, it could be decrypted in the same way they do it, and then everyone would have their passwords, making it easier than having to do the password hash reversing. Anyway, so their story finishes: "Today it emerged that an cross-site scripting flaw on the site could be exploited by hackers to hijack users' accounts. TechWeekEurope has seen evidence proving that the flaw exists and has warned Tesco about it, but received no response. The XSS code will not be published for the safety of Tesco shoppers."

And if anyone is a Tesco customer, I would recommend you go take a look at Troy Hunt's current blog posting because he has an extremely comprehensive posting where he goes into many problems with Tesco security. The more he looked, the more he found. So, and it may very well - it's probably not a coincidence that a cross-site scripting flaw has surfaced the day after Troy started looking because I would imagine that his brought a lot of attention over to Tesco's website security practices, and they have been found wanting.

On the brighter side, LastPass, our favorite, has announced two new tighter security options that I really got a kick out of. I thank Leon Zandman in the Netherlands, a listener of ours, for tweeting this to me. This just happened. So thanks to Leon I found out about it in time for this week's podcast. Two new options for LastPass: Restrict login to selected countries, which I think is very cool. I mean, how often are you, if you're not an international traveler, or even if you are, you may be bouncing between here and the U.K., for example, or the U.K. and Australia. But you're not planning to go to China or Russia. So why allow logins from countries you absolutely never go?

And I think this is an example of the kind of forward thinking I love about LastPass. And this is what everyone should have. I'm not going anywhere. So I absolutely don't want to allow any of my accounts to be logged into from anywhere else. And if I'm planning a trip, I know. And there ought to be, in the least, some extra-extraordinary login requirement if I try to log in from outside my normal geographic location. So I just think this is very slick. It's like, why isn't everybody doing this?

Leo: This is kind of like the Google thing where they tell you somebody accessed your Gmail from an odd spot. I think every site, everything should do this; right?

Steve: Yes. And in fact I would go further because Gmail will - I guess we are seeing some things that are saying, wait, we're going to deny really abnormal behavior. It's very much like how your credit card company will call and say, "Are you buying wigs in the Ukraine?" No.

Leo: No. No, no, no.

Steve: Only in Southern California.

Leo: And this is all - it's not somebody going, hmm, this looks odd. They use business intelligence software that is very good now at detecting odd patterns, abnormalities.

Steve: Yeah, well, it won't let me buy gas, which is annoying.

Leo: There, well, there are some things that maybe it's a little oversensitive. But I prefer my credit card gets blocked in excess than less often than it should be. We are - for some reason Bank of America with our business cards turns them off all the time. Just some companies, Chase, I also have a Chase card, they don't do it as much. Amex is very good. They'll call you. They really interact with you a lot.

Steve: I did add recently to my main card the ability to notify me by text. And it has come in handy.

Leo: Isn't that good. That's the way to do it, yeah.

Steve: Yes, because I can very quickly say - oh, in fact, it was when Google charged me for the Nexus 7. It had been a month since I ordered it, and I got the $249 one plus the case, so it was $303. And I got a text coming in, and it's like, yup, I know what that is. And I was able to acknowledge it right there on the spot. So it was very cool. And I'm going to talk to you about that in a second. And then the second feature - the first one was restrict login to selected countries. The second one is also very nice: Disallow logins from the TOR network.

Leo: Really. Now, why would that be good?

Steve: Well, because what occurred to them, when they implemented the first one they realized, wait a minute, there are TOR nodes in the U.S. So somebody outside the U.S. who is being blocked because of a geographic restriction could use TOR to proxy their connection inside the U.S. And so that would be a way around this. And so they said, oh, let's just toss that one in, too. We won't allow a TOR access to LastPass login. Which again is, like, really nice thinking.

Leo: Well, I'm going to go into my LastPass settings.

Steve: Yeah. You can just turn those on. They're off by default, although the U.S. is turned on for U.S. customers. So you're not blocked.

Leo: That's the nice thing is you can be in Europe and say, oh, no, no, turn that off.

Steve: Absolutely. Absolutely.

Leo: You just log in.

Steve: Computerworld picked up a nice note that I just wanted to share. We've talked a lot about Firefox's moving toward background updates following the successful Google Chrome browser model. Just one week after v14 of Firefox was released, 46 percent of all Mozilla browsers were using v14.

Leo: Wow. That's amazing. But it's automatic now; right? So that means the other 54 percent just never use Mozilla.

Steve: Oh, I don't know what that means.

Leo: Or they're so old, they're not in the automatic upgrade state.

Steve: That would be it, yeah, because if you're at 3.5 or 3.6 or back further, then it won't move you automatically. So you've got to be into that automatic mode. So half of Mozilla users have been manually updating themselves to the point now that they no longer need to, is probably the way to best phrase that.

Leo: That's great.

Steve: And I noted a few things. I saw a little blurb about Safari v6, which we all received - oh, my god, you're right, that was a long download, Leo. Oh, my goodness.

Leo: Well, it's half a gigabyte, isn't it? No, no, it's 4GB, 4.something gigabytes.

Steve: That's no excuse because I downloaded - what did I - I downloaded something that was 3GB just yesterday, actually it's the latest version of FreeBSD, the full DVD install. And it was 3GB, and it took a couple hours. But not, oh, my goodness. I think OS X v10.7 took all day. I mean, it was just like, just waiting for it.

Leo: Well, millions of people are downloading it. That's why. I mean, sounds busy.

Steve: So SAMS reported Apple has released an updated version of its Safari browser, Safari 6 for OS X v10.7. And they said Lion, but we know that's Mountain Lion, because the other one was just regular Lion?

Leo: Yeah, Lion.

Steve: That's what I thought.

Leo: I ain't Lion.

Steve: So it addresses more than - are we sitting down? - 120 security issues present in v5.x of the browser...

Leo: Jiminy.

Steve: Yah, that could have been exploited to allow cross-site scripting attacks, arbitrary code execution, and file theft. So, yes, everybody, 120 security issues. It may take all day to get it, and it costs $19.95, but probably a good idea. Safari 6 also incorporates several new features, including a "Smart Search Field" that can be used to search and to input site addresses, and an Offline Reading List that allows users to save pages to a list to be read even when an Internet connection is not available. Which would have been nice in 1997. I don't know when an Internet connection is not available today.

Leo: Hey, you know.

Steve: So I tweeted to @SGpad: For $199, I am very impressed and loving the Google Nexus 7.

Leo: Yeah, nice little tablet. In fact, I've heard of a number of people who stopped using iPad.

Steve: Yeah, well, I'm not that. But I did hear from someone who responded, saying that he used one of those "used devices, will buy your old stuff" sites, got so much money back that he was able to buy a Nexus 7 and take his girlfriend out to a nice meal. So, and he's very happy. And I am, too. I have been - now what I've been doing is I carry it with me because I always have my iPad, a notebook, mechanical pencil, eraser, and the Kindle DX. Now I've added to that, in a nice little case, I've added to that the Nexus 7 because I'm showing it to people, recognizing that there are people who aren't going to do an $800 iPad. Especially when they've got kids. One of my friends at Starbucks has a kid. She bought him a new iPhone, and he dropped it in the toilet the first day he had it. It's like, okay, well, this is not a kid you want to give anything really expensive to.

But for $199, I mean, and so I poked at it Saturday and Sunday at Starbucks in the morning. And I installed Amazon, a couple free apps. I poked around the Google Store. I dug deep in and changed settings and things. And it is what I wanted, which is it is responsive. I mean, it's smooth. It's a very impressive piece of work for 200 bucks. So I just wanted to make sure everyone listening to the podcast had heard that. I mean, it's - although I just saw some pictures of the expected 7-inch iPad toward the end of this year, and it looks pretty cute, too. I don't know if those are real yet, but it looks like we're going to be getting that. And we now know that it's going to be 1024x768, so the same resolution as the old iPad, the original iPad, in a smaller size. But, boy, the Google Nexus 7, if you're, I mean, if you're just a counterculture person, if you don't want to do Apple, you want to do Android, it's a beautiful piece of work.

Leo: And I actually like the 16x9 form factor. Apple's tablet, if the rumors are true, it's going to be like an iPad, and that makes sense.

Steve: Will still be 4x3, yeah.

Leo: And I have to say, even for reading - and we talked about this. But I think even for reading this is a nice aspect ratio, and certainly for watching video.

Steve: And I meant to bring that up again. What I did, "Damages" is in its fifth season. It went to DirecTV, season four and five. And so I was watching an episode of that. And it was so nice not to have to mess with iTunes, also. I just want to put this media on this tablet to go watch it. And so the experience was completely nice. It was widescreen. And I did want to mention, Leo, that I'm not finding as much a problem with the 16x9 form factor as I expected.

Leo: You were worried, yeah, I remember.

Steve: Although it would be nice if the home screen would also rotate. The home screen insists on being in portrait. It won't landscape.

Leo: Yeah, I don't know if that's a setting, but I think that that makes sense. Probably different launches would let you do that. But it's hard to rearrange those icons. Maybe on a 4x3 it isn't, but on a 16x9 there's such a difference between portrait and landscape that you really have to rearrange a lot of stuff. I think that my - I'm interested in it, but I like Android. But I was very interested to see the number of people who are very strong iOS supporters and iPad lovers say, yeah, you know what, it's actually - it was almost painful for them to admit, I think, it's actually not too bad. Kind of like it.

Steve: Well, I feel like we're really seeing a lot of collision now in the patent territory.

Leo: Well, yeah, that's another issue. That's a huge issue, of course.

Steve: Yes. I mean, so, for example, Apple, because they were there early and they did some good things on the iPhone, they locked down as inventions things which anybody else would have come up with if they'd been given the same problem. And this is the problem with our patent system is that the actual law says that it is not subject to patent if it would be obvious to somebody trained in the art. And I argue that a lot of what is having patents issued is just engineering. It's just how do I zoom? Oh, well, you pinch, and you expand. Duh.

Leo: Well, I loved it when the judge said, hey, anyone can write a rangeCheck. This was one of the issues, the patents in the Apple-Samsung case. Anybody could write

a rangeCheck. I just wrote one yesterday. I loved that. And it's true. That's an obvious patent. It shouldn't have been made a patent.

Steve: Yup. And so, for example, one of the things that I love on my BlackBerry is that I hold the key down, and it's initially lowercase, then it switches to uppercase. Well, they have a patent on that, so nobody else can do that.

Leo: That's too bad.

Steve: And so we're losing because of that, something which is arguably obvious. It's like, well, okay, how...

Leo: It's called "shift lock."

Steve: Yeah. And so the problem is...

Leo: You know, I completely forgot about that on BlackBerry. I do miss that. That's a great feature. Now, fortunately, BlackBerry apparently didn't patent the double-tap spacebar to put a period, space, and start a new sentence, because that's now on everything. Because that's useful, too. And when you don't have that, you miss it.

Steve: Yes. And so but what's happening is the ecosystem is being chopped up in pieces.

Leo: Exactly, exactly.

Steve: And good features from something cannot appear on something else because of the ridiculous level at which we're issuing patents, which is really annoying.

So I mentioned last week, cryptically, something which you have seen, which I just thought I would share with our listeners. And here it is: GRC.com/animation.htm. And this is - I've been writing some JavaScript.

Leo: Actually, let me refresh it because it starts with 0000, so when you first get to it...

Steve: I have it do that because it makes it a little more clear than if just - I actually originally had it so it was just up and running immediately, but I like having it start that way.

Leo: And then it gets the data. There's a one, and now we're starting to see some data come in. So what is this for, first of all?

Steve: So I've decided - there was somebody who asked on the podcast early this year, I think it was in January, he'd, like, looked around the GRC website and was trying to figure out what SpinRite was. He's a listener to the podcast, and he wanted to buy it, but he thought it would be nice if he knew what it did. And he said, "Is it a defragger? Is it an undeleter? What is it?" And I thought, you know, I don't think I ever really explain that.

So I decided I ought to create a video, because everyone can see videos now, where I in a short period of time explain about hard drive data recovery. Well, in order to explain about recovery, you need to explain about recording, I mean, how data is stored. So I'm going to produce a video to explain what SpinRite does in a few minutes. But I wanted some diagrams. And to make them fun and interesting, I thought they should be animated also because animation is often the right way to explain something that's going on. So GRC.com/animation.htm is just, more than anything, the page is 25k of code. It actually does a lot more than what you'll see because that's the fourth of five frames that I've designed that will end up being part of the video. But it's a nice little example of what can be done with JavaScript and the new HTML5 canvas API.

Leo: Oh, that's interesting. This is not like a PowerPoint slide. This is done in HTML.

Steve: Yes, it's pure web coding.

Leo: And JavaScript.

Steve: It runs beautifully on my iPhone, on my iPad, on my Nexus 7. It does not run at all on my BlackBerry. It's like you get about one frame every 30 seconds. It's like, oh, just give up on the BlackBerry for web stuff. But so it's universally cross-browser. Since I'm in XP still, I wanted to see about IE. But Microsoft, always the laggard here, didn't support the canvas API until IE9, and you can't run IE9 in XP. But because IE is so far behind, Google created an add-on for IE which, if the developer adds a tag in the header of a web page, will invoke the Google Chrome frame, and then the page runs in essentially a transparent Google frame under IE.

Leo: Oh, that's interesting.

Steve: So the point is that I'm in XP with IE8 and still able to look at this cool little animation, thanks to Google having created a frame for it. So...

Leo: GRC.com/animation.htm, if you want to test it on your particular browser. Are you using any JavaScript libraries? Or this is just the built-in JavaScript in the browser with HTML5?

Steve: All me, baby. No libraries.

Leo: No libraries.

Steve: In fact, there are no includes. There's nothing else. The page itself is the JavaScript. So if anyone's curious...

Leo: Oh, can I view source?

Steve: Yeah.

Leo: Oh, how nice of you.

Steve: And it's commented and all that.

Leo: That's seriously cool. As somebody who you've convinced that I really should learn JavaScript, this will be a very useful example. Thank you.

Steve: Yeah. So speaking of SpinRite, I thought I would share a nice story from actually someone named Guy Story. And he says KC5GOI. Those sound like call letters; right?

Leo: Yeah, that's a ham.

Steve: A call sign, KC5.

Leo: Yeah.

Steve: Okay, KC5GOI. He says, "I wanted to pass this on. I am the network admin for a cancer treatment company in Dallas. Today I received a phone call from the supervisor of our lab. One of our remote offices had reported that their lab PC was giving the BSOD on boot." Which we all know, those of us who have suffered through Windows, as the Blue Screen Of Death. "When I arrived onsite I found that XP was at a BSOD and had an unmountable volume. This system is under Dell Gold for troubleshooting, but not for hardware. It is less than two and a half years old. I'm still working to get that changed.

"So I booted up my personal copy of SpinRite and ran a Level 2 pass. SpinRite worked for a while and reported that two sectors were beyond repair, but that it had been able to recover and repair three other sectors. That appeared to be enough for XP and the needed application, since the system now ran perfectly. I ran the Dell diagnostics after SpinRite. I had to do this before calling Dell. Funny thing, the Dell diagnostics said the drive was okay. I guess it was, now that SpinRite fixed it. I ran SpinRite first, since it tries to recover data. The Dell app does not. I suspect the Dell app is not as thorough as SpinRite." Uh-huh, yeah.

"This PC does not store data, thus we do not have a regular backup of it. I ran SpinRite to get the workstation back online. Once I get the warranty issue fixed, we'll be rebuilding the workstation with a fresh drive. Once that is finished and blessed, I'll be making a ghost copy of it, along with the other lab workstations. If it was not for SpinRite, the employee would have had to rely on getting results faxed to her instead up

pulling them up in real-time. It would been midmorning the next day before she was back online. I'm going to be pushing my employer to buy a corporate license from GRC. Showing how SpinRite saved the day this time will make this an easier task. Thanks, Steve."

Leo: Aw.

Steve: And thank you, Guy, for sharing your story with me and our listeners.

Leo: And thank you, Steve, for sharing your source code. Boy, you're a clean coder. Wow.

Steve: You know what I've realized, Leo? The more I code, the more I appreciate how it's about communication. Coding is communication.

Leo: Not just with the computer, but with the human who might read this, including yourself.

Steve: With me when I come back later and go, okay, wait a minute.

Leo: Boy, this is elegant. Nice. Nice. I can't wait to kind of go through this. That is great. And by the way, it's really cool because this is the HTML I'm looking at. By the way, Safari does a very nice of view source. They've really got a code browser built-in here. But the HTML, really there's very little HTML, it's just - it's the script. It's all script. It's very cool, very, very cool.

Steve: Yeah, I think there's, like, two lines of HTML where I declare the canvas and the size.

Leo: And one of them is what happens if there's no script, no JavaScript enabled. It's awesome. Really beautiful. That is gorgeous. Wow. I can't wait. I'm going to get a good book, and I'm going to sit down, and I'm going to - I love language. I collect languages. And I've learned a lot of them. But I think from a pure pragmatic point of view, learning JavaScript today is really useful.

Steve: I really think. I mean, it is obviously, one, the world is moving to the client. We're seeing more and more Google-ish sorts of the app-is-the-client approach. It just makes sense.

Leo: Yeah. Very nice. Hey, let's take a break. And then we're going to get to Ali Baba's Cave. Ooh. Okay. This is going to be one where some steam might come out of your ears.

Steve: I think so.

Leo: That just means things are working right. All right. Get ready. We are about to enter the Cave of Ali Baba. Steve?

Steve: Okay. So I was talking at the beginning of the show about how we have, in traditional crypto protocol descriptions, we talk about Alice, Bob, and Carol.

Leo: From the movie "Ted and Bob and Carol and Alice," a '70s movie.

Steve: That's right. When we're talking about zero-knowledge interactive proofs, we use characters Peggy and Victor as the prover and the verifier.

Leo: Oh, I like that.

Steve: Now, in the formalization, the academic formalization of what is a zero-knowledge interactive proof, there are three requirements to, like, qualify for valid zero knowledge. And I'm going to go through these first before we talk about Ali Baba because you'll see how these come into play in the story, which will immediately follow.

So the first is completeness. The property of completeness says that the verifier always accepts the proof if the fact is true and both the prover and the verifier follow the protocol. So that's like the formal way of saying, if everything is done right, and the actors here act properly, then the verifier always gets what he needs. So that's called completeness, in this case, of the proof. The verifier always accepts the proof if the fact is true and both the prover and the verifier follow the protocol.

The second property is the property of soundness. The verifier always rejects the proof if the fact is false, as long as the verifier follows the protocol. So completeness says, if it's true, the verifier will come to that conclusion. Soundness is sort of the reverse. It says, if it's false, the verifier won't arrive at a false positive. The verifier will reject the proof. And so that's the requirement of soundness for the zero-knowledge interactive proof.

And finally - and this is the one that's a little tricky, but the story does cover it in a clever way - the property of zero knowledge is the verifier learns nothing about the fact being proved - except that it's correct - from the prover that he could not already learn without the prover, even if the verifier does not follow the protocol, as long as the prover does.

Leo: Let me see if I understand this. Didn't we talk about this last week in the question-and-answer where it said, when you log in, shouldn't it tell you if you got the email right or if you got the password right? Like if you got one thing wrong, just which one you got wrong. Is that the same as zero knowledge? It's leaking knowledge.

Steve: Yes, because, for example, this property goes on to say, in a zero-knowledge proof the verifier cannot even later prove the fact to anyone else. And that's really key.

Leo: That's key. That's the key.

Steve: So, again, the verifier learns nothing about the fact being proved, except that it's correct, from the prover that he could not already learn without the prover, even if he does not follow the protocol. And in a zero-knowledge proof the verifier cannot later prove the fact to anyone else.

Okay. So now we need to talk about Ali Baba, which I just love saying, "Ali Baba." I like saying that like "coconut." I love the word "coconut." And "Ali Baba."

Leo: Okay. You're just strange. Now it's just getting weird.

Steve: So, very long ago, in the Eastern city of Baghdad, there lived an old man named Ali Baba.

Leo: [Laughing] I love how this is beginning.

Steve: Every day Ali Baba would go to the bazaar to buy or sell things. This is a story which is partly about Ali Baba and partly also about a cave, a strange cave whose secret and wonder exist to this day. But I'm getting ahead of myself.

Leo: This is so cool.

Steve: One day in the Baghdad bazaar, a thief grabbed a purse from Ali Baba, who right away started to run after him. The thief fled into a nearby cave whose entryway forked into two dark, winding passages, one off to the left, the other off to the right. Ali Baba, who was following, did not see which passage the thief ran into, though he did see him enter the main entrance. So Ali Baba had to choose which way to go, and he decided to go to the left. The left-hand passage ended after a while in a dead end. Ali Baba searched all the way from the fork at the beginning to the dead end, but he did not find the thief.

Ali Baba said to himself that the thief must have been in the other passage. So he searched the right-hand passage, which also came to a dead end. But again he did not find the thief, figuring that the thief probably left from the right-hand passage while he was busy searching the left. "This cave is pretty strange," said Ali Baba to himself. "Where has my thief gone?"

The following day another thief grabbed Ali Baba's basket and fled, as the first thief had fled into the strange cave the day before. Once again Ali Baba pursued him, and again did not see which way the thief went. This time, however, Ali Baba decided to search to the right. He went all the way to the end of the right-hand passage, but did not find the thief. He said to himself that, like the first thief, the second thief had also been lucky in taking the passage Ali Baba did not choose to search first. This had undoubtedly let the thief leave again and to blend quietly into the crowded bazaar.

Days went by, and every day brought its thief. Ali Baba always ran after the thief, but never caught any of them. On the 40th day, a 40th thief grabbed Ali Baba's turban - boy,

he's down to his turban - and fled, as 39 thieves had done before him, into the strange cave. Ali Baba yet again did not see which way the thief went. This time Ali Baba decided to search the left-hand passage; but, again, he did not find the thief at the end of the passage. Ali Baba was very puzzled. He could have said to himself, as he had done before, that the 40th thief had been as lucky as each of the other 39 thieves. But this explanation was so far-fetched that even Ali Baba did not believe it. The luck of the 40 thieves was just too good to be a matter of chance. There was only one chance in a million million that all of the 40 would escape.

Now, pausing for a second, we know that there's a 50-50 chance, given that the two tunnels dead-end, and Ali Baba has to choose one. Every time he chooses he's got a 50-50 chance. 40 days, 40 thieves, that's 2^40, which is 1.1 times 10^12, which is in fact 1.1 million million. So that would be the chance, if the cave is as Ali Baba suspects or believes at this point, that in 40 tries he could never once catch the thief. That's very unlucky.

So Ali Baba said to himself that there must be another, more likely explanation. He began to suspect that the strange cave guarded a secret. And Ali Baba set out to discover the secret of the strange cave. He decided to hide under some sacks at the end of the right-hand passage. After a very uncomfortable wait, he saw a thief arrive. Sensing he was pursued by his victim, the thief whispered the magic words "Open Sesame." Ali Baba was amazed to see the wall of the cave slide open. The thief ran through the opening, then the wall slid closed again. The pursuer arrived and was all upset to find only Ali Baba hiding under the sacks at the dead end of the passage. The thief had escaped. But Ali Baba was happy, for he was finding out the secret of the strange cave.

Ali Baba experimented himself with the magic words. He discovered to his amazement that, when the wall slid open, the right-hand passage was connected with the left-hand passage. Now Ali Baba knew how all of the 40 thieves had escaped from him. The very next day a thief was caught. Ali Baba recorded this story and his discovery in a lovely illuminated manuscript. He did not write down the new magic words, but included some subtle clues about them. Ali Baba's lovely illuminated manuscript arrived in Italy in the Middle Ages, and today it's in the United States, somewhere near Boston.

Leo: Wow, that's specific.

Steve: There it recently acquired the full attention of several curious researchers. Through decryption of the subtle clues, these researchers rediscovered the magic words. After several archeological excavations in the ruins of the old Baghdad bazaar, the strange cave was relocated. It was not a myth after all. And despite the centuries, the magic words still worked. All agog, which is not a word you hear very often...

Leo: One of my favorites. Right up there with coconut.

Steve: All agog - ooh, coconut - the curious researchers went through the end wall between the two passages. The television networks were quickly made aware of the unusual events taking place in Baghdad, and a big American network even got an exclusive on the story. One of the researchers, whom we'll call Mick Ali, perhaps a descendant of Ali Baba, wanted to demonstrate that he knew the secret, but he did not want to reveal the secret. Here's what he did:

First, a television crew filmed a detailed tour of the cave with the two dead-end passages, just like Ali Baba had found all those centuries ago. Then everyone left the cave. Mick Ali went back in alone and went down one of the passages. Then the reporter, accompanied by the camera, went inside only as far as the fork, where he flipped a coin to choose between right and left. If the coin came up heads, he would tell Mick to come out on the right. If the coin came up tails, he would tell Mick to come out on the left. It was heads. So the reporter called out loud, "Mick, come out on the right." And Mick did just that.

In memory of the 40 thieves, this demonstration scene was played 40 times. Each of the times, everybody went back out of the cave, and Mick entered alone, all of the way down one of the passages, which he chose first. Then the reporter and the camera went as far as the fork, where a coin was tossed, giving Mick the order which cave to come out of. Mick succeeded all 40 times. Anybody who did not know the secret of the cave would have been exposed on the first failure. Each new test divided by two the chances of success for someone without the secret. On the other hand, the secret allowed Mick to come out each time through the required tunnel.

Employed by another television network, a jealous reporter wanted to also film a story about the strange cave. But Mick, honoring his nondisclosure and his exclusivity, refused to participate because he had given exclusive rights to the story to the first network. But Mick mischievously suggested to the jealous reporter that the story could be filmed without possessing the secret. The jealous reporter thought about that for a minute and then smiled to himself. He said, "I even know a stage actor who looks like you and who could be mistaken for you."

And the second story was filmed. In the course of the filming, half of the scenes were spoiled because Mick's double did not know the magic words and so could not get from one passage to the other as required to succeed every time. So the jealous reporter simply edited the tape and only kept the successful scenes until he had 40 of those.

The two stories were aired at the same hour on the same evening by the two competing American networks. And the matter went to court because it was believed that somehow this exclusivity was broken.

Leo: Oh. Even here, patent problems.

Steve: Yes. Both videotapes that were aired at the same time on the same night were placed into evidence, but the judges and the experts could not tell the tapes apart. Which tape was simulated? Which tape was genuine? The tapes alone were not enough to judge by. The simulation surely conveyed - now, here's the cool part. The simulation surely contained no knowledge of the secret because no knowledge of the secret was involved in creating the simulation, so it couldn't have any knowledge of the secret. But the simulation and the genuine tape were indistinguishable from one another. Thus the genuine tape also did not convey any knowledge of the secret.

The reporter who had gotten the exclusive story had been convinced at the time that Mick Ali knew the secret, and he was still convinced. But the reporter, despite all of his efforts in court, was unable to pass his conviction on to the judges. Or onto the television audience, either, because of course now he had a tape that was judged to be a fraud, or might be, because the other network had aired the same thing, apparently showing exactly the same miracle of this Ali Baba's Cave. So Mick Ali had achieved his real

objective. He wanted in fact to show that it is possible to convince without revealing, and so without unveiling his secret. And that's the story of Ali Baba's Cave.

Leo: And what have we learned from this, Steve?

Steve: Okay. So what does this tell us?

Leo: Yes, what does this tell us? It's clever, first of all.

Steve: Yes, it is. So the cave construction is something we see in many discussions because it's so clear that it's a real-world, physical, simple-to-understand example of how someone could prove something without revealing what it is by statistically demonstrating that they have a fact which they need to use in order to produce an outcome, yet the fact itself is not part of the outcome. And that's the key. So they're in command of something, some knowledge, and they must use the knowledge in order to prove an outcome.

But what's interesting is that this is a statistical result, a statistical proof. That is, we don't know with absolute utter certainty, even after 40 trials, that the person didn't actually just get phenomenally lucky because they could have. And we know that it's one in 1.1 million million chances, given 2^40, with each one having a 50-50 chance. But it's diminishingly unlikely that somebody without the knowledge could still provide this outcome.

So if we look back again at our three requirements, the formal requirements for zero-knowledge proof, the requirement for completeness is that the verifier will always accept the proof, if the fact is true and both the prover and the verifier follow the protocol. So clearly, in our little cave model, we have that. Which is to say that the verifier, understanding statistics and understanding everything about the structure of what's happening, but only lacking the knowledge of what's required to cross from one tunnel to the other, the verifier accepts the proof that the prover, Peggy, has the ability to cross tunnels by testing enough. So this gives us completeness.

Soundness is the property that the verifier will reject the proof, if the fact is false, as long as the verifier follows the protocol. So here, this would be, if Peggy were unable to cross between the backs of the tunnels in the cave, then all it would take would be one time that Victor the verifier says come out on the right; Peggy, unfortunately, went down the left tunnel. She can't, no matter how much she wants to, come out on the right because, if she doesn't have that fact, she can't prove her knowledge, then that gives us the property of soundness.

And finally, the property of zero-knowledge is the verifier learns nothing. So the verifier, Victor, out in front, learns nothing about the fact being proved, except that it is correct, from the prover that he could not already learn without the prover, even if the verifier does not follow the protocol. In a zero-knowledge proof, the verifier cannot even later prove the fact to anyone else. And that's probably one of the coolest things about this.

So Victor and Peggy, if we place them in the cave, Peggy can demonstrate her ability, her knowledge, as many times as Victor wants her to. Yet when they're done, they emerge from the cave, Victor says, "She absolutely definitely can cross between tunnels." And someone says, "Prove it." And Victor can't. He knows because, with

absolute statistical close-to-zero probability, he's absolutely sure. Yet he obtained nothing from the experience that he can pass on to anyone else. And this may seem rather abstract and wacky. There are some applications for exactly this that we will be covering in the future.

Leo: Did you write this story yourself? Or is this from somewhere?

Steve: I found it, and I modified it a little bit.

Leo: It's good.

Steve: Yeah, yeah.

Leo: It's good. Did you add the TV part, or was that in there?

Steve: No, it was written - actually, I excerpted some stuff that wasn't relevant for our purposes. And it was originally in French, and it was translated into English.

Leo: Wow. Very interesting.

Steve: Yeah. If you put in Google, like, "zero-knowledge and kids," or something, it's sort of meant to be a kids' story, a way of, like, explaining...

Leo: Oh, yeah, yeah. "How to Explain Zero-Knowledge Protocols to Your Children." The chatroom has given this to me. You guys are good. It's by Jean-Jacques Quisquater and a few other people.

Steve: Louis, yeah.

Leo: Yeah, Louis Guillou. Wow, that's hysterical. That's so good. There's illustrations. Not very good ones, but...

Steve: Yeah. Not very good ones. And you do run across this tunnel analogy all over the place. I mean, even in formal crypto papers. I have about five of them that I read in order to see whether there was anything, you know, in order to get myself the depth of understanding that I wanted. And they have much better graphics, but they're much less fun.

Leo: This was really interesting.

Steve: And so I thought that Ali Baba's Cave was something that our listeners will now

never forget.

Leo: Now, it says "How to Explain Zero-Knowledge Protocols to Your Children." I doubt that very many children would really - but it's a good story.

Steve: It's a great story.

Leo: I'm not sure they would come away with it saying, "Oh, Daddy, now I understand. Zero-knowledge." You're great. I love it. Steve Gibson is at GRC.com. That's the Gibson Research Corporation. That's where you'll find SpinRite, the world's best hard drive maintenance and recovery utility. Everybody should have a copy of SpinRite. You'll also find lots of other things for free there, including his health and nutrition information that Steve's done some really interesting work with. Somebody was in here a couple of days ago, said "When is Episode 3 of the Sugar Hill?" Do you plan one?

Steve: I feel like we ought to do a follow-up.

Leo: Yeah.

Steve: But there are a couple other things I really want to talk about. Magnesium is another component of health that I think is very critical, that we're all deficient in. And I have quite a story...

Leo: Oh, I'd love to hear that.

Steve: ... about my magnesium adventure.

Leo: All right. Well, maybe we'll do another one.

Steve: So if I can squeeze some more of your time free, Leo, I do think that there's a segment of our audience that appreciates it. And boy, I can tell you that the first two episodes have really helped a chunk of our listeners.

Leo: Helped me.

Steve: They're less chunky, in fact.

Leo: I'm a lot less chunky there. Actually, Saturday afternoons at 2:00 p.m. will soon be open, so that's a good time to do it, if you want to do it then.

Steve: Okay. I'll keep it in mind.

Leo: Keep that in mind when you feel up to it. "Sugar Hill 3" starring Wesley Snipes. It's coming to a theater near you. Also, GRC.com has 16Kb versions of this show for the bandwidth impaired, full text transcripts, always helpful. And we make audio and video versions available on our site, TWiT.tv/sn. We do the show, and you can watch live, if you want to challenge your brain, in real-time, 11:00 a.m. Pacific, 2:00 p.m. Eastern time, Wednesdays at TWiT.tv. That's 1800 UTC. Steve, thanks so much.

Steve: Always a pleasure. And we'll be back next with a Q&A episode. If any listeners have something in particular that is tickling their brain, they're wondering about or troubled by, drop a note to GRC.com/feedback. I'll get it, and we'll go through the mailbag, which I did hear from several people saying, hey, I'm still familiar with the term "mailbag." I don't think it's obsolete at all.

Leo: Well, yeah. In fact, I don't know we thought this, but every mail carrier has a mailbag still.

Steve: Yeah, or a box.

Leo: My mailman comes around with a big old bag with a big leather strap and a little sheepskin on the shoulder pad.

Steve: Perfect.

Leo: Yeah. And shorts.

Steve: Of course, you are in Mayberry.

Leo: We live in Mayberry, so we still have Andy, Opie, and the barber shop's just around the corner. Floyd will be glad to cut your hair for 50 cents. Thank you, Steve.

Steve: Thanks, Leo. Talk to you next week.

Leo: On Security Now!.