

Security Now! #588 - 11-29-16

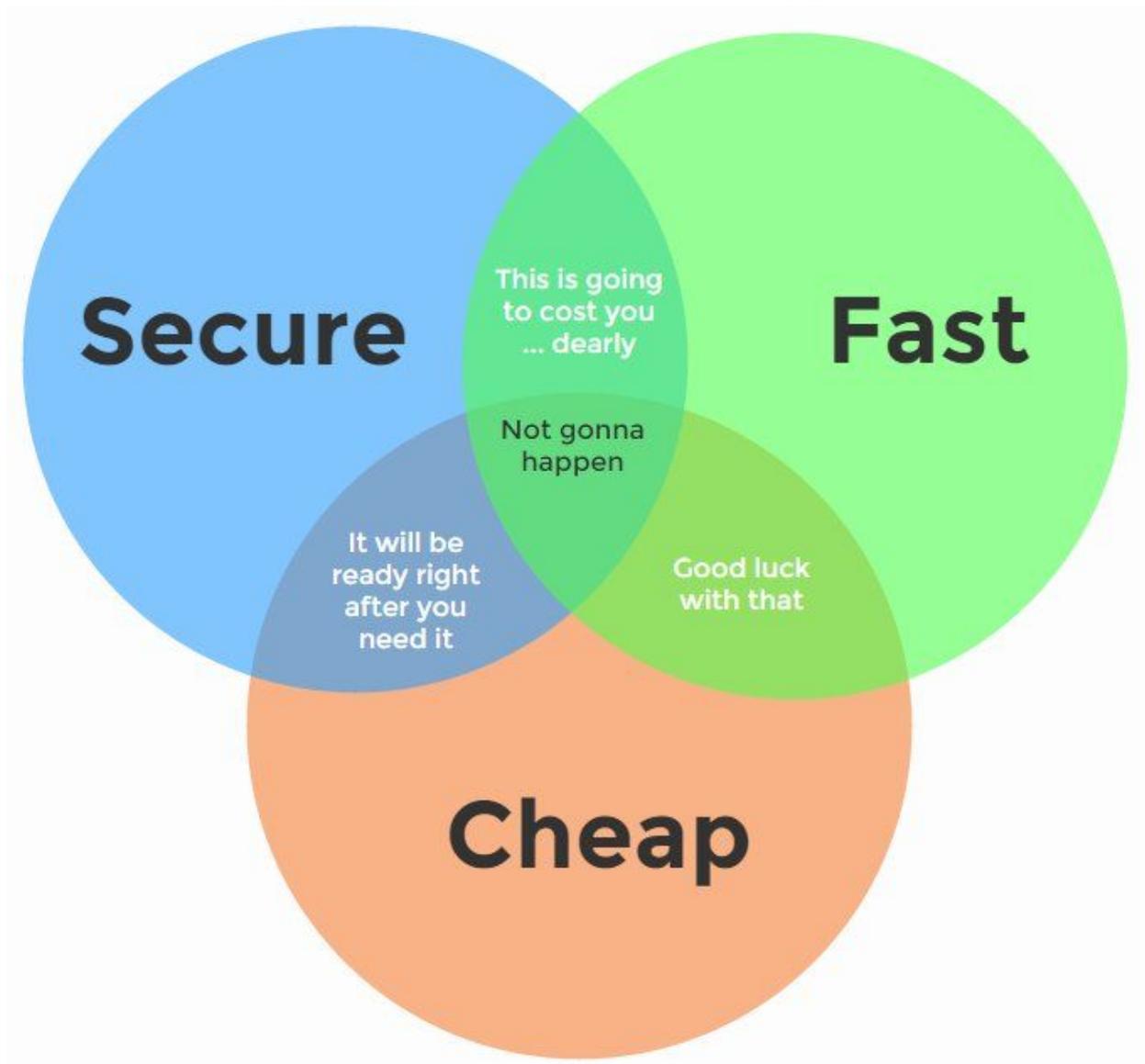
Q&A #243

This week on Security Now!

- A wonderful quote about random numbers, our standard interesting mix of security do's and don't's, new exploits (WordPress dodged a big bullet!), planned changes, tips & tricks, things to patch, a new puzzle/game discovery, some other fun miscellany... and, finally!... ten comments, thoughts and questions from our terrific listeners!

The Week's Wonderful Quote:

- "The generation of random numbers is too important to be left to chance."
- Robert R. Coveyou



Previous Episode Follow-up

From: Avocado Diaboli (Avocado Diaboli)

Hi Steve, thank you for your coverage of the OAuth analysis in SN585. I am friends with two of the paper's authors, and they are very grateful that you presented their work. One of them said about you: "Finally, someone understood our paper! Steve might even have understood it better than some of the paper's peer reviewers." Thanks and keep up the great work! Greetings from Germany, Clemens

Security News

So the screen read: "You Hacked, ALL Data Encrypted."

- That was the message on San Francisco Muni (Municipal) station computer screens across the city, giving passengers free rides all day last Saturday... because the entire fare-processing system was down in a cryptomalware cyberattack which knocked out 2,112 computer systems, citywide.
- The local CBS affiliate reported that their inside sources said the system had been hacked for days and the equivalent of \$73,000 in bitcoin was the stated ransom.
- When reaching at the provided email, the hacker provided a statement in broken English, which read:

"We don't attention to interview and propagate news! Our software working completely automatically and we don't have targeted attack to anywhere! SFMTA network was Very Open and 2000 Server/PC infected by software! So we are waiting for contact any responsible person in SFMTA but I think they don't want deal ! so we close this email tomorrow!"

- The SFMTA (San Francisco Municipal Transit Agency) officially confirmed the hack, but says it has not affected any service and refused to provide details using the excuse of an ongoing investigation. Meanwhile, the city's metro gates were wide open because the entire system is unable to process payment cards, and the ticket kiosks are down too.

An SFMTA spokesman said: "There's no impact to the transit service, but we have opened the fare gates as a precaution to minimize customer impact." (Gotta love that)

- The hack affects employees, as well. According to sources, SFMTA workers are not sure if they will get paid this week. (Happy holidays)
- Cyber attackers also hit Muni's email systems.
- CBS's reporting stated that the transit agency has no idea who is behind it, or what the hackers are demanding in return.... but

- Links to reporting:
 - <http://sanfrancisco.cbslocal.com/2016/11/26/you-hacked-cyber-attackers-crash-muni-computer-system-across-sf/>
 - <http://thehackernews.com/2016/11/transit-system-hacked.html>
 - <http://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni>

Google's SHA-1 death march drumbeat

- <https://security.googleblog.com/2016/11/sha-1-certificates-in-chrome.html>
- Google Blog: SHA-1 Certificates in Chrome / Posted by Andrew Whalley, Chrome Security
We've previously made several announcements about Google Chrome's deprecation plans for SHA-1 certificates. This post provides an update on the final removal of support.

The SHA-1 cryptographic hash algorithm first showed signs of weakness over eleven years ago and recent research points to the imminent possibility of attacks that could directly impact the integrity of the Web PKI. To protect users from such attacks, Chrome will stop trusting certificates that use the SHA-1 algorithm, and visiting a site using such a certificate will result in an interstitial warning.

- **Release schedule**

We are planning to remove support for SHA-1 certificates in Chrome 56, which will be released to the stable channel around the end of January 2017. The removal will follow the Chrome release process, moving from Dev to Beta to Stable; there won't be a date-based change in behavior.

Website operators are urged to check for the use of SHA-1 certificates and immediately contact their CA for a SHA-256 based replacement if any are found.

- (And, oh by the way, the Vogon demolition & construction fleet will be arriving shortly thereafter. However, no one will have cause to complain about either of these events because proper notice of the end of SHA-1 and Earth's pending destruction have both been clearly posted in our offices at Proxima Centauri.)
- Recall that it was exactly one year ago that, with DigiCert's terrific aid, I migrated GRC from SHA-1 to SHA-256 before the stroke of New Years.

"Deseat.me"

- Fortune magazine mentioned it recently.
- <https://www.deseat.me/>

Snooper's Charter Petition (via Simon Zerafa (@SimonZerafa))

- Repeal the new Surveillance laws (Investigatory Powers Act)
- @SGgrc Can I could ask you to retweet / pass on this Petition to UK listeners to repeal the Snoopers Charter: <https://petition.parliament.uk/petitions/173199>
- 136,565 signatures (Parliament considers all petitions that get more than 100,000 signatures for a debate)

ImageGate: Check Point reveals a new method for distributing malware through images.

- <http://blog.checkpoint.com/2016/11/24/imagegate-check-point-uncovers-new-method-distributing-malware-images/>
- Early details are annoyingly scarce, and full disclosure is being withheld until these sites (including Facebook and Linked-In) have fixed their problems. But it appears that executable files are being uploaded to social media sites -- as images -- and are then spread to unwitting users. When users click on the image, the browser prompts for the image to be downloaded (note: it should simply display it.) Unwitting users then "run" the image and are installing the "Locky" ransomware.
- Beware! Malicious JPG Images on Facebook Messenger Spreading Locky Ransomware <http://thehackernews.com/2016/11/facebook-locky-ransomware.html>
- Locky ransomware uses decoy image files to ambush Facebook, LinkedIn accounts <http://arstechnica.com/security/2016/11/locky-ransomware-decoy-image-files-boobytrap-facebook-linkedin/>

Your Headphones Can Spy On You — Even If You Have Disabled Microphone

- *Speake(a)r: Turn Speakers to Microphones for Fun and Profit."*
- <https://arxiv.org/ftp/arxiv/papers/1611/1611.07350.pdf>
- (demo: <https://www.youtube.com/watch?v=ez3o8aIZCDM>)
- ABSTRACT:
It's possible to manipulate the headphones (or earphones) connected to a computer, silently turning them into a pair of eavesdropping microphones – with software alone. The same is also true for some types of loudspeakers. This paper focuses on this threat in a cyber-security context. We present SPEAKE(a)R, a software that can covertly turn the headphones connected to a PC into a microphone. We present technical background and explain why most of today's PCs and laptops are susceptible to this type of attack. We examine an attack scenario in which malware can use a computer as an eavesdropping device, even when a microphone is not present, muted, taped¹, or turned off. We measure the signal quality and the effective distance, and survey the defensive countermeasures.
- Interestingly, the audio chipsets in modern motherboards and sound cards include an option to change the function of an audio port at a software level, a type of audio port programming sometimes referred to as jack retasking or jack remapping. This option is available on Realtek's (Realtek Semiconductor Corp.) audio chipsets, which are integrated into a wide range of PC motherboards today. Jack retasking – although documented in applicable technical specifications – is not well known
- The RealTek audio chip which is, by far, the most popular in the PC industry, almost exclusively used on PCs and Macs.
- Carbon granule (variable resistance) microphones in early telephone handsets.
- Motors & Generators
- Outboard amps are unidirectional... but they've been integrated onchip.
- Disable all audio hardware in the BIOS -or- use outboard one-way amp.

NTP DoS Exploit Released — Update Servers to Patch 10 Flaws

- <http://thehackernews.com/2016/11/ntp-server-vulnerability.html>
- NTP hasn't been much in the news recently... since the NTP-based amplification attacks were used for DDoS attack amplification.
- Vulnerable: v4.2.8p9, but not including ntp-4.3.94.
- The receipt of a single malformed UDP packet can cause a null-pointer reference which will trigger a memory protection fault and the supervising OS will terminate the NTP daemon.
- Nine other problems in the NTP service were also patched at the same time.
- Anyone having a PUBLICLY EXPOSED NTP daemon should update.

New federal guidelines seek to lock out apps on driver's phones.

- <http://arstechnica.com/tech-policy/2016/11/new-federal-guidelines-seek-to-lock-out-apps-on-drivers-phones/>
- Sort a "car mode" similar to "airplane mode" -- but this one turns off all distracting apps which are not arguably needed for driving. (Maps get to remain active... and presumably hands-free phone.)
- The National Highway Transportation Safety Administration published guidelines calling on smartphone makers to create a "Driving Mode" that shuts down app-use while a car is in motion.
- The 96-page voluntary guidelines are intended to reduce "driver distraction" by also calling for cars to be more easily "paired" with mobile devices so that drivers can access them through an in-vehicle interface.
- The "driver mode" envisioned by NHTSA would lock out things like typing out text messages, as well as displays of images or video not related to driving maps. It would also block most text content, like displays of most webpages, social media, books, and periodicals.
- And (here it comes...) the NHTSA says it's looking forward to developing technology that enables better "driver-passenger distinction," presenting the possibility of a future in which phones automatically lock into some type of "driver mode" without needing the driver to initiate it.
- We see this everywhere... people not noticing that the light turned green, and weaving out of their lanes FAR more often than in years past. If you extend the apparent addiction people have to their phones, as easily witnessed in restaurants... it's easy to see the size of this problem.

EFF: Tech Companies, Fix These Technical Issues Before It's Too Late

<https://www.eff.org/deeplinks/2016/11/tech-companies-fix-these-technical-issues-its-too-late>

The EFF presents this with an unnecessary and unworthy presidential politics spin, saying:

- "The results of the U.S. presidential election have put the tech industry in a risky position. President-Elect Trump has promised to deport millions of our friends and neighbors, track people based on their religious beliefs, and undermine users' digital security and privacy. He'll need Silicon Valley's cooperation to do it—and Silicon Valley can fight back."

The EFF continues:

- "If Mr. Trump carries out these plans, they will likely be accompanied by unprecedented demands on tech companies to hand over private data on people who use their services. This includes the conversations, thoughts, experiences, locations, photos, and more that people have entrusted platforms and service providers with. Any of these might be turned against users under a hostile administration."

And:

- "We present here a series of recommendations that go above and beyond the classic necessities of security (such as enabling two-factor authentication and encrypting data on disk). If a tech product might be co-opted to target a vulnerable population, now is the time to minimize the harm that can be done. To this end, we recommend technical service providers take the following steps to protect their users, as soon as possible:"

However, their recommendations to Internet-based services are spot-on:

1. Allow pseudonymous access.

Give users the freedom to access services pseudonymously. Real-name policies and their ilk are especially harmful to vulnerable populations. Even better, don't restrict access to logged-in users.

2. Stop behavioral analysis.

Do not attempt to use data to infer user preferences and characteristics that users did not explicitly specify themselves. If any form of behavioral tracking is performed, whether locally or across other services, provide a clear means for users opt out. This includes allowing users to modify or erase any data that's been collected about them previously.

3. Delete those logs. Do it now.

If you need them to check for abuse or for debugging, think carefully about which precise pieces of data you really need.... Then delete them regularly, perhaps weekly for the most sensitive data. IP addresses are especially risky to keep. Avoid logging them, or if you must log them for anti-abuse or statistics, do so in separate files that you can aggregate and delete frequently. Reject user-hostile measures like browser fingerprinting.

4. Always encrypt data in transit.

2016 is nearly past. (So is SHA-1 for that matter!) Could there still be any good reason for not running everything over HTTPS and TLS? Do your visitor's ISP and the entire internet need to know about the information users are reading, the things they're buying, the places they're going?

5. Enable end-to-end encryption by default.

If services include messages, enable end-to-end encryption by default. Are high value services, such as AI-powered recommendations or search that are blinded by encryption, being offered? Perhaps it's time to re-evaluate the privacy tradeoff this creates.

Hacking 27% of the Web via a WordPress Auto-Update vulnerability

<https://www.wordfence.com/blog/2016/11/hacking-27-web-via-wordpress-auto-update/>

- 27% of the Internet's websites are powered by WordPress
- Every WordPress installation makes a request to the servers at api.wordpress.org about once an hour to check for updates to plugins, themes, or the WordPress core.
- If updates are available, the update server returns a link to the download server containing the update, and the WordPress site obtains the updated code.
- The WordPress developers maintain their code at Github.
- To publish an update, Github makes a query to the WordPress update server(s) to inform them of the availability of new code, and to provide the URL from which the code should be fetched.
- Naturally... THAT update notice *MUST* be authenticated, otherwise anyone could create a malicious update package, inform the WordPress update that it's ready for distribution, and thus potentially push a malicious update to every WordPress site -- 27% of the Internet -- within one hour.
- How does the Github-to-WordPress authentication work?
- Both ends share a secret.
- An update specification packet is created. Then, for the purpose of "signing it", the shared secret is temporarily appended to the update spec. and is hashed. The shared secret is then removed from the spec... and the spec and the hash are sent to api.wordpress.org for verification and acceptance.
- To authenticate, api.wordpress.org appends its own copy of the shared secret to the update specification package and hashes the concatenation. The server verifies that the hash it obtains matches the hash (signature) which accompanied the update specification provided by Github.
- Since no 3rd-party knows the shared secret, no third party would be able to feasibly compute the proper hash to accompany a non-authentic malicious update.

So... what's the problem?

- The caller providing the update with hashed signature... also specifies the hashing algorithm to be used! <sigh>
- And, this is all PHP... and PHP supports many very old and low-security hashing algorithms, and, in the same category, even some non-cryptographically secure algorithms -- including CRC32, FNV32, and ADLER32.
- As we know and have discussed before, functions such as CRC32 were designed and intended to correct MISTAKES in communication, not PREVENT deliberate manipulation.
- Switching away from the 160-bit SHA-1 to one of the 32-bit functions, reduces the brute force space from 2^{160} down to 2^{32} . (4.3 billion). While this is a LOT weaker, it's still a large average number of guesses (~ 2.15 billion) for an online remote HTTPS exploit.
- But... the ADLER32 checksum function is even worse for this particular application than CRC32.
- Mark is best known for his work on data compression. He's the co-author of the zlib compression library and gzip. He contributed to Info-ZIP and participated in developing the Portable Network Graphics (PNG) image format. (Mark was also the Spirit Cruise Mission Manager for the Mars Exploration Rover mission.)
- But, compared with the cyclic redundancy check (CRC), Mark deliberately made the speed/quality tradeoff in favor of speed.
- The practical upshot is that the function's distribution of outputs is highly skewed.
- As we know, a cryptographic hash function produces some number of bits where every individual bit is a 1 half of the time (and a 0 the other half)... and where there is no detectable cross-bit correlation.
- But the ADLER32 function, never being intended as a hash, doesn't have these properties.
- The guys who did this very clever work (WordFence.com) analyzed the use of the ADLER32 function in this application and, due to the function's highly non-uniform output, were able to reduce the brute force space from 32-bits (2^{32}) down to between 100,000 to 400,000... which their proof of concept demonstrated makes an online brute-force attack possible.
- They notified WordPress of their discovery, provided a working exploit proof-of-concept, received a reward for their nice work... and WordPress fixed the problem before any of this went public.

Into the symmetry: All your Paypal OAuth tokens belong to me - localhost for the win

- <http://blog.intothesympetry.com/2016/11/all-your-paypal-tokens-belong-to-me.html>
- Yet another mistake made my OAuth implementers.
- ... this time in PayPal's implementation.

Miscellany

IRS Demands All Info On All Coinbase Customers

- <https://www.techdirt.com/articles/20161118/18090136088/irs-demands-all-info-all-coinbase-customers.shtml>

Supercapacitors in the news: A phone that charges in seconds!

- Highly forwarded to me. Even Amber MacArthur picked up on this story.
- University of Central Florida
- "UCF scientists bring it closer to reality with flexible supercapacitors"
 - <https://www.sott.net/article/334770-A-phone-that-charges-in-seconds-UCF-scientists-bring-it-closer-to-reality-with-flexible-supercapacitors>
- A Phone That Charges in Seconds? UCF Scientists Bring it Closer to Reality - UCF News - University of Central Florida Articles - Orlando, FL News
 - <https://today.ucf.edu/phone-charges-seconds-ucf-scientists-bring-closer-reality/>
- Current vs Voltage
- Electrochemical vs Electrostatic

TraptionBakery by Jonathan Prestidge. (iOS only - Free & delightful!)

- http://www.properbostin.com/traption_bakery/
- "An Upcyclepunk Postimperial Curio."
A curio for some or a right old puzzle for others, make no mistake.

Some say: some folk actually managed to bake a loaf of bread using this confounded contraption... but that is rumoured to be just a rumour.

There's no pressure... relax, ponder, prod, clank, crank, pull, push, watch... ponder more....sleep on it maybe... come back to it...ponder.

Along with the intriguing artwork there is the challenging puzzle with the ultimate objective of baking a loaf, but you can enjoy solving easier mile stones along the way like: ordering some grain, starting the mill, then milling yourself some flour, with this huge fully functional contraption. Look for clues written on the equipment, listen to the sound scape, and fathom the interconnections. Once you have solved the puzzle of how to bake a loaf then the simulator aspect of the game becomes apparent: you have to get the ingredients, mixing, proving and baking just right if you want to aspire to bake the perfect loaf. Your baking efforts are judged right at the end of the process... whether they be good, or bad.

- <https://itunes.apple.com/us/app/traptionbakery/id1068266222>

- A reviewer:
TraptionBakery by syntheticvoid

While I'm not really much of a puzzle gamer, this one drew me in. Being able to figure out this contraption and make it work was one of the best puzzler experiences I've ever had. Everything, and I mean EVERYTHING, from the way the game is designed, to the artwork, all of the small details that become clearer as you zoom in... the thought behind every little thing and how it all interacts with everything else, it's all absolutely perfect. I can't recommend this one enough to puzzle fans.

- Another reviewer:
I am no longer hesitating... 5 stars.

I wasn't aware of it when I started this game, but sounds are probably very important. Well at least it was to solve my first little thing. And my god, it is rewarding.

If you look at the screenshots, the game may seem static. But it is a drawing that becomes alive when you manipulate it. And it is very well done, the art is fantastic."

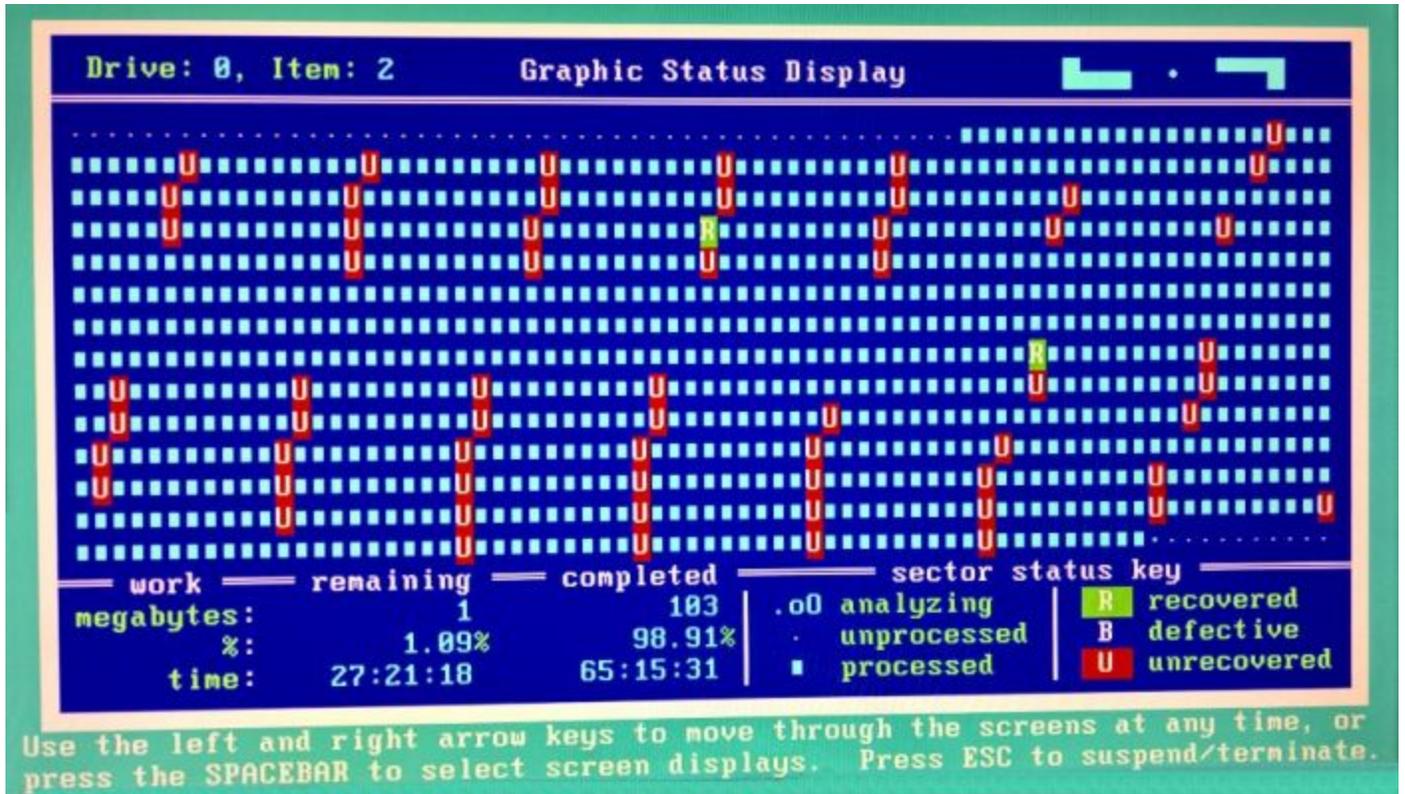
- The Making of...
<http://www.properbostin.com/anoraks/tb/index.html>

SpinRite

Gary Nevills (Gary Nevills)

Steve do these patterns in SpinRite indicate anything specific about the condition of the disk?

<https://twitter.com/messages/media/803284265542778884>



After a break... On to our Q&A!

:)