SECURITY NOW!

Transcript of Episode #99

Trusted Platform Module (TPM)

Description: Steve and Leo explain the virtues and misbegotten negative reputation of the entirely benign and extremely useful emergent crypto facility known as the "Trusted Platform Module."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-099.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-099-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 99 for the 5th of July, 2007: TPM.

It's time for Security Now!, the podcast that tells you why you should be afraid and what to do about it. Steve Gibson's here.

Steve Gibson: Now, we don't want to be accused of unnecessarily alarming people, Leo.

Leo: No, no, but it's true that there are things to fear. Fear's not the right word. Things to prepare for.

Steve: You know, I have to confess, and actually I mentioned this during the presentation, remember I was off in Cambridge speaking to - I was actually the keynote speaker for a conference that Harvard was hosting last week.

Leo: Wow, that's pretty prestigious.

Steve: And I've noticed that my own awareness of these security issues is heightened as a consequence of listening to myself when I'm, you know, talking to you.

Leo: Yeah, so you don't normally listen to yourself. No, it does, you know, and I'm not - "scared" is absolutely the wrong term. We're talking about what you should be aware of and what you should do prophylactically to protect yourself, that's all. And I think half of the value of this, maybe more, is just learning about all these interesting technologies, like crypto, that is useful. We're going to learn about one today that's very interesting.

Steve: Well, we are. And in fact I've had more and more people whose postings on the Security Now! page when they're submitting things are saying, you know, when you and Leo wander off topic, it's just fine. So don't let those grousy people who are complaining, you know, that you guys are talking about non-security stuff restrict you from doing so because...

Leo: That's why we do podcasts. If we wanted to keep on point we'd do it on the radio or on TV. Or we'd give speeches at Harvard. So today we're going to talk about TPM.

Steve: Yes, the Trusted Platform Module. It's something I've actually been looking into now for months in preparation for finally getting enough of a feel for it that I could characterize it. It's been an elusive thing for me to get a handle on because it's not - I don't know. I mean, now I have it, and it feels like, ah, well, of course, now I can explain what this all is. But for the longest time I just - I didn't get what it really was, where the limits were, where the boundaries were. I now understand it well enough, I think, to give people a coherent sense for what it's all about.

Leo: And it has been very controversial. So we'll talk about that, too. Let's...

Steve: And I know why, and I know why it was mis-marked. So, yeah, we'll definitely - don't let me forget to talk about that.

Leo: Yeah, we'll address those controversies.

Steve: I have to say now that I'm, you know, well, first I should mention that you and I are recording two podcasts today. We're doing 99, which is this one; and we're going to record next week's immediately afterwards. I guess are you...

Leo: I'm going to Canada, yeah.

Steve: You're up in Vancouver doing...

Leo: Steve is so dedicated. Some of the podcasts, the news ones, when I'm in Canada we don't really do. But Steve is so dedicated that we do two ahead of time so that we don't miss an episode. Possibly because you want to get to 100.

Steve: Well, yeah, we are there now.

Leo: We're one away. One away.

Steve: What I wanted to mention is, being 100 we're at a mod 4 also, of course, so it's going to be a Q&A episode. And so this morning I was rummaging through and catching up on a lot of the postings to the Security Now! page. And I don't know what's happened, Leo, but there's been a clear increase in, I don't know, our listeners' involvement and participation and feedback. What I'm getting is so much good commentary that - so I want to share some of it today. But what I'm thinking of doing maybe is we're getting so much good feedback from people, I mean, really interesting stories and sort of tangents off of what we're talking about that I'm - I mean, and so the mailbag is full to overflowing at this point - that I'm thinking maybe of doing mod 4 plus 2 would just be mailbag episodes.

Leo: Okay.

Steve: So the idea would be...

Leo: All mailbag, the whole thing.

Steve: Exactly. Because, I mean, there's a couple long ones that I want to share with people because they're really neat. And then we'll discuss them, of course. So it'll be like, you know, interesting stuff that our listeners are providing for us to talk about; not just a question to be answered, but whatever it is they want to discuss. And so we'll alternate between regular shows and mailbag and Q&A, essentially. So mod 2 plus 4 will be mailbag. But in the meantime, you cannot believe how many people told us how to pronounce the unpronounceable...

Leo: Aberystwyth.

Steve: Exactly. And it's Aberystwyth [aber-rist-with].

Leo: Aberystwyth.

Steve: Aberystwyth. And...

Leo: Well, you know who grew up next door, our very own Will Harris.

Steve: Oh, no kidding.

Leo: Yeah. So he of course immediately called me and said c'mon, mate, it's Aberystwyth or whatever it is.

Steve: It's Aberystwyth, yes. So I wanted to acknowledge everybody who posted, okay, here's how you pronounce that. So we now know.

A listener in Sacramento, who must have been anonymous or I would have put his name here, mentioned that referring to the - my mention that the - this was from our episode last, the identity metasystem stuff, where we were talking about Microsoft's...

Leo: Meta authentication, yes.

Steve: Exactly. We were talking about Microsoft's CardSpace. And I mentioned how I liked the prior name InfoCard better, that was their working name. And he commented that InfoCard is an Apple trademark because there was something called InfoCard back in the iMac days. He says he has an old copy of it, and that's why Microsoft was unable to use it.

Leo: Interesting.

Steve: Which, you know, it may be very true. I don't know that for a fact, but certainly sounds...

Leo: I never heard of it, but I'm sure it's, you know...

Steve: Plausible.

Leo: Who knows, yeah.

Steve: Bill Holton of Gainesville, Florida writes that he is human. And that reminded me that I had said, maybe it was in last week's podcast, that this week we were going to be talking about CAPTCHA technologies under the title "Are You Human?" And it wasn't until I saw his posting that I thought, ooh, that's right, that's what we were going to talk about. But I was all revved up and geared up to talk about TPM. So we'll perhaps do that next week. Not really sure. But anyway, he says...

Leo: It won't be next week, it'll be two weeks because we're doing...

Steve: Oh, there, thank you, Leo.

Leo: So 101 at the soonest.

Steve: So, oops. And that would be a mailbag episode already. So anyway, but...

Leo: We're out of control.

Steve: Oh, no, wait, it wouldn't be because of Q&A.

Leo: No, it wouldn't be, yeah.

Steve: Because mailbags are definitely divisible by two. So Bill Holton says, not only is he human, but that most computers don't think he is because he's blind.

Leo: Uh-huh. CAPTCHAs are a notorious problem for people with poor vision, yeah.

Steve: And so he says, "The increasing use of CAPTCHA is locking me and others like me out of more and more sites. When you do your 'Are You Human' podcast, please mention the need to find non-visual-based CAPTCHAs, and ones for the deaf blind" - oh, that's going to be a real challenge - "who can't even use the audio CAPTCHA sites like Google and Yahoo! are adopting to help the blind get around the CAPTCHA problem. You may want to try the audio CAPTCHA to see how unusable it is...."

Leo: Oh, you want to hear the audio CAPTCHA on mine? I'm using now for my emails, to avoid spam, I'm using the Carnegie Mellon one, which I know you're going to talk about because it's a really cool idea. It's the reCAPTCHA. And I thought, oh, this is great, because I had been sensitized to the issue of CAPTCHA. That's where they put that weird text that you can't - that machines supposedly can't read, and humans barely can. And you type it in, and then you know you're not a machine. But the problem is, of course, if you can't see, you can't type it in. So this has audio. But listen to this. This is how they get around the machine reading the audio.

[Audio CAPTCHA]

Steve: Oh, my God.

Leo: You can do it, though; right?

Steve: So they've done the same thing with the audio that they have done with the visual.

Leo: Yeah, exactly.

Steve: Oh, my God. I mean...

Leo: But, you know, I could do it.

Steve: I've got to say, sometimes I cannot type in the visual CAPTCHAs correctly.

Leo: Me, too. They're very difficult. And I have to say the audio is difficult, too. But that's kind of the point. I mean, I understand that it's difficult. You only have to do it once on my site. You get the email address, and you can use it from then on. But...

Steve: Not right.

Leo: ...you know, it's tough. Accessibility on the web is getting harder and harder as we get more and more Flash and scripted stuff. And it just - it's difficult. But it's certainly worth doing. We're redesigning the radio show site, and that's one of the things that has a very high priority is to make sure it's accessible. A lot of blind people, of course, listen to the radio. And podcasts, I might add.

Steve: Yeah, that really does make sense. Okay. Last mailbag submission. It was a long one, but interesting. Jeremy Clark of Ottawa, Canada says, "I love the podcast, and I listen to every single one. I think you have got EV certificates all wrong, though."

Leo: What's that?

Steve: Now remember the EV, I mentioned and was grousing about it a week or two ago. Those are the things that are super expensive from VeriSign which are what enables you to get the green background in IE7 as a phishing preventer. And the idea is that, you know, I'm already unhappy that this whole certificate thing just seems like such a scam, that they expire every couple of years, and I've got to pay $700 or something like that for another two years. Their EV is Enhanced Verification or some acronym of that sort, for which they get a ton of money. Anyway, he says, "EV certificates are a signal of legitimacy, not of security."

Leo: Yes.

Steve: "And they were created specifically to combat phishing."

Leo: Right.

Steve: "In the days before international banking, banks would build elaborate buildings. The reason for this is often considered by non-economists to be competitive. However, economists know that if it were out of competition, there would be similar architectural arms races in other industries. Yet banks were different somehow. The real reason is that the bank could afford to build beautiful buildings, while the fraudsters, who would open a bank and then skip town with the money deposited, could not. A baroque building was a signal of legitimacy. These scenarios are called 'signaling games' in economics and game theory that only a legitimate bank could afford to send.

"The problem in the online world, as you well know, is that people use the same rationale. If they go to a phishing site, and it has a nice layout with scripting and menus and animation, they assume it's real. Enter EV certificates, the online equivalent of building a nice bank. It only makes economic sense to get one if you plan on sticking around. A nice website is a signal that anyone can duplicate, and therefore it isn't a good signal at all. An EV-enhanced certificate that costs $15,000 per year is not easily duplicated and therefore is an effective signal. If you are legitimate and can't afford one, you probably are not a target for phishing in the first place." Which actually I thought was sort of a really good point that he made. "If you don't have the same need to signal your legitimacy as PayPal, eBay, Amazon, or an online bank, all of whom can afford one." And then he says, "I've written more on this exact topic if you're interested," blah blah blah. But anyway, I just - I loved what he said. I mean, this is the kind of really good stuff that's appearing in the mailbag now, so...

Leo: Yeah, it's fascinating. There is, I think, a flaw in the logic there I have to point out, which is that because maybe - and maybe it's a flaw in the way it's been communicated what that green bar means. But as long as you're doing that green bar, pretty soon people associate it with safe. And as he points out, you know, you can be safe and not be able to afford it. Unlike a bank, where you're saying, well, if he's a big bank he's going to be able to afford a nice building. It's not necessarily the case. So on a website, you know, you could be legitimate. And he says, well, it doesn't matter because nobody's phishing you. But it does matter to the end-user because they pay attention to whether there's a green bar or not.

Steve: Yes, exactly. And that's, of course, the foundation of my gripe is that...

Leo: Right. You're legitimate, but you can't afford it.

Steve: Well, I don't want to. Because, I mean, it's just extortion.

Leo: But he makes a good point. Nobody's going to phish GRC.com. Actually, I take it back. And that's the other flaw in this, is he's assuming economic gain. And if it's pure economics, that's true. But people might phish GRC.com to put a fraudulent security program out.

Steve: Sure.

Leo: So that isn't purely economic. So there are some flaws. This isn't exactly analogous to the bank. I think your gripe still stands. People would want to phish GRC because they could say, hey, get our free new security program, and it's a Trojan horse.

Steve: And if were something I could buy once, if I could get a lifetime - well, in fact that would create the kind of lock-in that VeriSign would like to have with their customers because, you know, in fact, they sent me a questionnaire the other day saying oh, how happy are you with our certificate services? And I just - I took the opportunity to tell them exactly how I felt about the fact that I was having to fork over all this money every couple years. I said, you know, I like your service. I've used it for years. But boy, if anyone came along that offered, you know, the same thing for less money, there is not much lock-in here. But as I was going to say, I would buy it once. I'd even spend 15 grand one time, if then I could have, like, a reduced annual rate and still get the greenness, having paid for it once.

Leo: Well, and again, I think there are people who are giving away good, free, legitimate security software who might be phished who have no economic value and no economic incentive and still can't afford this for a very good reason: They're not asking people to pay for it. So I think this is a particularly capitalistic point of view on the situation and doesn't really address the real issue. I agree with you, Steve. I don't even think it should be $15,000. I understand; but, you know, there are ways now to validate somebody without making them pay a lot of money. That's pure greed, I'm sorry.

Steve: Yeah, I know.

Leo: That's pure greed. We're not in the 18th century anymore.

Steve: And I think Jeremy did have a typo. I think it's 1,500, not 15,000.

Leo: Yeah, it's not 15,000, yeah. But even that's a lot.

Steve: I did have one more note here. I scrolled down. That one was so long. I have Eric Espinoza of Pasadena in the mailbag. He says, "I'm a systems security guy for a government organization." And actually his email gives it away, he's a well-known propulsion laboratory.

Leo: Oh, okay.

Steve: So he certainly does know his technology. He says, "...and have followed your podcast since the beginning. I usually recommend this podcast to people showing interest in technology. There are a few things we disagree on, but for the most part we're on the same page on everything. Just wanted to give an anecdote about how checking the certificate for a VeriSign or Thawte or {insert your trusted provider here} is not enough to ensure integrity of the site. My girlfriend, after seeing 'Blood Diamond,' which is a recent movie, is not any longer into mined diamonds."

Leo: Awesome.

Steve: "She prefers lab diamonds..."

Leo: Good for her.

Steve: "...and asked me to get her a pair of earrings from a site she saw advertising in the L.A. Times called 'Diamond Essence.' Turns out they misrepresented cubic zirconia as lab diamonds, but that's another story. I did my usual checks before putting my credit card in, which are as follows." I mean, this guy is way thorough. "Typed in the name into Google. Looked for horror stories. Checking the cert. Checked the CRL," that is, the Certificate Revocation List, "for the registrar involved. All looked good, so I proceeded. When I woke up the next day I got a call from my credit card company asking about various charges. My card had been hit by ten different places trying to rack up over $2,000 in charges. Fortunately, the bank blocked all but $10 of those transactions.

"Not being sure that this was the place where the whole thing originated, I decided to try one more time. This time I used a PayPal one-use virtual MasterCard."

Leo: Smart.

Steve: And I didn't even know that PayPal offered that. But now that I know, I'm going to look into that because that sounds like a cool thing.

Leo: Many Visa and MasterCard people do, and that's really neat, yeah.

Steve: Yeah. He says, "I had loaded up just the appropriate amount into my PayPal account and didn't allow the thing to pull from any other of my other accounts in the case of overdraft. I put the virtual MasterCard number into the site and, bam, got hit with a ton of charges that were immediately declined."

Leo: Interesting.

Steve: "I called up the company, asked to speak with management, and told him what had happened. He, probably oblivious to the situation, insisted that the problem was probably due to spam infection and so forth," you know, blah blah blah, not our problem, not our fault. "I informed him that I had already passed the info along to my bank, and that he should expect a call telling him that I wasn't being malicious, but had facts to back up that his site has been hijacked or hacked or something." And he says, "Anyways, I have tried contacting VeriSign to let them know of the incident, and today they are signed by Thawte. Not sure if they're still hacked," but I guess that means that they changed their certificate as a consequence. He says, "The point is, a valid cert is not enough certainly in every case. Unfortunately, there isn't anything better. I'm not here promoting PayPal or anything, but I think the use of one-time cards with simple dispute procedures is what is needed online. That way one can severely limit the amount of damage done. Since most hackers use a $1 charge to ensure the card is active, they'll take at most $1 from your account."

Leo: Right. Wow, very interesting saga.

Steve: So, I mean, we're just getting such good postings to the page that I think, you know, it may very well be that there'll be enough things to share.

Leo: Starting with 102 we'll be doing mailbag episodes. That's great.

Steve: And speaking of good things to share, I do have one of my really fun and interesting SpinRite success stories to share. This is from Aaron Jensen in I think it's Lumby, British Columbia. He says, "Hi, Steve. I'm a computer systems technician for a large manufacturing company. But like many others in this field I also support a few smaller clients and my family members in my off hours. I've been listening to Security Now! since the beginning and don't think I've missed a single episode. I must be honest and admit that, before you started talking about SpinRite success stories on the podcast, I was only familiar with GRC for the ShieldsUP! utility which I had been using for years in the past." So that's very cool that, you know, we're able to use this to get the word out.

"It was early into the Security Now! episodes when I had my first occasion to run SpinRite on a laptop owned by a customer's daughter. The system was only partially booting into Windows and then rebooting itself. This of course caused an endless loop many techs are familiar with. The daughter is an artist, and her laptop was the only storage location for gigabytes' worth of photos. Many of these photos were of her artwork that had long since been sold, and now the photos were her only record of these paintings in her portfolio. Needless to say she was terrified that all these images had been lost. I went online and purchased my first copy of SpinRite, ran it on the drive overnight, and the next day the system booted without even an error. We immediately backed up all her artwork photos, and she's still using the same hard drive to this day." Which I guess must be, like, more than a year ago since he's talking about early on in the podcasts that this began. So he says, "She's still using the same hard disk to this day, although she backs it up much more often."

Leo: Good.

Steve: Yeah, good. "Later I kept the copy of SpinRite for myself as it was licensed to me, but I went online with her parents and had them purchase another copy for their own use, just in case her laptop drive had more problems down the road." Then he says, "In the last year or more I've had three to four other occasions where my copy of SpinRite really saved the day. And in each case I went online with the computer's owner and helped them purchase a copy of the program. I wanted each of them to have a copy of SpinRite because it's so easy to use if they ever needed it again. Plus I really wanted to support you and the incredible job you've done with this application. These days, larger software developers seem to spend a lot of time trying to design the ultimate application for everyone. It has to do lots of things for lots of people so it can have the largest potential sales opportunities. But in my experience, I've always found that when a developer like yourself sinks tons of time and experience into an application that is designed to perform pretty much just one job, it almost always does that job better than anything else. In every case where I've had a need to run SpinRite, it has done the job better than I could have ever expected. Even my mom has all of her data on her new computer because SpinRite saved it all when her old computer's hard drive crashed."

Leo: Well, there you go.

Steve: "Keep up the good work with SpinRite and Security Now!, and congratulations on the recent milestones hit by ShieldsUP." So...

Leo: That's neat.

Steve: ...really nice, really nice posting. I thank Aaron for...

Leo: It's nice to have good customers. I like that.

Steve: Yeah. Well, and he is, I mean, I couldn't ever ask for anything more than him using his copy - which I have no problem with - to fix somebody, and then helping them to buy their own. You know, that's the perfect model.

Leo: Are we going to - I'm trying to think. Maybe we should do Nerds On Site and then we will get - no, you know what, I want to get to TPM. We've been waiting long enough, and I want to hear about it. We'll talk about Nerds On Site in a bit.

Steve: Okay. TPM.

Leo: Trusted Program Module?

Steve: Trusted Platform Module.

Leo: Trusted Platform, okay.

Steve: Okay. So what TPM is, basically it all comes down to being a chip. It is a chip on the motherboard, that is to say, on the platform. And now this doesn't have to be, though, a PC. It's entirely foreseeable that these things will be in PDAs and cell phones in the future. It is meant to be tightly integrated to the platform, that is to say, soldered onto the motherboard, although as it turns out it is on a small daughter board, even on IBM's ThinkPads, which are

TPM-enhanced laptops. So it doesn’t necessarily have to be non-removable, but it’s certainly not user-removable. That is, it’s not, you know, behind a door that anyone can open the screws and pull out. It’s meant to be integrated onto the platform. So the reason it’s called Trusted Platform Module is it is a component, like the processor chipset and so forth, that is not user-removable. And that’s part of the benefit it provides. So it is inherently just a microcontroller. It’s a smart engine that has a number of characteristics.

The good news is, it is completely open. The specification is open, freely downloaded. There is source code now that is completely open source and GPL’d. And, for example, Linux has drivers that can use the TPM. It got off to a somewhat rocky start because when Microsoft announced Palladium - that is, you may remember, Leo, their very controversial, we’re going to lock the system down so tight that nothing will be able to escape it, and we’ll know exactly what’s going on. I mean, Microsoft’s Palladium announcement raised a ton of controversy in the industry. Well, TPM is related very peripherally, if you’ll pardon the pun, because it is an enabling component of Palladium; but in no way is it Palladium, nor is it DRM. One of the other concerns was that Palladium was like another march forward in Microsoft’s DRM-directed campaign. So TPM, the Trusted Platform Module, got discolored as a consequence of...

Leo: Palladium.

Steve: ...its sort of, yeah, exactly, it being something that Palladium could use. Now, Microsoft actually called their hardware side an SCP, a Secure Crypto Processor. And so that was the acronym that they were using, saying that Palladium would be software and hardware, and on the hardware side would be an SCP.

Now, what’s interesting is that Microsoft has also just patented their approach upside down and backwards and sideways. So they’re saying, oh, no, this is not just us, you know, other OSes could use it. But it’s entirely clear that they could also foreclose that from happening by leveraging their patents. And of course we’ve just recently talked about Microsoft and their patents. So...

Leo: Right, and their leverage.

Steve: Exactly. So it’s very clear to me that TPM is - that’s the solution that’s probably going to win because it’s going to get industry support, and it’s going to get multiplatform support. You know, I have it on two machines. I have it on a motherboard that I recently purchased that’s - I think I’ve mentioned my quad core machine that has TPM, and my ThinkPad T60 laptop has it. And I’ve got it enabled. It’s worth noting, and this is in the spec actually, that it is disabled by default. So it is normally turned off because of the sensitivity there is to issues of privacy relating to this, even though I really think those are misnomers.

Okay, now, what is it? What it provides is a number of basically crypto services. The beauty of it is that there are things that you would like to do in crypto that you would like to shield from malicious software. And that’s really all it is. It’s the movement of some sensitive cryptographic operations into hardware for the sole purpose of preventing malicious software from having access to those operations. So it has non-volatile memory. So again, it’s a chip. And it’s like a little coprocessor. It’s got non-volatile memory. And the user is able to say "flush yourself and re-init," and it will do that. And you normally do these things from the BIOS. So you’ll have a TPM-enhanced BIOS which understands that it’s got the TPM hardware there with it on the motherboard. And you’re able to disable it completely, in which case all of its BIOS support and functionality and access by the operating system’s drivers are also disabled. Or you’re able to reinitialize it, basically saying forget everything you knew, I want you to restart.

Well, one of the things it has that we’ve talked about before that is very cool is a true random number generator, not a PRNG that is a pseudorandom number generator, true random numbers being what you are able to generate in hardware, taking advantage of things like thermal noise in the chip itself, like literally electron migration or electron tunneling or clock jitter, where it’s able to use just things that are non-algorithmic in order to generate its random numbers. So it’s even a better random number generator than anything that software could do because, as we know, as we’ve said before, software is 100 percent deterministic. So there isn’t a way that software can generate random numbers because it’s designed not to. It’s specifically designed not to. So an algorithm can’t be random. It can be very good pseudorandom, but not truly random.

Well, the TPM has true random number generation capability. It also has both volatile and nonvolatile memory so that it is able to store things persistently until such time as the user or the various APIs that are used to access it tell that to change. One of the things it has, for example, is a monotonic counter, which is also very useful. So it’s got a counter which counts up forever, meaning that it’s able to solve problems with any kind of replay attacks by having a counter which just starts at zero when it’s born, and it never wraps around. It’s got so many bits in the counter that it absolutely positively can never wrap around. And anytime the chip feels that it’s about to lose power, as soon as there’s, like, a power loss line, then it writes that counter into nonvolatile memory. It doesn’t continually write it because, as we know, EPROM technology wears out over time. So you would not want to be continually writing into the EPROM or the chip would burn itself out. But when you shut it down, then it stores the current state of the counter into nonvolatile memory so that when you power up again, it starts up where it left off, therefore guaranteeing that it will never reuse the same number again.

It also has full support for RSA asymmetric encryption. So RSA-compatible, you know, public key crypto. It’s able to generate public and private keys. It’s able to perform RSA operations. And any one of these you’re able to tell it what bit-length you want; but the spec requires at least 2,048 bits of equivalent RSA key length, so next-generation key length, aimed at the future. It also has built-in SHA-1 hashing of 160 bits minimum. So, for example, one of the things that the chip does is, when you initialize it and you say, okay, go, it will use the true random number generator to generate a public and private key pair, that is, an asymmetric key pair. And part of the coolness of this is there is nothing you can do, no commands you can give it, that will ever cause it to export its private key. So it’s got this magic 2,048-bit private key which it generated using its true random number generator, and there is no way you can ever force it to reveal it. No monitoring of the pins with the scope, no...

Leo: I’m always suspicious when I hear "never," though. I mean, hackers are so ingenious.

Steve: No, but, I mean, the technology doesn’t permit it. There’s no - well, okay, sure. You could have a bug in the chip. There could be a mistake in the microcode. There could be that kind of thing. But the specification does not allow for this private key to ever leave the chip. And all the crypto has been designed so that it doesn’t need to.

So essentially the chip has a number of features. It is a secure place for crypto to be done by the host operating system where there is no danger, at least for the crypto operation itself, of that being intercepted and abused in any fashion. But it also has a number of other things. There’s something called "hardware platform attestation" that is attesting to the hardware. The hardware has, like, any hardware has a whole bunch of settings in the BIOS. You’ve got hard drives with serial numbers. You’ve got a bunch of things about the platform at any given time. It’s possible for you, and the chip has this technology, to take a snapshot of the hardware platform, and the chip will then - it will hash that down into 160-bit hash representation of the current hardware platform settings.

And you’re able then, if you wish to - and again, all this is under software control, but you’re able to have the TPM chip attest to the state of the hardware and essentially certify that no changes have been made from now compared to the time that this hash was generated, so that you're able to say the hard drive hasn't changed; settings haven't changed. Whatever characteristics of the platform you want to be attestable, this will verify that. And you're also able to do the same sort of thing during the OS boot process. And, for example, the Linux implementation of this has that now, so that Linux is able to interact with this hardware during the boot process and essentially generate a series of hashes of the kernel as Linux boots so that you can absolutely verify that no change has been made to any of the Linux modules from the time that the snapshot was taken. So it gives you a means of booting into a secure known state...

Leo: That's nice.

Steve: ...that prevents - oh, it's way cool, Leo.

Leo: Yeah, yeah. It sounds like a really great idea. And the security, I mean, the issues that people are coming up with were more about things - and I think it was maybe more Palladium implementation of it, but things like revoking documents or revoking emails after they'd already been mailed. But that's not part of TPM, per se.

Steve: Well, and that's a perfect segue into my noting that, yes, people have been concerned that, for example, it could be used to give you better DRM, you know, Digital Rights Management, something more serious for software to lock onto.

Leo: Uncrackable.

Steve: Well, except that - and here's the point. There's no protection from the user. The protection is from malicious software.

Leo: Ah, okay.

Steve: And that's the key. The TPM specification does not try to protect itself from the user, from the owner, from someone having physical presence. It's designed to protect from malicious software. And so it's really not enhanced DRM because you could reset your TPM chip and say, okay, look, now I need to reauthorize myself. So it's not that. And several of the people that defend the spec make the point of saying, look, all this is, is better security. Sure, you can use better security for pro-user or anti-user benefit. But it's not the security's fault.

Leo: It's not inherent in security at all.

Steve: Precisely, in the same way that the Internet, you know, the Internet is not bad just because bad things can happen with it. It's just a capability. So and what I like about TPM is that it moves the sensitive operations out of software, where they are fundamentally open to compromise.

Now, certainly you still need a secure interface to TPM. And there are, there's some scenarios where, in fact, in order to make changes, the OS has to lose control, that is, you go through a full hardware reboot that takes you back into the BIOS, where you're back in control of a limited environment where you're got much better guarantee of a secure path between the keyboard and display and the TPM, in order to do some things. And then you go back into the operating system. So, I mean, there are scenarios that will be developed in the future where things that were not used to being done now will be done with TPM because the hardware platform support provides it. And I just think of it as an overall good thing. Once I understood what it was, I enabled it on my platforms. And as you know, for example, I'm using a fingerprint swipe on my ThinkPad which unlocks both the BIOS and unlocks my password-protected hard drive, and all of that is stored in the TPM chip.

I should mention a little bit more about the nonvolatile memory side. It's able to store the keys and certificates and other data that you would like stored in a way that nothing can get to it. The problem, if you store the stuff on a hard disk, is that it's there on the hard disk. But if you store your passwords and your certificates in this nonvolatile memory, and you lock it so that it requires a boot-time, power-on-time unlock, then there isn't any way for this to get compromised. It won't let that stuff out until you've provided it with something that hashes down to the same value it's got stored in this single chip. And nothing comes out of its pins until you've said, it's me, I need access to this stuff. So, I mean, it's like a very secure hardware-enforced crypto vault that is part of the hardware.

And, you know, when we've talked about multifactor authentication, we've talked about how single-factor username/passwords, something you know, is not safe; that really something you have would be nice to have added. Well, TPM provides very carefully designed second-factor authentication of something you have. You have the laptop. You have the cell phone or PDA or whatever the TPM chip has been installed in.

Leo: So a weak password would still have the same consequence if somebody stole your laptop, though; right?

Steve: Yes. Again, there's no way to prevent against that except that the TPM also, in the spec, at least in 1.2, the most recent version, they've got dictionary attack prevention. So it will shut itself down if it sees someone trying to guess your password. It will first lengthen the response time, and then lock out.

Leo: TPM is from Intel and Microsoft, or who was involved in TPM?

Steve: 120 different companies...

Leo: Oh, interesting.

Steve: ...are involved in this. I mean, virtually, it's a Who's Who. It's from the TCG is the Trusted Computing Group, which is an unaffiliated independent alliance of more than 100 companies that have gotten together and said we want an open spec, an open platform, and agreeing on what the functionality should be when we create what Microsoft calls SCP, the Secure Crypto Processor. Well, I'm really glad this wasn't done and spec'd by Microsoft. It was done independently. And, for example, yes, Intel's newer chipsets have all the TPM functionality built right into them. So...

Leo: But many other people make TPM microcontrollers. So it's so open that even other hardware manufacturers are involved in it.

Steve: Oh, exactly, it's multiplatform and evolving, complete open spec, all the PDFs are there. I think it's at TCP.org, the trustedcomputinggroup.org has all this. So, I mean, this is our foundation for moving crypto onto hardware and being able to securely store stuff we really want to be kept safe in a way that nothing that happens, no kind of system subversion is able to get there because it's implemented in hardware.

Leo: And you're using this on your T60?

Steve: Yes.

Leo: And it hasn't hindered you in any way, and it's worked reliably and...

Steve: No, I just like knowing it's there. I love...

Leo: So you don't see it, really.

Steve: Yeah, I love that when I swipe my fingerprint, the characteristics are found, they're hashed down, they're given to the TPM chip. It compares them with the various fingerprints because I've got two fingers from each hand. Which is actually a good thing because I've got a Band-Aid on my right forefinger right now, and I realized, wait a minute, I can't log in. Oh, wait a minute, I did my left hand, too, so, yeah.

Leo: Whew, a close thing. And how many manufacturers, I mean, so you can get it on your Lenovo. Dell, I think, is offering some machines with it; yes?

Steve: And Dell is definitely in the...

Leo: They're a big part of it.

Steve: ...Trusted Computing Group, yes.

Leo: Right. So you should probably look around, especially if you're getting a laptop, this is really important, and look for one that has TPM enabled.

Steve: Yes. I think for portable computing it offers the potential for really good security. And I can foresee the day where PDAs and cell phones will have a little fingerprint swipe sensor, and that'll go right into a little TPM chip integrated into the electronics to say, yes, this is me who has this device.

Leo: That's neat. That's neat. All right. Let's see, I think we've wrapped this up. We're going to do a question-and-answer session next week for our 100th episode. I apologize, I didn't get balloons or streamers or anything.

Steve: Never missed a week, Leo.

Leo: That's pretty impressive because there's no other podcast that can make that claim. No other TWiT podcast, and probably not many other podcasts, either. That's pretty impressive.

Well, good job. We'll celebrate next week. I hope you'll join us. I'm Leo Laporte. Don't forget to go to Steve's site, by the way, GRC.com. That's where you can get 16KB versions of this show, the low bandwidth versions. You can also get transcripts and all the show notes, and participate in his great security forums. That's GRC.com. It's also where you'll get SpinRite, the world's best, the one they're all copying, the finest disk maintenance and recovery utility in the world: SpinRite. GRC.com. Also great free security programs and ShieldsUP!.