Security Now! #507 - 05-12-15

Q&A #212

This week on Security Now!

- James Clapper's lie isn't going away.
- Appeals court rules that sweeping up Americans' data is illegal.
- New malware PoC hides in GPUs.
- Europe's Smart Grid crypto is dumb.
- Interesting noises about the future of UK privacy.
- Worries about SSD on-the-shelf data retention.
- Miscellaneous tidbits.
- Q&A from our listeners.

Best. Captcha. Ever.

Black plays; checkmate in one move

This is a chess CAPTCHA.
Click on the board to make your move, and prove you are human.

Security News!

Clapper just "forgot"

- (Director of National Intelligence) James Clappers attorney: "Jim Clapper wasn't lying when he wrongly told Congress in 2013 that the government does not "wittingly" collect information about millions of Americans... He just forgot.
- http://thehill.com/policy/technology/241508-spy-head-had-absolutely-forgotten-about-nsa-program
- Except that, later, Clapper said: After the fact, Clapper said that his statement was the "least untruthful" possible answer, given the secrecy of the program at the time.
- During a panel discussion last Friday, Robert Litt said that Clapper just didn't have a chance to prepare an answer for Ron Wyden and forgot about the phone records program when asked about it on the spot.
- "We were notified the day before that Sen. Wyden was going to ask this question and the director of national intelligence did not get a chance to review it," Litt said.
- Litt said: "He was hit unaware by the question, and after the hearing I went to him and I said, 'Gee, you were wrong on this.' **And it was perfectly clear that he had absolutely forgotten the existence of the 215 program.**"
- Litt, he said, also erred after the hearing by not sending a letter to the panel to correct the mistake. "I wish we'd done that at the time," he said on Friday.

Top federal court strikes down NSA bulk phone surveillance program! -- Illegal.

- http://rare.us/story/top-federal-court-strikes-down-nsa-phone-surveillance-program/
- http://www.tgdaily.com/mobile/132351-court-rules-nsa-bulk-phone-snooping-illegal
- Last Thursday, United States Court of Appeals for the Second Circuit in New York ruled that the NSA's snooping program that collects Americans' phone records in bulk is illegal.
- The court held that a provision of the USA Patriot Act known as Section 215 cannot be legitimately interpreted to allow the systematic bulk collection of domestic calling records.
- But... That's it.
  - No injunction ordering the NSA to stop.
  - No slap on the wrist.
  - Nothing.
  - All they said was that the program was illegal.
- Next month Congress will be deciding what to do about the 14 year old Patriot Act.

"Jellyfish" GPU-infected Malware, proof-of-concept

- GPU-based rootkit and keylogger offer superior stealth and computing power
  - http://arstechnica.com/security/2015/05/gpu-based-rootkit-and-keylogger-offer-superior-stealth-and-computing-power/
- New Linux rootkit leverages graphics cards for stealth
  - http://www.pcworld.com/article/2920612/new-linux-rootkit-leverages-gpus-for-stealth.html
- https://github.com/x0r1/jellyfish

- Github: Jellyfish is a Linux based userland gpu rootkit proof of concept project utilizing the LD_PRELOAD technique from Jynx (CPU), as well as the OpenCL API developed by Khronos group (GPU). Code currently supports AMD and NVIDIA graphics cards. However, the AMDAPPSDK does support Intel as well.
- Advantages of GPU-stored malware:
  - No GPU malware analysis tools available on web
  - Can snoop on CPU host memory via DMA
    - Note: Normally, inter-process isolation means that only the kernel can see all of the system's memory. Hardware virtual memory paging gives each process its own address space. It's difficult to get into the kernel. But now a user-land process can load code into the GPU... which then has access to the whole machine.
  - GPU can be used for fast/swift mathematical calculations like xor'ing or parsing
- Malicious memory may be retained across warm reboots.

Open Smart Grid Protocol rolled its own (fatally flawed) MAC:

- https://threatpost.com/weak-homegrown-crypto-dooms-open-smart-grid-protocol/112680
- http://www.theregister.co.uk/2015/05/11/smart_grid_security_worse_than_we_thought/
- Three years since inception
- More than four million smart meters now deployed.
- The standard of the European Telecommunications Standards Institute (ETSI).
- Two university researchers in Germany and Portugal published a paper exposing encryption weaknesses in the protocol: "Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol"
- Explains how the authenticated encryption scheme used in the OSGP is open to numerous attacks—the paper posits a handful—that can be pulled off with minimal computational effort.
- Specifically under fire is a homegrown message authentication code called OMA Digest.
- Of the OMA Digest, the researchers wrote: "This function has been found to be extremely weak, and cannot be assumed to provide any authenticity guarantee whatsoever."
- "The weaknesses in the OMA Digest can be used to determine the private key in a very small number of trials."
- Matt Green Tweeted on May 6th: Apparently the smart grid crypto protocols are so broken that researchers have to invent faster attacks… just to challenge themselves.
- So many problems you can pick your attack:
  - One attack needed just 13 queries to an OMA oracle to recover the 96-bit secret key.
  - And another in just four queries and 2^25 time complexity.
  - A different approach only requires one arbitrary valid plaintext-tag pair, and recovers the key in an average of 144 message verification queries.
  - Or one ciphertext-tag pair and 168 ciphertext verification queries.
- The encryption keys are derived from the OMA digest key, and because the encryption key is derived from the key used by OMA digest, the attacks break the confidentiality and authenticity of OSGP.

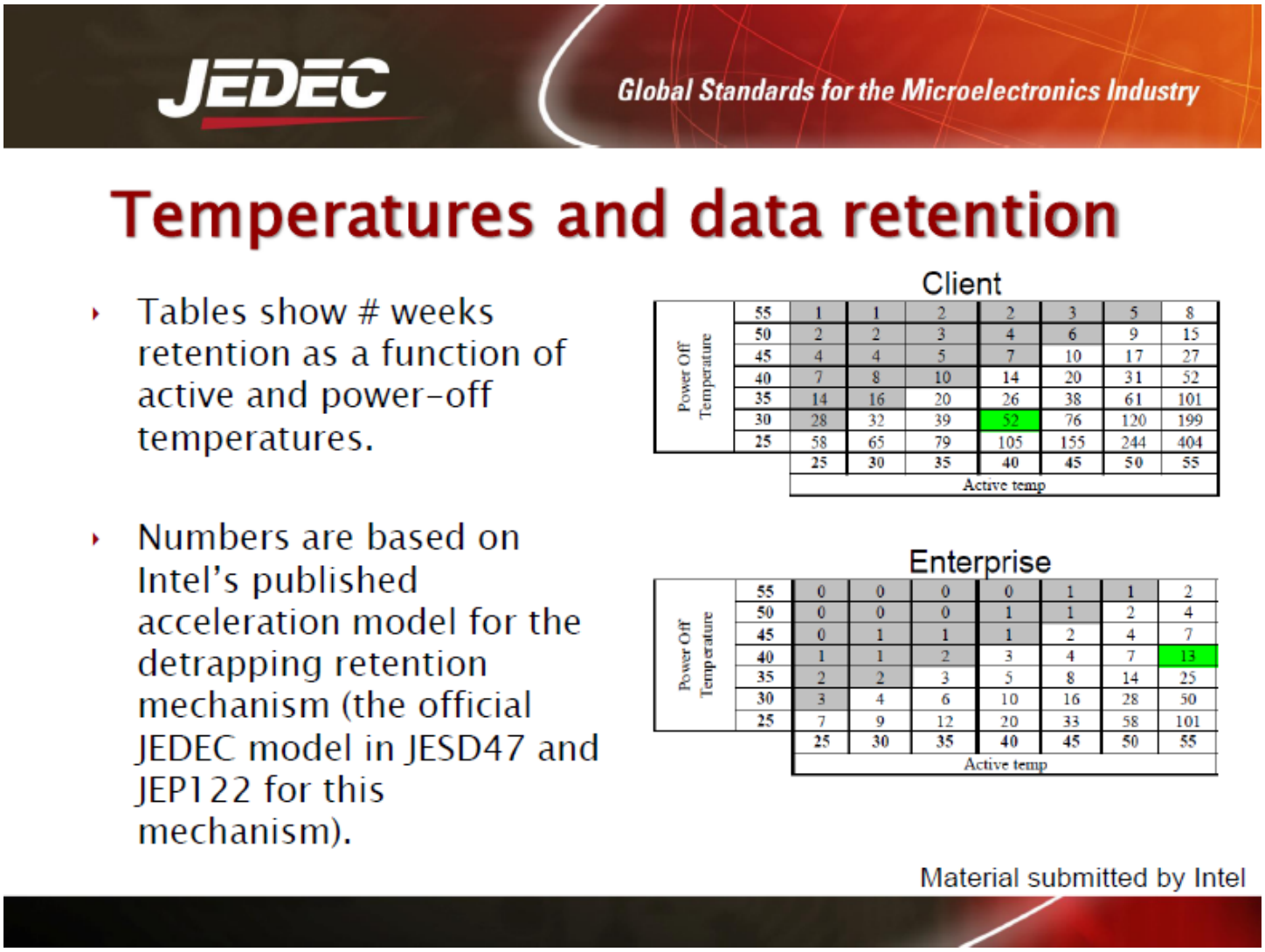
"Snooper's Charter" set to make a return in the UK:

- http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-set-to-return-to-law-as-theresa-may-suggests-conservative-majority-could-lead-to-huge-increase-in-surveillance-powers-10235578.html
- Snoopers' charter set to return to law as Theresa May suggests Conservative majority could lead to huge increase in surveillance powers.
- Previous attempts to introduce huge surveillance powers had been blocked by Liberal Democrat members of the coalition.
- Conservatives are already planning to introduce the huge surveillance powers known as the Snoopers' Charter, hoping that the removal from government of the Liberal Democrats that previously blocked the controversial law will allow it to go through.
- David Cameron has suggested that his party could introduce even more wide-ranging powers if he was re-elected to government. Speaking in January, he said that there should be no form of communication that the government was unable to read — likely causing chaos among the many internet services that rely on encryption to keep users' data safe.

SSD Storage - Ignorance of Technology is No Excuse

- https://blog.korelogic.com/blog/2015/03/24#ssds-evidence-storage-issues
- <quote> A stored SSD, without power, can start to lose data in as little as a single week on the shelf.
- http://www.jedec.org/sites/default/files/Alvin_Cox%20%5BCompatibility%20Mode%5D_0.pdf

Application Class	Workload	Active Use (power on)	Retention Use (power off)	Functional Failure Rqmt (FFR)	UBER
Client	Client	40°C 8 hrs/day	30°C 1 year	≤3%	$\leq 10^{-15}$
Enterprise	Enterprise	55°C 24hrs/day	40°C 3 months	≤3%	$\leq 10^{-16}$



Miscellany:

A note from Dan Rosen, the founder and CTO of VideoRedo:

I found your private eMail address in our database, so I hope you won't mind me using it. Along with the rest of the VideoReDo team, I wanted to say thanks for this week's shout-out. I've been a long-time fan of your show, Leo and the TWIT network in general. It was really a thrill to hear us mentioned in such glowing terms.

If there are any VideoReDo features or enhancements you would like to see, or even just want to discuss video encoding technologies, please let me know.

Although I haven't needed it in quite a while, SpinRite has saved my "bacon" a number of times, so thanks for that as well.

Daniel Burstiner in Uniontown, Ohio wonders about downloading from a TiVo:

Okay, Steve, you mentioned Video Redo in context with downloading fro TiVo. How do you download recorded programs from your TiVo? I've been a TiVo user for MANY years and still have not been able to do it reliably. I am also a SpinRite owner from long ago. In fact I just went through my collection of 3.5" floppy disks and tossed ALL of them except my original SpinRite disk, for sentimental reasons.

[Kmttg: http://sourceforge.net/projects/kmttg/]

"Coin"?... No. Now we have "Plastc."
https://www.plastc.com/card
eInk, Touch surface, $155 pre-order, no fees. Includes a card reader.

If programming languages were vehicles
http://crashworks.org/if_programming_languages_were_vehicles/

SpinRite:

Henry Cocozzoli in Livonia, Michigan " <henry.cocozzoli@gmail.com>
Subject: SpinRite does it again
Date: Wed, 06 May 2015 15:08:24 -0000

Hi Steve and Leo,

I had a user come to me on Monday. He had been copying his data from his old machine to his new machine, when the old machine's hard drive failed.

He thought he had a CrashPlan backup. He never enabled it!

First step was to enable CrashPlan on his new system.

Next, I booted up SpinRite and let it run on level 2 on the old system. When it was done, lots of Green Rs, and a few red Us.

Next, I booted off a thumb drive, so I wouldn't stress the disk more. I copied the data to an external drive. Now I could work with the copy.

Because the drive was Encrypted with DDPE (Dell Data Protection | Encryption), I had to decrypt the data to make it readable.

Thank you for the best drive recovery software in the universe.Let me know if you need testers for 6.1.

Screen Savers, Security Now and SpinRite fan. Keep the Netcasts coming.