SecureZIP

Description: Steve and Leo examine the operation, features, and security of PKWARE's FREE SecureZIP file archiving and encrypting utility. This very compelling and free offering implements a complete PKI (Public Key Infrastructure) system with per-user/per-installation certificates, public and private keys, secure encryption, digital signing, and other security features we have discussed during previous podcasts.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-201.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-201-lq.mp3

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

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

This is Security Now! with Steve Gibson, Episode 201 for June 18, 2009: SecureZIP. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that covers all things secure, Windows - and there he is. Look at the smiling, shining face of Steve Gibson from GRC.com, the creator of - I shouldn't say the creator of spyware, the coiner of the term "spyware."

Steve Gibson: Oh, yes, please. I've never created any, and I never would.

Leo: Nor was he really the discoverer. Well, I guess you were. It was something you found on your system and raised the alarm.

Steve: Yep. Certainly it existed before. But I found a piece, and it was during a conversation with Gregor Freund that I said, you know, this is spyware.

Leo: Gregor. Gregor, this is spyware.

Steve: He says, oh, I like the - he says, "I like that, that spyware."

Leo: Well, Steve, what are we going to talk about today?

Steve: Today something very cool that I mentioned a couple months ago that I wanted to get to, and today seemed like a perfect opportunity. And this is sort of where the formal ZIP utility has evolved to. We talked about it briefly in the past. And this is something called SecureZIP, which is a very compelling set of features in a 100 percent free download from the people who invented the ZIP format, PKWARE. And of course...

Leo: Oh, yeah, that's Phil Katz; right?

Steve: Phil Katz. PK stands for Phil Katz, K-a-t-z. And he - you remember old-school back - the whole SEA, remember SEA and the older sort of prequel to the ZIP format. There was...

Leo: SEA, yes, yes. But before ZIP there was ARC; right?

Steve: Oh, yeah, I think ARC predated - A-R-C, right, predated. And anyways...

Leo: SEA was Self-Extracting Archive, so that was a ZIP. But it was a ZIP you could double-click.

Steve: Well, yeah, right. And in fact, you know, there have been self-extracting ZIPs and EXEs that use this compression and so forth, where they bundle into the file the little decompression engine. What is exciting about this program is, for many of our listeners, this could be their first exposure to the so-called PKI, in this case not Phil Katz. This is Public Key Infrastructure that we've talked about. In fact, we've been - this is like a perfect, practical, real-world example of all the stuff we've talked about before, that is, public keys and private keys, symmetric and asymmetric encryption. SecureZIP has all that but has wrapped it in a really user-friendly package that frankly, as I've been playing with it, it's like, wow, this, I mean, this just works. I've got friends who I don't want to find out about this because they will never send me a non-secured, non-encrypted, non-digitally-signed ZIP again because it's just too fun to do it. So anyway - and, of course, super secure.

Leo: Now, there are freeware programs, I use one called 7-ZIP, that do ZIP. In fact, nowadays Windows and Macs both come with ZIP compression built in. So PKWARE has to come up with something better to convince people to buy something; right?

Steve: Yes. And I'm going to explain today what they've done and why this is - as I said to you before we began recording, Leo, you're going to be a little jealous. Now, it isn't available for the Mac, which is why I said you'll be a little jealous of the Windows platform. They have a bunch of support for IBM mainframe end of things, and also UNIX and Linux servers. But the only desktop product is available for Windows. Which, as they

point out, is still the lion's share of the market. But it is - it's really slick the way they've put this together. So I'm going to tell our listeners all about it today.

Leo: I can't wait to find out about it. Also I imagine there's some security news from the front lines of security. But not much.

Steve: Not much this week.

Leo: It was all last week when we had that gigantic 31...

Steve: Well, you know, that was a record breaker. It was a formal record-breaking update. So, yeah.

Leo: 31 patches.

Steve: For Windows.

Leo: For Windows. But we did get a big one from Apple. I guess Apple finally sat up and listened.

Steve: Yes. We talked about this last week, and maybe even the week before, that there was still - that they were the only surviving remaining platform that had not dealt with the at that time very well-known, substantial, significant, important, even critical Java problems, you know, known problems with the Java system. So when I turned my Mac on a couple hours ago to get it warmed up for our podcast it said, oh, you've got a 158MB security update. Now, what's interesting, in my case, I don't know why, but it failed the first time. It just said, uh, can't update you.

Leo: You know, mine did, too.

Steve: Isn't that interesting.

Leo: I think maybe if a browser is open or something like that.

Steve: No. I never had - at no point did I have any browser open. It just - it was the empty machine with nothing running. But it said, uh, no, sorry.

Leo: That's funny because I was going to investigate because it failed. And I thought, oh, I must have something going. So even then. But yet it did it later.

Steve: Yes. Well, I just stopped, I rebooted, tried it again, and second time was a charm

in this case.

Leo: All right. I'm going to do that.

Steve: Who knows what was going on. But it's like, okay, fine. And so it did a 158MB update and restarted the machine after that. Actually, it didn't. It didn't need to. I did just because...

Leo: Why not?

Steve: ...reboots are good, yes, and I had time. But it did not make me reboot afterwards.

Leo: Just to recap, what was the flaw?

Steve: You know, I wish I were better prepared to answer. I've forgotten now what it was.

Leo: Yeah.

Steve: I know that...

Leo: I know it was very serious. It allowed a hacker to craft a malicious Java applet and put it on a web page that would, without warning, I think, give them access to your system.

Steve: That's exactly what it was. I'm just bumping back here through...

Leo: Well, anyway, people can explore that.

Steve: But essentially, get it.

Leo: Yeah.

Steve: You know, this is not one where it's like, uh, do I really need that or not? Yes, you do. You want that.

Leo: Yeah, yeah. Thank you, Apple, for - you know, it's interesting what happened there. We talked about this a couple of weeks ago. The guy who discovered this

exploit finally tired of Apple's inaction.

Steve: Right.

Leo: And as sometimes happens in the security community, he pressed the company into action by releasing code.

Steve: He said, okay, you guys have had lots of time to get this fixed, and you've had notification. So...

Leo: It's on you now; you know?

Steve: Exactly.

Leo: And it worked. I don't know if that's the best policy. But boy, Apple does sit up and take notice when all of its users are at risk.

Steve: Yup, yup. Well, and oddly, it's been a very quiet week in security. So that's all I had to offer...

Leo: Good.

Steve: ...in terms of news and anything that is significant.

Leo: You'll never hear me complain about that.

Steve: I thought I would take that example to, or I would take this opportunity to share a little bit longer, although when I was actually reading it, it's like, okay, it's not that much longer, little SpinRite story from a David Brant, who sent this at the beginning of June. He said, "I've owned SpinRite for a couple of years now, so I have a ton of routine SpinRite success stories that I could tell. But that would just bore you." Maybe not.

Leo: I don't think it would bore Steve, no.

Steve: "So I selected two unusual stories for your entertainment."

Leo: Oh, all right.

Steve: "First story: The patient was an aging Pentium 4 PC with 4GB of RAM running

Vista."

Leo: [Doddering voice] "I'm a Pentium 4."

Steve: Yeah, I know. I was thinking, running Vista? Okay, I guess it's...

Leo: I don't know how.

Steve: "One fine day I was just writing something in the word processor when, boom, a blue screen. A real bad one. It wouldn't boot. I couldn't even coax it into Safe mode. Nothing. The SpinRite CD was sitting there on my desk, so I stuck it in and Level 4'd it." We're now using SpinRite's levels as verbs. I Level 4'd it. I gave it a Level 4.

Leo: Oh, dear.

Steve: Take that. Take that.

Leo: Is that the highest level of...

Steve: Yeah. That's full deep cleaning, just, yeah, exactly. He said, "I came back the next afternoon and tried my luck. It booted straight into Windows without even offering Safe mode, as if nothing had happened. Even my document that had been open at the time of the BSOD..." - which is the acronym we know as Blue Screen of Death. You have to imagine that Microsoft's not happy with that particular acronym.

Leo: No, no.

Steve: So, he says, "I looked around and couldn't find any evidence of lost files. Perfect. So I just went right back to work on my document. About 10 minutes into my new work session, Vista put up a friendly dialogue, telling me that the license for this copy of Vista was already in use on another computer.

Leo: Oh, geez.

Steve: It only gave me the option of purchasing a new license from Microsoft. Oh, really. Well, that was it. That was really it. I closed my document and quickly copied all my files to another computer. I shut down the machine and removed the hard disk. I carried it into the next room where I installed it as the third internal in my main workstation" - get this - "formatted it under Mac OS X Extended, and put it into service as a documents disk."

Leo: Oh, that's an interesting choice.

Steve: This guy has obviously multiple platforms and machines to run on. And he thought, hey, I'm not buying another copy of Vista just because Vista decided that I've pirated it. I'll just turn it into a document storage. He says, "That was about a year ago. It has been working perfectly ever since, thanks to the Steves." And he made that one plural, apparently lumping me in with Jobs. And then he says, "P.S." And of course remember this guy's name is Dave Brant. He said, "P.S.: As I write this, I am half watching a little sci-fi flick in which another Dave has also become quite exasperated..."

Leo: "I'm sorry, Dave."

Steve: Uh-huh, "...has also become quite exasperated with his computers telling him what he can and can't do. He also decided to dismantle it. Perhaps this was Kubrick's most prophetic insight..."

Leo: [Singing] "Daisy, Daisy...."

Steve: "...into the world of the 21st-century computing."

Leo: You know, I use that - of course talking about Hal in "2001," I use that on my radio show. Almost - at least monthly somebody'll call up and say, "My hard drive, I've been getting strange errors or whatever." And I'll say, "Well, immediately back up because it could be failing." But it's still operating, or it's making funny noises. So I always use that line from "2001" where Hal says, "I suggest we put the unit back into operation and let it fail." Because, you know, I mean, well, I usually say, "Buy SpinRite." And then when they balk, because they often do because SpinRite costs about the same as a new hard drive - people buy SpinRite when they have data that they've got to get back; or, and this is why I bought it say back when, if you use a lot of drives. If you're always, you know, if you're putting - we go through a drive a week on the TriCaster, stuff like that. If you're, you know, we have dozens of computers. In fact on my desk I have dozens of computers. If you're always using new drives, then it's really worth, what is it, 80 bucks?

Steve: Yeah. 89.

Leo: Yeah.

Steve: So his story number two is a different one, but you'll like this one because it sort of relates to what you were just saying. He says, "This time the patient was an elderly Series I DirecTiVo."

Leo: Oh, yeah. Those are like gold because they're not protected.

Steve: Right. Or, well, they often have...

Leo: Less protected.

Steve: Yes. Actually they're hacker-friendly. You can do all kinds of things to them. And you can get them with lifetime paid-for subscriptions that never expire as long as TiVo doesn't go out of business. So he says, "...an elderly Series I DirecTiVo. It still worked fine except that the menu system had gradually become dead slow. It had gotten to the point where it would take a minute or longer to respond to a single down-arrow press. Once you had brought up the main menu, it could take as long as 15 minutes to navigate down the Now Playing list to choose the show that you wanted to watch."

Leo: Now, my experience there is if you reset the TiVo it usually, you know, erase all data and start over usually fixes it.

Steve: Well, he didn't have to do that. You know what he had to do.

Leo: Oh, interesting.

Steve: He says, "I realized it was time to act. I wrestled the hard drive out of the TiVo." And actually that is - that does take some wrestling. They use the Torx screws for everything. And you have to have a #10 and a #15, I think they...

Leo: I have my Torx tools with me at all times.

Steve: He says, "I wrestled the hard drive out of the TiVo and installed it in a spare PC." He says, parens, "(See story number one, above.)" So that was apparently the machine that was now free of its hard drive he used as his SpinRite operating station. He said, "I planned to Level 4 it, but needed to change my plan. Instead of the usual screen, SpinRite put up a screen that said something like, 'WARNING: DANGER AHEAD.'" He has it here in all caps. He says, "I forget the exact wording. It had determined that drive failure was imminent and even one SpinRite run might be the last thing it ever did. It told me to copy any files I could first. But I decided to go for it anyway. When it got started I noticed on SpinRite's SMART monitoring screen that the top row was all red. No wonder."

Leo: Wow. That means - all red means that the sectors are bad?

Steve: It means that the - and the reason he immediately got that warning was that SpinRite was - one of the first things SpinRite does is ask the drive, "How are you feeling today?" And the drive was able to say, "I'm really sick." In which case SpinRite says, "Whoa, hold on. Just to let you know, the drive is saying that it doesn't have much life left." Which is really, it happens in this day and age, and real-time continuous background SMART polling is one of the features that I added in the SpinRite 6 from SpinRite 5. Remember it was a little controversial at the time among our developers, the people who hung out in the SpinRite.dev newsgroup because they were saying, "Oh, you

can't really be polling SMART all the time." And I said, "Why not?" "Well, we don't know. But we heard you can't." That's like, okay, fine, well, I'm going to ignore that.

Leo: SMART has a lot of - SMART has a lot of mythology because it doesn't, you know, it kind of works, it doesn't work, I mean, nobody knows what it's supposed to do.

Steve: Yeah, well, and the problem is that there isn't a defined set of meanings for these parameters. They're just sort of like, oh, it's not as good as it should be, or it's like sort of a number. It's like, well, what does that mean? We don't know. But if it's lower, that's worse. It's like, okay, fine.

Leo: Um, okay.

Steve: So anyway, I've managed to integrate all that into SpinRite so that it does the right thing. And in this case SpinRite was saying right off the bat there's a problem. So he says, "It survived its intense SpinRiting, seemingly without expiring on the operating table. I reinstalled the drive into the TiVo and hoped for the best. I went into the menu after bringing up the TiVo and found that the problem was completely cured. The menus were now as fast and responsive as new. So maybe a routine run of SpinRite every few months might help a sluggish PC, as well.

Leo: Okay. It would, wouldn't it. Because as we've talked about before, sluggish can mean it's just trying really, really hard.

Steve: Well, I would say it could.

Leo: Could.

Steve: Wouldn't say it would.

Leo: Yeah.

Steve: In the case of DirecTiVo, well, or any of the TiVos, one of the things that they do is they redundantly store all of the critical system files and other material in multiple places, specifically so that it can generally survive the slow death of the hard drive. You know, there's no provision for TiVo to say the hard drive is having trouble because it's meant to be a turnkey consumer product that you just sit down and plug in and you never think about it. I mean, the idea of, for me, TiVo is always recording. Everything coming in is going onto the hard drive into an on-hard-drive buffer. So when you pull the cord out of it the way you do a VCR or a clock radio or anything else, you've just blown whatever chunk of drive was underneath the head at that time because it was busy writing. So when you pull the plug out of it, it's unable to finish that. But the TiVo system is designed to heal itself, or at least survive that kind of abuse. For myself, I always go into the menu system and do a system reset if I'm going to unplug it. That way basically

it's rebooting, and it's not in a mode where it's writing to the hard drive. Then I'll pull the cord out if I have to move it somewhere else, or if our power company has notified us we're going to have a power failure in the afternoon to repair equipment and so forth. So, yeah.

Leo: Very, very good stuff. You know, if you've got one computer and one hard drive, okay. But, yeah, everybody should really own SpinRite. I just think it's just a natural thing. And a TiVo. That's a really interesting use of it.

Steve: Well, we do hear from a lot of people who have SpinRite and who say, hey, I'm still waiting for my success story. I'm running it on all my drives. So maybe I'm never going to have one.

Leo: I think you need it less if you use it all the time; right?

Steve: Oh, you probably need it never.

Leo: Right.

Steve: I mean, all these stories where finally the drive died on some event, some morning, his BSOD where he ran it and it fixed it. Had he run it the day before, it wouldn't have died the day after because it would have had a chance to, I mean, it's sort of like you could think of it like defragging, but in the preventative sense, like defragging puts things back where they have sort of wandered off from. Well, running SpinRite really reads and rewrites the entire drive in a way that allows the drive to deal with incremental low-level problems, underneath the level of the file system, before they get to be really severe. So certainly a good thing.

Leo: All right, Steve. Let's talk - you're going to - okay. Steve has a challenge. He's going to make me jealous. How could you possibly make me jealous? I have built-in compression on my Mac. What more could I want?

Steve: Well, what...

Leo: That's a setup.

Steve: Yeah. What PKWARE has done is they've evolved their PKZIP program - and PKZIP still exists separately from SecureZIP. SecureZIP offers all of the kind of technology we've been talking about in the past in a really simple-to-use, state-of-the-art, really pleasant user interface. But they've basically taken all of the configuration and setup hassle out of the process. The program will compress files in ZIP format, TAR, BZ2 - which is Block Zip 2 - BZ2, GZIP. It'll UUEncode, XXEncode. Also will compress in LZMA, PPMd, and Java (JAR) files. It can open and decompress ZIP, TAR, JAR, BZ2, RAR, GZIP, CAB files, LZH, LZMA, PPMd, UUEncode and XXEncode. So it's not just ZIP format. It's a broad spectrum archiving utility.

What really makes this thing stand out is the built-in and really easy-to-use support for asymmetric, that is to say, public key encryption. As you install this in your system - it's about a 20MB download. They use CacheFly as their delivery system. If you just put into Google "SecureZIP," the first link that comes up is to the free SecureZIP download. There is a commercial version for the individual user. There's also lots of enterprise support for this. So for our listeners that have more of the corporate IT enterprise side, keep that in mind when I'm talking about this. I'm focusing sort of on our typical listener end-user person. But there's tons of enterprise stuff.

So if you wanted a purchase-it version, it's $39.95 for a single end-user person. But what that gives you is integration into Office and email, that is, seamless integration where, like, in the file menu of Word there's "Save as a secure file." And so it's just as simple as selecting that option in the file menu, and you're able to do that. So the free version has that stuff for 30 days so you can see what it's like, decide if it's worth to you $39.95 to keep that after 30 days. If so, you're able to upgrade and do it. Otherwise it'll go away after a month. And you're still able to use SecureZIP with its nonintegrated features, which is just like a standard archive manager, which in my opinion is still spectacular. I'll explain why.

During the setup you give it your name and your email address. It then transparently, sort of automatically, goes to Comodo and registers a certificate, a standard PKI - Public Key Infrastructure - certificate, under your name and email address and creates it, downloads it, and installs it, all sort of automatically. So you end up with a private key installed in your certificate store in Windows which you're able to use to sign or encrypt any of the archives that you create with this. So the other thing that you get is it automatically places this in the SecureZIP global directory for - that is, it places a reference to your certificate, and the public key is available globally.

So what it means is that somebody else who is also a SecureZIP user is able to build an archive that they want only you to be able to access. They literally, when they say they want to encrypt it, they're able to put your email address into the program itself, which transparently queries the global directory to get your public key. It then encrypts the archive using your public key, creating an archive that absolutely only you, that is, the machine where you've set up your SecureZIP, are able to decrypt. And what's even cooler is, if you only select that user's public key, you get a little warning dialogue that says, hey, we're happy to do this for you, but you're encrypting this with only this public key. Not even you can decrypt it. And so it says, you know, you could if you'd like also encrypt it with your public key so that you have the option of decrypting it if you ever, for whatever reason, want to. So it gives you a little reminder that basically, when we're saying only that the destination user can decrypt it, we're not kidding.

Leo: Right.

Steve: Now, we know...

Leo: That's great. That's really neat, yeah.

Steve: Oh, it really is cool. And the other thing you can do is you can sign it. Since you and only you know your private key, you're able to sign the archive or sign a file. You don't even need to encrypt it. You can just use SecureZIP as a public key technology

signing tool. So you're able to apply your digital signature to the archive. So you could do two things. You could encrypt it using a public key that is just found for you using your target user's email address, which this thing finds for you. The whole thing is transparent. It just says, oh, here's the person. And you go, yeah, okay, cool. I want to encrypt it for them. And I want to sign it so that they know whatever this is actually came from me. So that process is just done beautifully. I mean, I'm really impressed with the whole UI of this. It just couldn't be any easier.

Then you end up with this ZIP file, which you can then email or stick on your website for somebody, I mean, get it to them however you want to. But only their system where they have this certificate installed is able to read it because - so they've got the private key on their system. So when this ZIP comes, they're simply able to open it. I mean, it'll open. It won't open anywhere else, but they're able to open it.

And in addition to all this, you also have secure passphrases so that you could also protect it, not only with a public certificate, but you could also protect it with a passphrase that's as long as you want it to be. There's a big, plenty ample dialogue box where you're able to type in anything that you want to, which will further lock this ZIP so that the recipient would have to have both the knowledge of the passphrase that you used this particular time to send or encrypt this particular ZIP file, and they would have to have a digital certificate. Or you don't have to use digital certificates. You could just use a passphrase. So you could use either a passphrase or a digital certificate or both.

And say that you wanted a ZIP file that three people would be able to see, would be able to open, but nobody else. Again, you're able to simultaneously apply multiple digital certificates so that you've got multiple - you've encrypted it once, yet you've then encrypted the symmetric key which was randomly arrived at. Remember we've talked about this multiple times. You don't actually encrypt the payload of the ZIP with your public key. Instead on the fly you create a so-called "session key," a long, 128, 196, 256-bit whatever, and all of this is just done for you. You create a completely random session key. That's what you encrypt with your asymmetric key. And then the encrypted result is just bundled in with the ZIP.

So the idea is, if you wanted three different people to be able to decrypt this ZIP file, you're able to attach their certificates to that file. And essentially it takes their public key and encrypts this one-time-use symmetric key for each of them and connects it. So that when any of them receive it, they're able to open the file, and they're able to inspect the certificates that are bundled along with it. And, for example, if you decided you wanted to sign it securely, they're able to inspect the signature to verify that it came from you.

It's just - it's beautifully put together. I mean, and I would recommend it, frankly, to our users, if they want to play around with public key infrastructure technology. We've talked about this over and over extensively. Here's just a useful and simple-to-use turnkey application that incorporates all of these concepts that we've been talking about in something which is extremely easy to use.

Leo: Sounds...

Steve: And it doesn't run on the Mac.

Leo: That's okay. I can live. I can live. It does sound great. So reiterate. The

features that I'm not going to get if I don't pay for - I know I get to try them at first.

Steve: Yes.

Leo: But the features that will turn themselves off after, what is it, a month?

Steve: Yeah. All they are, the only things that die after 30 days are the integration into Microsoft Office and Outlook.

Leo: I don't even use those, so I can live without that. That's fine.

Steve: Right, right. But all...

Leo: Everything else works.

Steve: Yes. Everything else works.

Leo: Wow, that's great.

Steve: The certificate has a one-year life. And it is possible, though, to renew it. I also, just for the hell of it, I went over to Comodo, and I said, hey, let's pretend you just didn't make a certificate for me through this built-in UI that was easy. You're able to go, if you put into Google "Comodo personal certificate," the first link that comes up, again, is to Comodo's free certificate. They call it an email certificate, which is the one that we're using for this case. And it's completely free.

So I tried this. I created a - I went to Comodo. I said, hey, I want a certificate. I used a different email address, gave them my name. They sent me email containing an authorization code. I clicked on that. The browser, using scripting, automatically created with Comodo, and without me having to do anything else, a certificate just like the one which had been created for me automatically during installing SecureZIP, and installed it in my machine. Now I have two. So I didn't even need to use the certificate that SecureZIP created on the fly while I was installing it. I was able to use that.

And you are able to export the certificate that you've created. If you, for example, were someone who had multiple laptops or multiple computers, you didn't want to only be tied, didn't want that certificate tied to one machine, you are able to export it and import it into other Windows platforms. So, for example, you create one certificate, and you stick it on the various machines you're using. All of those will be able to open ZIP files which have been keyed to your certificate, even though they're on different machines.

Leo: You know, one thing I did - I'm looking on the web page. It just says "across all major computing platforms." But correct me if I'm wrong. It sounds like if I use

SecureZIP on a file, I cannot unzip it on a Mac, for instance.

Steve: Yes, I'm sure that's true.

Leo: Yeah. So that's a little misleading when they say "all major computing platforms," and they leave out Macintosh.

Steve: Yeah, or the Linux desktop.

Leo: Or Linux. I mean, it's really - it's a Windows application.

Steve: Well, they also - they do have support, non-desktop support for UNIX and Linux servers, they say, for Windows clients and servers, and then a bunch of IBM machines, like mainframe sort of world.

Leo: Oh, I see. Okay. Okay. I get it. Yeah, wow, that's neat. So the certificate I get from Comodo, I don't get from PKWARE.

Steve: I hope I didn't confuse people with that. Either certificate works.

Leo: Oh, I could use PKWARE's, as well. Okay.

Steve: Yeah. Well, and PKWARE's actually - PKWARE got theirs from Comodo. They just did that negotiation...

Leo: Automatically.

Steve: ...through the user interface automatically.

Leo: I see, I see.

Steve: And I was just curious because, okay, so the certificate lasts a year. And when you first get it you'll see, for example, mine said, oh, it's good until 6/17/2010. So I'm thinking, okay, what happens after that? I don't want everything to die or, like, things to stop working. Well, first of all - and I posed the question to the guys at PKWARE. And they said, oh, you know, you'll get email two weeks before it expires, telling you here's the link you click to renew it for another year. And as long as Comodo or anyone makes certificates available for free, you'll always be able to create certificates. And even if a certificate has expired, all that happens is it's expired. Remember we talked - actually, coincidentally, we answered this question in last week's Q&A. Someone said what happens if - like in this case it was a web server certificate expired. And I said, well, the

only thing that happens is you're warned that this server's certificate is expired. But it still works. And that's absolutely the case with SecureZIP. So you could be using a certificate if you were a curmudgeon and for whatever reason five years from now you didn't want to keep updating a certificate. You're still able to use it, and it still works just fine. It'll just be giving you warnings saying that the certificate you're using is expired, just FYI. But it's easy to renew, and still free.

Leo: Cool. And somebody who sees an expired certificate may be a little nervous at that.

Steve: Well, yes, that's exactly it. So, for example, if you didn't renew your certificate, and you told somebody to send you a ZIP file - so essentially what this means is that you would be using SecureZIP, and anybody else could send you a ZIP content that is, like, the industry's strongest available security that only you can open. And so they're able to encrypt it knowing that only somebody with your private key, which is installed on your machine in the Windows certificate store, is going to be able to open this file. So they might wonder why they were being warned that the certificate that you've told them to use is expired, though they still could use it.

Leo: Well, this is good. Yeah, I'm going to download it on my Windows machines. And be nice to have it on my Mac. But that's - so it's really - it still can be used as a ZIP utility. But really, I mean, the idea is transfer and protection of files and encryption.

Steve: Well, yes. It's absolutely...

Leo: Does all the ZIP stuff, yeah.

Steve: It's got all the ZIP stuff. It's multi-format, you know, BZ2 is a...

Leo: Oh, is that built in?

Steve: Yes.

Leo: Oh, I love BZ2.

Steve: Yeah, I was going to say, it's probably my favorite compression mode because it gets really good compression.

Leo: I think it's - I don't know of anything that does smaller, let's put it that way, unless it's a specialty for a certain kind of file format.

Steve: Right, exactly. That Block Zip 2 format, that block zip compression is really good

compression. So it will do ZIP and TAR, BZ2, GZIP, among others. So I'm just very, very impressed. I think for users who are curious, or I should say our listeners who are curious about learning about, or like, you know, having experience of public key stuff, and certainly anybody who has this need - again, I'm a little maybe of an exception. I just - I'm not needing to send secure stuff from one place to another. But I know I've got some friends who, as I said at the top of the show, if I told them about this, they'd be using it all the time. They'd just think it was so cool to be able to send ZIPs to me that only I could decrypt. And in fact, if you put "Steve Gibson" into the global directory, you will find me now under SecureZIP since I just used my name when I set up my certificate. And it's like, oh, you know, cool. There's my public key, which is available globally to anybody who wants it.

Leo: Very good, Steve. That's a nice find. A lovely little program.

Steve: Thought I wanted to tell our listeners that it's very, very cool.

Leo: PKWARE.com. You can get it right now.

Steve: Yup.

Leo: And Steve, we'll see you next week for another great lesson in security. Everybody should go to GRC.com, by the way. That's where you'll find SpinRite, the world's best hard drive maintenance and recovery utility; also Steve's free stuff like ShieldsUP!, Wizmo, Shoot The Messenger, DCOMbobulator, Unplug n' Pray, and soon some wonderful new software, I know, I know.

Steve: Coming, yes.

Leo: And find out more there about Perfect Paper Passwords, too. Also show notes; transcriptions for every show, so you can read the shows; 64 and 16KB versions for the bandwidth-impaired. It's all at GRC.com. And next week we're going to do question and answer. So if you go to GRC.com/feedback, you can leave a question for Steve, and he'll be glad to answer at least 12 of them next week.

Steve: Yes, and please do, again, GRC.com/feedback. I really, really love to get everyone's thoughts, feelings, feedback, ideas, everything.

Leo: Steve, have a great summer day. We'll see you next time on Security Now!.