CHRIS BEARD, SYSADMIN EDMS

MELTDOWN AND SPECTRE: STAYING SAFE

WHAT ARE MELTDOWN AND SPECTRE?

- Security issues requiring malicious code to be run locally.
- This code abuses **speculative execution**, a performance feature common to most CPUs since 1995.
- Exploits allow less-privileged processes to access privileged information.
- Mac, iOS and tvOS devices affected. WatchOS is not affected.
- Apple: “No known exploits currently impacting customers.”

https://support.apple.com/en-us/HT208394 - 'About speculative execution vulnerabilities in ARM-based and Intel CPUs’

MORE ON MELTDOWN

- CVE-2017-5754 or "rogue data cache load."
- Named because it "melts" security boundaries, breaking memory isolation.
- Enables a user process to read kernel memory.
- Intel chips definitely affected. AMD/ARM unlikely.
- Has most potential of the two to be exploited. Easiest attack vector would be a malicious app.

References:
https://support.apple.com/en-us/HT208394 - 'About speculative execution vulnerabilities in ARM-based and Intel CPUs'

MORE ON SPECTRE

- "Speculative execution side-channel attack”
- CVE-2017-5753 or "bounds check bypass,"
- CVE-2017-5715 or "branch target injection”
- “These techniques potentially make items in kernel memory available to user processes by taking advantage of a delay in the time it may take the CPU to check the validity of a memory access call.”
- Remote attacks could potentially come via Javascript in a web browser.

References:
https://support.apple.com/en-us/HT208394 - 'About speculative execution vulnerabilities in ARM-based and Intel CPUs’

FULL TECHNICAL INFO

- Google Project Zero blog
  - https://googleprojectzero.blogspot.co.uk/2018/01/reading-privileged-memory-with-side.html
- Carnegie Mellon University CERT (Computer Emergency Readiness Team)
  - https://www.kb.cert.org/vuls/id/584653
- Slack post 'Spectre & Meltdown Vulnerabilities Summary'
  - Useful links for securing other OSs
  - https://slack-files.com/T04QVKUQG-F8NB2PNTX-9eaf19c4a1

WHAT CAN BE DONE TO PROTECT YOUR ESTATE?

- CERT's initial recommendation was:
- “replace CPU with an unaffected alternative”.
  - https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=584653&SearchOrder=4
- As updates have been released this has been refined to "Apply updates, then Consider CPU options".

WHAT APPLE UPDATES ARE AVAILABLE?

- Apple Support article 'About speculative execution vulnerabilities in ARM-based and Intel CPUs'
  - https://support.apple.com/en-us/HT208394

OS UPDATES TO "HELP DEFEND" AGAINST MELTDOWN

- Released 17/12/2017
- macOS High Sierra 10.13.2
  - NOT macOS Sierra 10.12 or OS X El Capitan 10.11, as previously stated in Apple post.
- iOS 11.2
- tvOS 11.2

References:
https://support.apple.com/en-us/HT208394 - 'About speculative execution vulnerabilities in ARM-based and Intel CPUs'

SAFARI & WEBKIT UPDATES TO "HELP DEFEND" AGAINST SPECTRE

- macOS 10.13.2 Supplemental Update
  - Resulting Safari version: 11.0.2 - build 13604.4.7.1.6 or 13604.4.7.10.6
- macOS 10.12
  - Safari version 11.0.2 - 12604.4.7.1.6
- OS X 10.11
  - Safari version as for macOS 10.12
- iOS 11.2.2

References:
https://support.apple.com/en-us/HT208394 - 'About speculative execution vulnerabilities in ARM-based and Intel CPUs'

WILL IT MAKE MY DEVICE SLOWER?

- Apple’s Meltdown mitigations…
  - "Our testing with public benchmarks has shown that the changes in the December 2017 updates resulted in no measurable reduction in the performance of macOS and iOS as measured by the GeekBench 4 benchmark, or in common Web browsing benchmarks such as Speedometer, JetStream, and ARES-6.”
- Apple’s Spectre mitigations…
  - "Our current testing indicates that the Safari mitigations have no measurable impact on the Speedometer and ARES-6 tests and an impact of less than 2.5% on the JetStream benchmark. We continue to develop and test further mitigations within the operating system for the Spectre techniques, and will release them in upcoming updates of iOS, macOS, and tvOS."

References:
https://support.apple.com/en-us/HT208394 - Apple briefing 'About speculative execution vulnerabilities in ARM-based and Intel CPUs'

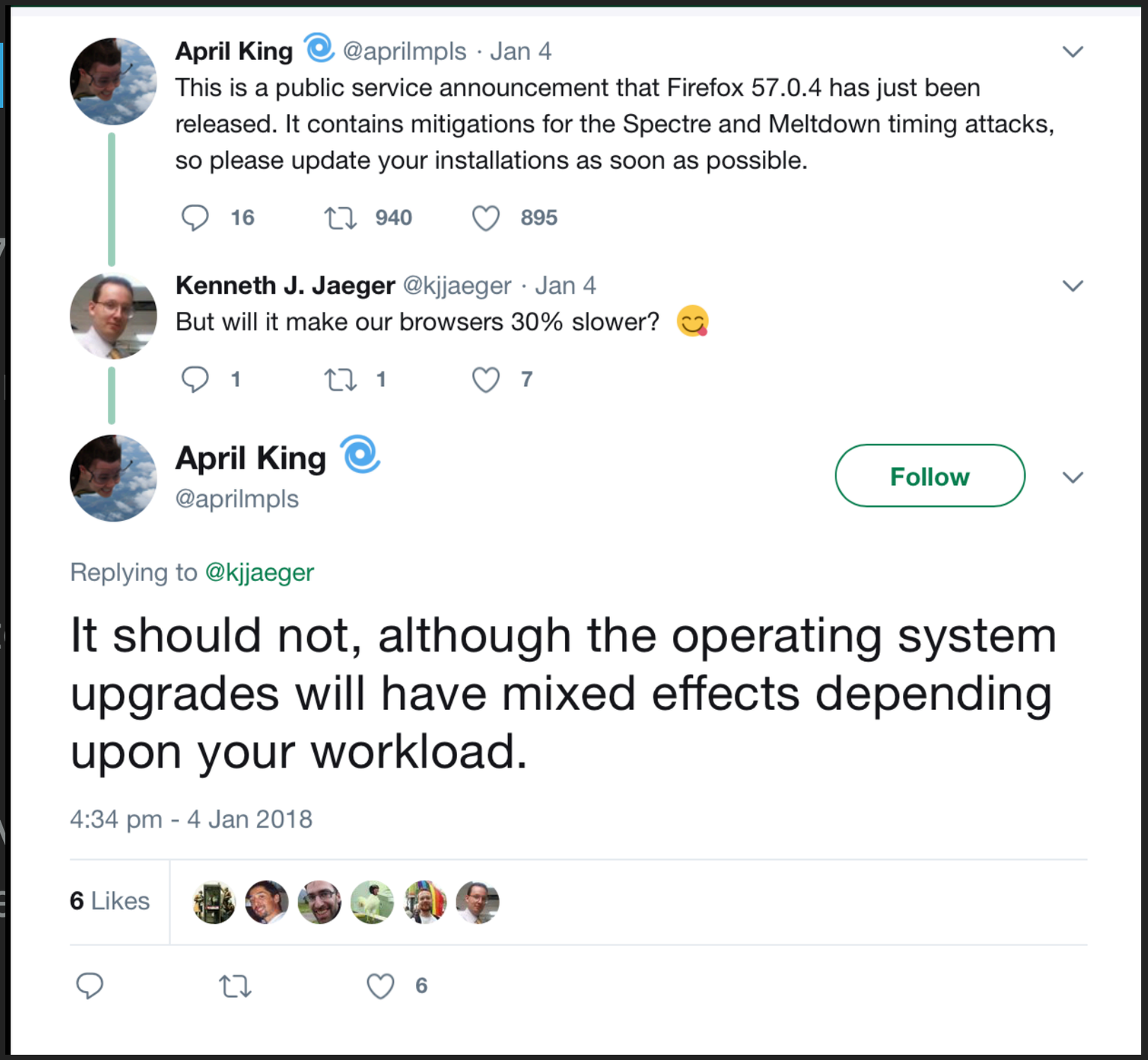
SPECTRE MITIGATIONS FOR OTHER BROWSERS:

- Firefox v57.0.4
  - Various mitigations
- Chrome
  - v63 - Site Isolation: 10-20% increase in memory usage
  - v64 - JavaScript engine mitigations: Extra resource use down to 10% max

References:
https://support.google.com/faqs/answer/7622138#chrome

SPECTRE MI

- Firefox v57
  - Various
- Chrome
  - v63 - Sit usage
  - v64 - Jav resource



References:
https://support.google.com/faqs/answer/7622138#chrome

SPECTRE MITIGATIONS FOR OTHER BROWSERS:

- Firefox v57
  - Various r
- Chrome
  - v63 - Site usage
  - v64 - Jav resource

Google Chrome Browser

Current stable versions of Chrome include an optional feature called Site Isolation which can be enabled to provide mitigation by isolating websites into separate address spaces. Learn more about Site Isolation and how to take action to enable it.

Chrome 64, due to be released on January 23, will contain mitigations to protect against exploitation.

Additional mitigations are planned for future versions of Chrome. Learn more about Chrome's response.

Desktop (all platforms), Chrome 63:

- Full Site Isolation can be turned on by enabling a flag found at chrome://flags/#enable-site-per-process.
- Enterprise policies are available to turn on Site Isolation for all sites, or just those in a specified list. Learn more about Site Isolation by policy.

Android:

- Site Isolation is available in chrome://flags but may have additional functionality and performance issues.

iOS:

- Chrome on iOS uses Apple's WKWebView, so JS compilation mitigations are inherited from Apple.

References:
https://support.google.com/faqs/answer/7622138#chrome

HOW CAN YOU KEEP USERS SAFE?

- **1. Promptly install available updates**
  - Apply available patches for their OS version
  - Ideally upgrade to latest OS, as Meltdown is currently only addressed in macOS 10.13

References:
https://support.apple.com/en-us/HT208394 - Apple briefing 'About speculative execution vulnerabilities in ARM-based and Intel CPUs'

HOW CAN YOU KEEP USERS SAFE?

- **2. Avoid installing malware:**
  - Apple advises only installing apps from trusted sources, eg App Store.
  - Enforce ‘Allow apps downloaded from’ setting in System Preferences to ‘App Store only’. Advise admin users not to relax this.
  - Advise Admin users to avoid using right-click > Open to defeat Gatekeeper in order to open an untrusted app.
  - Advise users to not run anything that macOS flags can damage your computer (XProtect part of Gatekeeper).

RESOURCES

- Apple briefing 'About speculative execution vulnerabilities in ARM-based and Intel CPUs’
  - https://support.apple.com/en-us/HT208394
- Carnegie Mellon University CERT (Computer Emergency Readiness Team): Vulnerability Note VU#584653 - CPU hardware vulnerable to side-channel attacks
  - https://www.kb.cert.org/vuls/id/584653
- Slack, MacAdmins: 'Spectre & Meltdown Vulnerabilities Summary' post
  - https://slack-files.com/T04QVKUQG-F8NB2PNTX-9eaf19c4a1
- iMore: ‘Meltdown' and 'Spectre' FAQ: What Mac and iOS users need to know about the Intel, AMD, and ARM flaw
  - https://www.imore.com/meltdown-spectre-faq
- Daniel Miessler, ‘A Simple Explanation of the Differences Between Meltdown and Spectre’
  - https://danielmiessler.com/blog/simple-explanation-difference-meltdown-spectre/

MELTDOWN AND SPECTRE: STAYING SAFE

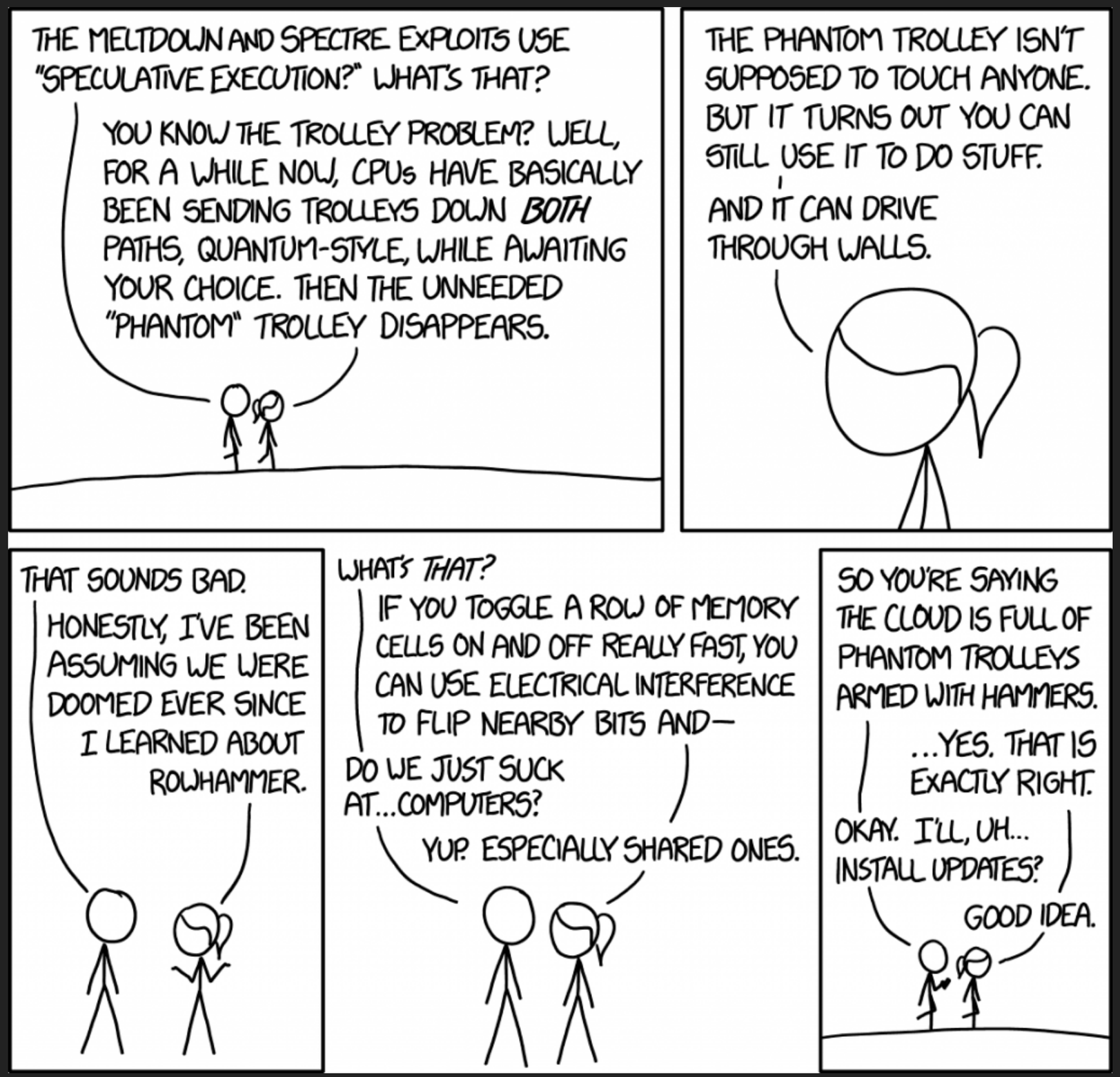


IMAGE CREDIT: XKCD #1938 BY RANDALL MUNROE