Encryption: Law Enforcement's Whipping Boy

Description: Leo and I discuss a wide range of security news, Steve's feelings about the new iPad Pro, and lots of interesting bits of miscellany. We then revisit the newly controversial question of Internet encryption which has been raised with great emphasis after last week's terrorist attacks in Paris.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-534.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-534-lq.mp3

SHOW TEASE: It's time for Security Now!. We've got a lot of security news. Steve is up in arms on this one, CMU taking a million dollars from the NSA to break Tor. What's that all about? And we'll look at the drumbeat, it's increasing once again, to put backdoors in encryption so the bad guys can't do bad things. Steve has a rebuttal. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 534, recorded Tuesday, November 17, 2015: Encryption and the Law.

It's time for Security Now!. Oh, I look forward to this every week. Every week there are security stories, and I go, oh, I can't wait to hear what Steve Gibson's take on this is.

Steve Gibson: Well, and Leo, you know, I have to say that you're clearly paying attention because I listen to you being the security expert on your other podcasts.

Leo: I've absorbed it, yeah.

Steve: No, no, you have, accurately and perfectly. So I just sort of smile, and I think, yup, that's exactly right.

Leo: I'm storing it away up here, Steve, and I know everybody else is. 534 episodes later, if you've been listening to every show, you are a security expert. If you've understood every word, you're a master. Steve Gibson sometimes gets pretty deep. This one is going to be more about, it sounds like, more about policy than about

[crosstalk].

Steve: Yeah, in the wake of the Paris terrorist attacks, not surprisingly, encryption is now back in the forefront. It's being used as, oh, well, if we only had pervasive ability to decrypt communications, then we'd be able to stop these things. And so there's been some really bad reporting. And of course the security experts that we're familiar with, Bruce Schneier comes to mind, Matt Blaze is involved, I mean, they understand the details. Largely our listeners do. But I want to look at some of the mainstream reporting and then the flipside because Schneier refers to Glenn Greenwald's piece, which was really good.

Leo: Mm-hmm, mm-hmm.

Steve: And of course, you know, everybody's got a dog in the race. We understand that. We know where people stand. But of course, from our standpoint, the podcast's standpoint, we're going to cut through this and look at the reality of what value it would be for them even to have what they say they want, and why the horses have already left the barn. But we also have all kinds of crazy stuff to talk about. Some really interesting news this week. As promised, we've got MIT's analysis of the value and virtue, or maybe lack of, of tinfoil caps. We also have a bunch of interesting miscellany. I've heard you, and I've got my responses to living with my iPad Pro for a week.

Leo: Oh, yeah, that's right.

Steve: And I'm up to speed on all of yours and Rene's, and of course Andy's was totally predictable. He did not disappoint in the previous podcast on MacBreak Weekly, just before this one. And I also heard you sort of talking about the iPad Pro as a gaming pad, and looking for something that could really use it. And I was brought to mind of the fact that there is a game/puzzle that I've never mentioned, that years ago completely preoccupied my spare time - the good news is, not just for iOS, iPhone/iPad, but also for Android - that we will talk about. And so if my going on in infinite detail here in the second half of the show with The New York Times article and Glenn Greenwald gets a little much for you, no one will know if you have downloaded this and have begun to be absorbed by it because it is amazing. So all kinds of fun stuff to talk about.

Leo: All right, Steve. The security news of the week.

Steve: Yes. Starting with the Picture of the Week...

Leo: Oh, yeah.

Steve: ...which was tweeted to me, thankfully, from one of our listeners, because this really does really finally resolve this question.

Leo: Puts a nail in that coffin.

Steve: Yes. Researchers prove that tinfoil hats actually boost receptivity to government signals.

Leo: What? Like putting an antenna on your head.

Steve: This was a formal study done by researchers at MIT, titled "On the Effectiveness of Aluminum Foil Helmets: An Empirical Study." It was brought to us by How-To Geek. Researchers at MIT, using a network analyzer, tested the impact of tinfoil helmets on receptivity of radio-frequency signals. They highlight the method and results in the study, which is abstracted here. The abstract reads - and that's all I'll bother everybody with, but it's fun.

They said: "Among a fringe community of paranoids, aluminum helmets serve as the protective measure of choice against invasive radio signals. We investigate the efficacy of three aluminum helmet designs on a sample group of four individuals. Using a $250,000 network analyzer, we find that, although on average all helmets attenuate invasive radio frequencies in either direction" - meaning either emanating from an outside source or emanating from the cranium of the subject - "certain frequencies are, in fact, greatly amplified. These amplified frequencies coincide with radio bands reserved for government use, according to the Federal Communication Commission. ?Statistical evidence suggests the use of helmets may in fact enhance the government's invasive abilities. We speculate that the government may in fact have started the helmet craze for this very reason." So bottom line, take off your tinfoil helmet.

Leo: I am calling foul on this one. It's tin foil, not aluminum foil. They've got to go back and do it with tin.

Steve: Ah. The lead could be important. You're right.

Leo: Uh-huh.

Steve: Yes.

Leo: I think maybe...

Steve: That would change its electrical characteristics.

Leo: Yeah, nobody says an "aluminum foil hat." First of all, nobody can pronounce it, especially if they're crazy paranoid.

Steve: And speaking of which, "aluminium," are there enough letters in that word to give

you that many syllables?

Leo: It's spelled that way in Britain, with an extra "I."

Steve: Oh.

Leo: They don't just pronounce it differently, they also spell it differently.

Steve: Well, they would have to because I'm sure you'd run out of letters if you were trying to say "aluminium," spelling it the U.S. way.

So, top of the news is a little distressing, and lots of people were upset. The news was broken last Wednesday by motherboard.vice.com, that picked upon the fact that evidence that was revealed in a lawsuit from 2014 revealed that the FBI had used information from "an educational institution," I think is all it said, they were trying not to say too much, in order to bust some Silk Road 2 purveyors. We'll remember of course, famously, Silk Road was a dark web, Tor service-based meeting ground/marketplace, where buyers and sellers were transacting in illegal merchandise and substances and so forth. And there was, after that was found and shut down, a duplication of that effort.

So here's what's distressing, and this is from the day after this news broke last week, the Tor Project Blog wrote the following: "The Tor Project has learned more about last year's attack by Carnegie Mellon researchers on the hidden service subsystem. Apparently these researchers were paid" - okay, we're talking university security researchers paid by the FBI a million dollars - "to attack hidden services users in a broad sweep, and then sift through their data to find people whom they could accuse of crimes. We publicized the attack," wrote Tor, "last year, along with the steps we took to slow down or stop such an attack in the future."

And of course we covered that a year ago on this podcast, all about hidden services. And this was a traffic confirmation attack. And as I have held, before and since, that's the biggest weakness that Tor has. And that is, if you suspect endpoints, then it's virtually impossible to block confirming their connection. Less easy to get the connection; but, once you suspect it, confirming, that's really hard not to be able to get a high level of confidence on.

So continuing with Tor's blog: "There is no indication yet that they had a warrant or any institutional oversight by Carnegie Mellon's Institutional Review Board." And we'll come back to this because Matt Green has really interesting commentary about this whole question of an institutional review board, which is typically something you have in the medical practice, where you want to verify that subjects of a double-blind crossover study, for example, like if an effect of a test drug is found to be so bad or good, the study needs to be shut down prematurely because, on one hand, you don't want to deny the people getting the placebo the benefits of the good outcome drug, or vice versa. So this is the first time...

Leo: I think, though, that it is also common practice in universities to have such a review board for other academic stuff, especially government grants.

Steve: No.

Leo: No?

Steve: Well, I don't know. But Matt Green does address this issue.

Leo: Oh, okay.

Steve: So we'll be getting there. So there's no indication yet that they had a warrant or any institutional oversight by Carnegie Mellon's Institutional Review Board. "We think it's unlikely they could have gotten a valid warrant for CMU's attack as conducted, since it was not narrowly tailored to target criminals or criminal activity, but instead appears to have indiscriminately targeted many users at once." Basically what we believe is it was show us all of the users and services that you can. We're then going to look at them, find criminality, and prosecute.

Leo: Fishing expedition.

Steve: It was a pure fishing expedition. And they did prosecute, which is how this all came to light.

Leo: But it was a child pornographer, so it's okay. Right?

Steve: Yeah. "Such action," writes Tor, "is a violation of our trust and basic guidelines for ethical research. We strongly support independent research on our software and network, but this attack crosses the crucial line between research and endangering innocent users. This attack also sets a troubling precedent. Civil liberties are under attack if law enforcement believes it can circumvent the rules of evidence by outsourcing police work to universities. If academia uses 'research' as a stalking horse for privacy invasion, the entire enterprise of security research will fall into disrepute. Legitimate privacy researchers study many online systems, including social networks. If this kind of FBI attack by university proxy is accepted, no one will have meaningful Fourth Amendment protections online, and everyone is at risk.

"We," says Tor, "teach law enforcement agents that they can use Tor to do their investigations ethically, and we support such use of Tor. But the mere veneer of a law enforcement investigation cannot justify wholesale invasion of people's privacy, and certainly cannot give it the color of 'legitimate research.' Whatever academic security research should be in the 21st Century, it certainly does not include 'experiments' for pay that indiscriminately endanger strangers without their knowledge or consent."

Leo: Right on. Right on, Matt.

Steve: Yup. And then Matt Green, our cryptographer at Johns Hopkins, writes on "Research Ethics," was the title, "Why Tor Attack Matters." He says - and I snipped the

first couple paragraphs because it was sort of introduction that our listeners don't need. He said: "You might wonder why this is important. After all, the crimes we're talking about are pretty disturbing. One defendant is accused of possessing child pornography; and, if the allegations are true, the other was a staff member on Silk Road 2.0. If CMU really did conduct Tor deanonymization research for the benefit of the FBI, the people they identified were allegedly not doing the nicest things. It's hard to feel particularly sympathetic.

"Except for one small detail," writes Matthew. "There's no reason to believe that the defendants were the only people affected. If the details of the attack are as we understand them, a group of academic researchers deliberately took control of a significant portion of the Tor network. Without oversight from the University's research board, they exploited a vulnerability in the Tor protocol to conduct a traffic confirmation attack, which allowed them to identify Tor client IP addresses and hidden services. They ran this attack for five months and potentially deanonymized thousands" - probably more, really - "of users, users who depend on Tor to protect them from serious harm.

"While most of the computer science researchers I know are fundamentally ethical people, as a community we have a blind spot when it comes to the ethical issues in our field. There's a view in our community that Institutional Review Boards are for medical researchers, and we've somehow been accidentally caught up in machinery that wasn't meant for us. And I get this. IRBs are unpleasant to work with. Sometimes the machinery is wrong. But there's also a view that computer security research can't really hurt people, so there's no real reason for that sort of ethical oversight machinery in the first place. This is dead wrong; and if we want to be taken seriously as a mature field, we need to do something about it. We may need different machinery, but we need something. That 'something' begins with the understanding that active attacks that affect vulnerable users can be dangerous and should never be conducted without rigorous oversight, if they must be conducted at all.

"It begins with the idea that universities should have uniform procedures for both faculty researchers and quasi-government organizations like CERT, if they live under the same roof. It begins with CERT and CMU explaining what went on with their research, rather than treating it like an embarrassment to be swept under the rug. Most importantly, it begins with researchers looking beyond their own research practices. So far, the response to the Tor news has been a big shrug. It's wonderful that most of our community is responsible. But none of that matters if we look the other way when others in our community fail to act responsibly."

And it's worth mentioning also that there was a planned presentation at Black Hat of this, which was quietly pulled from the calendar.

Leo: Yeah. They might have been stormed. Well, and somebody, I think Dallas in the chatroom said, "Well, yeah, but who suffered from this?" As Matthew Green points out, everybody who was using Tor during that period of time, which was like six months, right, was potentially deanonymized.

Steve: Right.

Leo: Not just the criminals.

Steve: Right. It's important to understand, for example, why we have a constitutional protection against unreasonable search and seizure, why there must be reasonable suspicion that can be demonstrated to a court in order to generate a search warrant, which then empowers law enforcement to essentially breach one's sanctity, one's privacy, for searching. And of course this came from England, when the King's men could just walk into anyone's home any time they wanted and do anything they wanted. When we set up the United States, we said, no, we're not going to have it that way.

And so this is something that, I mean, we have it because it's controversial. But I think it's one of the strengths that the Constitution provides. And so I love this notion, and I think it was Snowden who said, when he was speaking about free speech, just because I have nothing to say that requires protection, doesn't mean that free speech isn't valuable. So, I mean, these are interesting issues. And of course this is all about encryption comes into this same argument deeply.

Leo: Was it CMU's own exit nodes that were compromised? They used an exploit, didn't they, to compromise others, as well. I can't remember.

Steve: I don't remember. What I remember seeing is that they set up, like, they talked about a cost of...

Leo: Yeah, a honeypot kind of a thing, yeah.

Steve: Yeah, I think they talked about a cost of, in one instance, I saw $3,000 quoted in the Black Hat presentation. I saw $50,000 of expense elsewhere.

Leo: They got a million dollar grant.

Steve: Exactly. They made money on this sucker. They made some money.

Leo: So it's also an insult to the taxpayers.

Steve: So I think they set up a lot of their own exit nodes, and then got those to be used. They may have been cloud based rather than physical because you can do that now. And then they monitored the traffic and then built an inference engine to infer the incoming and outgoing traffic and used it to deanonymize. And we've talked about Tor deanonymization from time to time because it's a fascinating topic, sort of, in security theory and privacy theory.

So, again, this is the kind of thing that has to happen. I'm glad it's gotten a lot of attention. And people will get slapped, and I imagine that there will be consequences in terms, I mean, exactly along the lines that Matthew suggests, which is in the same way that medical researchers have to get their studies approved by medical oversight boards, and I've been reading a lot of medical research in the last decade - and, boy, have I developed a new empathy for rats and mice. Oh. But they really are [crosstalk] so put upon.

Leo: They don't get their blood taken any more than you do.

Steve: Well, no, it's the homogenizing of their brains.

Leo: No, I know.

Steve: Because you want to determine what the neurochemical balances are. It's like, oh, boy, you know. But they do everything, they say, in an ethical fashion. It's like, well, okay. And of course this always harkens back to Douglas Adams, who asserted that, in fact, mice are the way a multidimensional superbeing is actually testing us.

Leo: Manifests...

Steve: Yeah, it's popping little mice into existence, into our 3 space. And the mice are running mazes, and we're thinking we're determining what they're doing, but in fact they're under the control of this other entity. It's like, okay, Douglas.

Leo: Yeah, yeah.

Steve: So, interesting report from French and German researchers, who decided to tackle this growing concern of the Internet of Things and the embedded firmware in devices - routers, VoIPs, cable modems, webcams. They collected all of the firmware they could find from 54 different vendors, 1925 different BIOSes, so just short of 2,000 firmware images spanning devices produced by 54 different vendors. They then set up a cloud-based, basically emulation system, based on Ubuntu Linux and QEMU to provide the hardware emulation layer. And they did software emulation of the chips running the firmware.

So they essentially set up a virtual cloud-based lab and then applied both static and dynamic analysis - and we have, of course, recently been talking about that relative to the iOS App Store stuff - both looking at the code statically and running the code actively. And then they also brought in both their own technology and existing known exploit kits - Metasploit, Nessus, and so forth, that we've talked about in the past - and applied all of these tools. What they found was important, critical, actually, vulnerabilities in 185 firmware images which affected nearly a quarter of the vendors. They have, under responsible disclosure, they have contacted all of them that they've been able to and notified them of the problems.

So the report that's just out, it was titled "Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces." And I think 99% of these had web interfaces. Many of them were running PHP behind the scenes because they themselves were running little versions of Linux. And in their report, and I've got of course the links in the show notes, they break out the percentage of which web servers were being used, what software packages were there - basically, a complete analysis of the operating firmware that they discovered in 1925 different instances of turnkey devices. And from about 25% of the vendors they found 185 critical vulnerabilities right now, in, like, today's most recent versions of what's out there.

So a really interesting piece of work. The concern is we're seeing this explosion of Internet of Things things. Who's responsible for keeping them secure? How do we do this? And what these guys have demonstrated is it is feasible to - we don't know that they found them all, but it's certainly better than nothing. They found 185 important problems across devices from 54 different vendors.

So, yay. And cool that we're able to do this at scale because it means that there could be a facility where firmware is sort of dropped into a big pot as it comes out, and something runs it in a virtual environment and pounds on it and performs some sort of verification to increase the chance - again, not perfectly, but better than nothing - that if there's a problem that we know about, sort of the type of problem that we know about, we can make sure this particular instance doesn't have it.

Oh, and this one. So a company named iPower Technologies was asked to create a cloud-based facility for uploading video from police body cameras to make it more convenient to manage and track and handle police body cam video. They purchased a couple of the cameras that the people who contracted with them were buying, from a company called Martel Electronics. And upon connecting this brand new body cam to one of their systems, their AV immediately flashed up and warned them and shut down. They said, huh, what?

Turns out the brand new body cams being sold by Martel Electronics, known as the Vid-Shield Body Worn Police Camera, were infected with our old friend the Conficker worm. This one in particular, Conficker.B. Remember it ranges A through E. We haven't talked about Conficker for years, but it was at one point very prevalent. It was the first worm that we saw that was doing dynamic DNS generation where it used an algorithm to algorithmically create DNS domain names so that, in the future, it would know what a possible DNS domain would be where it could find its command-and-control server.

And this made it very difficult to track because, first of all, it generated, like, 50. And investigators who caught it and then reverse-engineered it had to preemptively register 50 DNS domains. And then the next day there would be another 50, and then another 50, and another 50. And then it would choose one, or it would try them all, and one of them would actually have the command-and-control server on it. Anyway, we talked about this at length years ago. So basically what this means is that this Vid-Shield Police Worn Body Camera, or something about the manufacturing process, is pre-infecting these with this old-school malware. Now, I went to this company's site, and I was gratified to find out that they are in stock now and offer free shipping.

Leo: Oh, good, well...

Steve: So you can get Conficker B...

Leo: Worms have never been more affordable.

Steve: ...as part of the deal. Yes, but you must call for pricing. You always know it's going to hit you hard when you have to have somebody on the phone before they'll tell you want this thing costs.

Leo: Oh, yeah, yeah.

Steve: It does, however, have a five-star rating and eight product reviews. Their site says: "The Vid-Shield police body video camera not only records in high-definition, but it also" - they said "shots," I guess they mean "shoots" - "12 megapixel still images, equivalent to the best digital cameras in the world."

Leo: Not really, no.

Steve: I know. I knew you were going to - when I read this, I thought, oh, Leo will have a comment about that one.

Leo: Yeah.

Steve: "The Vid-Shield has the time/date stamp embedded into the video and photos that cannot be tampered with, making it perfect for evidence." And it goes on and on and on. I won't bother anybody with it. But I got a kick out of it. What was interesting was it's like, okay, yeah, so what?

Well, Dan Goodin, writing for Ars Technica, I think, put it perfectly. He wrote: "Alternatively known as Downup, Downadup, and Kido, Conficker took hold in late 2008, a few days after Microsoft issued an emergency patch for a Windows vulnerability that allows self-replicating exploits. Within a few months, Conficker had enslaved as many as 15 million Windows PCs. Its sprawling botnet of infected machines eluded the vigorous takedown efforts of the Conficker working group, which was made up of Microsoft and more than a dozen partners in the security and domain registration industries.

"Conficker was especially hard to contain," writes Dan, "because it used a variety of advanced methods to self-propagate, including exploiting weaknesses in the Windows autostart feature when users inserted USB drives into their computers. The malware also generated hundreds of pseudorandom domain names each day that infected machines could contact to receive new instructions. The scheme allowed the botnet to survive even when old domain names were turned over to the working group. There are at least five significant variations of Conficker that are denoted with the letters A through E."

And finally, he says, "A report that police cameras are shipping with Conficker.B preinstalled is testament to the worm's relentlessness. It's also troubling because the cameras can be crucial in criminal trials. If an attorney can prove that a camera is infected with malware, it's plausible that the vulnerability could be grounds for the video it generated to be thrown out of court, or at least to create reasonable doubt in the minds of jurors. Infected cameras can also infect and badly bog down the networks of police forces, some of which still use outdated computers and ineffective security measures."

Leo: You wonder how they got on there; right?

Steve: Yeah. And it's interesting because, when iPower discovered this, they posted this,

they uploaded it to VirusTotal, and it was, even today, I mean, it may be so old that it's coming around again because it was only seen, it was only detected by 40 out of 54 of the total detectors. And, interestingly, Malwarebytes and McAfee were among those that did not detect it. So if the police station were using McAfee or Malwarebytes, that body cam, and, for example, an XP that didn't have patches installed for, like, forever, I mean, it's got to be a really old machine for that to still happen, but as Dan notes, can happen. But even if it weren't, the fact that it was being infected, the fact that reasonable doubt could be made that, wait a minute, you're saying that you have to have chain of custody.

Leo: Yeah. Whoops.

Steve: But if you've got malware in there...

Leo: Yeah, yeah, chain of custody.

Steve: ...all bets are off.

Leo: Yeah, no, that's a very good point, yeah.

Steve: Yeah.

Leo: I bet you on "The Good Wife" they jump right on that one.

Steve: So WhatsApp. Of course it's one of the most famous, maybe now the most famous messaging platform. About 800 million users are using it. A bunch of researchers decided they wanted to take a close look at a new feature that had recently been added. So they put together a report, and in their little abstract they said: "WhatsApp is a widely adopted mobile messaging application. Recently, a calling feature was added to the application, and no comprehensive digital forensic analysis has been performed with regard to this feature at the time of writing this paper. In this work, we describe how we were able to decrypt the network traffic and obtain forensic artifacts that relate to this new calling feature which include the WhatsApp phone numbers, the WhatsApp server IPs, the audio codec in use, the call duration, the phone numbers, and call termination."

And then they say: "We explain the methods and tools used to decrypt the traffic, as well as thoroughly elaborate on our findings with respect to the WhatsApp signaling messages. Furthermore, we also provide the community with a tool that helps in the visualization of the WhatsApp protocol messages."

Now, it's important to note that the communication keys were not retrieved; but they speculate in their paper that they were present, and that further reverse-engineering and analysis may have produced additional revelations. So at the very least, the current instance of WhatsApp is trying to encrypt its metadata. And these guys cracked it, meaning that - and I saw somewhere else, but I didn't run it down, that this had something to do with a ubiquitous use of a repeating public key, that is, there was some public key encryption, but the same one was used. And so as a consequence, the weakness of metadata protection in WhatsApp, there is a weakness which is present that

essentially cracks the metadata encryption.

And then, of course, the question is, could this be known? Or who knows it? And where is it known? And if we're relying on obscurity, then as these guys note, we didn't fully reverse-engineer the app. We don't know what else is in the metadata. But in the metadata that we decrypted, we did find stuff that users are presuming they're being protected from. And we know they're not.

So again, the fact that it's popular and that it's using encryption really doesn't tell us anything. This stuff is complicated. And in fact it's because it's so complicated that I'm worried about the future of encryption relative to legislation because, boy, it is hard to explain things to people that really don't want to understand them.

Okay. Piece of hardware note. I've talked several times about pfSense and about the Soekris hardware that I like, a really great company based in Scotts Valley, California. I was aware of an alternative and sort of lost track of it. Then somebody tweeted to me the platform they use, which is way less expensive. And I thought, oh, good, I'm glad I found it. And that fell through the cracks, too. So the second time somebody said, hey, Steve, I use these, they're great, I said, oh, that's the one. I'm not going to lose it again. So PCEngines.ch. Sorry, didn't pronounce that very well, .ch, PCEngines.ch.

These guys are a very affordable, for a do-it-yourself person, multi-NIC, because you need two or three, and like they have three NICs, so you could have a WAN, a LAN, and a DMZ, just beautiful little pfSense-compatible hardware platforms where, for example, the case costs $10 rather than $125, and the board itself is a hundred bucks, that kind of thing. So for anyone who is interested in perhaps rolling their own hardware gateway, PCEngines.ch is a great site. I don't have any particular hardware there. You can poke around, see what fits your budget and so forth.

And I'm glad that - thank you, everybody, for tweeting this to me several times. I'm sorry it took several times. But this is the hardware that I was aware of before. It's good stuff. And it's like, it's not overkill. Soekris is sort of the high-end approach. I mean, this is completely adequate. And there Leo has a picture of it onscreen, showing a Compact Flash card, so you can boot from Compact Flash, you know, multiple NICs, a range of speeds and options, just really nice, very inexpensive, very affordable hardware.

Leo: Small; right? I mean, these look pretty compact, yeah.

Steve: Yeah, oh, it's a tiny little thing, like maybe...

Leo: Does it come with a case, or you just...

Steve: I think it's 10 bucks for a case.

Leo: Oh, nice.

Steve: So they've got one.

Leo: It almost looks like a Raspberry Pi. I mean, it's pretty simple.

Steve: Yeah, it's sort of a high-end, multi-NIC - because you need multiple NICs because you want to...

Leo: [Crosstalk], yeah.

Steve: Yup, so you're able to have a WAN and a LAN. But that's the kind of thing you would load whatever your choice gateway software is, pfSense or whatever.

Leo: Yeah. And not expensive. That's great.

Steve: No. Okay, my friend. iPad Pro.

Leo: Ah. You got yours.

Steve: Miscellany.

Leo: You didn't get a Pencil, though; right? Nobody has those, yeah.

Steve: No, yeah, I did not. So I set the alarm for midnight on Wednesday night, got up at midnight. Had not updated. I waited till about 12:30, I'm sorry, till about 12:15, and it was still not showing. So I thought, okay. And of course the 11.11 was just a rumor anyway, so we didn't - there was no...

Leo: No, no, Apple did release a press release the day before.

Steve: Oh, okay. I didn't know that.

Leo: So, yeah, by then it was real, yeah.

Steve: So I thought, well, just on the off chance. So I set my alarm to 1:00 a.m. I got up, I was reawakened at 1:00 a.m., hit refresh, and the first time the site didn't come up. So [gasp] that got my attention.

Leo: Yeah.

Steve: Yes. So I hit it again, and I got the page, immediately pushed my order through, and was told it would be two business days delivery. But as it turned out, it was the next

day.

Leo: Oh, nice, yeah.

Steve: So I was very pleased. I got it immediately. And as you noted, the Pencil is, I was told, one to two weeks out. I haven't looked recently, looked back to see if there's an update. I heard you quote a specific date, so maybe I have one, too.

Leo: Yeah, they told me December 7th through 10th. But let me check, just to see if it's been updated.

Steve: I did look, I did check the site later that day, and I saw that the one to two business days had gone to five to seven for the iPad Pro. So immediately they got backlogged. But I was glad to have mine right away.

Leo: Yeah. So?

Steve: So here's the good. The good, it is fast. It's got a more powerful processor.

Leo: Yeah, very fast, yeah. Noticeably so.

Steve: One of the things that I appreciate about the newer keyboard, that I had forgotten how annoying it is on the current keyboard, that is, on the smaller pad keyboards, and that is less shifting. That is, the newer keyboard gives you the number rows along the top, dedicated, so you don't have to shift in order to get a number. And just, you know, it's nice to have that. Yes, the sound is amazing. Four speakers built in. And if you've seen the iFixit Teardown, you know, they've got like four large resonant chambers. A lot of space was given to those speakers, which I thought was interesting. And as you have noted, watching video with the screen and sound is great. Okay. Now I'm out of good.

Leo: Uh-oh.

Steve: The bad: It's too big.

Leo: It's really big, isn't it.

Steve: It really is. And in fact my body's muscle mass has increased. So it's physically cumbersome. It's physically awkward. I lived with it for almost a week. And it is my - I took it with me. So when I out, I brought it with me. The second time I went out I brought a backup power supply because this thing does not have battery life equal to the Pad.

Leo: That's not my experience. I hope you didn't get a lemon.

Steve: No. Now, maybe you don't have it turned up bright. Because I was outside on a patio in the shade, but I was running it at - and that makes a huge difference. This is a large screen, and it's a lot of screen to light up. What that means is that it's - and we know that backlighting is where a lot of the power goes. If it's turned up full brightness because you're in an outdoor setting in the shade, it actually runs hot. And it drains the battery faster than power can be put in. It consumes power at that rate. So that I've got something giving it 10 watts of 2.1-amp power, and at full brightness I'm losing ground while it's plugged into power. That's how much power the thing uses. But at 50% brightness, which is certainly usable indoors, then it's fine. It's funny because, in my notes of annoyance, I had the things that you've already mentioned, Leo. For example, it's really annoying that they have not used the screen well.

Leo: Yeah.

Steve: Like the icons. They're, like, spaced apart.

Leo: Yeah.

Steve: It's like, wait, I don't - I've got, like, eight pages.

Leo: There's a lot more room here, guys. You could use that, yeah.

Steve: Yeah, I've got eight pages of scrolling using lots of folders. It's like, I would like to have twice as many icons on the screen.

Leo: Yeah, yeah.

Steve: And I would like to have a whole bunch more in my dock down at the bottom, too, because those are the things I use all the time.

Leo: Yeah, lots of room, yeah, yeah.

Steve: It's like, and the apps themselves, Mail, for example, you get a little column of text in the middle of the screen.

Leo: Right.

Steve: It doesn't use the space. Now, the web browser uses the space because of course the web is mature about properly using the resolution it has. But what this really

represents, I think, is a sad first shot. I hope they fix it in the future. But it's just, yeah, it's, I mean, and that's what I meant when I said the screen is too big, and they have not utilized the space well. So also the big keyboard, the problem is it's too big for one-finger typing. You end up, you're going to get some new form of carpal tunnel. I mean, your arm gets exhausted moving back and forth a foot in order to go from one side of the keyboard to the other. I mean, it's just huge.

Leo: Yeah.

Steve: So, and the sound effect volume is very low. I've never been able to, like, it kind of whispers, even though I've got the volume turned all the way up.

Leo: Oh, that's interesting.

Steve: It doesn't make sound effects loud for me. So, and finally, just a generic annoyance with iOS is that iOS appears to be collapsing. I'm finding it more and more buggy. The web portal login often fails. It just - I don't - it says I've got a connection [crosstalk]...

Leo: Oh, the captured portal functionality, yeah, yeah.

Steve: Yup, yup. And so I'll have to, if I reboot the machine, then it works perfectly. It runs for a while. I'm seeing Safari pages that, when you scroll up, the bottom is blank. And if I force close Safari and then just reopen it, then it redisplays that page correctly. And things are locking up and hanging. So I'm disappointed that it's showing its age.

Now, in fairness, I restored my regular iPad, I backed up my regular size iPad and restored it to the big one so that I didn't have to do all the setup from scratch. So maybe there's some age or some cruft or some app collision or something which I replicated through the backup and restore. I may at some point just wipe my most used Pad and start over again.

I think that the sidebar should have its own MRU, that is, its own Most Recently Used list, because the things you do with a sidebar tend to be different than what you do with the main screen, and it'd be nice if they weren't sharing the same MRU. I think that would be a nice thing to say. And I did learn a nice trick, which is to close the sidebar, you don't have to, like, start at the edge of it and push right, which makes no sense really because while you're using the sidebar the whole rest of the screen on the left is grayed out. So you just swipe anywhere you want to, to the right, to close it.

But anyway, here's the final piece. And that is, today when I ran out to grab a bite, I fell back to my original Pad. And, oh, I was so much happier.

Leo: Yeah, it's much more - I don't think you'd want to travel around too much with the Pro.

Steve: You can't, no.

Leo: It's too big, yeah.

Steve: No. So I'm super interested in the Pencil experience. Like you, I'm not an artistic drawer, but I'm a diagrammer. And just the other day I was drawing a circuit diagram with my finger, and it was just - it was annoying. I mean, I had the Pro. I was using Dan Bricklin's note-taking app, which is a great tool for drawing. But it was just, I thought, wow, if I had the Pencil, these schematics would look so much better. So I'm hopeful for that. My life will be complete if the next small Pad has Pencil functionality. I don't know if they'll do it, but that's what I want. If the 10-inch Pad could be compatible with the Pencil, my life is complete.

Leo: Yeah. We'll see. As Rene Ritchie has pointed out, it's almost like two different devices because, in order to do the Pencil and the touch, there's other things you can't, I mean, it's tough.

Steve: Yeah.

Leo: I suspect Apple's going to make a big distinction, and they're not ever going to do a Pencil for the smaller ones.

Steve: Or they could not ever give the smaller Pad the 3D Touch.

Leo: Multitouch, yeah.

Steve: And give it the stylus instead.

Leo: They might do that, yeah, yeah. We'll see.

Steve: I'm kind of feeling that my fingers are just too big to touch on things.

Leo: Yeah, no, you want the Pencil, I think, yeah.

Steve: Yeah. I could see using the Pencil as a beautiful, fine-tip just button presser, just going dink dink dink dink dink in order to, like, just to do things with greater accuracy than with fingers.

Leo: Well, that's what I do with the Microsoft Surface Book, to be honest.

Steve: Yes, yes. So on TWiT I loved the roundtable of blank expressions when you mentioned that Gene Amdahl had died.

Leo: Ohhh, that made me sad.

Steve: It was very sad. Of course you and I know Gene. And a lot of our older listeners will remember Amdahl. He was at IBM, and then he left to build high-performance IBM clones, essentially, was his business. And, I mean, he was a pioneer at the high end of the mainframe computer business for years. And he died last week at the age of 92. And then when all the screens around you, because you had Skyped-in people, they were just silent. And you noticed nobody was saying anything. And you said, "You people don't know who Gene Amdahl was." And they're like, uh, no.

Leo: Yeah.

Steve: And then you said, Osborne, anyone? And they're like, nah, no, no Osborne, either. And there were a couple other earlier industry pioneers. And I just, I thought, wow. And then my favorite anecdote from that was, and I don't remember where it came from, but it was something where some little toddler ran over, her father had a 3.5-inch diskette. And of course I have drawers full of them.

Leo: Yeah, there you go.

Steve: Because I think you had - was it on...

Leo: Wasn't this on The New Screen Savers, we had a guy who continues...

Steve: That's right, on Saturday.

Leo: ...who continues to sell floppy disks at FloppyDisk.com.

Steve: Anyway, I loved the anecdote of someone's daughter saying, "Daddy, you 3D printed the Save icon." I thought, isn't that perfect.

Leo: It was Iain Thomson. That was such a funny...

Steve: She's never seen a floppy.

Leo: No.

Steve: She doesn't know what the Save icon represents. So she sees one in real life and thinks, oh, look, the Save icon's been 3D printed. Oh, just - I loved that.

Leo: So funny.

Steve: Okay. So, okay. I know that my puzzle recommendations have been a huge hit among our listeners. People love the things that I find that I love. This is old, but I've never mentioned it before. And if anyone has liked anything that I have recommended, Auralux.

Leo: Auralux. I'm downloading it right now.

Steve: A-U-R-A-L-U-X.

Leo: Okay.

Steve: Auralux. It is available for iOS, iPhone and iPad, and Android. And apparently it hails from the PC era, or there is a PC version. I get the sense that these were ports from that. So the PC version predated it. So even Paul Thurrott can use Auralux.

Leo: He might remember this.

Steve: And Leo...

Leo: Is that it? Is it like planets and...

Steve: Okay. So it is wonderful. There are - it's sort of planetary. It starts off with two sort of different objects, kind of orbs. And each of them generate new items, dots. They sort of pulse. And they generate them at a certain rate. And so they begin to populate gravitationally. And then, by swiping, you can send - you're able to, like, corral and send a bunch of them off on a mission to go and neutralize other ones.

Anyway, from their own description, they said: "Auralux, formerly Aurora, is an abstract, essentialized, and simplified real-time strategy game. You have only one type of unit to command and only one type of order to give those units. You and your automated opponents start the game with equal resources. Quick reflexes will get you nowhere. The only path to victory is through strategy.

"Auralux features a slow, floating feel and," they say, "gorgeous minimalistic graphics. The entire world pulses to a rhythm of ambient music, and the player's actions evoke sounds that smoothly coalesce into melody. This game is meant to provide a relaxing, cerebral experience. Every action has its reaction, and every option has its costs. Auralux is a game in which your choices matter."

And I will tell you it is one of my all-time favorites. I thought of it when you were talking about needing something for the iPad Pro.

Leo: Yeah, this is nice.

Steve: And, oh, boy, let me tell you, it's, I mean, it is, it's just meditative. It's one of those where it starts out simple. It's free, by the way. I think you have to pay to unlock additional levels, so you can optionally choose to, if you get addicted to it. But, oh. And so, like, it's exactly what you want because you start out not really understanding it. So you learn incrementally as you see how things work. You then adapt your strategy. Anyway, I just - there's no risk for me overselling this. Our listeners who don't already know about it are going to be cursing me a month from now because it has consumed so much of their life.

Leo: I love this. It's musical.

Steve: It is musical.

Leo: Yeah, yeah.

Steve: Strategic. It's fascinating. I mean, I could just go on for an hour like Andy Ihnatko on something that he loves. In this case, I won't, because I've said enough. Auralux. Get it. It's free. iOS and Android and PC. And good luck with your social relationships.

Leo: This is beautiful. Yeah, yeah.

Steve: It's a keeper, Leo.

Leo: Yeah [singing along].

Steve: Oh, it's just so great. And every time - you can see everything throbbing? If you look, two new little dots are produced for every throb.

Leo: Oh.

Steve: And so that's where the dots are coming from. And then, but if enough dots can converge on sort of that thing acting like a black hole, then it grows in size, and then it produces three dots every iteration.

Leo: Ah.

Steve: If it grows again, then it produces four dots. That way, so you want to make yours bigger because then the rate of dot production increases.

Leo: Oh, I see.

Steve: If you want to keep the other, you want to keep your adversaries from getting theirs to be bigger, so to keep their rate of dot production low. And then you want to send - you send fleets of dots off to attack the other guys. And so you're able to, like, circle a bunch and then tell them where to go. And so they sail off on that mission autonomously while you then do a thing - oh, anyway, it's just - it is so wonderful.

Leo: It's fun. It's fun. I'm liking it, yeah, yeah. I don't know what I'm doing, but I'm liking it.

Steve: So, and that's the way you start. You just start by screwing around. And you're always able to go back and redo an earlier level, or you'll see that you lose, and you notice the way you lose, and then you try it again. No, I mean, the reward and pain system that's built in, it's absolutely amazing. In fact, now I'm wanting to play it.

Leo: Yeah, yeah. Let's wrap up this show. We've got stuff to do here.

Steve: Okay. So I did want to revisit "Spectre," just to note that it has broken two Guinness World Records. And quoting from IMDB, the last time I looked it gave it a 7.3, whereas "Skyfall," which people seemed to like more, I saw the comments that your podcast had, I think it must have been on TWiT, maybe, or maybe it was something else, "Skyfall" gets a 7.8. So the world seems to think it was, in fact, better than "Spectre" at 7.3.

But Movies.com writes of the two Guinness World Records: "The latest James Bond movie has broken a few box office records since its release, including the one for biggest opening of all time in the U.K. But 'Spectre,' which also topped the box offices in the U.S. over the weekend, has achieved some other feats that don't have to do with theatrical performance. The movie officially features the largest film stunt explosion in history, as acknowledged by Guinness World Records." And I'll skip talking about that because I don't want to give anything away, except that they use 68.47 tons of TNT equivalent, which was the result of detonating 8,418 liters of kerosene with 33 kilograms of powder explosives, and that lasted over 7.5 seconds.

And I will say it was an amazing explosion. And you could tell this was not a model. This was not some cheesy, we're going to cut corners. This was they blew the crap out of something really big. And anyway, so, yes, the world's record for the biggest explosion. For what it's worth, it did also make box office history with the biggest openings in the Netherlands, Finland, Norway, Denmark, and Sweden. So it's not a crappy film. I liked it. I thought it had - it did drag in places. I mean, if I wanted to be critical, I could find some criticism. But I don't. It's Bond. So it's a fun movie.

Okay. Last, and then we'll get onto seriousness. I talked, years ago, about a series on, I guess it's on CBS, I hope it's on CBS because I just said it is, "The Good Wife." And I remember when other people were telling me about it. But it was like, what? "The Good Wife?" That just doesn't sound like something that I'm going to be interested in. How many explosions is it going to have? How many phaser beams and teleportation and stuff? Zero. So, like, how does a good wife, you know, okay, what? But finally I was

moved to try. And I fell in love. I know that you have started it and are also enjoying it. For what it's worth, it is a great series. It does not take itself too seriously. It's now in its seventh season. So for people who like to binge, there's plenty to binge on.

I'm bringing it up because last Sunday's episode, which was titled "Driven," and that's Season 7, Episode 7 last Sunday, was about autonomous vehicles. And so here's what I think. If any of our listeners who were curious wanted to get a taste, watch last Sunday's episode titled "Driven," Episode 7, Season 7. It stands alone. You won't know any of the back story. You won't know who the characters are. But I think anyone would enjoy it because - and it does involve some fun characters and autonomous vehicle problems in an interesting way. And my guess is you will end up thinking, okay, I've got to know what's going on, so start with Season 1. And you've got lots of enjoyable time ahead of you. So if I can get more people addicted to it, I think that would be a good thing. And we have not yet said while we're recording, Leo, that you fell in love with...

Leo: Oh, "Fargo," yeah.

Steve: ..."Fargo."

Leo: Oh, yeah, sure, great show. Love the show.

Steve: You and Lisa blew through the first season.

Leo: Yeah. One week, we watched the whole thing, eh.

Steve: Yeah. You just [crosstalk].

Leo: Yeah, and then you start talking like this all the time.

Steve: Eh, okay.

Leo: You know who's really good in that there, is that Martin guy, the hobbit. He's really good in that. But the best is Billy Bob Thornton.

Steve: Billy Bob, he plays...

Leo: Oh, Billy Bob.

Steve: ...a really good evil guy.

Leo: Good bad guy, yes, oh, sure, yeah, he's good.

Steve: Yeah. So I had recommended it. But it was after we stopped recording last week where you suddenly realized we hadn't closed the loop on that, and you said, oh, my god.

Leo: I love it. I love it.

Steve: Yeah.

Leo: Definitely, it's violent, ultraviolent, as you mentioned.

Steve: Yeah. So...

Leo: Actually, this new season's even worse.

Steve: Yeah. If you're not - and as I described it, it's a little Tarantino-esque.

Leo: Yeah.

Steve: In terms of being a little over the top. So if that just turns you off, I completely understand. But if you don't mind it, it's just - it's art. It's artistry. And I hate to use that was a segue to SpinRite.

Leo: No. [Crosstalk].

Steve: But I did receive - there is another good lesson here. Simon, oh, I'm going to mispronounce his name, Guettier? Guettier, I guess, G-U-E-T-T-I-E-R. Sorry, Simon. Thank you for the testimonial. He wrote this yesterday. He's in Waddesdon Village, Buckinghamshire, or is it Buck - oh, it's Buckinghamshire.

Leo: Buckinghamshire.

Steve: Buckinghamshire. Okay. I can't do it.

Leo: And by the way, it's Guinness Book of World Records, just like the beer.

Steve: What did I say?

Leo: Guineas.

Steve: Oh.

Leo: Just, you know, as long as I'm correcting, I want to get it all in one swell foop.

Steve: Thank you.

Leo: Sorry about that.

Steve: Guinness.

Leo: Guinness, yes.

Steve: Guinness. He's obviously in the U.K., in England. So his subject was "SpinRite blows away the storm that blew away my PC." And he said: "Hi, Steve. This morning I booted my desktop PC, and to my alarm it was behaving monstrously at startup, basically just being incredibly sluggish. Desktop icons wouldn't appear at all. Browser launch took over five minutes. Nothing worked at all. I was puzzled because the day before I'd done a complete fresh install of Windows, and all appeared fine then. When I powered down the PC the night before, all had been fine.

"Then I remembered that the day before my village had suffered some power glitches. I live in the small village of Waddesdon near Oxford in the U.K. We'd had severe storms, and believe it or not, mains power to the village is at least in part still delivered by overhead power lines. In storms, the lines get whacked by trees and outages are common. The day before, there were two outages and two instances where the mains voltage dipped alarmingly for 1-2 seconds each time. My PC was on at the time, though I wasn't sitting at it. Could this be the cause of the dreadful slowdown in performance?

"'Let's try SpinRite,' I thought. My PC has a 256GB SSD as the operating system drive, and a large 2TB standard hard drive which serves for data. I ran SpinRite at Level 2 on the SSD, no errors. At this point I almost stopped, thinking that the other 2TB drive was not really mission critical and shouldn't really affect performance. But what the hell. I did another Level 2 check which took quite a bit longer." Well, because it's 2TB as opposed to a quarter terabyte. "I was watching those little blue squares from time to time, no greens or reds. But at one point I did notice that for a while SpinRite took ages before it would put a blue square up, for several squares in a row, perhaps 10. Anyway, it finished, all normal, no green or red indications." Meaning overt recovery or lack of recovery.

"I wasn't terribly convinced that I'd found the problem as no errors were reported. So you can imagine my surprise on rebooting to find that all was well again, and the PC behaved just as it should. This is the second time SpinRite has rescued me. I managed to rescue a friend's badly corrupted drive when she had many irreplaceable photos of her father who had passed away. So I reckon I've had my money's worth. I look forward to the new version. With best wishes, Simon Guettier." I hope I'm - oh, there it is, Guettier. No, Guettier. Simon Guettier. Thank you for the pronunciation, Simon. Sorry it was too late. Simon Guettier. And thanks for sharing your SpinRite recovery.

I mean, this is something I've talked about before, where what happened was SpinRite

showed the drive, you've got problems here, buddy. And so it wasn't necessary to force recovery. It wasn't necessary to guess at the data in the sector. It wasn't necessary to partially recover it. It just said to the drive, look. It just basically rubbed it in its face. Fix this. Finally, the drive said okay and swapped the sector out. Or maybe SpinRite was able to get a good read, and then it rewrote it. Since there wasn't anything wrong with that spot, it was caused by a power failure, it was just miswritten. So in reading it, finally getting it read, and then rewriting it, it was able to then be read without any trouble. So again, no frank recovery or failure, but we did fix the problem. And that's what SpinRite always does by the time it gets through.

So, okay. Our listeners understand the issues because we've been discussing this for a while. And of course years ago I aborted my work on CryptoLink because this was in the air, and I thought, you know, I would hate for encryption to be outlawed after I invested years of my time creating something that I intended to have as a commercial product. You know, something that I spend a day or two on that's freeware, or even the DNS Benchmark that I spent months on, but I had never intended to sell it. It would really throw my plans off. And as it turns out, there was lots of life left in SpinRite anyway. So I'm glad, for what its worth, this happened, although I wish I had CryptoLink, too. Except that we're still not sure whether, you know, what's going to happen with encryption.

So as we said at the top of the show and just before the sponsor announcement, Leo, not surprisingly, last week's attacks in Paris have stirred this up again. And anyone observing it I think objectively would recognize that, without evidence, all anyone has is speculation. And you have to be so careful in reporting. So, for example, here's a perfect example, and I don't mean to single out Ars Technica. They're needing to cover the news. And they're not doing it any differently than everybody else. But the details are important because the details are what leave impressions in people's minds.

So Ars Technica of this wrote, and this is referring to a New York Times article that I excerpt a paragraph from next, but so Ars wrote: "The investigation into last Friday's coordinated terrorist attacks has quickly turned up evidence that members of the Islamic State (ISIS) communicated with the attackers from Syria using encrypted communications, according to French officials."

Leo: Yeah.

Steve: Okay. That's not true. None of that is true.

Leo: Oh.

Steve: But there it is. They link to The New York Times article, where the only thing it mentions is to say: "European officials said they believed the Paris attackers had used some kind of encrypted communication, but offered no evidence."

Leo: Oh.

Steve: Okay, even though Ars said "has quickly turned up evidence." And then, quoting a senior European counterterrorism official, New York Times wrote: "The working assumption is that these guys were very security aware, and they assumed they would

be under some level of observation and acted accordingly." This guy spoke on the condition of anonymity because he was discussing confidential information. Well, first of all, he didn't say anything. And so what we have is we have no information, but we're already blaming encryption because, oh, well, if they were, you know, they probably used it because why wouldn't they? So, okay.

Leo: Which is true. Why wouldn't they?

Steve: Okay, right, yeah. Unfortunately, it's not evidence.

Leo: Speculation.

Steve: So, okay, yeah. So The New York Times, a different article - The New York Times wrote two, and I have links to them. And this is well reported, and this frames it well, but sort of with the same bias. It was titled "Encrypted Messaging Apps Face New Scrutiny Over Possible Role in Paris Attacks." So again, okay, possible.

Leo: You know this is being fed to them by officials with an agenda.

Steve: Exactly.

Leo: Yeah.

Steve: So: "American and French officials say there is still no definitive evidence to back up their presumption that the terrorists who massacred" - let's highlight that - "129 people in Paris used new, difficult-to-crack encryption technologies to organize the plot." So right off the bat we're going to say that no one knows anything about how this was done, but we're going to write a whole story about how encrypted messaging apps are probably to blame.

"In the interviews, Obama administration officials say the Islamic State has used a range of encryption technologies over the past year and a half, many of which defy cracking by the National Security Agency. Other encryption technologies, the officials hint, are less secure" - oh, get this. "Other encryption technologies" - like, you know, the bad ones, the weak ones, like, you know, what, paper for writing it down maybe.

Leo: Email.

Steve: Yeah. "Other encryption technologies, the officials hint, are less secure than terrorist and criminal groups may believe, and clearly they want to keep those adversaries guessing which ones the NSA has pierced." Oh, give me a break. Okay. First of all, unfortunately, these people are not stupid. And we have an open environment where we've got websites rating the security of encrypted apps with evidence. I mean, you don't have to just take their word for it. You can, you know, certainly there are cryptographers who don't have the world's best interests at heart. Mathematicians. Oh.

Anyway, they write, "Some of the most powerful technologies are free, easily available encryption apps with names like Signal, Wickr and Telegram, which encode mobile messages from cell phones. Islamic State militants used Telegram two weeks ago to claim responsibility for the crash of the Russian jet in the Sinai Peninsula that killed 224 people, and used it again last week..."

Leo: See, I told you Telegram was secure.

Steve: Yeah.

Leo: I'm sorry.

Steve: Yes.

Leo: I shouldn't laugh.

Steve: They did it by sending emojis, a certain sequence of...

Leo: [Crosstalk] stickers, yeah.

Steve: Of stickers, yeah, a plane and a bomb and a...

Leo: Yeah, we did it.

Steve: ...explosion. And then "...last week, in Arabic, English, and French, to broadcast responsibility for the Paris carnage. It is not yet clear whether they also used Telegram's secret messaging service to encrypt their private conversations."

Okay. Now, so again, reading this objectively, state officials would know if they used it, but couldn't crack it. Instead, they don't know anything. So to say that, oh, well, maybe...

Leo: It's a guess, right.

Steve: It's like, yes, it's like, well, yeah, okay. "Nonetheless," write The New York Times reporters, "such end-to-end encryption technology is now so widespread that the attack has revived vitriolic arguments between American intelligence officials and Silicon Valley. Only weeks ago, the matter appeared settled, at least temporarily, with a decision by President Obama that it would be fruitless for the government to try to compel the technology companies to provide the keys to protected conversations and data. Apple has already made encryption technology a standard part of its iMessage service."

Oh, and by the way, there is a site that ranks iMessage on a scale where the most secure were listed on the left, then the next most secure, then the okay secure, the not so good, and the not secure. iMessage was in the middle as, eh, because, as I've said, Apple manages the keys, and that's the weakness of iMessage. So you can't really trust it, not absolutely. There are absolutely trustable solutions.

And the problem is they're in the wind already. They're math. You know, I was thinking of the bomb analogy, where it takes expertise to make a bomb, but the bomb requires raw materials. And of course we know that many raw materials, the production and sales and shipping and tracking are being watched because that's a tipoff to the idea that maybe these are going to be put together into something that goes boom.

The problem is encryption isn't that way. Encryption has no raw materials that anyone can track or find. Its use has a footprint, so you can know that this looks like pseudorandom noise, and then that you either can or cannot get into it. But the point is it's math. And so the strongest argument that I have, which I've actually used in talking to some aides of senators about this who were trying to explain to their bosses months back, like I was contacted, "Steve, how do we explain to my boss, that isn't technical, why he can't just pass a law to make this happen?"

And we spent a couple hours going over arguments. And the best one, I think, is it's too late. This stuff is just math. And the math is now known and published. And so all we would succeed in doing, if we forced the legal organizations to weaken their crypto, is then the bad guys would use illegal crypto. And I heard you mention on TWiT, talking about, again, another suspicion, although I just read that it maybe had been debunked, that maybe PlayStation 4 network had been used.

Leo: Yeah.

Steve: I don't know one way or the other. But that's a perfect example of Apple and Google and anyone else offering strong crypto is forced to create backdoors, and then so they don't use it. The bad guys don't use it. They communicate during World of Warcraft instead.

Leo: Right.

Steve: Or they take a message, and they encrypt it with strong crypto that the NSA cannot break because that exists independent of services. All the services do is make it easier to use the crypto. But bad guys don't care how easy it is. Regular people care. Bad guys will go out of their way to use strong crypto that isn't easy. That's fine with them. And then they'll take this message and encode it using steganography in the low bits of an image that they post anywhere, anywhere on the 'Net. And now they have encrypted communications which no one can find. And if they did find it, they can't decrypt it.

So anyway, this article continues just to say: "But the speed of the encryption wave has touched off alarm among law enforcement and intelligence officials, who say it significantly increases the chances that they will miss evidence of an impending attack." Again, you can argue exactly against that, as I just did, with as much strength.

"Prime Minister David Cameron of Britain threatened late last year to ban such technologies, although he soon backed down. France is threatening to insist on access;

and, if the French do, so will China, many fear, raising questions about whether the same technology used to crack terrorists' communications will be used to track dissidents, as well."

And then Michael Morell, a former deputy director of the CIA, said: "I think this is going to open an entire new debate about security versus privacy. We have, in a sense, had a public debate." And he was interviewed just this past weekend on CBS's "Face the Nation," where he said: "That debate was defined by Edward Snowden. Now we're going to have a new argument defined by what happened in Paris." So anyway, I won't go on with the rest of this. There's more, if anyone's interested in the whole article, in the show notes.

But Matt Blaze was quoted, Matt Blaze, the again world-class cryptographer and signer of the various petitions and pleas to our government not to do anything wrong, not to force this - oh, where is this? "Security experts counter that such arguments ignore the fact that even end-to-end encrypted technology leaves a trail of metadata behind that can be used to parse who is talking to whom, when, and where. Encryption is really good at making it difficult to hide the content of communications, but not good at hiding the presence of communications. Mr. Blaze also noted that the authorities can still read communications if they hack into the target's device, or what security experts call the 'endpoint.' He said: 'All the encryption in the world doesn't help if the endpoint that holds the keys are compromised.' So this idea that encryption makes terrorist communications go completely dark has a pretty big asterisk next to it."

So then of course Bruce Schneier, famous cryptographer, his blog posting was titled "Paris Attacks Blamed on Strong Cryptography and Edward Snowden." And so he said, "Well, that didn't take long." And then he cites "The Daily Dot" that wrote: "As Paris reels from terrorist attacks that have claimed at least 128 lives, fierce blame for the carnage is being directed toward American whistleblower Edward Snowden and the spread of strong encryption catalyzed by his actions." And so then Bruce wrote...

Leo: That's not true.

Steve: I know. And he wrote: "Now the Paris attacks are being used as an excuse to demand backdoors." Then he said, "I was going to write a definitive refutation to the meme that it's all Snowden's fault, but Glenn Greenwald beat me to it."

Leo: Yeah. He nailed it, yeah.

Steve: And I'm not going to drag us through that. But I urge, you can probably google "Exploiting Emotions About Paris to Blame..."

Leo: It's on The Intercept, yeah.

Steve: Yes, The Intercept, "Exploiting Emotions About Paris to Blame Snowden, Distract from Actual Culprits Who Empowered ISIS." It is a really good piece. He basically - and of course we know he's got a dog in the race. He worked with Edward to publish this. But despite the fact that he has a view, doesn't mean he's wrong. And he reminds us of all the terrorist attacks which did occur, often perpetrated by people law enforcement

already knew of and had their eyes on before Snowden's revelations, going back through time. So it's not like we were catching them all before, and after Edward Snowden, now we're no longer able to catch them. And in fact the FBI, I mean the Chief of Police in New York, who's been so vocal about this, talks about thwarting 30 different attacks. I don't remember what the timeframe was. But he says we're catching them and stopping them all the time. So it's like, yes. Even with strong encryption, and even with, you know, after Snowden.

And my argument is that encryption exists. It cannot be taken back. It's math. And that what we've really got with Apple and the various instant messaging is convenient strong encryption; and that, if it is broken, the bad guys won't use it. All that will happen is that it risks weakening the convenient high-volume use where it matters, strong encryption, by making it less than that. The bad guys will continue to use less convenient strong encryption and will do it through encryption least significant bits of photos that can't be cracked and can't even be found.

So, I mean, lord knows I'm not on their side. But I am on the side of sanity and not having our legislators make a big mistake that will not help law enforcement. It will not help them.

Leo: That's the bottom line. It won't make any difference, and it will in fact weaken encryption for everybody else.

Steve: Yes.

Leo: So I think that those are provable points, both of them.

Steve: Yes.

Leo: Yeah. Certainly from experience, anyway. Well, it's a shame. And I'm already, you know, I'm seeing CNN, you just watch this, I mean, it's just you can see it happening. But I don't think you have to ascribe nefarious motives to law enforcement, to American spy agencies or GCHQ in Britain or the French spy agencies. They want to protect the homeland. I mean, I think they're doing this with absolutely pure intent. But I don't think they understand the issues.

Steve: Yes, I hope I didn't make it sound like, I mean...

Leo: No, they're trying to do the best thing. But they just don't understand the risks involved and the fact that it's not going to help you.

Steve: And also it's been pointed out that no one has been able to show a single instance where decrypting communications actually did solve, like was the crucial piece of information. So, I mean, it's one of those things that seems logical. It would make sense. Which is why it sells so well, and why headlines are so powerful, and why all the talking heads are saying it. And, I mean, Barbara Boxer is running around saying we have to get Silicon Valley under control. And it's like, no. It will not make a difference. It

just won't.

Leo: It's going, I mean, it's going to be hard with this drumbeat for Silicon Valley...

Steve: I think we're going to lose. I'll be surprised...

Leo: Really.

Steve: ...if we, yeah, I mean, I don't know how. I mean, we spent some podcasts demonstrating that it's not possible.

Leo: Right.

Steve: Things like valuable things, like Perfect Forward Secrecy, cannot be used because Perfect Forward Secrecy is continually changing the keys. And so you can't have Perfect Forward Secrecy, which now everyone wants, if you're going to allow a captured encrypted previous dialogue to be decrypted because the keys are inherently ephemeral. So that would require somehow logging the keys. I mean, and this is the problem, is no one wants to look at the actual details. And they assume that Silicon Valley is just dragging their heels.

Leo: Right.

Steve: Like Apple is selling security as a marketing vehicle, and so it's not that it cannot do it, it just chooses not to. And it's like, no, when you really get down to it. There was a great analysis that talked about, like, if you were going to do this on an Android phone, then nothing prevents the bad guys from loading an Android app which is secure, which would be available on the black market, into their Android phone and using it. Because nothing prevents it.

Leo: Yeah.

Steve: And so, okay. So if we were to really firmly outlaw encryption, well, first of all, is a backdoor feasible? And the problem is now all of communications looks like random noise. So what does the NSA do? All of the communications looks like random noise. Do they have the ability to decrypt all of the communications in order to return it to plaintext, in order to run it through their pattern recognition? I mean, no one is suggesting that. No one is suggesting that all of the communications gets decrypted.

So we're in a world where everything is encrypted. It's just hiss. It's white noise. So that says they have to use the metadata or endpoint recognition to find the specific dialogues they want, and then have a way of decrypting those on demand, and then seeing if there's anything there. And we know that the problem is that means that all, any arbitrary communication, can then be decrypted. If they're able to decrypt any one of them, then they can decrypt them all.

Leo: Wow.

Steve: So I just - and again, it risks damaging the high volume, ease of use case, which is what Apple, to quote a Silicon Valley target, what Apple gives us is very, very, secure instant messaging, as do all the other IM clients, super ease of use. But that's all. It's the ease of use. So if you don't need that, and somebody - well, a perfect example is Threema. Threema is my choice for instant messaging client because it's less easy to use.

Leo: Right.

Steve: You have to physically exchange the key, and that's cumbersome. So people don't use Threema because that's, boy, you know, that's a few hoops to jump over. Well, if you absolutely have to have security, that's what you do. And then you use a courier to exchange a couple QR codes written on paper, which he can burn or eat, depending upon what, in order to get the keys exchanged. And then you have absolute security. But iMessage just kind of works. So that's what everyone uses. So my point is that it's like it's the wrong target. It's why it's a whipping boy. It's why it's a complete red herring.

Leo: Because it's easy. Right. Great stuff, as always. And the problem is that everybody listening to the show knows that.

Steve: Yeah.

Leo: And I'm not sure, I mean, I guess the thing to do is just keep saying it.

Steve: But they do know people. They do know people.

Leo: Yeah. And keep saying it because it will eventually, well, I think people convinced David Cameron that it couldn't be done.

Steve: Yes, and I don't know if I had any influence to this one senator whose aides had me on speakerphone.

Leo: It bet you did. I bet you did.

Steve: But, you know, somebody told them to call me.

Leo: Right.

Steve: Because I could explain it to them. And I ended up giving them a strong

argument, which was unfortunately you can't take back the math. The math is already out there.

Leo: It's already out there.

Steve: Yeah.

Leo: You know, we know this. Because remember when people were wearing T-shirts with a strong encryption code on it, going...

Steve: Because copyright was trying to be used.

Leo: Well, [crosstalk].

Steve: That source code is copyrighted. And it's like, oh, come on.

Leo: Yeah. I mean, I think that we know this already, that this is a - there's no way to stop it. The horse has left the barn.

Steve: Yeah. And the fact is, you know, sure, maybe your corner criminal will use his iPhone stupidly. But no people...

Leo: But not the really bad buys.

Steve: Exactly. Not the ones we really care about.

Leo: We know they're smart enough because Osama bin Laden was living in a compound for years where it was expressly forbidden to have any Internet. He knew.

Steve: And it was by...

Leo: [Crosstalk] with couriers.

Steve: Yes, it was by torturing, or, no, we don't use that word, it was by extreme interrogating a courier that we were able to get the information.

Leo: That's, by the way, not clear either. But that's the story.

Steve: Yes, true.

Leo: Yeah. Well, Steve, from your lips to the congresscritters' ears. And by the way, I'm having a lot of fun with this game. Man.

Steve: Oh, Leo, it's going to suck you in.

Leo: I feel like it's "Ender's Game" going on here; right?

Steve: Yeah.

Leo: It's really fun. It's beautiful, and it's slow, which is nice, so you don't have the panic thing going on. I think I'm starting - how do you get a planet to expand, though? I can't...

Steve: Okay, now, what you're not doing is draw a circle, I mean, like, draw a cord across one those things, and that selects them all.

Leo: Yeah.

Steve: And then tap where you want it to go.

Leo: Right. Well, I've been kind of - I've been doing it one at a time, ones and twos, because I want to reinforce these planets as I maintain this forward base.

Steve: Exactly.

Leo: It takes a long damn time. That's the only negative. But it's really fun. Really fun.

Steve: It's not meant to be rushed.

Leo: Yeah. Yeah.

Steve: It's just kind of slow.

Leo: He says, and I think this is true, he's tried to strip the elements of real-time strategy games down to the bare, you know, essentials, which is this; right?

Steve: Yes. You have one thing you can do, and one type of action. But yet there's a huge decision process.

Leo: Right.

Steve: Ooh, and look at those guys fighting each other right now.

Leo: Oh, it's a battle. But I think I'm going to prevail. Yeah, yeah, yeah. That orange guy. More reinforcements to the forward posts. See, I'm - whoops, didn't mean to do that. Don't go back there, guys. Go here. So I'm trying to bring up the guys in the rear to strengthen.

Steve: Auralux, A-U-R-A-L-U-X.

Leo: It's a fun game. Oh, man. All right. Thank you. Steve. I'm going to be kind of busy. That's on iOS and Android, by the way.

Steve: Yes.

Leo: Which is nice. You can play it on all your platforms. Steve Gibson is at GRC.com. That's his website, and that's where you'll find Security Now!, of course, including transcripts, written transcripts. There's no way to pause this, is there. I just have to let the war go on.

Steve: Good question.

Leo: I don't think there is. So you'll forgive me if in between I just tap some planets. You'll find written transcripts - oh, my god. You'll find [mimicking bugle]. You'll find 16Kb versions. That's the lowest quality audio we offer, but it's for people with bandwidth limitations, which increasingly is everybody. We also have lots of free stuff there. All of his SQRL and the Perfect Paper Passwords. And of course his bread and butter, SpinRite, the world's best hard drive maintenance and recovery utility. If you have a hard drive, you must have SpinRite.

We have on our website both audio and video, TWiT.tv/sn. We also have put versions up for every podcatcher to get. So you can subscribe. And please do. That way you'll get every episode. Just search for TWiT. You'll find what you're looking for. We do the show on Tuesdays, 1:30 Pacific, 4:30 Eastern time, 21:30 UTC, if you want to watch live or join us in the chatroom. I think that's everything. Steve, have a great week. Enjoy...

Steve: Will do. Oh, GRC.com/feedback.

Leo: Oh, questions and answers, yeah.

Steve: Because next week is a Q&A.

Leo: And I got an email from Oscar on my PiDP-8.

Steve: Oh, yeah.

Leo: He said, "Oh, I forgot to send it to you."

Steve: Yay.

Leo: Well, yeah. So he refunded my money. Thank you, Oscar. And then he said, you know...

Steve: Oh, so he didn't...

Leo: Well, I said don't go to - because I guess he'd sent everything out. Don't go to crazy lengths to get another one for me.

Steve: Oh.

Leo: He said, "No, no, I'm going to get you one." So we'll see what happens. We'll see what happens.

Steve: Okay, good, good.

Leo: That's the Raspberry Pi-based PDP-8. You know, yesterday I had Larry Wall, the creator of Perl, on. And we were talking about his early days of computing with PDP-11.

Steve: Oh.

Leo: I should have told him. We've got something for you, Larry. All right, Steve. Thanks for joining us.

Steve: Okay, my friend. Talk to you next week for a Q&A.

Leo: All right.