Security Now! #506 - 05-05-15

Law Enforcement Backdoors

This week on Security Now!

- The "Pixie Dust" failure of WPS
- Disabling RC4
- Mozilla putting on the pressure to phase out HTTP
- Anti-analysis malware aggressively attacks researcher's machines
- A deeper look into the evolution of DDoS.
- A handful of updates and announcements.
- Two very different and well thought out statements about law enforcement backdoors.

"Well, your quantum computer is broken in every way possible simultaneously."

Security News!

"Pixie Dust" offline attack on WPS

- SN #337: "WPS: A Troubled Protocol" Jan 25th, 2012
  - 8-digit PIN printed on the router's label, sometimes on an LCD screen.
  - Often there's a pairing button.
  - You need to know the PIN *or* press the button.
  - "Reaver" was a brute force attack.
  - Devices added a one-minute lockout to prevent brute forcing.

- Dominique Bongard discovered that some WiFi APs have weak ways of generating the 128-bit E-S1 and E-S2 nonces... that MUST be unpredictable.
- If an attacker can determine their values, the WPS PIN is easily determined.
- "Enrollee nonce" is a public shared value.
- E-Hash1 = HMAC<sha-256> (E-S1, PSK1, PKE, PKR)
- E-Hash2 = HMAC<sha-256> (E-S2, PSK2, PKE, PKR)

- Ralink APs:
  - E-S1 = E-S2 = 0
- Broadcom/eCos devices:
  - The two "secret" E-S1 and E-S2 nonces are generated immediately after the enrollee nonce. And we know the function that gives us this data (Linear Congruential PRNG with *NO* external entropy). So if we substitute in seeds, we will find matching nonces, and from there we can find the E-S1 and E-S2 nonces.
- In Realtek:
  - The PRNG directly uses the time in seconds from January 30th, 1970 until the generation of the data.
  - The chip uses the same generator to make the Enrollee nonce as it does to make E-S1 and E-S2.
  - If the entire exchange occurs within that same second, E-S1 = E-S2 = Enrollee Nonce.
  - If it occurs over the course of a few seconds, all we have to do is find the seed that gave us the Enrollee Nonce, and then increment it and taking the output as E-S1 and E-S2.

RC4 was disabled in FFv36 (we're now at 37.0.2)

- RC4 is now considered insecure and all UI indicators will react as such.
- SSLv3 has been disabled by default in Firefox 34, but the UI has been changed to help the user better understand what's happening.
- Also, RC4 is no longer offered in the initial handshake of TLS.

Last Thursday (4/30), Mozilla Security Blog:

- https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/
- "Deprecating Non-Secure HTTP"
- Firefox Security Lead Richard Barnes:
  <quote> Today we are announcing our intent to phase out non-secure HTTP.
  After a robust discussion on our community mailing list, Mozilla is committing to focus new development efforts on the secure web, and start removing capabilities from the non-secure web. There are two broad elements of this plan:
  - Setting a date after which all new features will be available only to secure websites
  - Gradually phasing out access to browser features for non-secure websites, especially features that pose risks to users' security and privacy.
- Interesting approach: New features that sites might use would require HTTPS, though without HTTPS older less desirable "workarounds" could still be used. Thus putting pressure on the site from the developer end.

Anti-Analysis Malware:

- A new strain of spyware that logs keystrokes and steals data has a destructive side to it, unleashing wiper capabilities if it detects it's being analyzed and audited.
- Craig Williams of Cisco: "It sounds cliché, but this is really a digital arms race and we're seeing the next evolution of it here. Malware authors are no longer content with detect-and-shut-down. Now, if malware realizes it's being audited, the binary will destroy the system. It's a simple case of attackers trying to dissuade researchers from going after a sample."
- Many anti-analysis features designed to evade analysis:
    - Contains 8000 executable functions that are never used.
    - Writes a byte of data to memory 960 millions times to break sandbox logging. (Would create a 100Gb log file.)
    - Unpacking code:
        - <quote> The unpacking code is monstrous and has many times the complexity of the anti-analysis code. The code contains dozens of functions overlapping with each other and unnecessary jumps added only to increase complexity. The result is a nightmare of a control flow graph with hundreds of nodes."
    - It hashes itself and, if any change is detected, overwrites the user's MBR. If it cannot, it encrypts each file in the user's home folder with a randomly generated key.

Cloudflare Blog: An introduction to JavaScript-based DDoS

- https://blog.cloudflare.com/an-introduction-to-javascript-based-ddos/
- Traditional NTP or DNS reflection attacks
- The new attack vector: JavaScript.
- A malicious page hosts JS which created image tags to induce the browser to request images.
- A shared JS library repository is compromised!
    - jQuery: ~30% of websites using it in 2014.
    - In 2014 jQuery.com's website was compromised.
- Facebook SDK, Google Analytics
- **Introducing "Sub Resource Integrity" -- SRI -- Proposal from the W3C**
    - <script src="https://code.jquery.com/jquery-1.10.2.min.js">
    - <script src="https://code.jquery.com/jquery-1.10.2.min.js" integrity="sha256-C6CB9UYIS9UJeqinPHWTHVqh/E1uhG5Twh+Y5qFQmYg=" crossorigin="anonymous">
    - This is new and not well supported... but Chrome and Firefox have it in the works.
- Repository breaches are typically found and corrected quickly, so attacker need something more.
- The need is to get many browsers to load a malicious script.
- So if you cannot reliably modify the source of the script, intercept it.
- Man In The Middle attacks are TRIVIAL to implement for ANY non-HTTPS site.
    - <<explain that and drive that point home>>
- The solution for MITM attack prevention... is encryption.

Miscellany

YouTube/SGgrc

- First video: testimony edited down.
- Video ReDo. --- editing/cutting/cropping existing MPEG-format streams.
    - "I" - independent frame
    - "P" - uses previous frame data to represent changes from them.
    - "B" - backward ... can look upstream into the future as well as at previous frames.

Hook:

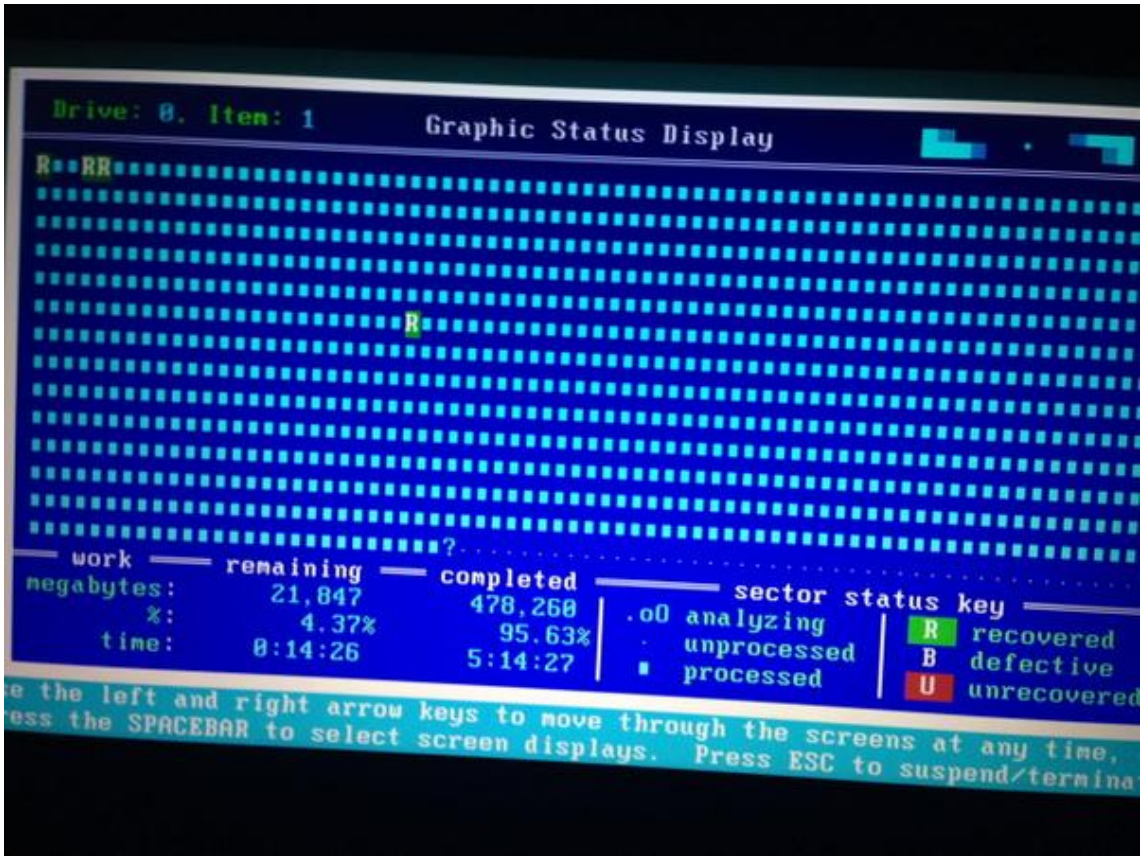
- Kongregate is FLASH
- Hook's author is going in another direction next...

Quote of the week:

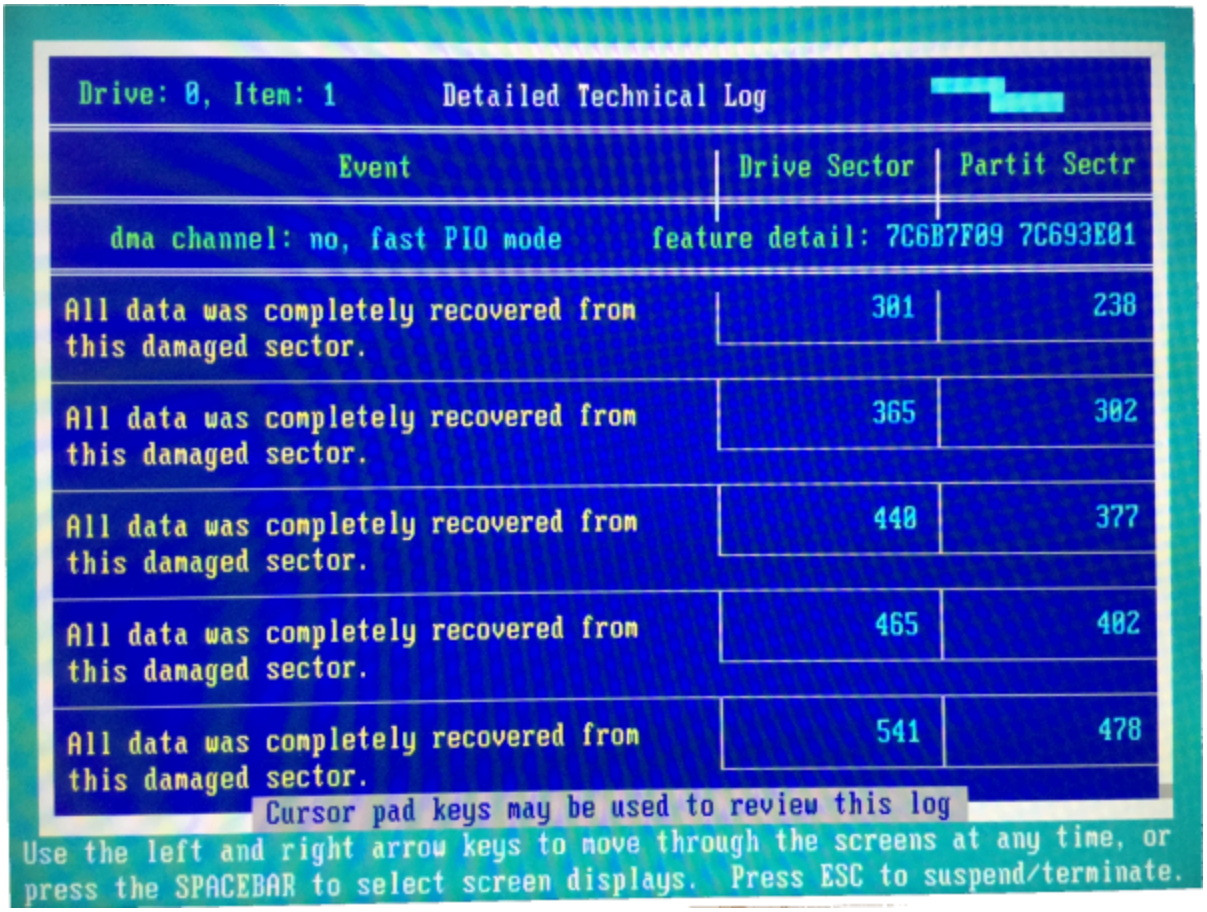
- Gene Hastings (@ehastings)
- @SGgrc You may think that "IoT" means "Internet of Things." But really, it means "Internet of Targets."

SpinRite:

- askapache (@askapache) 4/30/15, 11:05 AM
- @SGgrc Steve SpinRite saved my drive! Even the bios wasn't recognizing it! pic.twitter.com/6SiBv9yfbA



- SpinRite just saved *ME* many days of work...



- A revelation about end-user RAID protection.

Law Enforcement Backdoors

Matt Blaze

- B.S. Computer Science, 1986, City University of New York (Hunter College).
- M.S. Computer Science, 1988, Columbia University
- M.A. Computer Science, 1989, Princeton University.
- Ph.D., Computer Science, 1993. Princeton University.
  (Thesis: Caching in Large-Scale Distributed File Systems)

Jonathan Mayer, Computer Scientist + Lawyer at Stanford

- "You Can't Backdoor a Platform"
- http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform/

Imagine how very creepy it would be if it was actually illegal for an individual to use strong crypto software to encrypt a file they wish to store in the cloud.