Security Now! #600 - 02-21-17

The MMU Side-Channel Attack

This week on Security Now!

Microsoft's February patch Tuesday changed from "delayed" to entirely cancelled amid a flurry of serious problems; it's not only laptop webcams that we need to worry about; the perils of purchasing a previously-owned Internet connected auto; Chrome changes its UI making certificate inspection trickier; the future of Firefox Add-Ons; Win10's lock screen is leaking the system's clipboard; a collection of new problems for Windows; a amazing free Crypto book online from Stanford and New York University; pfSense and Ubiquity follows-ups; a bit of geek humor and miscellany… And a deep dive into yet another sublime hack from our ever-clever friends, led by professor Herbert Bos at the University of Amsterdam.

"Of course this website is safe. As an extra measure of security, they make you sign in with your Social Security number, mother's name, your bank account, home address, phone number and date of birth."

Security News

February 2017 Security Update Release -- Cancelled

- UPDATE: 2/15/17: We will deliver updates as part of the planned March Update Tuesday, March 14, 2017.
- https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/

Hackers who took control of PC microphones siphon >600 GB from 70 mostly-Ukraine targets

- US-based Cyber-X Labs of Framingham, MA, focusing on industrial cybersecurity: Operation BugDrop: CyberX Discovers Large-Scale Cyber-Reconnaissance Operation Targeting Ukrainian Organizations

- https://cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

- <quote> CyberX has discovered a new, large-scale cyber-reconnaissance operation targeting a broad range of targets in the Ukraine. Because it eavesdrops on sensitive conversations by remotely controlling PC microphones – in order to surreptitiously "bug" its targets – and uses Dropbox to store exfiltrated data, CyberX has named it "Operation BugDrop."

  CyberX has confirmed at least 70 victims successfully targeted by the operation in a range of sectors including critical infrastructure, media, and scientific research. The operation seeks to capture a range of sensitive information from its targets including audio recordings of conversations, screen shots, documents and passwords. Unlike video recordings, which are often blocked by users simply placing tape over the camera lens, it is virtually impossible to block your computer's microphone without physically accessing and disabling the PC hardware.

  Most of the targets are located in the Ukraine, but there are also targets in Russia and a smaller number of targets in Saudi Arabia and Austria. Many targets are located in the self-declared separatist states of Donetsk and Luhansk, which have been classified as terrorist organizations by the Ukrainian government.

- CyberX is keeping the identities of the affected organizations private, but give us a high-level peek: Examples of Operation BugDrop targets identified by CyberX so far include:
  - A company that designs remote monitoring systems for oil & gas pipeline infrastructures.
  - An international organization that monitors human rights, counter-terrorism and cyberattacks on critical infrastructure in the Ukraine.
  - A scientific research institute.
  - An engineering company that designs electrical substations, gas distribution pipelines, and water supply plants.
  - Editors of Ukrainian newspapers.

- Operation BugDrop is a well-organized operation that employs sophisticated malware and appears to be backed by an organization with substantial resources. In particular, the operation requires a massive back-end infrastructure to store, decrypt and analyze several GB per day of unstructured data that is being captured from its targets. A large team of human analysts is also required to manually sort through captured data and process it manually and/or with Big Data-like analytics.

  Initially, CyberX saw similarities between Operation BugDrop and a previous cyber-surveillance operation discovered by ESET in May 2016 called Operation Groundbait. However, despite some similarities in the Tactics, Techniques, and Procedures (TTPs) used by the hackers in both operations, Operation BugDrop's TTPs are significantly more sophisticated than those used in the earlier operation.

- For example, it uses:
  - Dropbox for data exfiltration, a clever approach because Dropbox traffic is typically not blocked or monitored by corporate firewalls.

  - Reflective DLL Injection, an advanced technique for injecting malware that was also used by BlackEnergy in the Ukrainian grid attacks and by Duqu in the Stuxnet attacks on Iranian nuclear facilities. Reflective DLL Injection loads malicious code without calling the normal Windows API calls, thereby bypassing security verification of the code before its gets loaded into memory.

  - Encrypted DLLs, thereby avoiding detection by common anti-virus and sandboxing systems because they're unable to analyze encrypted files.

  - Using legitimate free web hosting sites for command-and-control infrastructure. C&C servers are a potential pitfall for attackers as investigators can often identify attackers using registration details for the C&C server obtained via freely-available tools such as whois and PassiveTotal. Free web hosting sites, on the other hand, require little or no registration information. Operation BugDrop uses a free web hosting site to store the core malware module that gets downloaded to infected victims. In comparison, the Groundbait attackers registered and paid for their own malicious domains and IP addressees.

- Operation BugDrop infects its victims using targeted email phishing attacks and malicious macros embedded in Microsoft Office attachments. It also uses clever social engineering to trick users into enabling macros if they aren't already enabled.

A Cautionary Tale: It's too easy to steal a second-hand connected car

- http://www.welivesecurity.com/2017/02/20/easy-steal-second-hand-connected-car/
- http://money.cnn.com/2017/02/17/technology/used-car-hack-safety-location/
- by Graham Cluley
- Charles Henderson, Global Head of X-Force Red, IBM Corporation

- Graham: Not too long from now it will be pretty much impossible to buy a new car which isn't connected to the internet in some fashion.

  Many modern purchasers are more swayed by the gadgety bells and whistles their car includes than its performance, and with in a world where everything seems to have to have an associated smartphone app, why should vehicles be any different?

  If most new cars are going to be internet-enabled then you know what that means? Yup, second hand cars are going to be increasingly "smart" as well as vehicles are sold on after a few years.

  Oh, and yes, as I'm writing on We Live Security it should go without saying that it also means security threats.

  This point was brought home last week at the RSA Conference in San Francisco, where IBM's Charles Henderson described how – over two years after he had traded it back in to the original authorised dealer – he was still able to access his old car via a smartphone app.

  Despite deauthorising all associated accounts, satellite radio and garage door openers, resetting the Bluetooth, as well as surrendering all the keys at the time of sale, Henderson discovered that his mobile app never forgot his old car.

  The app allowed Henderson to track the geolocation of the car, adjust its climate control, send its SatNav systems new directions and even trigger its horn.

  But perhaps most alarmingly of all, the app also gave Henderson the ability to remotely unlock the vehicle.

  Fortunately the IBM researcher isn't one of the bad guys. But it is easy to imagine how a car thief or stalker would exploit such a feature.

  As Henderson explained to CNN, the new car's owners would have no clue that they were potentially at risk:

  > "The car is really smart, but it's not smart enough to know who its owner is, so it's not smart enough to know it's been resold. There's nothing on the dashboard that tells you 'the following people have access to the car.'"

  It turns out that although Henderson took more effort than probably most people in ensuring that he had wiped the car's knowledge of him and associated accounts before trading it in, that wasn't enough.

  As the researcher explains, that's because a full factory reset of the unnamed vehicle does not revoke access by the smartphone app – the information still lurks in the cloud, and can only be wiped by a factory-authorised dealer.

One has to wonder how often that occurs. Henderson's own investigation discovered four major vehicle manufacturers were allowing previous owners to access cars from a mobile app.

This is the Internet of (insecure) Things at work again folks. In the rush to add "bells and whistles" features are not being properly thought through, and security is not uppermost in manufacturers' minds.

Until more effort is made by vendors to integrate the internet in a safe way into the myriad of devices that surround us, we are going to hear more and more stories of security breaking down like this.

Chrome 56 upate has hidden our connection certificate info

- "Domain"
  "Your connection to this site is private. Details"

- https://www.howtogeek.com/292076/how-do-you-view-ssl-certificate-details-in-google-chrome/

- You can find this information by going to the Three Dots Menu -> More Tools -> Developer Tools, then click on the Security Tab. This will give you a Security Overview with a View Certificate Button.

- Windows users can press Ctrl-Shift-I to view cert.
  - This is a shortcut to the same place.

The Future of Firefox Add-Ons

- https://www.bleepingcomputer.com/news/software/the-future-of-firefox-add-ons/

- Over the coming year, Firefox will be putting the finishing touches on a plan it set in motion in 2015, which was to replace the aging Add-ons API with a new system called WebExtensions, based on the same extensions API used by Chromium browsers such as Chrome, Vivaldi, Opera, and others.

  After launching limited support for WebExtensions in August 2016 with the release of Firefox 48, Mozilla has slowly added new features in following releases, moving forward for full WebExtensions support.

  Here are Mozilla's publicly stated plans for Firefox's handling of add-ons in 2017 and beyond, along with how multi-process support will also factor into consideration. We are currently at Firefox 51.

- Firefox 53
    - Set for release on April 18, this release marks an important point in the Firefox timeline.
    - No new legacy add-ons will be accepted on addons.mozilla.org (AMO)
    - Developers and users will be able to update legacy add-ons
    - Firefox will run with multi-process support for most users
    - Firefox add-ons confirmed as multi-process incompatible will be disabled in Firefox
    - Firefox will fall back to single-process if the user uses a multi-process incompatible add-on

    - Legacy add-ons = Firefox add-ons built on the old Add-ons API, XUL overlay extensions, bootstrapped extensions, SDK extensions, and Embedded WebExtensions.

- Firefox 54-55-56
    - Firefox will expand its sandbox security feature to include multi-process support.

- Set for Firefox 54.
    - Firefox will expand multi-process support from two processes to three and more.

- Set for Firefox 55.
    - Some legacy add-ons will stop working due to the two changes above.

- Firefox 57
    - Set for release on November 14, this is the end of the line for old Firefox add-ons. If developers don't migrate their code from the old Add-ons API to the new WebExtensions API by then, their add-ons will stop working for good.

        - Firefox will run only add-ons built on the new WebExtensions API
        - addons.mozilla.org (AMO) will continue to list legacy add-ons
        - No timeline has been provided for when addons.mozilla.org (AMO) will stop listing legacy add-ons

    - According to Mozilla, the reason old legacy add-ons will stop working in Firefox 57 is because they plan to remove a workaround that allowed non-multi-process code to run on the new Firefox engine.

    - Removing the workaround means no code will run in Firefox if it hasn't been optimized for multi-process support. This automatically means all legacy add-ons.

- A bumpy road ahead
    - WebExtensions and multi-process support are two important updates through which the Mozilla Foundation plans to speed up Firefox and reduce browser crashes.

      The downside to these two new technologies is that it will kill Firefox's main feature, it's huge add-ons repository.

      Already, some old and prolific Firefox add-on developers have said they don't plan

to migrate their code to the new WebExtensions API.

The upside to WebExtensions is that users will be able to install Chrome extensions in Firefox when Mozilla finishes implementing the WebExtensions API.

Nevertheless, existing Firefox add-ons have more customization power over Firefox than what Chrome and Firefox allow the new WebExtensions API, meaning the new add-ons won't be their own fully-contained apps, but more like scripts that work with what the browser allows them to. A large number of users have voiced their displeasure regarding the new WebExtensions API, with many vowing to move to Firefox ESR or Pale Moon distributions.

The Lock Screen of Win10 & 8.1 Leaks Clipboard Contents... and Microsoft doesn't care.

- https://hexatomium.github.io/2017/02/15/windows10-clipboard-lockscreen/
- Earlier this year, Norwegian MVP Oddvar Moe made a rather shocking discovery that went mostly under the radar. He found that on Windows 10, there is a way to easily read clipboard contents from the screen of a locked machine without requiring any form of authentication.

  In any enterprise environment any coworker could easily go through a few PCs at lunch time, harvesting potentially juicy information (such as passwords) without leaving any traces.

  The frighteningly simple PoC goes as follows:
  - 1. Win+L: Lock workstation
  - 2. Win+ENTER: Start Narrator
  - 3. CapsLock+F1: Open Narrator Help
  - 4. Ctrl+V: to paste the clipboard into the narrator

- This can also be achieved through the WiFi selector UI on the lock screen.

- The issue affects all editions of Win10 & 8.1.

- According to Oddvar, Microsoft does not consider this to be a security issue as it requires physical access.

- Possible mitigations include disabling these features through the appropriate Group Policy settings, or using ClipTTL, which is a small utility written by Firas Salem to protect against this and other cases of accidental clipboard pasting.

- ClipTTL is an automatic clipboard wiper to prevent accidental or malicious "pastes".
  - By Brussels, Belgium-based Security Consultant "Firas Salem"
  - https://www.trustprobe.com/fs1/apps.html
  - https://www.trustprobe.com/fs1/dl_rcc.php?appname=ClipTTL.exe
  - He also wrote the "RCC" for finding potentially rogue certificates in Windows and Firefox.

Project Zero's 90-day time-limit expired on a worrisome Windows flaw:

- https://bugs.chromium.org/p/project-zero/issues/detail?id=992
- Windows gdi32.dll heap-based out-of-bounds reads / memory disclosure in EMR_SETDIBITSTODEVICE and possibly other records.
- Reported to Microsoft on 2016-Nov-16.
- Deadline: Exceeded last Tuesday, February 14th, 2017. (90 days)
- All details, including a PoC went public on schedule.
- SetDIBitsToDevice
- EMF - Enhanced Metafile
- The proof-of-concept file attached here consists of a single EMR_SETDIBITSTODEVICE record (excluding the header/EOF records), which originally contained a 1x1 bitmap. The dimensions of the DIB were then manually altered to 16x16, without adding any more actual image data. As a consequence, the 16x16/24bpp bitmap is now described by just 4 bytes, which is good for only a single pixel. The remaining 255 pixels are drawn based on junk heap data, which may include sensitive information, such as private user data or information about the virtual address space. I have confirmed that the vulnerability reproduces both locally in Internet Explorer, and remotely in Office Online, via a .docx document containing the specially crafted EMF file.

Project Zero: Attacking the Windows NVIDIA Driver

- https://googleprojectzero.blogspot.com/2017/02/attacking-windows-nvidia-driver.html
- Posted by Oliver Chang:
  Modern graphic drivers are complicated and provide a large promising attack surface for EoP (elevation of privilege) execution opportunities and sandbox escapes from processes that have access to the GPU (e.g. the Chrome GPU process). In this blog post we'll take a look at attacking the NVIDIA kernel mode Windows drivers, and a few of the bugs that I found. I did this research as part of a 20% project with Project Zero, during which a total of 16 vulnerabilities were discovered.

- NVIDIA's response
  The nature of the bugs found showed that NVIDIA has a lot of work to do. Their drivers contained a lot of code which probably shouldn't be in the kernel, and most of the bugs discovered were very basic mistakes. One of their drivers (NvStreamKms.sys) also lacks very basic mitigations (stack cookies) even today.

  However, their response was mostly quick and positive. Most bugs were fixed well under the deadline, and it seems that they've been finding some bugs on their own internally. They also indicated that they've been working on re-architecturing their kernel drivers for security, but weren't ready to share any concrete details.

- Conclusion
  Given the large attack surface exposed by graphics drivers in the kernel and the generally lower quality of third party code, it appears to be a very rich target for finding sandbox escapes and elevation of privilege vulnerabilities. GPU vendors should try to limit this by moving as much attack surface as they can out of the kernel.

"A Graduate Course in Applied Cryptography"

- http://toc.cryptobook.us/
- https://crypto.stanford.edu/~dabo/cryptobook/draft_0_3.pdf
- 580 page tour de force.
- One of the co-authors, Victor Shoup, modestly describes it as: "A preliminary/partial draft of a textbook on cryptography that I am writing with Dan Boneh."
- Dan Boneh
    - Professor of Computer Science and Electrical Engineering, Stanford University.
    - Co-director of the Stanford Computer Security Lab
- Victor Shoup
    - New York University

- From the Preface:
  Cryptography is an indispensable tool used to protect information in computing systems. It is used everywhere and by billions of people worldwide on a daily basis. It is used to protect data at rest and data in motion. Cryptographic systems are an integral part of standard protocols, most notably the Transport Layer Security (TLS) protocol, making it relatively easy to incorporate strong encryption into a wide range of applications.

  While extremely useful, cryptography is also highly brittle. The most secure cryptographic system can be rendered completely insecure by a single specification or programming error. No amount of unit testing will uncover a security vulnerability in a cryptosystem.

  Instead, to argue that a cryptosystem is secure, we rely on mathematical modeling and proofs to show that a particular system satisfies the security properties attributed to it. We often need to introduce certain plausible assumptions to push our security arguments through.

  This book is about exactly that: constructing practical cryptosystems for which we can argue security under plausible assumptions. The book covers many constructions for di.erent tasks in cryptography. For each task we define a precise security goal that we aim to achieve and then present constructions that achieve the required goal. To analyze the constructions, we develop a unified framework for doing cryptographic proofs. A reader who masters this framework will be capable of applying it to new constructions that may not be covered in the book.

  Throughout the book we present many case studies to survey how deployed systems operate. We describe common mistakes to avoid as well as attacks on real-world systems that illustrate the importance of rigor in cryptography. We end every chapter with a fun application that applies the ideas in the chapter in some unexpected way.

- Intended audience and how to use this book

  The book is intended to be self contained. Some supplementary material covering basic facts from probability theory and algebra is provided in the appendices.

  The book is divided into three parts. The first part develops symmetric encryption which explains how two parties, Alice and Bob, can securely exchange information when they

have a shared key unknown to the attacker. The second part develops the concepts of public-key encryption and digital signatures, which allow Alice and Bob to do the same, but without having a shared, secret key. The third part is about cryptographic protocols, such as protocols for user identification, key exchange, and secure computation.

A beginning reader can read though the book to learn how cryptographic systems work and why they are secure. Every security theorem in the book is followed by a proof idea that explains at a high level why the scheme is secure. On a first read one can skip over the detailed proofs without losing continuity. A beginning reader may also skip over the mathematical details sections that explore nuances of certain definitions.

An advanced reader may enjoy reading the detailed proofs to learn how to do proofs in cryptography. At the end of every chapter you will find many exercises that explore additional aspects of the material covered in the chapter. Some exercises rehearse what was learned, but many exercises expand on the material and discuss topics not covered in the chapter.

pfSense and Ubiquity Follow-Ups

- Dan Moutal (@scruffydan) / 2/14/17, 8:19 PM
  @SGgrc Listening to this week's Security Now and the Edgerouter also allows you to restrict UPNP by IP address (need to use the CLI though). Need to use the CLI and the upnp2 service to create the upnp ACL

- @SGgrc what was the name of the new pfSense box that you mentioned on SN599?
- I don't think you mentioned the name, just that it had 2 ports.
  - SG-1000
  - https://netgate.com/products/sg-1000.html
  - $149
  - Unknown bulk throughput -- will it run at full line rate?

- SGgrc Hi Steve. I'm listening to SN599. You can use the Ubiquity Edgerouter X with the small pfsense box for network segmentation

Other Follow-Ups

- miniLock.io

- miniLock is currently audited, peer-reviewed software. An initial public release is available for Google Chrome and Chrome OS.

- Originated by Nadim Kobeissi, the PhD at the INRIA Paris Prosecco Lab who first brought us CryptoCat.

- Easy to use
  miniLock uses your email and secret passphrase to generate a miniLock ID. miniLock IDs are small and easy to share online — anyone can use your ID to encrypt files to you, and you can encrypt files to friends using their miniLock IDs.

- (In other words, as Leo was promoting last week... public key crypto.)

- Modern
  Enter your miniLock passphrase on any computer, and you'll get access to your miniLock ID. No key storage or management — just a single passphrase to access your miniLock identity anywhere.

- miniLock uses modern cryptographic primitives to accomplish this securely.

- Widely implemented, independently verified
  miniLock is audited, peer-reviewed software. It's developed by experts, using proven cryptographic standards and under the scrutiny of the open source cryptography community. miniLock also benefits from a strong community that has contributed formal verification as well as third-party implementations in Go, ECMAScript, Python, Java and C#, in addition to the original implementation in JavaScript.

- https://github.com/kaepora/miniLock

- User Flow:
  Alice wants to send a scan of her passport to Bob. Sending it over email would compromise personal information, so Alice decided to first encrypt the scan using miniLock.

  Bob opens miniLock and enters his email address and passphrase. miniLock displays his miniLock ID, which is tied to his passphrase and is persistent. He sends Alice his miniLock ID, which looks something like: quBSaJLXKsRiaSrhgkPnswKocth711H29ZamMi1H9j4Mb

  Alice drags and drops her passport scan into miniLock and enters Bob's miniLock ID as the recipient. She clicks the encrypt button and sends the resulting .minilock file to Bob. Once Bob drags the encrypted file into miniLock, it automatically detects it as a miniLock-encrypted file destined to Bob, and decrypts and saves the passport scan on his computer.

Links to last week's HTTPS INsecurity research

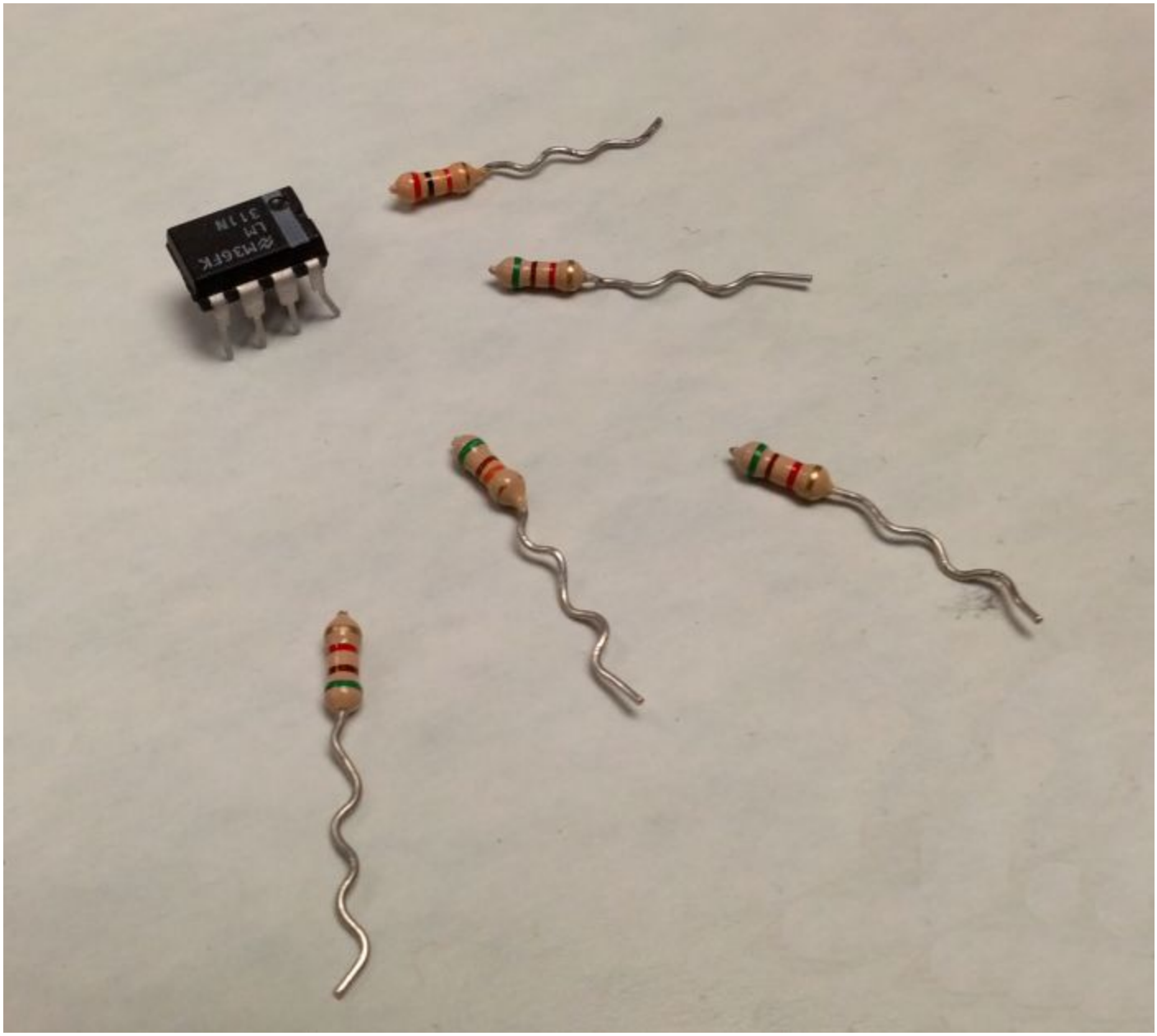
- https://media.grc.com/misc/HTTPS-Interception.pdf

On the Lighter Side

Riddle:

- Q: Why are Assembly programmers always wet?
- A: They work below C level.

And THAT'S how computers are made...



http://imgur.com/gallery/qleuW

SpinRite

Bob McKinstry in St. Louis, MO

Hey Steve:

I'm a listener of Security Now since year 1 and a SpinRite owner. A few days ago, one of the residents in our training program asked how he could get help with his Dell laptop as our IT department doesn't support machines they don't own.

The story is classic: After a power outage his laptop would not boot into Windows. It would blue screen, reboot, rinse and repeat.
Without hesitation, I told him about SpinRite. I lent him my trusty SpinRite CD (told him he'd have to purchase SpinRite if it did fix his machine). I told him he had to be patient and let the program do its work. He fired up SpinRite and went to bed. When he woke up in the morning, he was good to go. Just like that.

SpinRite is a great product. Another drive saved. Another happy customer. Thanks for all that you do with GRC and thanks for all the great podcasts that you've done with Leo on the TWIT network.

The MMU Side-Channel Attack

Press Coverage:

- A Chip Flaw Strips Away a Key Hacking Safeguard for Millions of Device
  https://www.wired.com/2017/02/flaw-millions-chips-strips-away-key-hacking-defense-software-cant-fully-fix/
  Uh, no. It has nothing to do with a "Chip Flaw" -- these guys have figured out how to very cleverly leverage a fundamental operational characteristic of all modern processor architectures to penetrate the randomization of all Address Space Layout Randomization.

- New ASLR-busting JavaScript is about to make drive-by exploits much nastier
  https://arstechnica.com/security/2017/02/new-aslr-busting-javascript-is-about-to-make-drive-by-exploits-much-nastier
  Uh, no. It doesn't make them nastier, it makes them significantly more possible and likely.

- JavaScript Attack Breaks ASLR on 22 CPU Architectures
  https://www.bleepingcomputer.com/news/security/javascript-attack-breaks-aslr-on-22-cpu-architectures/
  Uh, no. It breaks on ALL contemporary CPU architectures.

- A Simple JavaScript Exploit Bypasses ASLR Protection On 22 CPU Architectures
  http://thehackernews.com/2017/02/bypass-aslr-browser-javascript.html
  There's nothing whatsoever simple about it!

Who these guys and why should we believe them? Their previous work:

- Flip Feng Shui - #576
  https://www.vusec.net/projects/flip-feng-shui/
  Flip Feng Shui (FFS) is a new exploitation vector that allows an attacker virtual machine (VM) to flip a bit in a memory page of a victim VM that runs on the same host as the attacker VM. FFS relies on a hardware vulnerability for flipping a bit and a physical memory massaging primitive to land a victim page on vulnerable physical memory location.

- Drammer - #583
  https://www.vusec.net/projects/drammer/
  Drammer is a new attack that exploits the Rowhammer hardware vulnerability on Android devices. It allows attackers to take control over your mobile device by hiding it in a malicious app that requires no permissions. Practically all devices are possibly vulnerable and must wait for a fix from Google in order to be patched. Drammer has the potential to put millions of users at risk, especially when combined with existing attack vectors like Stagefright

AnC - VUSec

- https://www.vusec.net/projects/anc/
- ASLR on the Line: Practical Cache Attacks on the MMU
  - https://www.vusec.net/download/?t=papers/anc_ndss17.pdf
- Reverse Engineering Hardware Page Table Caches Using Side-Channel Attacks on the MMU
  - https://www.vusec.net/download/?t=papers/revanc_ir-cs-77.pdf

What is ASLR?

- DEP - data execution prevention - prevents data from being executed.
- If malware knows where userland OS code is located, it can use ROP (return-oriented programming) to execute snippets of existing OS code at the ends of existing subroutines to get its work done.
- ASLR eliminates the absolute positioning of code so that malware won't/can't know where those existing bits of code are located.
- But some API's have been found to leak their own addresses. -- Whoops.

MMU: Modern Memory Management Units.

- Virtual vs Physical addresses
- 64-bit virtual address space.
  - 48 bits are used.
    - 36 (4 x 9)
    - 12 bits - 4K page tables.
- TLB - Translation Lookaside Buffer
- Hidden cycles used to fetch page table entries.
  - Caching the page tables is the only way to do this quickly
- The memory management MUST be OS-secret.

Modern processor caches:

- L1, L2 and L3 caching
- L1I & L1D - small and fast - per core
- L2 - larger - per core
- L3 - much larger, slower, and shared among all cores.

The Critical Error made by ALL modern processors

- Cache Sharing: Using the same cache for the MMU's page tables as the program's data.

- As a consequence, the recent history of memory address de-virtualization will be present in the program's shared data cache.

- So, for example, an access to the program's local dynamic storage allocation heap, which is not already present in the TLB, will force a processor lookup of the virtual to physical address mapping by reading the page tables which MUST BE KEPT SECRET. But immediately afterward those page table entries will be in the program's shared data cache.

Cached or Uncached? The challenge of timing in a browser's JavaScript

- Chrome and Firefox have deliberately reduced the resolution of the JavaScript accessible timestamp to 5us.

- The RDTSC instruction is a clock-cycle-counter, so insanely granular.
    - (SQRL's Entropy Harvester uses the RDTSC as a source of unknownable data.)

- If you only have a 5us 'tick' what can you do?
    - If the 5us tick is uniform, you wait for one tick, perform the operation, then time until the next tick.

- If you have WebWorkers with shared memory, you use another thread to spin a counter to create a high resolution elapsed timer.