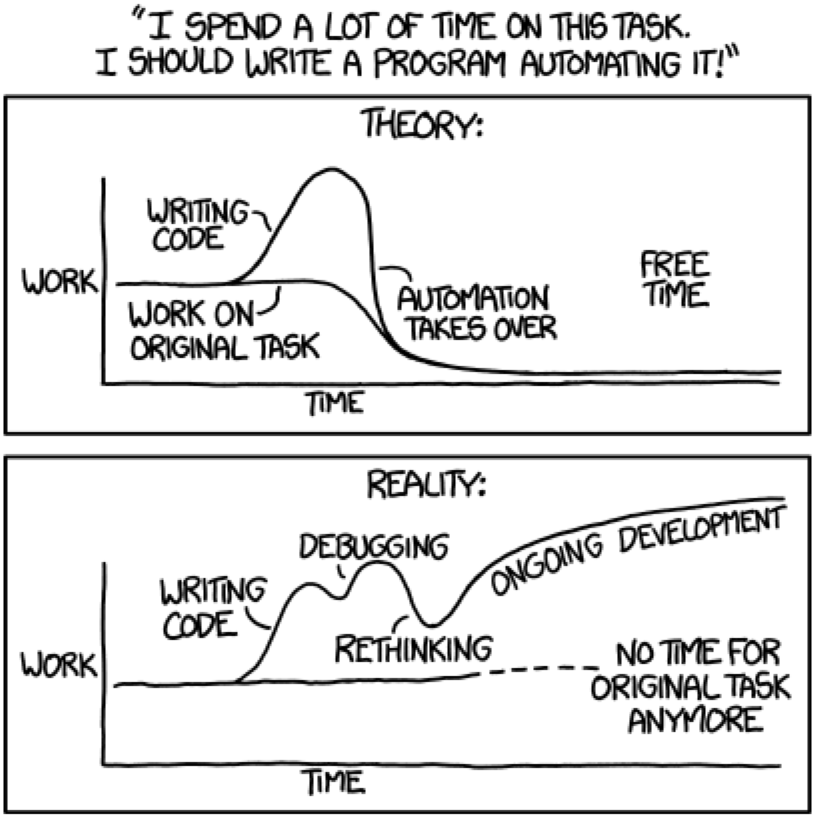
Security Now! #503 - 04-14-15

Q&A #210

This week on Security Now!

- EFF wins its Podcast Patent Challenge
- Update on CNNIC's root certificates
- Massive Botnet takedown
- The Mac "Rootpipe" vulnerability
- Kaspersky offers Ransomware Decryption
- Split-Keying government crypto access
- Banking sites Cipher Suite ordering

XKCD captures reality once again: http://xkcd.com/1319/



Permanent link to this comic: http://xkcd.com/1319/
Image URL (for hotlinking/embedding): http://imgs.xkcd.com/comics/automation.png

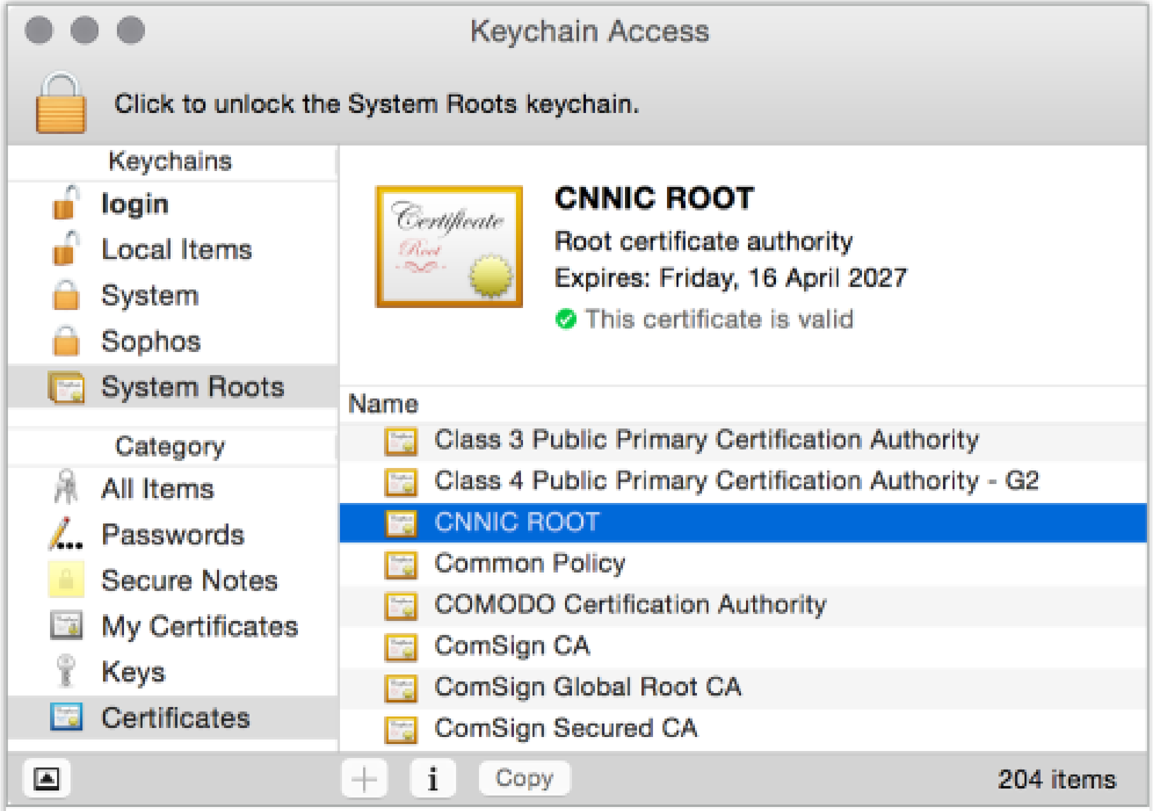
Podcast Industry Patent!

- **Whew!**
- https://www.eff.org/press/releases/eff-busts-podcasting-patent-invalidating-key-claims-patent-office
- https://www.eff.org/files/2015/04/10/personalaudiodecision.pdf

Security News

CNNIC... okay by MSFT & APPLE... not okay by GOOGLE & MOZILLA

- Nice explainer by Sophos: https://nakedsecurity.sophos.com/2015/04/14/tls-certificate-blunder-revisited-whither-china-internet-network-information-center/
- Neither Chrome nor Mozilla will trust any CNNIC certs signed after April 1st, 2015.
- And Google says even that will only last long enough to allow CNNIC's customers to change CA's.
- Apple just updated its official list of Root CAs, known as its Trust Store, in the latest OS X and iOS updates. The entry CNNIC ROOT kept its spot:



Click to unlock the System Roots keychain.

CNNIC ROOT
Root certificate authority
Expires: Friday, 16 April 2027
✓ This certificate is valid

Name
Class 3 Public Primary Certification Authority
Class 4 Public Primary Certification Authority - G2
CNNIC ROOT
Common Policy
COMODO Certification Authority
ComSign CA
ComSign Global Root CA
ComSign Secured CA

204 items

CNNIC ROOT certificate in Apple's System Roots keychain

- Microsoft sends root certs on demand... and a fresh install of Windows 10 obtained the CNNIC root.

"Simda" Windows botnet had enslaved 770,000 computers in 190 countries.

- 128,000 new machines per month.
- A large highly-coordinated multi-national effort involved the seizing of 14 command-and-control servers located in the Netherlands, US, Luxembourg, Poland, and Russia.
- US was most infected, with 22% of the total infections.
- Followed by UK & Turkey with 5% & Canada and Russia with 4% each.
- Exploited known vulnerabilities in Java, Adobe Flash & Microsoft's Silverlight.
- Highly stealth bckdoor Trojan which morphed into a new A/V-undetectable form every few hours.
- Altered the HOSTS file to redirect "connect.facebook.net" and "google-analytics.com".

Mac OS X "Rootpipe" privilege escalation bug.

- http://blog.cylance.com/redirect-to-smb
- Swedish security researcher, Emil Kvarnhammar, calls the privilege escalation bug "Rootpipe."
- Unprivileged code running in a user's machine could obtain root access without having to obtain the root password from the user.
- Responsible disclosure:
  - On October 6th, 2014, Emil tweeted:
  - Details on the #rootpipe exploit will be presented, but not now. Let's just give Apple some time to rollout a patch to affected users. — Emil Kvarnhammar (@emilkvarnhammar)
- Only OS X v10.10 “Yosemite” gets patched.
- To protect yourself:
  - Do not run the system under an Admin-privilege account.
  - Create a second "Admin" account, named admin.
  - Login as that Admin user and remove Admin privileges from the normal account.
  - Logout out and only use the Admin account when needed.

Kaspersky offers Ransomware Decryption

- https://noransom.kaspersky.com/
- Some CoinVault keys were found... so there MIGHT be hope.

NSA proposing "Split-Keying" for Smartphones

- http://arstechnica.com/tech-policy/2015/04/nsa-dreams-of-smartphones-with-split-crypto-keys-protecting-user-data/
- Critics have also raised concerns that any type of portal that gives government officials access to encrypted contents has a strong likelihood of backfiring. They said criminals or spies from hostile countries may exploit the weaknesses to obtain classified or confidential data, possibly on a mass scale. The split-key approach floated by Rogers, for instance, requires a complicated system to allocate the keys, deliver them to each involved party, recombine them when a legitimate court order is issued, and destroy the key once it was used. "Get any part of that wrong and all your guarantees go out the window," Matt Green, a Johns Hopkins University professor and an expert in

> cryptography, told The Washington Post.
>
> The approach is only one of several options being studied by the White House. One alternative under consideration would have a judge direct a company to set up a mirror account so that law enforcement officials conducting a criminal investigation could read text messages shortly after they are sent. To obtain encrypted photos, the judge could order the company to back up the suspect's data to a server while the phone is turned on and its contents are unencrypted.
>
> White House aides hope to report to the president this month.

Banking sites Cipher Suite ordering

- Many people tweeted their despair at discovering just how lame their own banks were.
- It seems to be nearly universal... that banking websites have awful cipher suite ordering.
- Unfathomable.

Miscellany

Podcast Awards announced TONIGHT during the 10th Annual Podcast Awards Ceremony

- Live streaming: http://podcastone.com/ (beginning 6pm Pacific.)

Randy Thomas in Rapid City South Dakota notes that Season 3 of "Orphan Black" starts this coming Saturday the 18th!

SpinRite

Hi everybody,

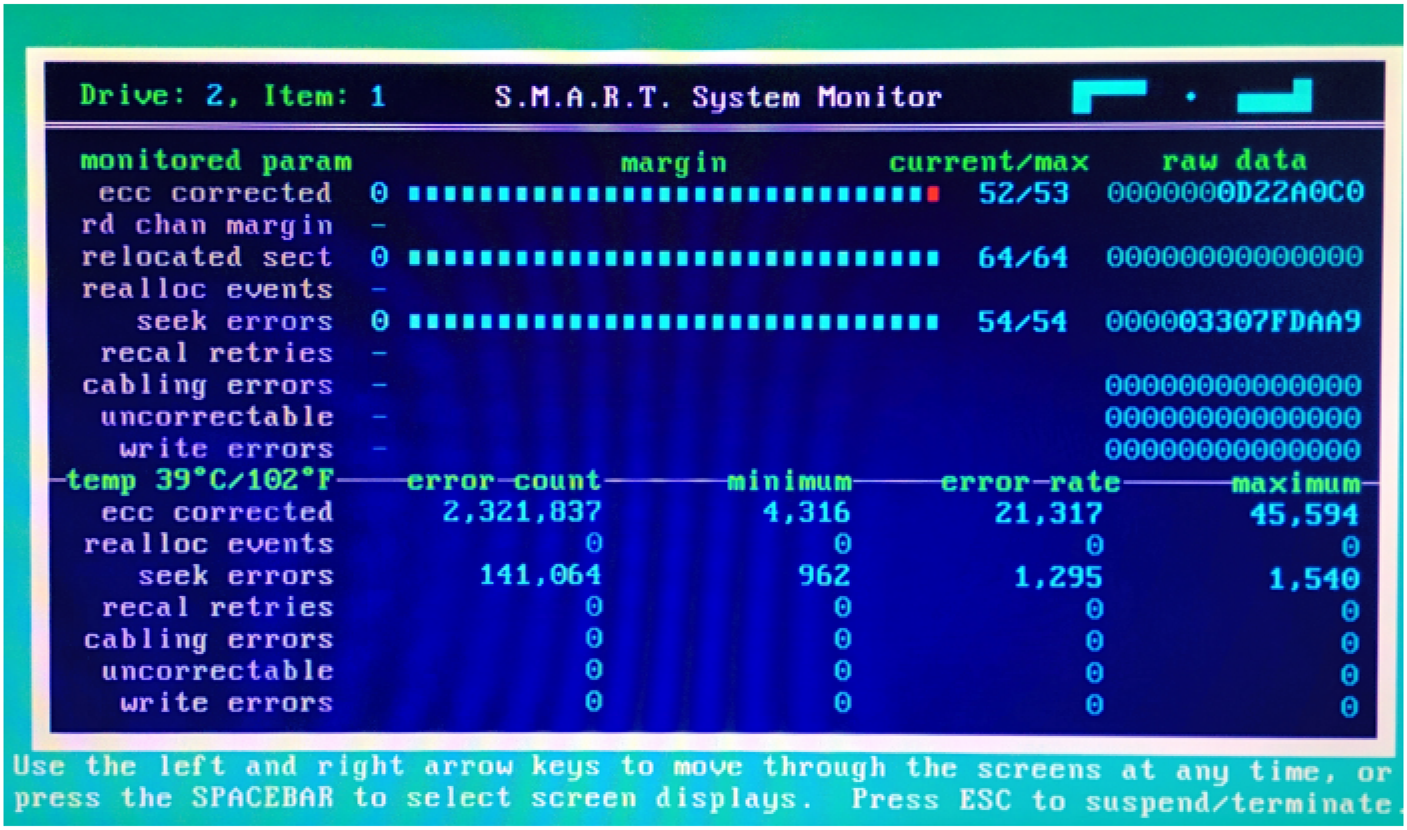
First, I want to apologize for my imperfect English (I'm French speaking). I want to share with you my SpinRite story.

I purchased a license to SpinRite, mainly to support you: I'm a big fan of Security Now. Anyway, I never got the chance to really test my version of SpinRite, since I bought it, I mainly use the program for maintenance (preventive scanning).

A couple of weeks ago my Cisco Explorer 8300HD DVR (cable TV set-top box) started to behave strangely. A lot of recorded shows would pause and skip frames. In the worst case, I got some shows who would not record at all.

I suspected the hard drive to be the problem, but since these devices runs on custom "encrypted" file system, it was impossible for me to run any usual programs like Windows ScanDisk. So, I plugged the DVR HDD into my main PC and ran SpinRite (level 2) on it. When

I checked the SMART screen, I immediately saw the problem:



```
 Drive: 2, Item: 1        S.M.A.R.T. System Monitor

 monitored param              margin              current/max    raw data
   ecc corrected  0 ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■   52/53   0000000D22A0C0
  rd chan margin  -
  relocated sect  0 ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■   64/64   00000000000000
  realloc events  -
     seek errors  0 ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■   54/54   000003307FDAA9
   recal retries  -
  cabling errors  -                                            00000000000000
   uncorrectable  -                                            00000000000000
    write errors  -                                            00000000000000
─temp 39°C/102°F───error─count──────minimum──────error─rate───────maximum─
   ecc corrected     2,321,837        4,316          21,317         45,594
  realloc events             0            0               0              0
     seek errors       141,064          962           1,295          1,540
   recal retries             0            0               0              0
  cabling errors             0            0               0              0
   uncorrectable             0            0               0              0
    write errors             0            0               0              0
Use the left and right arrow keys to move through the screens at any time, or
press the SPACEBAR to select screen displays.  Press ESC to suspend/terminate.
```

The HDD was slowly dying! I was lucky enough, the faulty HDD was the external one (expansion). SpinRite fixed it, then I replaced it, and since then I can enjoy my recorded TV shows and I feel confident about my schedule recordings.

Another example on how SpinRite can help in some unexpected situation: throw any disk at it and let it do it's "magic". ;)

Thanks Steve (and all who work with you on SpinRite)!

Steve Rodrigue