Situational Awareness: Security (& Privacy)

My personal view on the past 6 months

Stefan.Lüders@cern.ch

For the CERN Computer Security Team

HEPix Fall 2014 @ U Nebraska, Oct. 13-17 2014

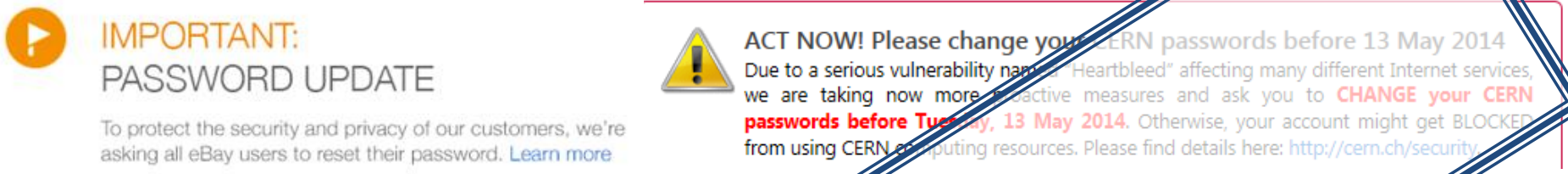
Preamble

“Freedom, security, convenience --- choose two” (Dan Geer)

Consequently:

“Security will always be exactly as bad as it can possibly be while allowing everything to still function.” (Nat Howard)

(2014/5) Heartbleed Ripples



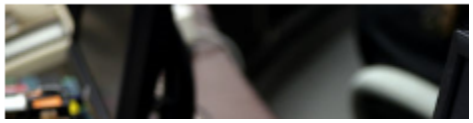
- Password resets initiated by e.g. eBay, Doodle, CERN
- Avalanche of copy cats looking for similar vuln's (still today!)
- Failure of review process in OpenSource community (what is responsibility of software houses using OpenSource?)

Mitigation: Prompt & agile patching

NSA Said to Exploit Heartbleed Bug for Intelligence for Years

By Michael Riley Apr 12, 2014 6:00 AM GMT+0200 | - Comments Email Print

The U.S. National Security Agency knew for at least two years about a flaw in the way that many websites send sensitive information, now dubbed the Heartbleed bug, and



http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

(2014/5) EU right to be fogotten

Press and Information

Court of Justice of the European Union

PRESS RELEASE No 70/14

Luxembourg, 13 May 2014

Judgment in Case C-131/12
Google Spain SL, Google Inc. v Agencia Española de Protección de Datos,
Mario Costeja González

An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf

- Google provided webform for EU and CH citizens:

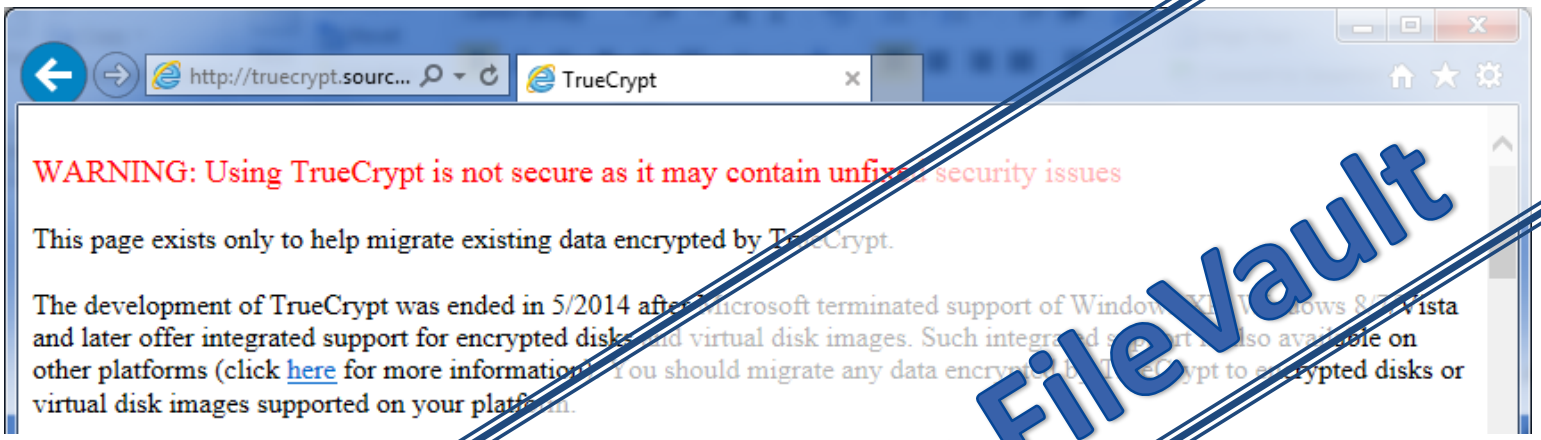
  https://support.google.com/legal/contact/lr_eudpa?product=websearch

- But now:

  How to avoid that information of common interest, historical data or other important information goes down the drain??!

  http://www.nzz.ch/aktuell/digital/google-setzt-recht-auf-vergessenwerden-um-1.18312335

(2014/5) R.I.P. Truecrypt

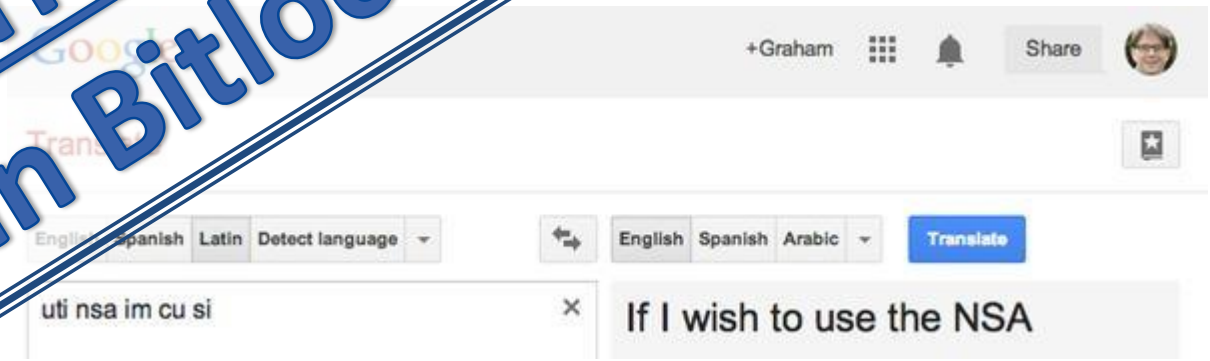


http://truecrypt.sourceforge.net/

- Unclear why: Initially suspicion: Defacement hack
- Current version with good reputation and few weaknesses…

http://opencryptoaudit.org/

Alternatives: Win Bitlocker, Mac FileVault



http://grahamcluley.com/2014/06/truecrypt-hidden-message/

(2014/6) Facebook Research

Experimental evidence of massive-scale emotional contagion through social networks

Adam D. I. Kramer[a,1], Jamie E. Guillory[b,2], and Jeffrey T. Hancock[b,c]

http://www.pnas.org/content/111/24/8788.full.pdf+html

- Manipulating 300k News Feeds: Can FB influence mood of users? (they can only to a minor extend)
- Perceived misuse as Guinea Pigs: FB AUP adapted 4 months later
- Irish data protection authorities embarrassed but fail to act

Questions have been raised about the principles of informed consent and opportunity to opt out in connection with the research in this paper. The authors noted in their paper, "[The work] was consistent with Facebook's Data Use Policy, to which all users agree prior to creating an account on Facebook, constituting informed consent for this research." When the authors provided their paper for publication in PNAS, they stated that: "Because this experiment was conducted by Facebook, Inc. for internal purposes, the Cornell University IRB [Institutional Review Board] determined that the project did not fall under Cornell's Human Research Protection Program." This statement has since been confirmed by Cornell University.

http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/

Mitigation: Opt-out Facebook?!

(2014/6 & 7) Hacking the IoT

Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable

BY KIM ZETTER 06.25.14 | 6:30 AM | PERMALINK

http://www.wired.com/2014/06/hospital-network-leaking-data/

How Hackable Is Your Car? Consult This Handy Chart

BY ANDY GREENBERG 08.06.14 | 6:30 AM

Tesla Model S hack reportedly controls locks, horn, headlights while in motion

Share Tweet 76

Tesla Motors officials vow to investigate reports that its Model S sedan is susceptible to hacks that can remotely control the car's locks, horn, headlights, and skylight while the car is in motion, according to a published report.

http://arstechnica.com/security/2014/07/tesla-model-s-hack-reportedly-controls-locks-horn-headlights-while-in-motion/

http://www.wired.com/2014/08/car-hacking-chart/

Mitigation: Prompt & agile patching, again

- What about our accelerators & experiments?

https://indico.cern.ch/event/21745

(2014/7) “BadUSB“

- Many USB firmware chips are unprotected
- “BadUSB” mal-firmware can take over PCs via keystroke injection or pretend being a network card (and sniff traffic)

  http://www.pcworld.com/article/2460540/most-usb-thumb-drives-can-be-reprogrammed-to-silently-infect-computers.html
- Source code published recently

  http://gizmodo.com/now-anyone-can-get-the-malware-that-exploits-usbs-funda-1641821985
- No protection means ☹

COMPUTER ACCESSORIES hardware, security, security, usb drives, hacking

Most USB thumb drives can be reprogrammed to silently infect computers

Lucian Constantin Jul 31, 2014 2:46 PM

Now Anyone Can Get the Malware That Exploits USB's Fundamental Flaw

Adam Clark Estes 68,943 7
Filed to: HACKERS Thursday 5:13pm

Mitigation: None (but Epoxy glue)

(2014/8) More hacking of the IoT

UPDATE 1-All at sea: global shipping fleet exposed to hacking threat

Jeremy Wagstaff
Wednesday, 23 Apr 2014 | 9:54 PM ET

REUTERS

Hacker says to show passengers that at risk of cyber attack

BY JIM FINKLE
BOSTON | Mon Aug 4, 2014 8:09am EDT

http://www.reuters.com/article/2014/08/04/us-cybersecurity-hackers-airplanes-idUSKBN0G40WQ20140804
http://www.cnbc.com/id/101608644

Hacking Traffic Lights is Amazingly Really Easy

Wednesday, August 20, 2014 Swati Khandelwal

RESEARCHER DISCLOSES WI-FI THERMOSTAT VULNERABILITIES

by Chris Brook September 22, 2014 , 3:14 pm

http://thehackernews.com/2014/08/hacking-traffic-lights-is-amazingly_20.html
https://threatpost.com/researcher-discloses-wi-fi-thermostat-vulnerabilities/108434

Mitigation: Prompt & agile patching, thirdly

- In an IoT world: How prompt and agile must patching be done?

(2014/8) Cybersecurity as Realpolitik

- Keynote of Dan Geer to BlackHat U.S.A.

  http://geer.tinho.net/geer.blackhat.6viii14.txt

- Source code liability for whatever damage your software causes when it is used normally unless you allow disabling any unwanted functionality.

```
If a builder builds a house for someone, and does not construct
it properly, and the house which he built falls in and kills
its owner, then the builder shall be put to death.
    -- Code of Hammurabi, approx 1750 B.C.
```

- Any unsupported software must become public domain, e.g. WinXP w/o updates…
- Mandatory reporting regime for cybersecurity failures as with CDC disease reporting (and with a similar medical privacy) or (near-miss) aviation accident reporting?
- Overpay bounty hunters to increase talent pool of vulnerability finders and devaluate findings by making them public.

(2014/9) Shellshock

- "Heartbleed on steroids": Vulnerability of BASH allowing for remotely bypassing access restrictions and eventually execute system commands (CVE-2014-6271,6277,6278,7169)

  https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

```
() { _; } >_[$($())] { echo hi mom; }; }
```

```
env X='() { (a)=>\' sh  date" cat echo
```

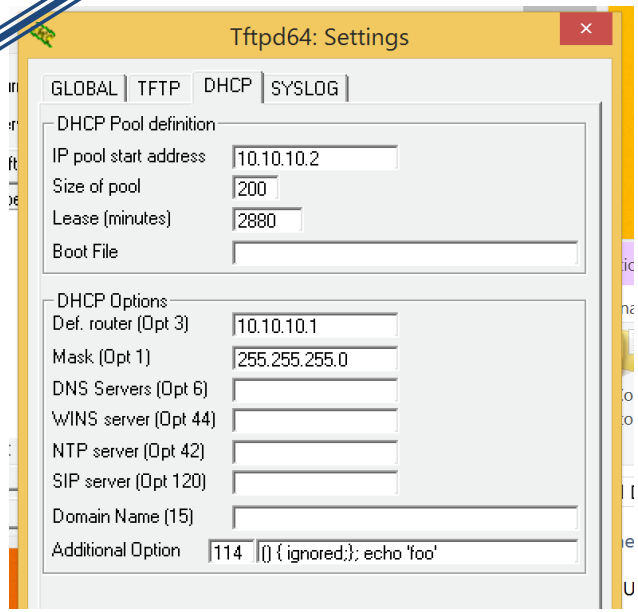
```
() { _; }; x() { _; } <<a; }
```

  http://en.wikipedia.org/wiki/Shellshock_(software_bug)

- Affecting Mac OS, Linux since 1992!
- Easy to detect vuln, but not compromize…
- Mass update a success for non-nerds (as it didn't come via „Software Update")

  http://support.apple.com/kb/HT6495

- (Thanks to PerfSonar experts for updating)



Mitigation: Prompt & agile patching…

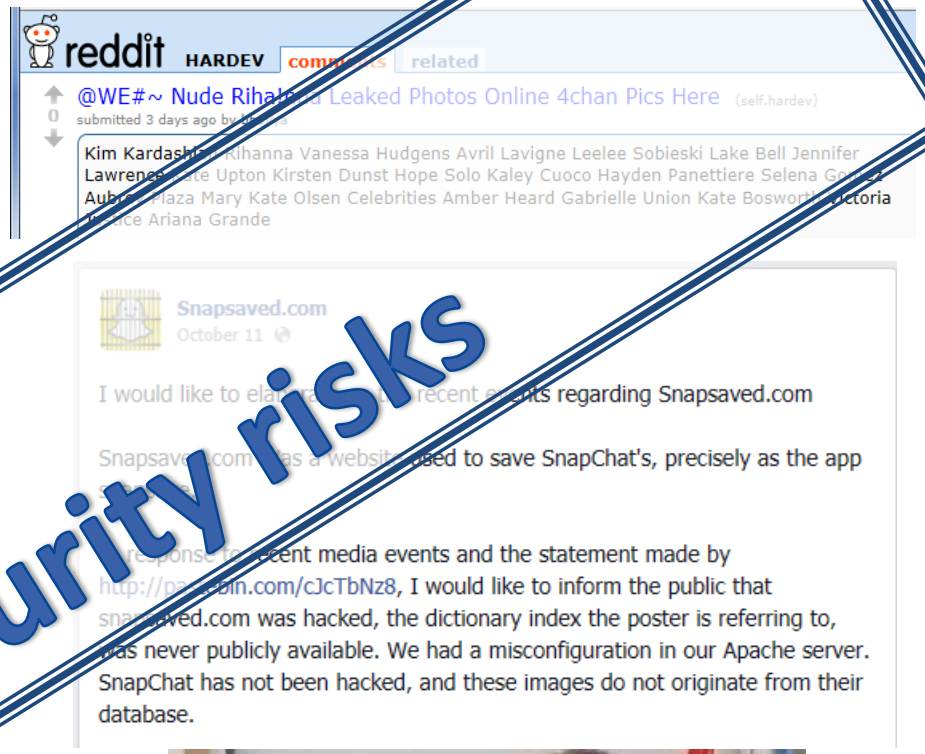
(2014/9) Selfies & Naked Teddy Bears

- iCloud accounts of celebrities compromised and “selfies” disclosed
- (2014/10) Snapchat (i.e. “Snapsave”!) followed…
- Lawyers threatening to sue Google on $100M (but not Apple!)

http://pagesix.com/2014/10/01/lawyers-for-hacking-victims-sue-google-for-failing-to-stop-sharing-nude-pics/

- What about taking photos of alleged iPhone thieves?

http://www.spiegel.de/netzwelt/gadgets/hacker-dieb-per-twitter-gesucht-rechtlich-fragwuerdige-suche-a-994020.html



Mitigation: ACK cloud security risks

(2014/9) Run for the cleanest TLD

SWISS INTERNET SECURITY ALLIANCE

11/09/2014

by Michael Hausding

Leave a comment

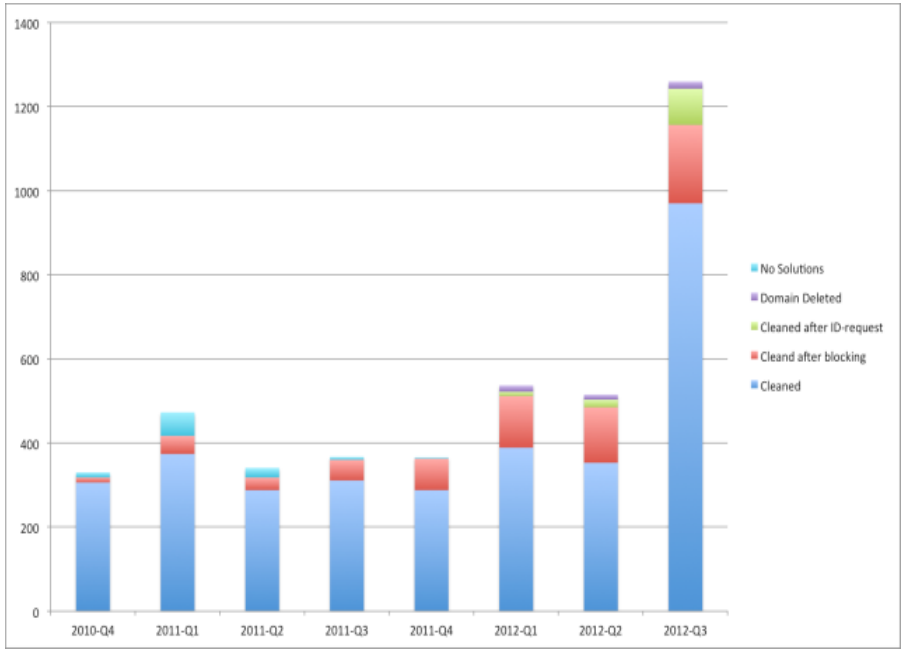
Swiss economy makes online security its priority

Switzerland is one of the safest countries in the world. To make also the Internet a secure place in Switzerland, the Swiss online economy has started the Swiss Internet Security Alliance (SISA). The goal of the alliance is to make Switzerland the "cleanest" Internet country in the world! The organization launched an online security check today

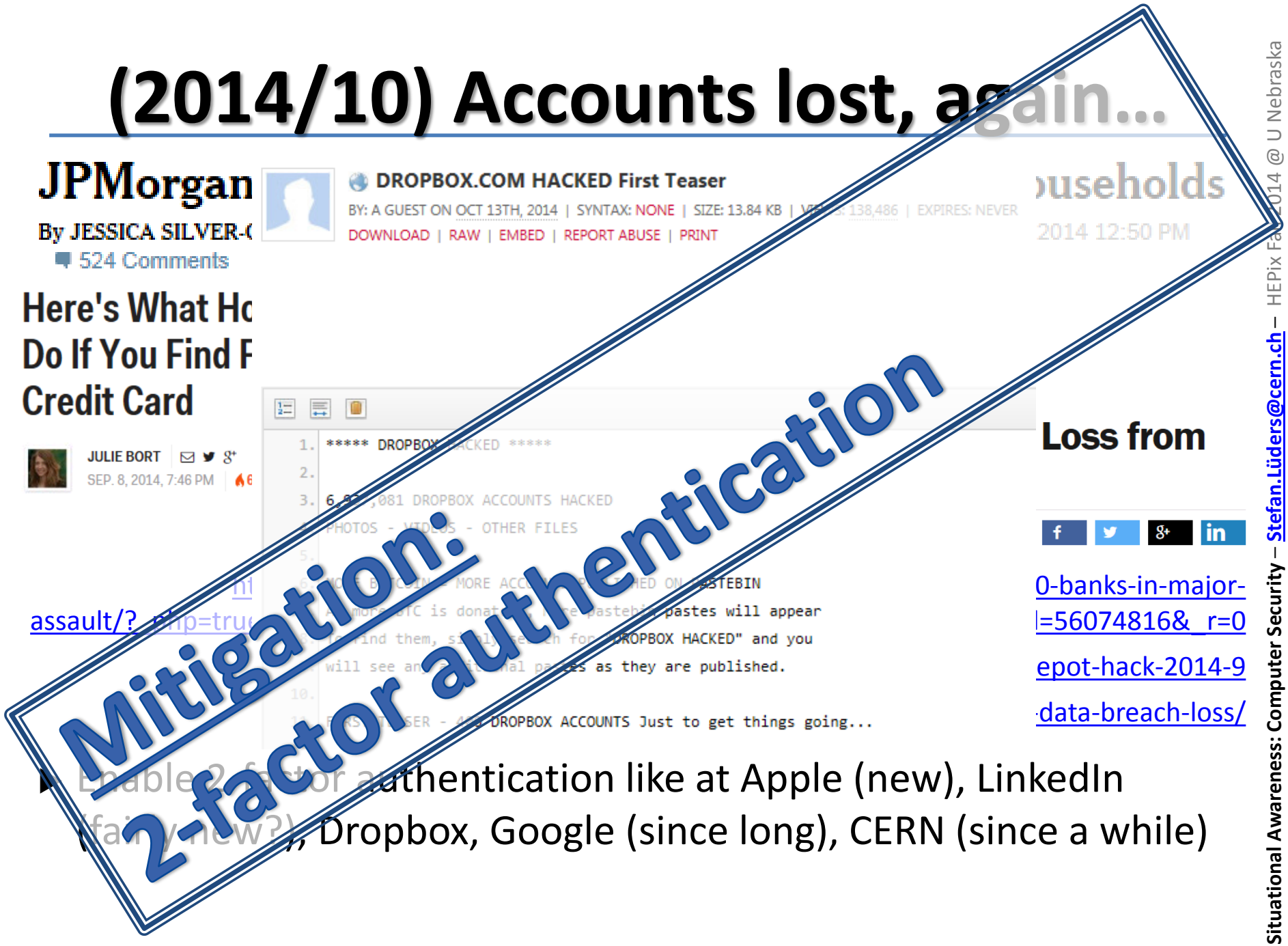
- Registrar allowed to block malware hosting domains for up to 5 days

  http://securityblog.switch.ch/2014/09/11/swiss-economy-makes-online-security-its-priority/

- Backed up by Swiss law
- Start of a competition between TLDs!!!!



(2014/10) Accounts lost, again...



Mitigation:
2-factor authentication

- Enable 2-factor authentication like at Apple (new), LinkedIn (fairly new?), Dropbox, Google (since long), CERN (since a while)

(2014/10) One Last Thing

Nasty SSL 3.0 vuln to be revealed soon – sources

So worrying, no one's breathing a word until patch is out

By Darren Pauli, 14 Oct 2014

37

Internet Security Threat Report 2014

Gird your loins, sysadmins, *The Register* has learned that news of yet another security vulnerability – this time in SSL 3.0 – is probably imminent.

Maintainers have been quiet about the vulnerability in the lead-up to a patch release, which is expected in the late European evening, or not far from high noon Pacific Time.

Details of the problem are under wraps, purportedly due to the severity of the vulnerability. *El Reg* cannot confirm whether or not it is indeed a serious bug as we have not received details of the vuln.

RELATED STORIES

OpenVPN open to pre-auth Bash Shellshock bug research

Update Patch Bash NOW! 'Shellshock' bug

Mitigation: Disable SSL 3.0

http://www.theregister.co.uk/2014/10/14/nasty_ssl_30_vulnerability_to_drop_tomorrow/

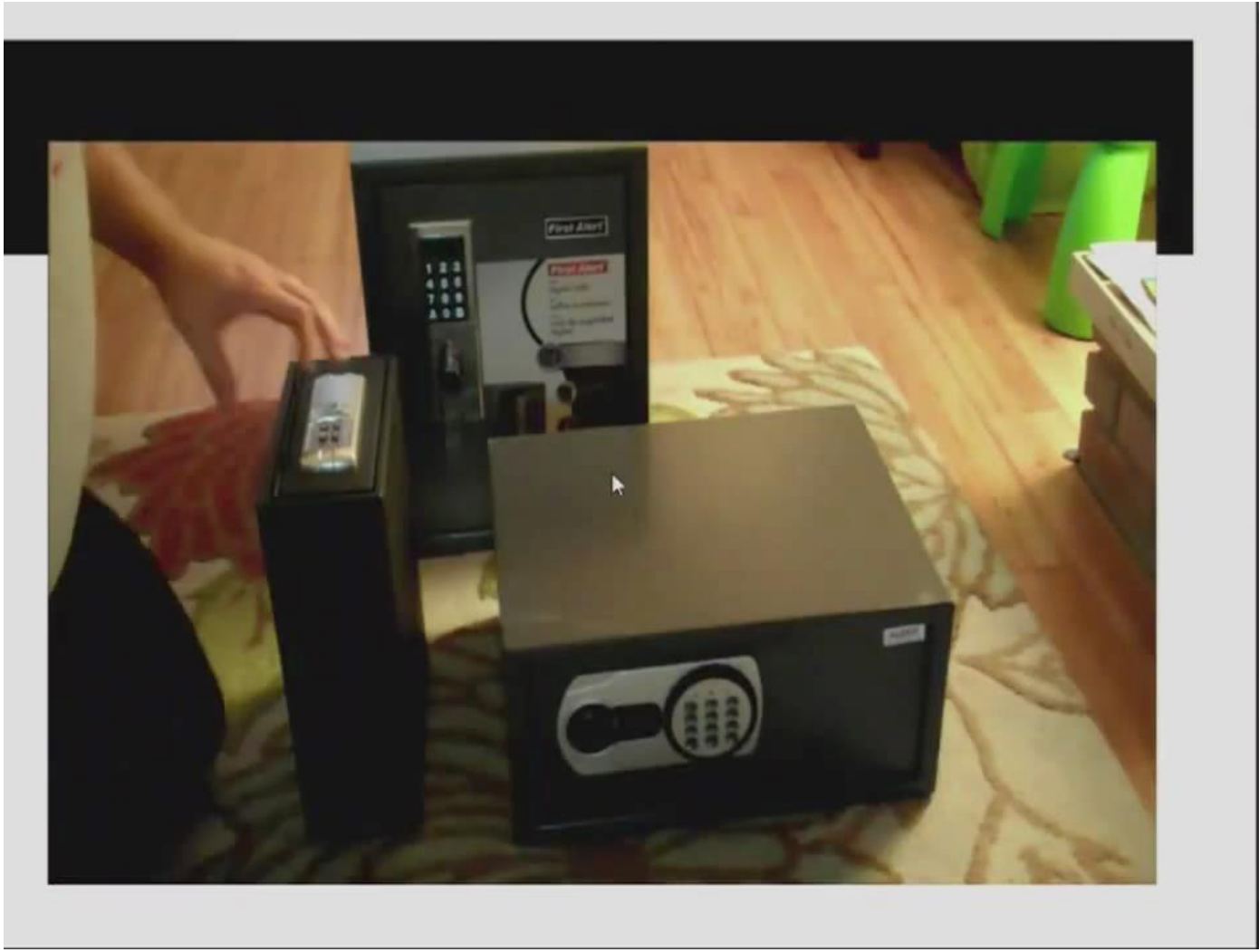
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

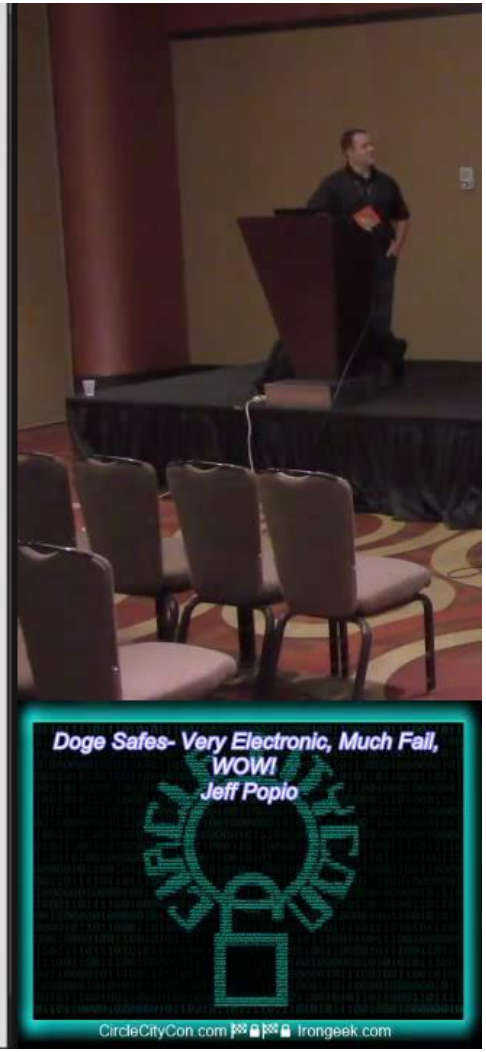
Conclusions

If we want to **win/keep up with this marathon**, we should/must(!)

- More often **choose "security"** instead of "convenience"
- More often **consider "privacy"** instead of "freedom";
- Have deep direct **ties with the community** to learn quickly about the bad (and where it affects us);
- Have good **traceability & logging in place** to figure out whether/where(!) we are affected;
- Have good **configuration management** for prompt and agile patching (data center *and* control systems!);
- Accept that we do not and cannot control the full phase-space. Protection is often difficult/impossible.

Bonus: Failsafe





http://www.irongeek.com/i.php?page=videos/circlecitycon2014/211-doge-safes-very-electronic-much-fail-wow-jeff-popio