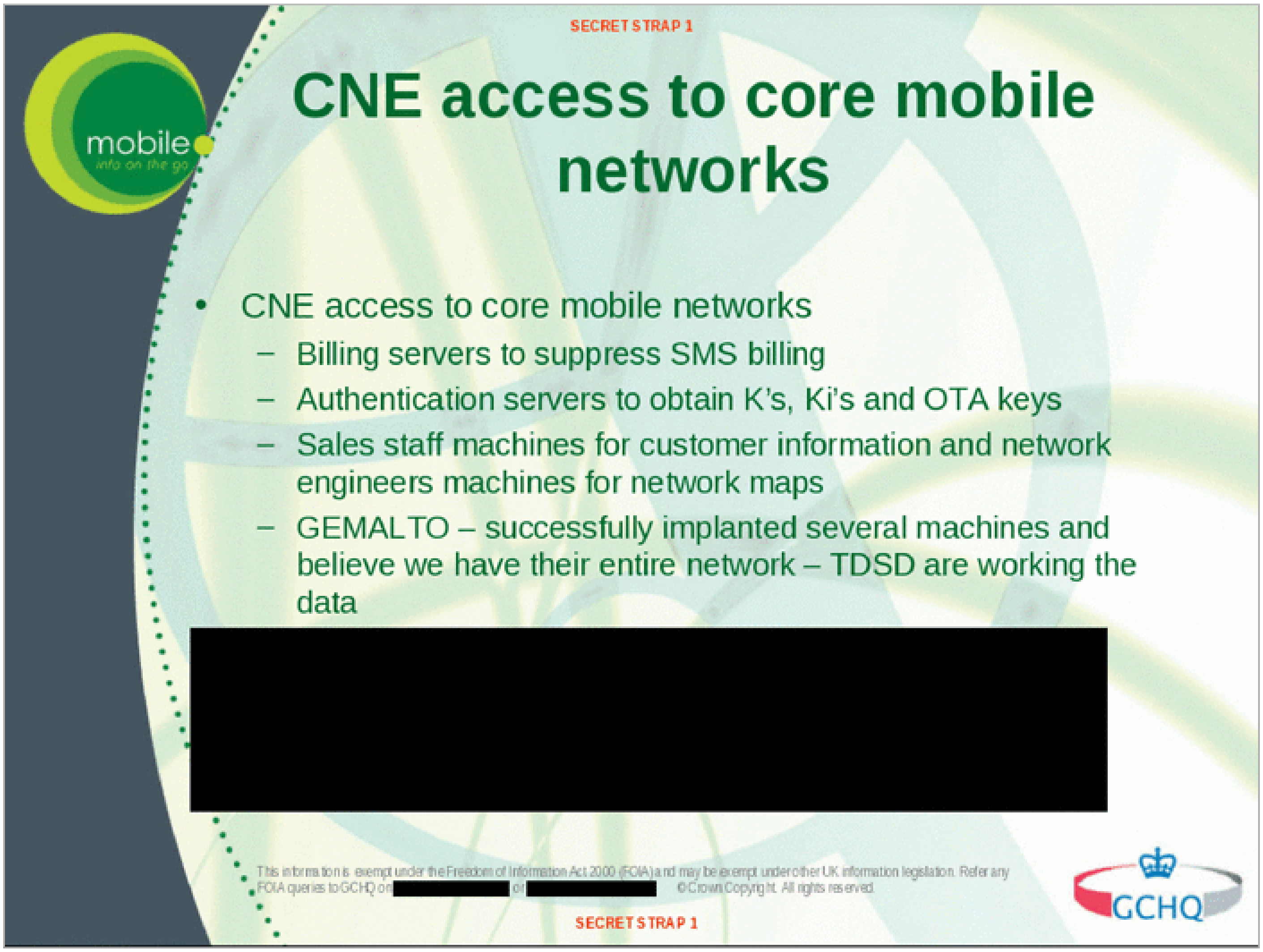
Security Now! #496 - 02-24-15

Q&A #207

This week on Security Now!

- Lenovo's big mistake
- Another stunner from Edward Snowden
- TrueCrypt news,
- HSTS gains a final major supporter
- Tidbits, follow-ups, and ten questions and thoughts from our terrific listeners.

All your SIMs are belong to us.



mobile
info on the go
GCHQ

SECRET STRAP 1

CNE access to core mobile networks

- CNE access to core mobile networks
  - Billing servers to suppress SMS billing
  - Authentication servers to obtain K's, Ki's and OTA keys
  - Sales staff machines for customer information and network engineers machines for network maps
  - GEMALTO – successfully implanted several machines and believe we have their entire network – TDSD are working the data

[redacted]

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted] ©Crown Copyright. All rights reserved.

SECRET STRAP 1

Image of the Week, thanks to Edward Snowden & The Intercept

Security News

Scheduling Note: NEXT WEEK WE SWITCH to 1:30pm

Lenovo was found to be using a bad HTTPS proxy.

- Lenovo --> Superfish
- Superfish --> Komodia
    - "Visual Discovery"

- Komodia
    - https://www.youtube.com/watch?v=dkp1KoP7nTc
    - Komodia's poor SSL/TLS technology is in over 100 products. (Only one of which is Superfish.)

- The Komodia site has been down since this began
    - http://web.archive.org/web/20150220003144/http://www.komodia.com/products/komodias-ssl-decoderdigestor
    - http://web.archive.org/web/20140715080934/http://www.komodia.com/products

- Komodia's Technology:
    - HTTPS Proxy Certs
        - Installs the same Root CA cert into every system's trusted root store.
        - Contains the private cert needed to sign on-the-fly fake certs.
        - Uses the password "komodia" for the private cert.
    - HTTPS Proxy Problems
        - Supports really poor cipher suites:
            - 40-bit RC4 with MD5 hash
            - 40-bit DES
    - Does not properly validate the remote server's certificate, easily spoofed.

- Check for the problem:
    - https://filippo.io/Badfish/

Of equal or perhaps greater concern is that the move to HTTPS is putting pressure on traditional tools.

- MANY A/V systems are now doing the same thing.

Lenovo / Superfish / Komodia Link:

- http://techreport.com/news/27849/the-rest-of-the-story-komodia-lenovo-and-superfish
- http://marcrogers.org/2015/02/19/will-the-madness-never-end-komodia-ssl-certificates-are-everywhere/
- https://blog.lastpass.com/2015/02/are-you-at-risk-from-superfish-check-now.html/
- http://blog.cryptographyengineering.com/2015/02/how-to-paint-yourself-into-corner.html
- https://www.eff.org/deeplinks/2015/02/further-evidence-lenovo-breaking-https-security-its-laptops
- https://infected.io/120/lenovos-superfish-security-nightmare

- http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/
- http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html
- http://pastebin.com/CFsqPgfq
- http://www.bbc.com/news/technology-31533028
- http://www.komodia.com/products/komodias-ssl-decoderdigestor
- http://www.theregister.co.uk/2015/02/20/lenovo_caves_in_face_of_public_firestorm_release_superfish_killer/?mt=1424404680018
- http://www.pcworld.com/article/2886690/lenovo-cto-admits-company-messed-up-and-will-publish-superfish-removal-tool-on-friday.html

GEMALTO's SIM Keys were intercepted...

- https://firstlook.org/theintercept/2015/02/19/great-sim-heist/
- Gemalto:
  - A multinational firm incorporated in the Netherlands that makes the chips used in mobile phones and next-generation credit cards.
  - Among its clients are AT&T, T-Mobile, Verizon, Sprint and some 450 wireless network providers around the world.
  - The company operates in 85 countries and has more than 40 manufacturing facilities. One of its three global headquarters is in Austin, Texas and it has a large factory in Pennsylvania.
  - Gemalto produces some 2 billion SIM cards a year. Its motto is “Security to be Free.”

- With these stolen encryption keys, intelligence agencies can monitor mobile communications without seeking or receiving approval from telecom companies and foreign governments.

- Possessing the keys sidesteps the need to get a warrant or a wiretap and leaves no trace on the wireless provider’s network that the communications were intercepted.

- Bulk key theft enables intelligence agencies to unlock any previously encrypted communications they had already intercepted, but did not yet have the ability to decrypt.

- As part of the covert operations against Gemalto, spies from GCHQ — with support from the NSA — mined the private communications of engineers and other company employees in multiple countries.

- Gemalto was totally oblivious to the penetration of its systems — and the spying on its employees.

- Gemalto won't comment other than to say that they had no prior knowledge that the agencies were conducting the operation.

- Cryptographer Matthew Green (Johns Hopkins) explained to "The Intercept":
  - "Gaining access to a database of keys is pretty much game over for cellular

encryption."

- Matthew Green's blog posting about cellular encryption:
  - http://blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html

- Cellular Security:
  - 2G - still the dominant platform globally is trivially cracked.
  - 3G, 4G & LTE are much stronger and require keys.
  - SIM Cards were introduced to control billing fraud, an early problem.
  - There never was a strong concern about privacy.
    - Remember that simple scanners allowed eavesdropping on the original analog phones.
    - Consequently, there was never a huge amount of security surrounding the supply chain.

Wither TrueCrypt?

- Tweet: Matthew Green @matthew_d_green
- We've been making progress on the Truecrypt audit despite the lack of news. I'll post a update later this afternoon. http://news.ycombinator.com/item?id=9069295
- http://blog.cryptographyengineering.com/2015/02/another-update-on-truecrypt-audit.html
- Synopsis:
  - In late 2013, crowdfunded audit of TrueCrypt raised $70k.
  - Part 1 - Examined the boot and initialization process. Came out clean.
  - Part 2 - (Much more challenging part) is a detailed look at the cryptography of Truecrypt, ranging from the symmetric encryption to the random number generator.
  - Late spring 2014, the TrueCrypt authors pulled the plug on the TC project.
  - After recovering, Part 2 will now move forward by "NCC Group's Cryptography Services"
  - Phase 2 will evaluate the original Truecrypt 7.1a, and it will begin shortly. However to minimize price -- and make your donations stretch farther -- we allowed the start date to be a bit flexible, which is why we don't have results yet.
  - https://cryptoservices.github.io/fde/2015/02/18/truecrypt-phase-two.html

Internet Explorer gets HSTS in Windows 10.

- http://blogs.msdn.com/b/ie/archive/2015/02/16/http-strict-transport-security-comes-to-internet-explorer.aspx
- https://hstspreload.appspot.com/
- http://caniuse.com/#feat=stricttransportsecurity
- chrome://net-internals/#hsts

Miscellany:

Errata: "HPACK compression" -- zlib was abandoned due to worries over CRIME

- http://tools.ietf.org/html/draft-ietf-httpbis-header-compression-09
- http://tools.ietf.org/pdf/draft-ietf-httpbis-header-compression-09.txt

CitizenFour

- 8.3/10 on IMDb -&- 98% on Rotten Tomatoes.
- Now Playing on HBO - 1h, 54min
- 2015 Oscar for Best Documentary.
- The sense I came away with: Privacy is a right.

Sci-Fi:

- Finished "The Expanse" Book #3
- ... and I finally know why it's called "The Expanse."
- The first 10-episode SyFy series is just book one.
- Book #4 is the first of the additional three that have been commissioned.

SpinRite

Fred Elbel
Subject: testimonial for SpinRite

Dave: This is a testimonial for SpinRite. You may place the following text on your website, but you may not publish my email address.

Just after doing a backup on an old XP system, it failed and would not boot because of a boot drive error. I wasn't sure that the backup had even completed ok.

Then I remembered reading about SpinRite and wondering what the heck it actually did. After reviewing the material, video, and testimonials, I decided to give it a shot.

I created a SpinRite CD image on another system and booted it up on the bad system. I then ran it in level 2 against the bad drive. The next morning, the computer had powered off, so I ran SpinRite again. It completed in an hour or so. At that point, the computer booted and ran flawlessly!

SpinRite is a fantastic tool and is certainly worth the purchase price.

Fred Denver, Colorado, USA