Security Now! #560 - 05-17-16

Z-Wave Goodbye

This week on Security Now!

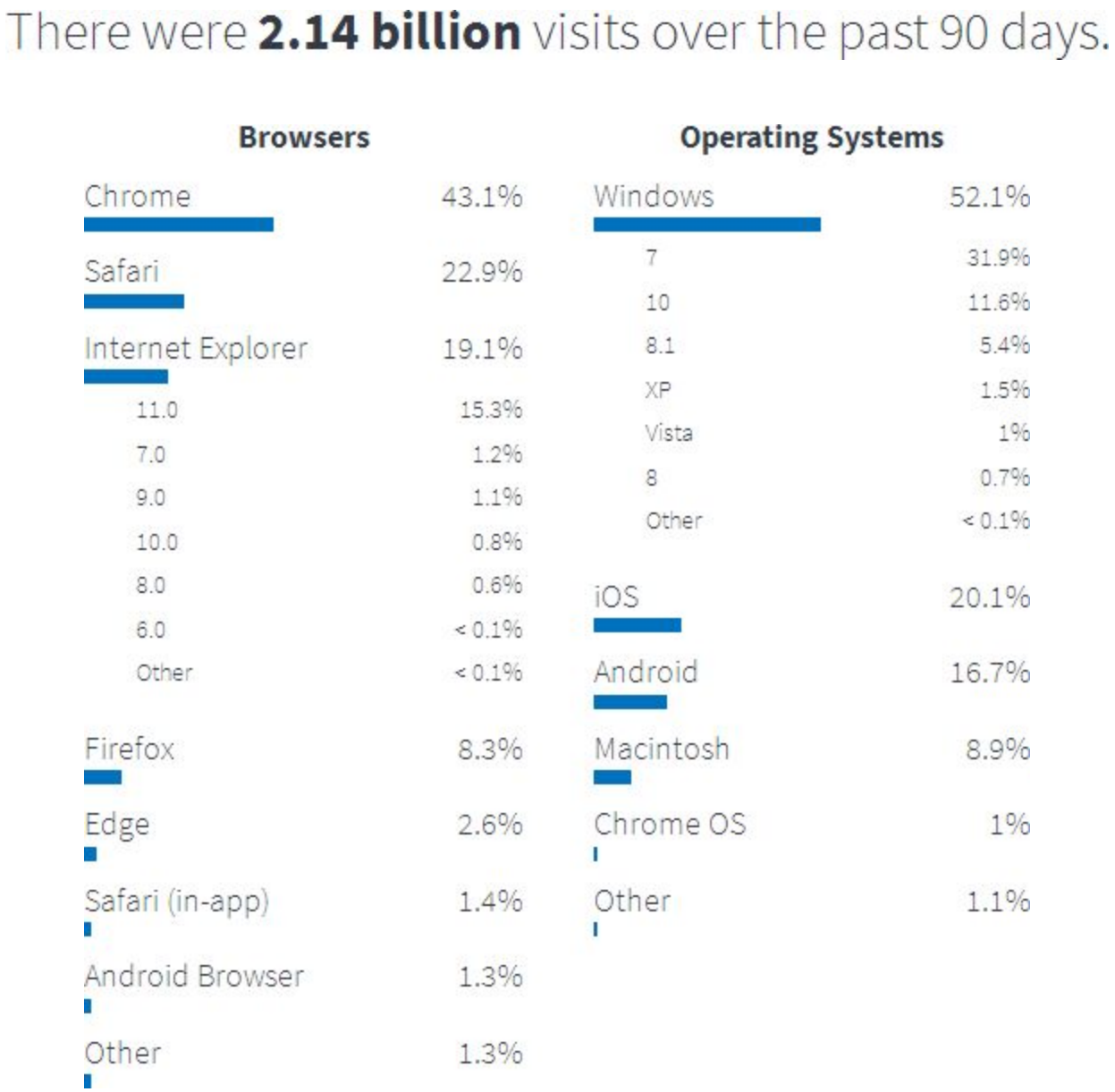
- Steve's long love affair with Windows
- The Oracle/Google JAVA API lawsuit
- The pending registration of "burner" phones
- Surveillance microphones found in public areas
- John McAfee and team cracks WhatsApp encryption?
- The Ring Doorbell may need another update
- A security-related Kickstarter which Security Now listeners would never fall for.
- A controversial feature being removed from Windows 10
- A worrisome and exploitable heap corruption in the popular 7-Zip application
- ... and a look at the Z-Wave Home Automation system

What was last week's **3035583** refresh all about?

Security News

"Why does Steve hate Windows 10 so much?"

- Let's get this straight, everyone: I LOVE WINDOWS.



Source: https://analytics.usa.gov/

- 83.60% = Win7/44.56% Win10/17.90% Win8.1/10.30% WinXP/7.46% Win8/3.38%
- My complaint is that Windows is a commercial, closed-source, profit center for a massive corporation which **must** keep finding ways to leverage Windows' market share for its own profit.
- For me, Windows is not a curio, a toy, or a platform for instagram and social media. Windows is a tool. **It is my chosen tool.** But Microsoft needs to keep changing it, NOT TO MAKE IT BETTER, but **only** for the sake of making it new.
- So there is an inherent tension between Microsoft's interests and my own.

- An operating system should manage file systems, manage the system's memory, manage applications and services, provide I/O services… and more recently provide a comfortable and convenient desktop environment for its user.

- Never10 does **=not=** represent my hatred of Windows, or even of Windows 10. Never10 was born to empower users. Empowering users is what I have always done.

- "Windows 10" is the most secure Windows ever. Nonsense. That's just Microsoft playing off of user's security fears. "Windows XP is the most secure operating system ever." Code Red, Nimda, MSBlast… and on and on.

- "Security" is only something that history can judge. By definition is cannot possibly be affirmed at launch.

- Microsoft is not going to be able to resist the temptation of leveraging Windows 10 connectivity into additional sales and marketing. Already we're hearing reports of advertising appearing on the desktop and apparently it recently began promoting Office 365.

So… please don't anyone get me wrong: I love Windows… so much so that I'm mourning what my beloved operating system, which I have loved so much and for so long, is becoming.

The Oracle Lawsuit: $ 9,300,000,000.

First: A summary of the history by the EFF:
https://www.eff.org/cases/oracle-v-google

At issue in Oracle v. Google is whether Oracle can claim a copyright on Java APIs and, if so, whether Google infringes these copyrights. When it implemented the Android OS, Google wrote its own version of Java. But in order to allow developers to write their own programs for Android, Google's implementation used the same names, organization, and functionality as the Java APIs. For non-developers out there, APIs (Application Programming Interfaces) are, generally speaking, specifications that allow programs to communicate with each other. So when you read an article online, and click on the icon to share that article via Twitter, for example, you are using a Twitter API that the site's developer got directly from Twitter.

In May 2012, Judge William Alsup of the Northern District of California ruled that APIs are not subject to copyright. The court clearly understood that ruling otherwise would have impermissibly—and dangerously—allowed Oracle to tie up "a utilitarian and functional set of symbols," which provides the basis for so much of the innovation and collaboration we all rely on today. Simply, where "there is only one way to declare a given method functionality, [so that] everyone using that function must write that specific line of code in the same way," that coding language cannot be subject to copyright.

Oracle appealed Judge Alsup's ruling to the U.S. Court of Appeals for the Federal Circuit. On May 30, 2013, EFF filed an amicus brief on behalf of many computer scientists asking the

Federal Circuit to uphold that ruling and hold that APIs should not be subject to copyright. On May 9, 2014, the Federal Circuit issued a disastrous decision reversing Judge Alsup and finding that the Java APIs are copyrightable, but leaving open the possibility that Google might have a fair use defense.

On October 6, 2014, Google filed a petition asking the U.S. Supreme Court to review the Federal Circuit's decision. On November 7, 2014, EFF filed an amicus brief on behalf of many computer scientists that asked the Supreme Court to grant Google's petition for review, reverse the Federal Circuit, and reinstate Judge Alsup's opinion. Unfortunately, in June 2015 the Supreme Court denied Google's petition. The case will now return to the district court for a trial on Google's fair use defense.

- (See https://www.eff.org/cases/oracle-v-google for many links and related documents.)

- The crucial importance of open standards -- literally: civilization is built upon them.
- The idea of modular standard interfaces is so ubiquitous it's almost impossible to imagine an "ad hoc" world without them.
    - The way a car is driven.
    - Standard nut and bolt THREADING.
    - The x86 instruction set.

... Oracle Says:
http://www.computerworld.com/article/2970944/android/oracle-google-has-destroyed-the-market-for-java.html

Oracle has expanded the scope of its ongoing copyright battle against Android and accused Google of "destroying" the market for Java.

Oracle made a request late last month to broaden its case against Android. Now, a supplemental complaint filed Wednesday in San Francisco district court encompasses the six new Android versions that have come out since Oracle originally filed its case back in 2010: Gingerbread, Honeycomb, Ice Cream Sandwich, Jelly Bean, Kit Kat and Lollipop.

Oracle charged: *"As with previous versions of Android, these six Android releases copy thousands of lines of source code from the Java platform, as well as the structure, sequence and organization of that platform. This copying constitutes copyright infringement."*

Oracle also noted that Android has expanded beyond smartphones over the years to include wearable devices, TVs, cars and various household appliances. Advertising on the mobile platform has increased dramatically as well, it said, thereby bolstering Google's core source of revenue and allowing the search giant to *"reap enormous profits from both its direct and indirect exploitation of the infringing code."*

As a result of all this, Oracle's Java business has been seriously harmed, it said.

Oracle wrote: *"Given the widespread dominance Android has achieved with its continued unauthorized use of the 37 Java API packages over the past few years, Android has now irreversibly destroyed Java's fundamental value proposition as a potential mobile device operating system"*

The end of "burner" phones?

- Four days ago, Friday, May 13th: **Steve Gibson** @SGgrc
  Wow. A new law proposed in the US House of Reps requiring legal identification for the purchase of "burner" phones: j.mp/HR4886
- To require purchasers of pre-paid mobile devices or SIM cards to provide identification, and for other purposes.
- This Act may be cited as the "Closing the Pre-Paid Mobile Device Security Gap Act of 2016".

- SEC. 2. Identification requirement.
  Prior to the completion of any sale of a pre-paid mobile device or SIM card to a purchaser, an authorized reseller shall require the purchaser to provide the following information:
  - (1) The full name of the purchaser.
  - (2) The complete home address of the purchaser.
  - (3) The date of birth of the purchaser.

- SEC. 3. Identification verification.
  (a) In-Person sales.—An authorized reseller making a sale to a purchaser in person shall verify the purchaser information provided under section 2 by requiring the purchaser to display either of the following:
    - (1) A photographic identification card issued by the Federal Government or a State government, or a document considered acceptable for purposes of subparagraph (B), (C), or (D) of section 274A(b)(1) of the Immigration and Nationality Act (8 U.S.C. 1324a(b)(1)).
    - (2) Any 2 of the following:
      - (A) A Form W–2 Wage and Tax Statement received from the Internal Revenue Service, provided that such form has been received from the Internal Revenue Service within the prior 18 months.
      - (B) A Form 1099 Social Security Benefit Statement received from the Social Security Administration, provided that such form has been received from the Social Security Administration within the prior 18 months.
      - (C) A Form 1099 received from any other agency of the Federal Government other than the Social Security Administration, including the Internal Revenue Service, provided that such form has been received within the prior 18 months.
      - (D) Any document containing personal identifying information that the Attorney General finds, by regulation, to be acceptable for purposes of this section.
- (b) Other sales.—An authorized reseller making a sale to a purchaser not in person shall verify the purchaser information provided under section 2 by requiring the purchaser to submit the following information:
    - (1) Valid credit or debit card account information.
    - (2) Social Security number.
    - (3) Driver's license number.
    - (4) Any other personal identifying information that the Attorney General finds, by regulation, to be necessary for purposes of this section.

Hidden Microphones Exposed As Part of Government Surveillance Program In The Bay Area

- http://sanfrancisco.cbslocal.com/2016/05/13/hidden-microphones-exposed-as-part-of-government-surveillance-program-in-the-bay-area/
- http://cbsloc.al/23OVmmp
- "Speaking in a public place does NOT mean that the individual has no reasonable expectation of privacy."
- "A private communication in a public place qualifies as a protected "oral communication" under Title III... and therefore may not be intercepted without judicial authorization."

John McAfee -- Uber-Hacker!

WhatsApp Message Hacked By John McAfee And Crew
http://cybersecurityventures.com/whatsapp-message-hacked-by-john-mcafee-and-crew/
John McAfee claims to have cracked secure WhatsApp messages
http://www.msn.com/en-gb/money/technology/john-mcafee-claims-to-have-cracked-secure-whatsapp-messages/ar-BBt5r1b
John McAfee claims he can read encrypted messages on Android (updated)
http://www.engadget.com/2016/05/15/john-mcafee-claims-to-crack-whatsapp-messages/
John McAfee Apparently Tried to Trick Reporters Into Thinking He Hacked WhatsApp
http://gizmodo.com/john-mcafee-apparently-tried-to-trick-reporters-into-th-1776765480

It appears that McAfee has tried to trick reporters again, by sending them phones pre-cooked with malware containing a keylogger, and convincing them he somehow cracked the encryption on WhatsApp. According to cybersecurity expert Dan Guido, who was contacted by a reporter trying to verify McAfee's claims, McAfee planned to send this reporter two Samsung phones in sealed boxes. Then, experts working for McAfee would take the phones out of the boxes in front of the reporters and McAfee would read the messages being sent on WhatsApp over a Skype call. McAfee offered this story to at least the International Business Times and Russia Today. One additional source said he also shopped the story to Business Insider.

Dan Guido said: "John McAfee was offering a couple of news organizations to mail them some phones, have people show up, and then demonstrate with those two phones that [McAfee], located in the remote mountains of Colorado, would be able to read the message as it was sent between the phones. I advised the reporter to go out and buy their own phones, because even though they come in a box it's very easy to get some saran wrap and a hair dryer to rebox them."

Moxie Marlinspike, who developed the encryption protocol used in WhatsApp and assisted in implementing it, told Gizmodo that McAfee also admitted his plan to him. Moxie said: "Some reporters that had been contacted by McAfee about a demo got in touch with me. I talked to McAfee on the phone, he reluctantly told me that it was a malware thing with pre-cooked phones, and all the outlets he'd contacted decided not to cover it after he gave them details about how it'd work."

Ring Doorbells "crossing the streams" ??
"Smart doorbell owners saw video from other houses thanks to a weird bug."
http://www.theverge.com/circuitbreaker/2016/5/14/11675430/ring-smart-doorbell-stranger-video-bug
Excellent, non-hysterical reporting by The Verge:
<The Verge> Sometimes the wheels can just come off this whole internet of things... thing. When cameras are talking to the cloud, there's room for them to make mistakes, and these devices are filming pieces of your private life so that can be a little worrisome. Unfortunately, some owners of the Ring Doorbell Pro recently experienced just this sort of mixup when the "smart" system showed them video of visitors outside — only it wasn't their own home that the feed was coming from. They were getting video from other Ring users.

Now this isn't the worst thing to have happen security-wise. It's pretty hard to tell someone's address from a doorbell camera, so once you come to the realization that you're not seeing your house, all you're left with is a video of a total stranger. And for what it's worth, Ring claims that there were only 10 instances of this problem out of over million "calls" that its doorbells make each day.

Still, it's the sort of problem that absolutely can't happen if we're going to invite smart home gadgets into our everyday lives 24/7. To that end, the company says it's taken steps so that this weird and semi-creepy bug won't repeat itself in the future.

<Ring's Response> We use random numbers to generate a call ID from Ring products. We did a very robust Beta test of the new Ring Video Doorbell Pro on experimental software, and when we moved it out of Beta for the commercial launch, some customers' numbers were in two different databases. As a result, those call ID numbers were overwritten. We believe, based on all the data we have analyzed, that this caused less than ten instances - out of more than 4 million calls per day and over 84 million calls in total - where video recordings overlapped for Ring Video Doorbell Pro users only. We are in the process of merging those databases so this will no longer occur. This issue only effected Ring Video Doorbell Pro users, not users of our other products, Ring Video Doorbell and Ring Stick Up Cam.

DataGateKeeper
https://www.kickstarter.com/projects/datagatekeeper/datagatekeeper-the-first-impenetrable-anti-hacking
Kickstarter Campaign: DataGateKeeper: First Encryption Software Engineered to Defeat Hacking

Programs, Granting Impenetrable Data Protection & Cloud Storage
Presenting the DataGateKeeper Total Data Protection Software™ & SafeDataZone™ Cloud Storage
Protect your LIFE, your BUSINESS, your FUTURE
Guaranteed Privacy and Confidentially with One Click.

Everyday You Use Flawed Data Protection. Not By Choice

Due to these flaws, cybercriminals and hackers steal and profit from your stored and transmitted personal and business data everyday.

Designed before the turn-of-the-century, AES or Advanced Encryption Standard, is older than most of the cars on the road today, however, it forms the basis of our global data security protection. And its failing.

AES Hacking Solutions are readily available for sale on dark web.

In the late 1990's, AES, while under 'well-intentioned' government oversight, somehow, a 'back-door' found its way into this 'approved' data security solution, — as has been widely reported. The unintended consequences of this back-door allows for complete access to your data, without your permission, to data monitoring, data-mining and active eavesdropping. Effectively, voiding your right to privacy and confidently[sic]. So common is this practice it has a name: Active Snooping.

SSL is a Myth. Cybercriminals know about these flaws and back-door. They are stealing, compromising, and profiting from your data everyday.

The commitment to build an impenetrable data encryption solution, free of outside influence, began nearly 3 years ago. At the same time we were developing the DataGateKeeper (code-named Deterrence), unfortunately, over 150 million personal and confidential files were compromised, stolen or hacked in the U.S. alone. And those were just the ones that were reported (see, Timeline). We knew we needed to be successful.

To accomplish our goal of building an impenetrable data security solution, we first had to be able beat hackers at their own game using their own tools. To do this, we reverse engineered several commercially available automated password cracking programs, and two which are not, to understand these programs methodologies. Following the decompile and disassembly[sic] procedure, we designed and built our own cracking program, and then we set about defeating our new 'super hybrid'. […] Goal met.

The DataGateKeeper Total Data Protection Software is the first data protection software specifically designed and engineered to defeat automated hacking and code cracking programs. Exclusively, the DataGateKeeper contains no backdoor and disallows automated repetitions, the core method used in brute force attacks. We built an 'exploit' that destroys their 'exploit'.

You don't have to be 007 to Use the DataGateKeeper Encryption Software...

Or be an international spy to need it. Never has it been easier, or less expensive, to protect your digital privacy and secure your confidentiality on-line than it is today. Our DataGateKeeper Total Data Protection Software™ provides you a mathematically impenetrable data security solution with just one-click of a mouse.

Why settle for inferior data protection and Cloud storage? Enjoy uncompromising data security with the DataGateKeeper and convenience of the SafeDataZone Cloud for the same price you're paying today, for out-of-date, flawed and failing cloud service.

The chart below compares the highest MSRP of our DataGateKeeper Total Data Protection Software™ & integrated SafeDataZone™ versus the competitors lowest available published price,

and security solution, for data ‘at-rest’ and ‘in-motion’.

Simply, ‘the other guys’ use standard SSL (Secure Sockets Layer), and the failing AES, in an attempt to secure your Privacy & Confidentiality. The same data security hackers took advantage of in the breach of Target, Home Depot, iCloud, Sony, Anthem...you get the idea. You Deserve Better.

Providers		Dropbox	Google Cloud	OneDrive	Carbonite	IDrive
512-Bit Encryption	✓	⊘	⊘	⊘	⊘	⊘
“At Rest” Protection	✓ 512kb DGK	⊘ 128kb AES	⊘ 128kb AES	⊘ 128kb AES	⊘ 128kb AES	⊘ 128kb AES
“In Motion” Protection	✓ 512kb DGK (SSL[6])	⊘ 128kb-256kb SSL	⊘ 128kb-256kb SSL	⊘ 128kb-256kb SSL	⊘ 128kb-256kb SSL	⊘ 128kb-256kb SSL
Encrypt All File Types	✓	⊘	⊘	⊘	⊘	⊘
Storage	500GB	1TB	1TB	1TB	Unlimited	1TB
Price	$129.99	$119.88	$122.88	$83.88	$99.99	$59.50

The government employs entire teams of experts to protect their organizations to keep ahead of cybercriminals. As a private citizen you deserve the same ability to protect your private and confidential information. By joining the growing community using the DataGateKeeper Software you now have your very own Data Angel expert sitting on your shoulder.

Data Protection Unlike Any Other

The DataGateKeeper™, our mathematically impenetrable encryption engine, provides 6 million times greater protection than current 256-bit data security protocols deployed by Google, Facebook, Apple and others.

The DataGateKeeper Total Data Protection Software™ includes complimentary, 500GB of the SafeDataZone™, our unique Cloud Storage and Sharing Solution. MyDataAngel.com provides Impenetrable Civilian Data Protection plans beginning at 512-bit encryption.

Exclusively On Kickstarter. Our 64GB Flashdrive

Our limited edition 64GB 3.0 USB flashdrive comes with the DataGateKeeper™ software pre-installed. Oh... and it is hardened and waterproofed up to 100 meters!
(A full-chested woman shown taking the cap off the USB drive.

For Mr. Wizard...

DataGateKeeper Total Data Protection Software™ Versions
512kb / 50 Years of Protection / Civilians
768kb / 75 Years of Protection / First Responders, Police, Retired & Active Duty Military
1024kb / 100 Years of Protection / Enterprise

The Building of an Impenetrable Data Security Solution & Cloud

Our goal was to purposefully design and engineer a mathematically impenetrably encryption algorithm where users could control the security of their data, on their device, prior to transmission or storage. For operational security, we elected to do our research, design and implementations free from outside influence, or prying eyes.

'Exploit' the 'Exploit'

Following months of research, decompiling, and disassembly, we had a baseline for Deterrence and developed our cipher utilizing cryptanalysis. We created a cipher that is 6,000,000 times stronger than current data security, as proven by algorithmic mathematics. You now have a choice to secure your data in the digital age. Protect your Future - Secure Your Data. Choose the the DataGateKeeper Total Data Protection Software.

Controversial WiFi Sense password contacts sharing being removed from Win10
https://blogs.windows.com/windowsexperience/2016/05/10/announcing-windows-10-insider-preview-build-14342/
Windows 10 Insider Preview Build 14342
<quote> Other items of note
We have removed the Wi-Fi Sense feature that allows you to share Wi-Fi networks with your contacts and to be automatically connected to networks shared by your contacts. The cost of updating the code to keep this feature working combined with low usage and low demand made this not worth further investment. Wi-Fi Sense, if enabled, will continue to get you connected to open Wi-Fi hotspots that it knows about through crowdsourcing.

7Zip Heap Corruption
Multiple 7-Zip Vulnerabilities Discovered by Talos (Cisco)

- http://blog.talosintel.com/2016/05/multiple-7-zip-vulnerabilities.html
- http://www.7-zip.org/

Miscellany

Brandon O'Neal @brandononeal:

- Another Never10 success story.
- ----------
- Steve, I'm a tech enthusiast and a professional wedding photographer. Our support groups have been bombarded with photographers who are surprised to find their workstations suddenly upgraded to Windows 10, seemingly without their input. I've been glad to enlighten them to the fact that it's not entirely their fault, and even more happy to save so many others from this forced upgrade by suggesting they download Never10. Thanks - from the photography industry - for all the work you do! Cheers!

Marry Jo Foley / Paul Thurrott

- Mary Jo Foley @maryjofoley
- Microsoft comes through with its promised 'convenience rollup' of updates and fixes for Windows 7:
- http://www.zdnet.com/article/microsoft-comes-through-with-rollup-of-updates-and-fixes-for-windows-7/
- KB3125574

SpinRite

Brad in New South Wales, Australia
Subject: SpinRite success on iMac SSD
Date: 14 May 2016 06:40:13
:
Hi Steve and Leo,
I have been listening to your show for about 3 years and really enjoy it.
I need to give a bit of background to this story as there is a lot involved.

I have a 2009 iMac that hasn't missed a beat since I purchased it. A year ago, it started to slow down somewhat. Not wanting to fork out a few grand just yet for a new machine, I managed to pull the machine apart and upgrade the optical drive and 3.5" mechanical drive to 2 new HDDs. One a higher capacity spinning drive, the other, an SSD. The SSD was installed by a built for purpose blanking plate in the shape of the optical drive and was installed in the optical drive's original location. Once the SSD was in place, the machine ran like new.

Recently, the SSD was showing signs of failure and was no longer booting properly. Not wanting to pull the iMac apart again I researched a solution. I came across a video (I think you mentioned in a previous episode) where it was possible to run SpinRite from within MacOSX.

I installed OSX onto an external HDD and booted to it. I then downloaded VirtualBox and ran up a DOS virtual machine. I attached the dying SSD managed to the DOS virtual machine then booted SpinRite with its ISO file. I ran level 2 on the iMac's SSD and after rebooting she now runs just like new again.

Thanks for a great podcast!
Cheers,
Brad

Z-Wave Goodbye

- We need an open public protocol for IoT as we have for everything else that matters.
- The protocol for IoT cannot be single-sourced proprietary
- Abstract— The Z-Wave wireless communication protocol has been widely used in home automation and wireless sensors networks. Z-Wave is based on a proprietary design and a sole chip vendor. There have been a number of academic and practical security researches on home automation systems based on ZigBee and X10 protocols, however, no public vulnerability research on Z-Wave could be found prior to this work.

  In this paper, we analyze the Z-Wave protocol stack layers and design a radio packet capture device and related software named Z-Force to intercept Z-Wave communications. This device enables us to decode different layers of the Z-Wave protocol and study the implementation of encryption and data origin authentication in the application layer. We then present the details of a vulnerability discovered using Z-Force tool in AES encrypted Z-Wave door locks that can be remotely exploited to unlock doors without the knowledge of the encryption keys.
- Z-Wave proprietary protocol developed by Sigma Designs, Inc.
- The protocol specification and software development kit (SDK) are not open and are only available to OEM device manufacturers under a legally binding non-disclosure agreement Sigma Designs.
- The SDK costs between $1500 to $3500 US dollars, and the NDA prohibits any public disclosure of the SDK's content.
- Z-Wave operates in the sub-gig Industrial, Scientific, Medical band (908.42 Mhz) in the U.S.
- Each Z-Wave controller manages ONE network, identified by a 32-bit (4.3 billion) "Home ID."
- The Home ID value is written to the controller’s Z-Wave chip by Sigma.
- Individual "nodes" within the network are identified by an 8-bit node ID.
- … And they found an exploit that allows them to unlock anyone’s door. :(