Welcome to

Overvågning og hacking

PROSA Stud Svendborg 2014

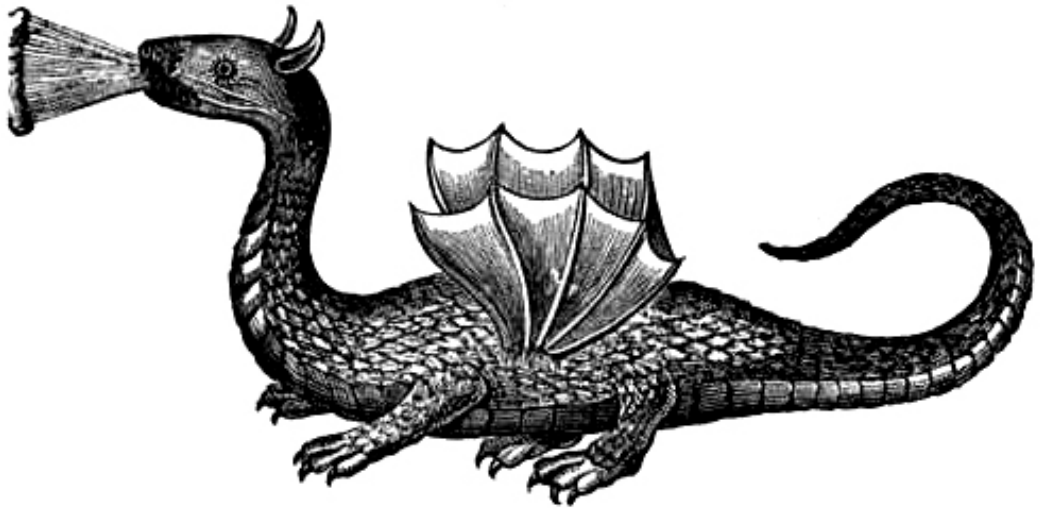
Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Agenda

Internet - Here be dragons



KI 11:30-13:00

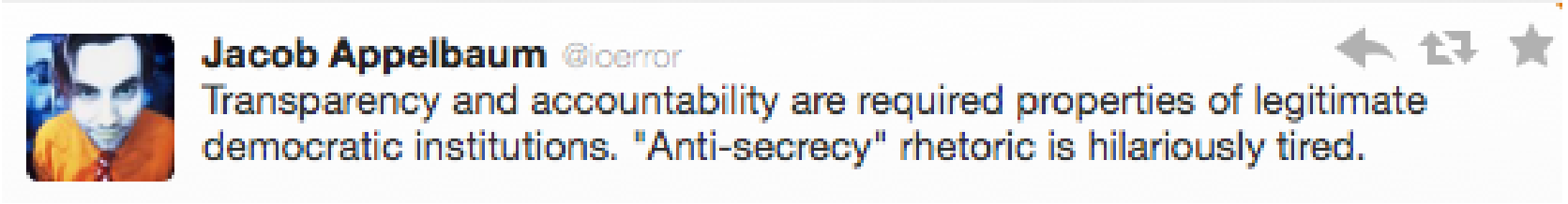
Paranoia defined

What are the risks, vulnerabilities and threats

Reduce risk and mitigate impact

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Goals: Why?



Demokrati: Et frit demokrati fordrer borgere med frihed som har evnen til at tage beslutninger uden konstant at være overvåget.

Et demokrati fordrer borgere som aktivt vælger hvornår de afgiver personlige data om deres liv og færden og kryptografi er en fredelig protest mod indsamling at data.

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Indsamlede data vil altid blive misbrugt

Data som indsamles **bliver misbrugt** enten til kriminelle formål, kommercielle formål uanset oprindelige formål med indsamlingen - under dække af beskyttelse mod terror, ekstremisme, nazisme, misbrug af børn, ... Le mal du jour / dagens onde.

Derudover stalking, ekskærester, arbejdsgivere, forældre, ...

Du bestemmer - det er privatliv og demokrati

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Why think of security?

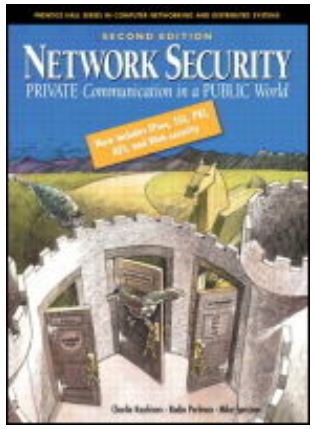
> Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. A Cypherpunk's Manifesto by Eric Hughes, 1993

Copied from `https://cryptoparty.org/wiki/CryptoParty`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Rejsen starter

Hvor skal vi nu starte denne rejse?



Private Communications in an Public World

Anbefalelsesværdig bog som gennemgår grundlaget for kryptering, teknikker og protokollerne der bruges på internet idag, herunder: IPsec, SSL/TLS, PGP, PKI, AES m.fl.

Vi troede krypto kunne hjælpe os med næsten alle problemer ...

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Part I: Paranoia defined

par·a·noi·a

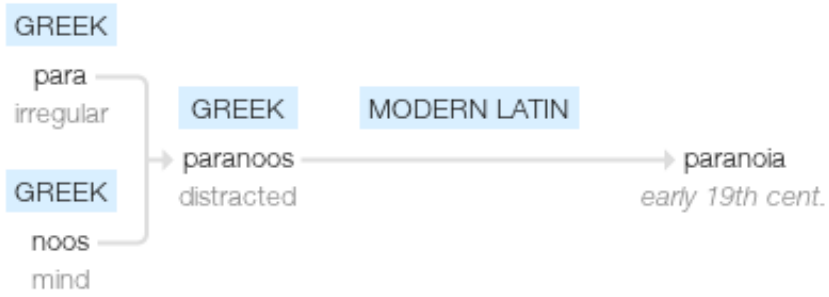
/ˌparəˈnoiə/

noun

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
   synonyms: persecution complex, delusions, obsession, psychosis More
- suspicion and mistrust of people or their actions without evidence or justification.
  "the global paranoia about hackers and viruses"

Origin



More

Source: google paranoia definition

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Face reality

From the definition of paranoia:

> suspicion and mistrust of people or their actions **without evidence or justification**. **”the global paranoia about hackers and viruses”**

It is not paranoia when:

- Criminals sell your credit card information and identity theft
- Hackers trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population
- Governments implement censorship, threaten citizens and journalist
- Governemnts monitor your sexting and naked chats over instant messaging apps
- Companies gather your personal data and sell access
- ... and the list goes on!

You are not paranoid when there are people actively attacking you!

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Risk management defined

Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. ***Information risk management (IRM)*** is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Example UK: Seize smart phones and download data

Officers use counter-terrorism laws to remove a mobile phone from any passenger they wish coming through UK air, sea and international rail ports and then scour their data.

The blanket power is so broad they do not even have to show reasonable suspicion for seizing the device and can retain the information for ”as long as is necessary”.

Data can include call history, contact books, photos and who the person is texting or emailing, although not the contents of messages.

Source: http://www.telegraph.co.uk/technology/10177765/Travellers-mobile-phone-data-seized-by-police-at-border.html

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Example: UK wouldn't seize data like that, you are lying

SOLIDO NETWORKS

> (Reuters) - British authorities came under pressure on Monday to explain why anti-terrorism powers were used to detain for nine hours the partner of a journalist who has written articles about **U.S. and British surveillance programs** based on **leaks from Edward Snowden**.
>
> Brazilian David Miranda, the partner of American journalist Glenn Greenwald, was detained on Sunday at London's Heathrow Airport where he was in transit on his way from Berlin to Rio de Janeiro. **He was released without charge**.

Source:
http://www.reuters.com/article/2013/08/19/us-britain-snowden-detention-idUSBRE97I0J520130819

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Governments blanket surveillance

NSA - need we say more?
`http://en.wikipedia.org/wiki/PRISM_(surveillance_program)`

Governments also implementing censorship, including danish gov.

Outlaw and/or discredit crypto, google: FBI director James Comey

Go after Tor exit nodes and their operators :-(

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Use protection - always

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

A vulnerability can and will be abused

Investigative organizations, like europol, FBI and other want a ”golden key” which they can get with a court order. This cant happen! This wont work. See below link, and Google: clipper chip and crypto wars

What if I told you:

Criminals will be happy to leverage backdoors created by government

It does not matter if the crypto product has a weakness to allow investigations or the software has a backdoor to help law enforcement. Data and vulnerabilities WILL be abused and exploited.

Source: `https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Ånden til at hacke

Don’t Panic!

Hacking betyder idag indbrud, kriminalitet, hærværk m.v.

Oprindeligt betød hacking at man udforskede, undersøgte, involverede sig

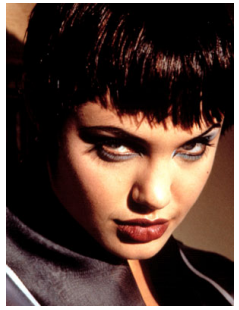
Vi skal bruge ånden fra hacking til forskning, udvikling

Mange regler om at man ikke må noget er imod hacking.

Lad være med at bryde love, men bøj gerne regler ☺

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Hackerværktøjer



- Nmap, Nping - tester porte, godt til firewall admins `http://nmap.org`
- Metasploit Framework gratis på `http://www.metasploit.com/`
- Wireshark avanceret netværkssniffer - `http://http://www.wireshark.org/`
- Burpsuite `http://portswigger.net/burp/`
- Skipfish `http://code.google.com/p/skipfish/`
- OpenBSD operativsystem med fokus på sikkerhed `http://www.openbsd.org`

Kilde: Angelina Jolie fra Hackers 1995

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Kali Linux the new backtrack

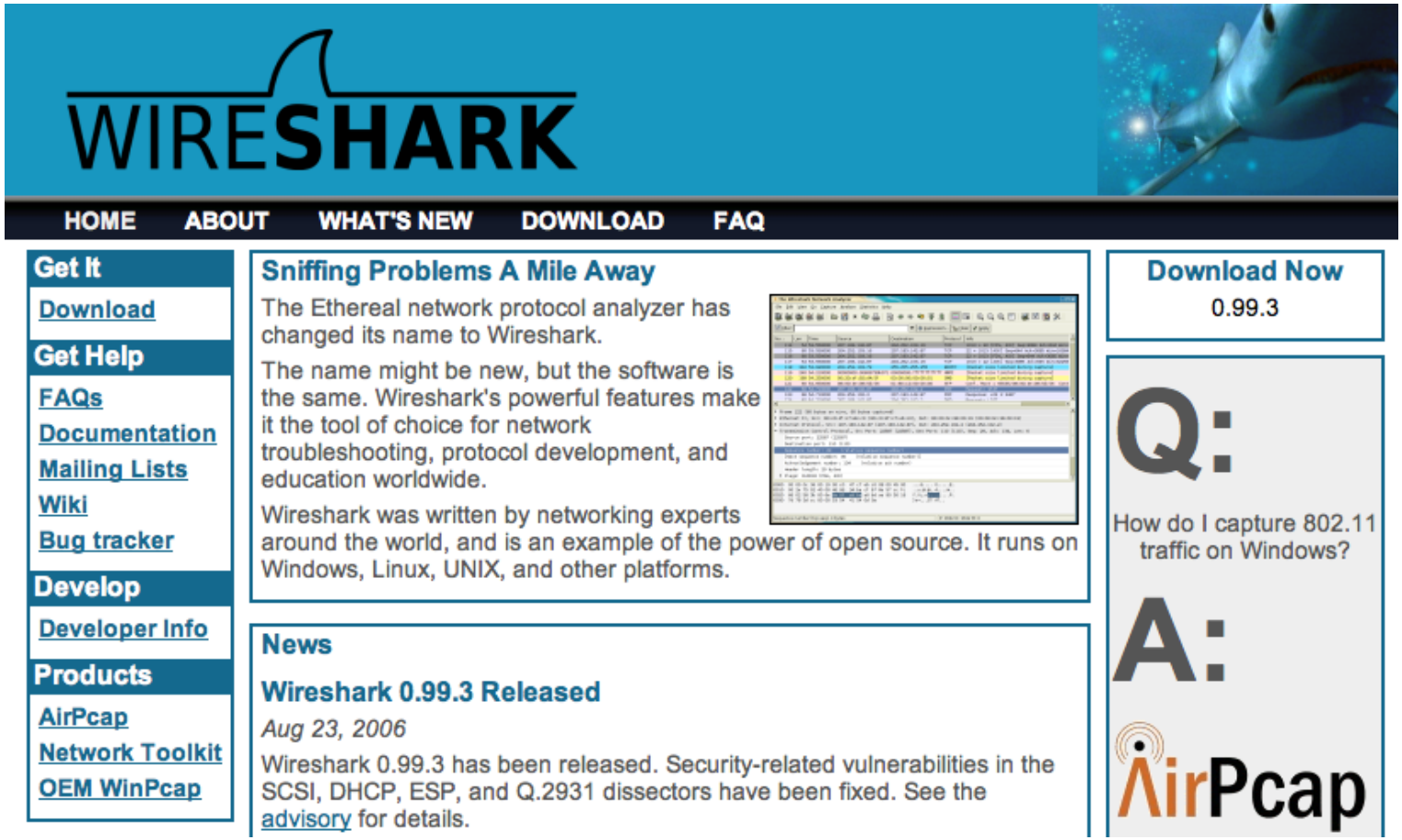
BackTrack `http://www.backtrack-linux.org`

Kali `http://www.kali.org/`

Wireshark - `http://www.wireshark.org` avanceret netværkssniffer

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Wireshark - grafisk pakkesniffer

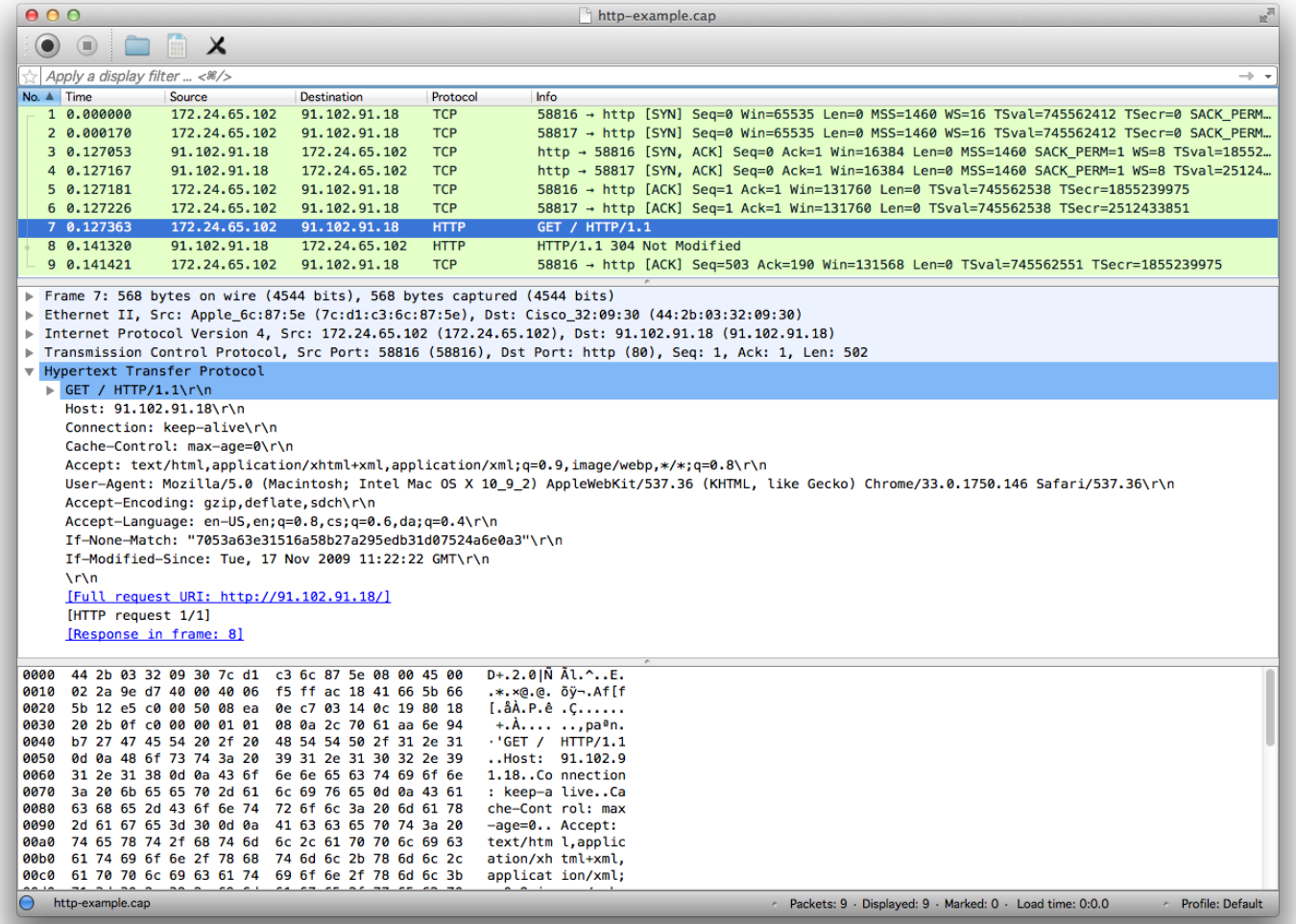


`http://www.wireshark.org`

både til Windows og Unix

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Brug af Wireshark



Læg mærke til filtermulighederne

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Getting to your data: Google for it

Google as a hacker tools?

Concept named googledorks when google indexes information not supposed to be public `http://www.exploit-db.com/google-dorks/` Originally from Johnny Long

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Hacking er magi

Hacking ligner indimellem magi

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

MAC adresser

```
00-03-93    (hex)          Apple Computer, Inc.
000393      (base 16)      Apple Computer, Inc.
                           20650 Valley Green Dr.
                           Cupertino CA 95014
                           UNITED STATES
```

Netværksteknologierne benytter adresser på lag 2

Typisk svarende til 48-bit MAC adresser som kendes fra Ethernet MAC-48/EUI-48

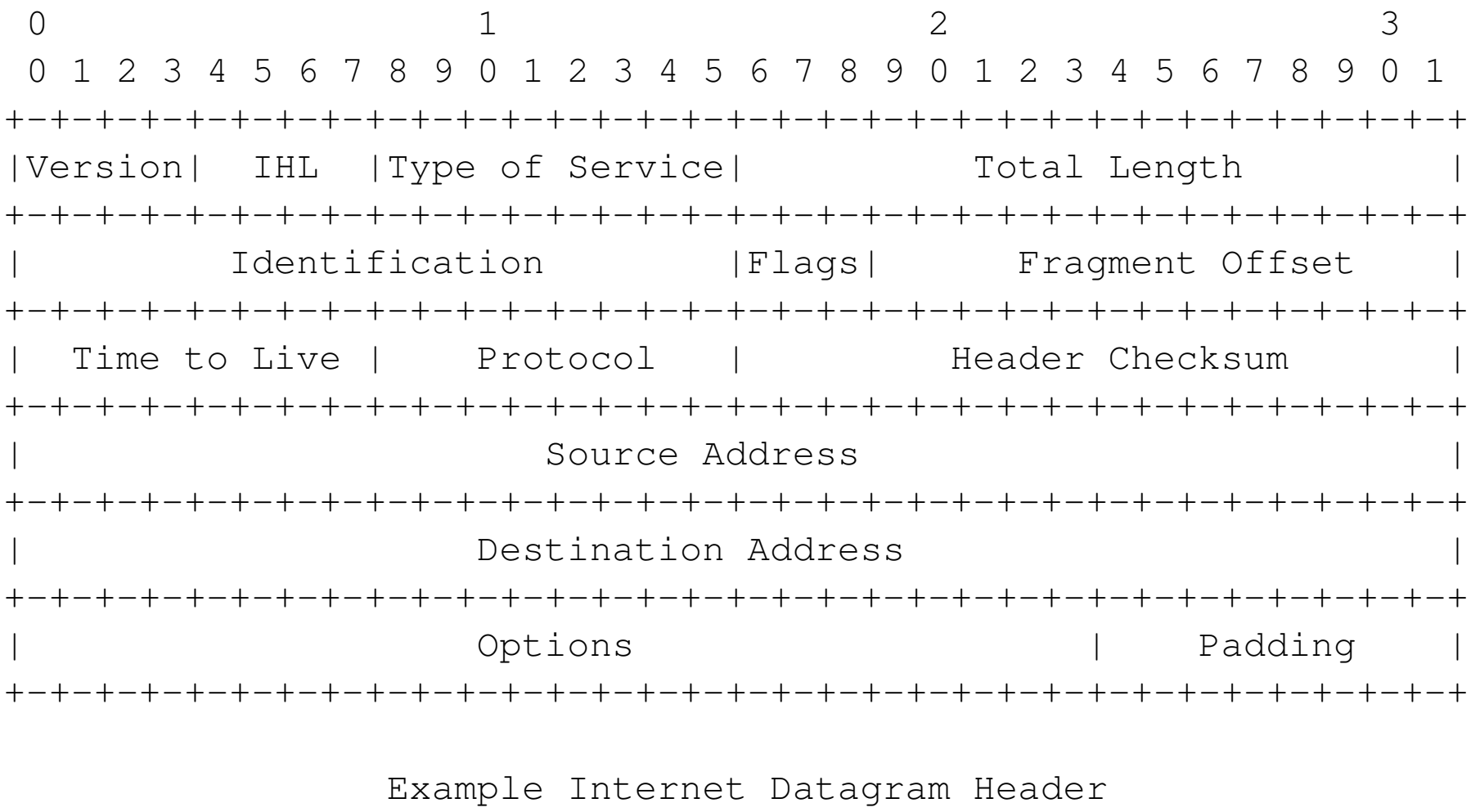
Første halvdel af adresserne er Organizationally Unique Identifier (OUI)

Ved hjælp af OUI kan man udlede hvilken producent der har produceret netkortet

`http://standards.ieee.org/regauth/oui/index.shtml`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

IPv4 pakken - header - RFC-791



Example Internet Datagram Header

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Demo investigating the current network

SOLIDO NETWORKS

Old skool tools: dsniff

one sniffer for old protocols includes **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

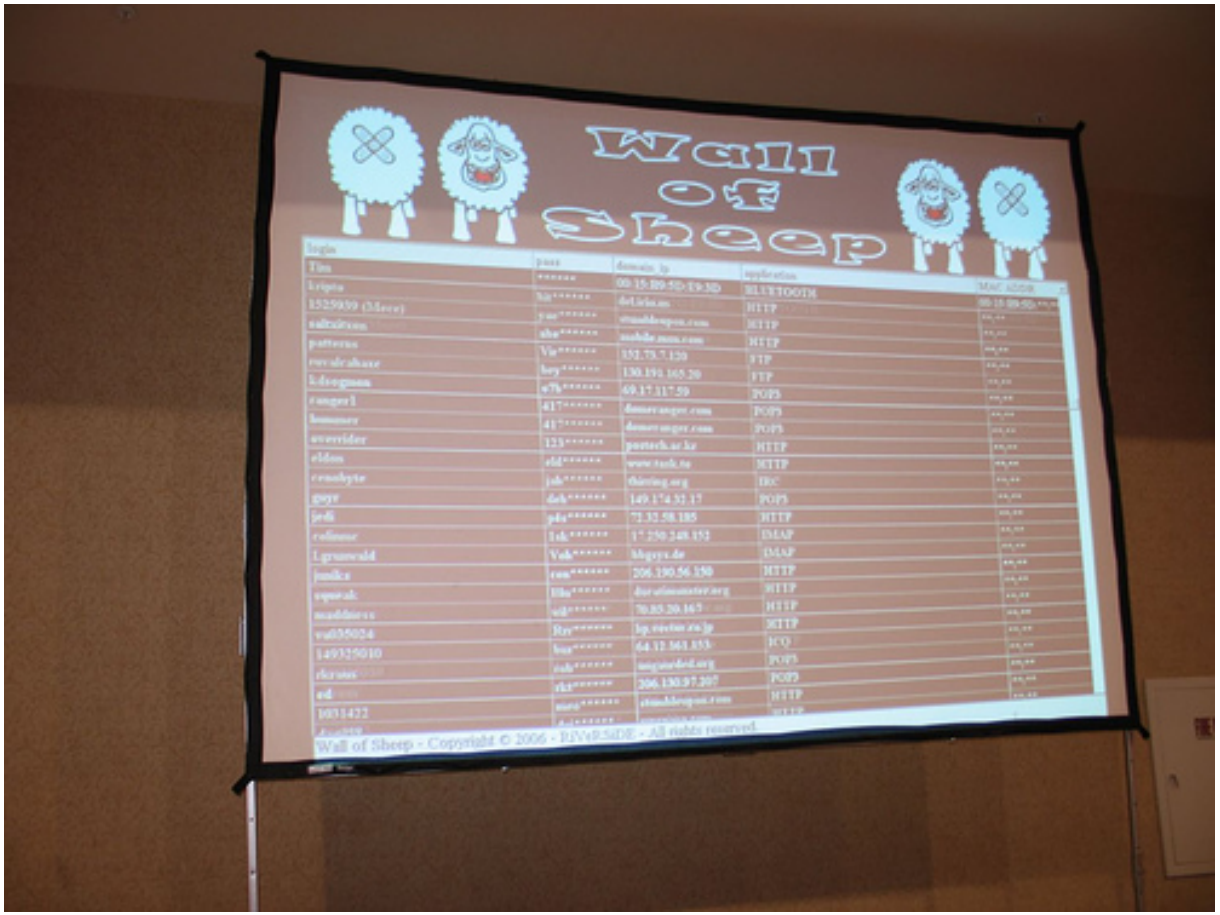
Want a gui, try Ettercap

```
dsniff is a password sniffer which handles FTP, Telnet,
SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,
RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft
SMB, Oracle SQL*Net, Sybase and Microsoft SQL protocols.
```

Note: requires access to network traffic, like open wireless

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Wall of sheep



Defcon Wall of Sheep
Husk nu at vi er venner her! - idag er det kun teknikken

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Quick Wins: Opsec Light

Operations security (OpSec, OPSEC), what do you need?
`https://en.wikipedia.org/wiki/Operations_security`

Great description
”OpSec is about attracting the right amount of attention and not to raise any suspicion.”
`https://www.cryptoparty.at/opsec`

Use multiple devices, isolate data

less critical on phone, most critical on laptop with full disk encryption

Using different password for each service, unpossible!

OTP One Time Password, sniff one and you can use it, if you have a time machine ☺

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Yubico Yubikey

› YubiKey Standard

Our flagship product, making strong two-factor authentication, easy and affordable for everyone.

› YubiKey NEO

Our premium YubiKey, combining USB, NFC, one-time password and PKI technology.

› YubiKey Nano

The world's smallest one-time password token, designed to stay inside the USB-slot.

› YubiKey VIP

A YubiKey Standard pre-configured with a Symantec VIP credential, enabling two-factor authentication against Symantec VIP enabled services, such as PayPal.

› LastPass YubiKey

LastPass Premium is the leading cross platform password manager supporting the YubiKey. We offer a number of discounted bundles of YubiKey + LastPass Premium Subscriptions.

› Password Safe YubiKey

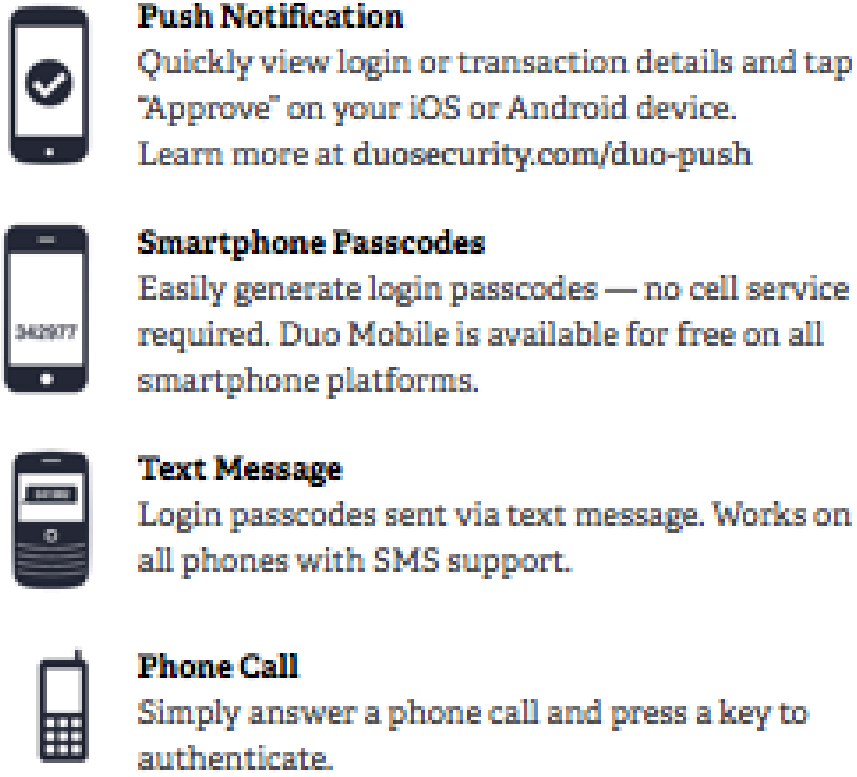
Pasword Safe is an open source password manager initiated by Bruce Schneier. The YubiKey is used in Challenge-response mode to for 2 factor encryption of the database.

A Yubico OTP is unique sequence of characters generated every time the YubiKey button is touched. The Yubico OTP is comprised of a sequence of 32 Modhex characters representing information encrypted with a 128 bit AES-128 key

`http://www.yubico.com/products/yubikey-hardware/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

TwoFactor authentication: Example Duosecurity



Push Notification
Quickly view login or transaction details and tap "Approve" on your iOS or Android device.
Learn more at duosecurity.com/duo-push

Smartphone Passcodes
Easily generate login passcodes — no cell service required. Duo Mobile is available for free on all smartphone platforms.

Text Message
Login passcodes sent via text message. Works on all phones with SMS support.

Phone Call
Simply answer a phone call and press a key to authenticate.

Video `https://www.duosecurity.com/duo-push`

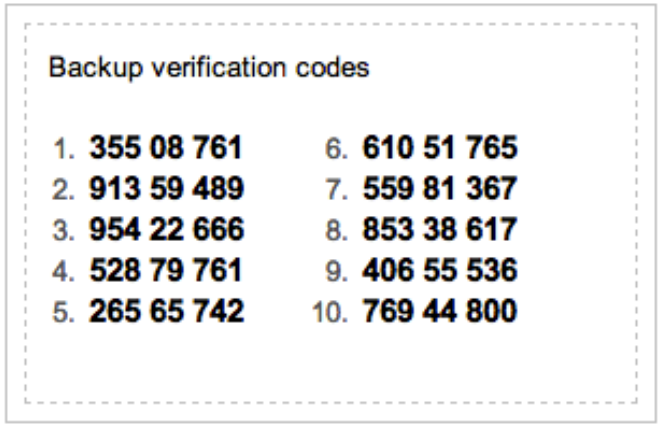
`https://www.duosecurity.com/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Low tech 2-step verification

SOLIDO NETWORKS

Printing code on paper, low level pragmatic



Login from new devices today often requires two-factor - email sent to user

Google 2-factor auth. SMS with backup codes

Also read about S/KEY developed at Bellcore **in the late 1980s**
`http://en.wikipedia.org/wiki/S/KEY`

Conclusion passwords: integrate with authentication, not reinvent

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Integrate or develop?

SOLIDO NETWORKS

Dont:

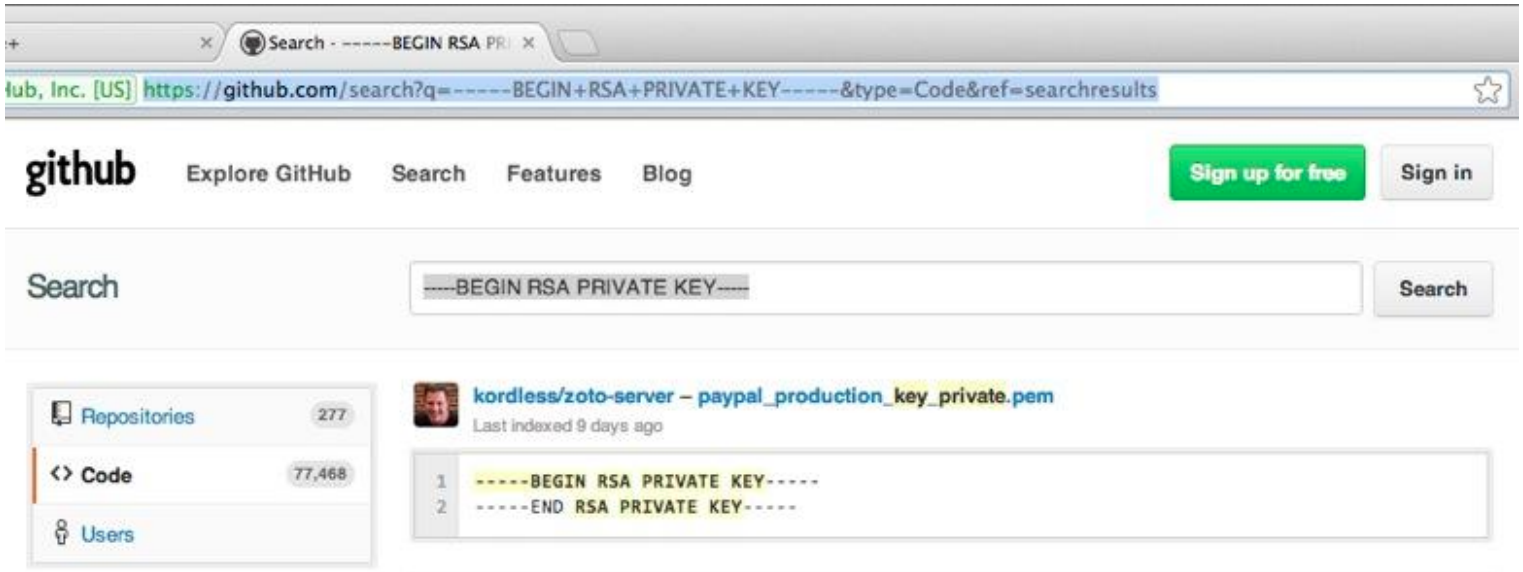
- Reinvent the wheel - too many times, unless you can maintain it afterwards
- Never invent cryptography yourself
- No copy paste of functionality, harder to maintain in the future

Do:

- Integrate with existing solutions
- Use existing well-tested code: cryptography, authentication, hashing
- Centralize security in your code
- Fine to hide which authentication framework is being used, easy to replace later

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

January 2013: Github Public passwords?



Sources:

https://twitter.com/brianaker/status/294228373377515522

http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-de

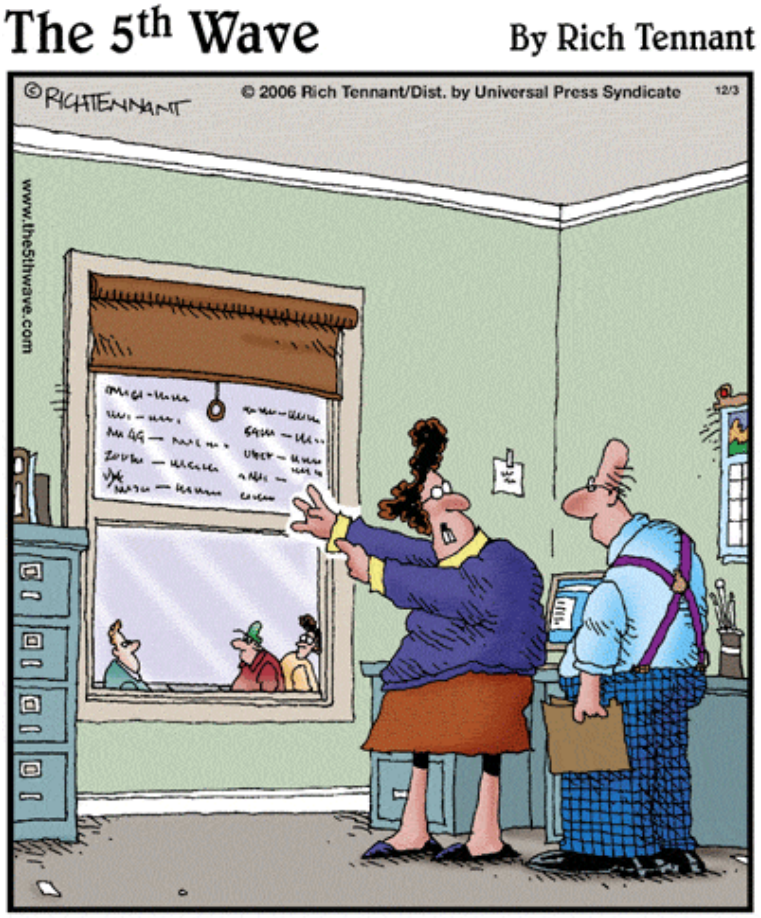
http://www.leakedin.com/

http://www.offensive-security.com/community-projects/google-hacking-database/

Use different passwords for different sites, yes - every site!

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Opbevaring af passwords



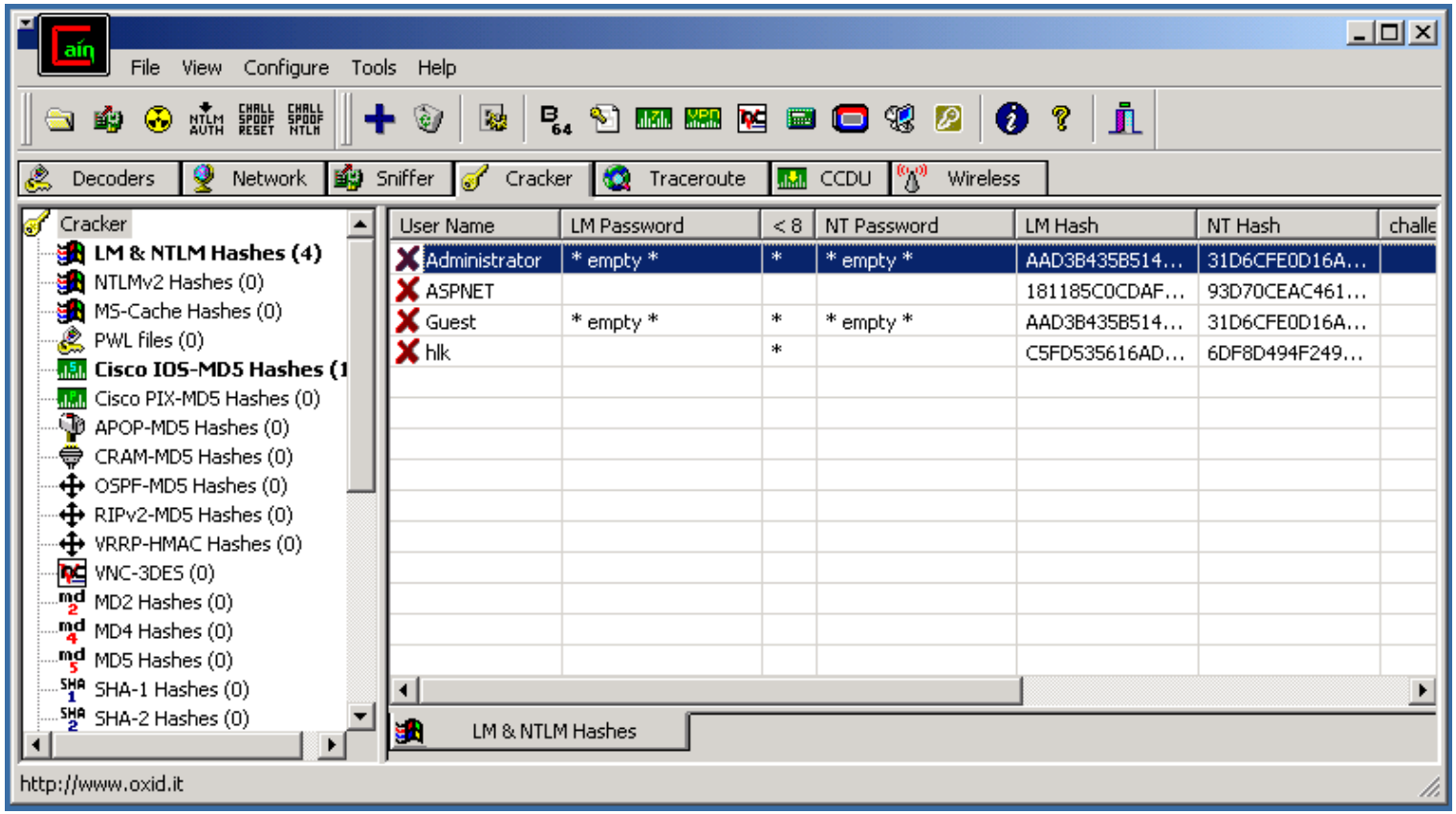
"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

Use some kind of Password Safe program which encrypts your password database

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Cain & Abel

Dont forget that hashes can often be cracked



sniff, crack and hack `http://www.oxid.it`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

John the ripper

> John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.

UNIX passwords kan knækkes med alec Muffets kendte Crack program eller eksempelvis John The Ripper `http://www.openwall.com/john/`

Jeg bruger selv John The Ripper

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Cracking passwords

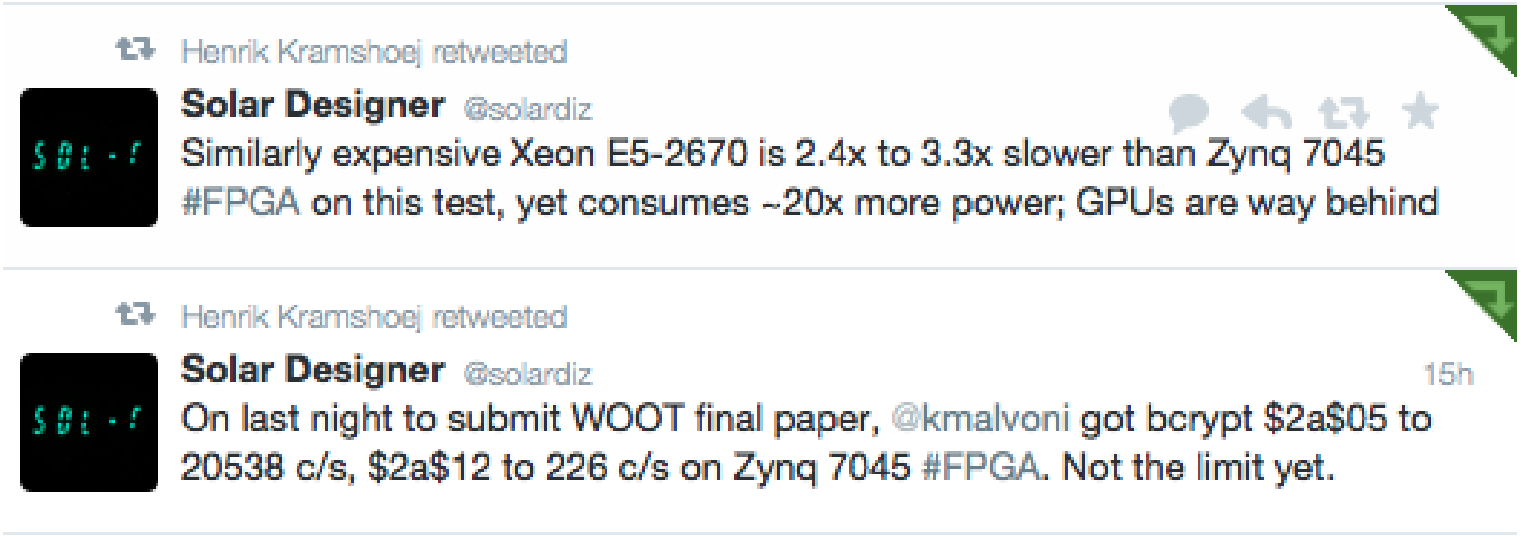
- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:

`http://hashcat.net/wiki/`
`http://www.openwall.com/john/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Parallella John

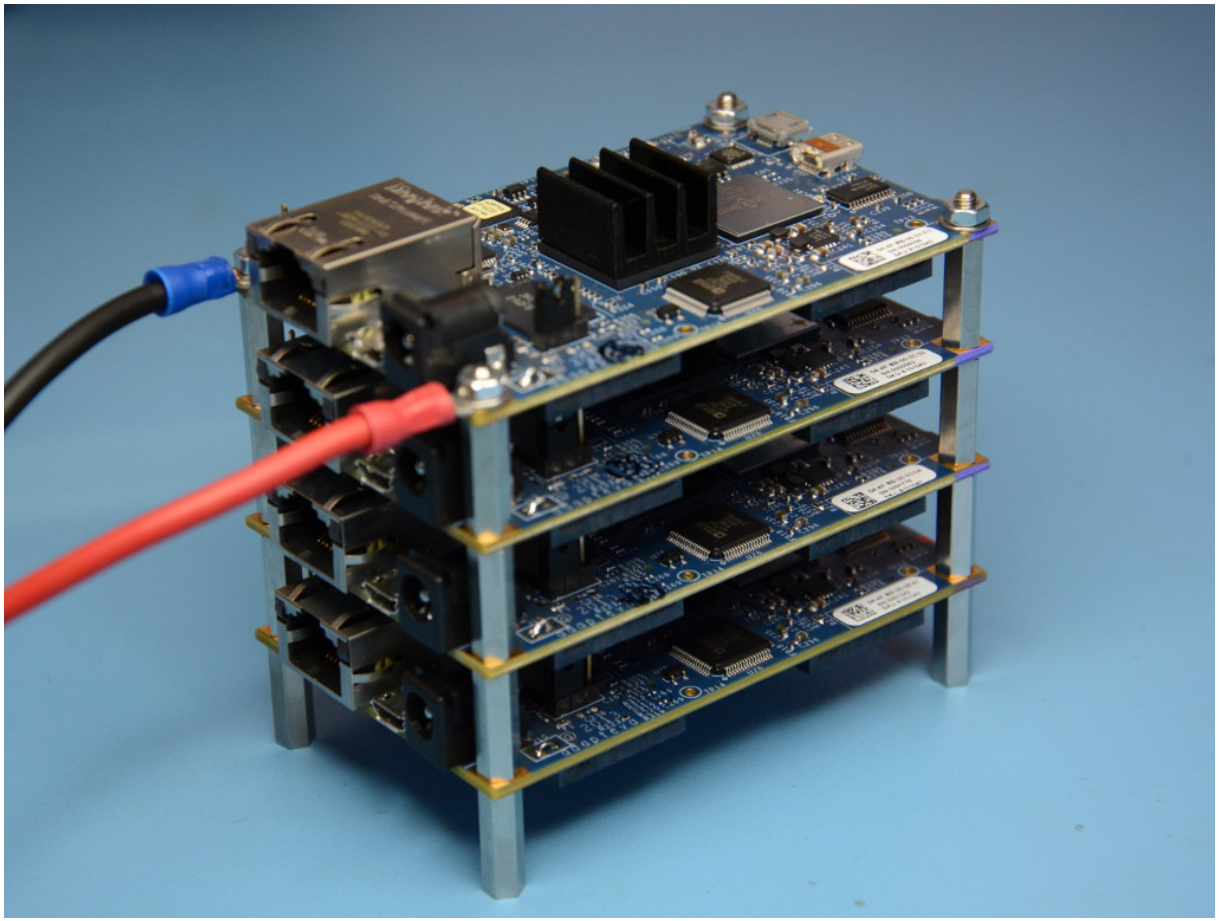


https://twitter.com/solardiz/status/492037995080712192

Warning: FPGA hacking - not finished part of presentation ☺

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

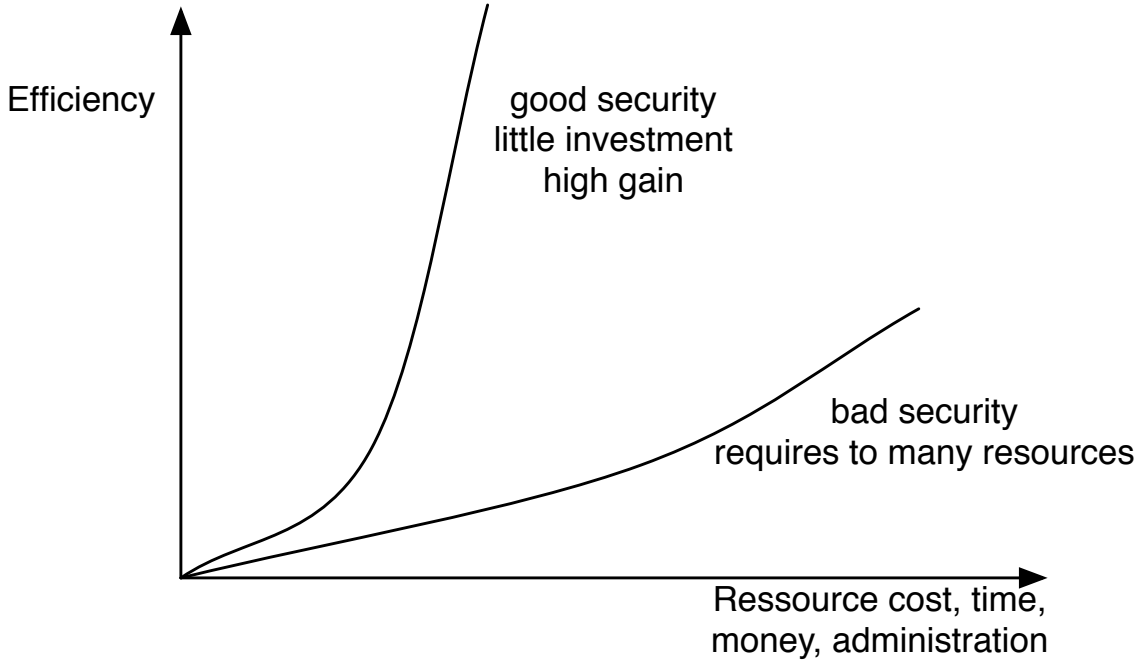
Stacking Parallella boards



http://www.parallella.org/power-supply/

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Good security



You always have limited resources for protection - use them as best as possible

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

First advice

Use technology

Learn the technology - read the freaking manual

Think about the data you have, upload, facebook license?! WTF!

Think about the data you create - nude pictures taken, where will they show up?

- Turn off features you don't use
- Turn off network connections when not in use
- Update software and applications
- Turn on encryption: IMAP**S**, POP3**S**, HTTP**S** also for data at rest, full disk encryption, tablet encryption
- Lock devices automatically when not used for 10 minutes
- Dont trust fancy logins like fingerprint scanner or face recognition on cheap devices

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

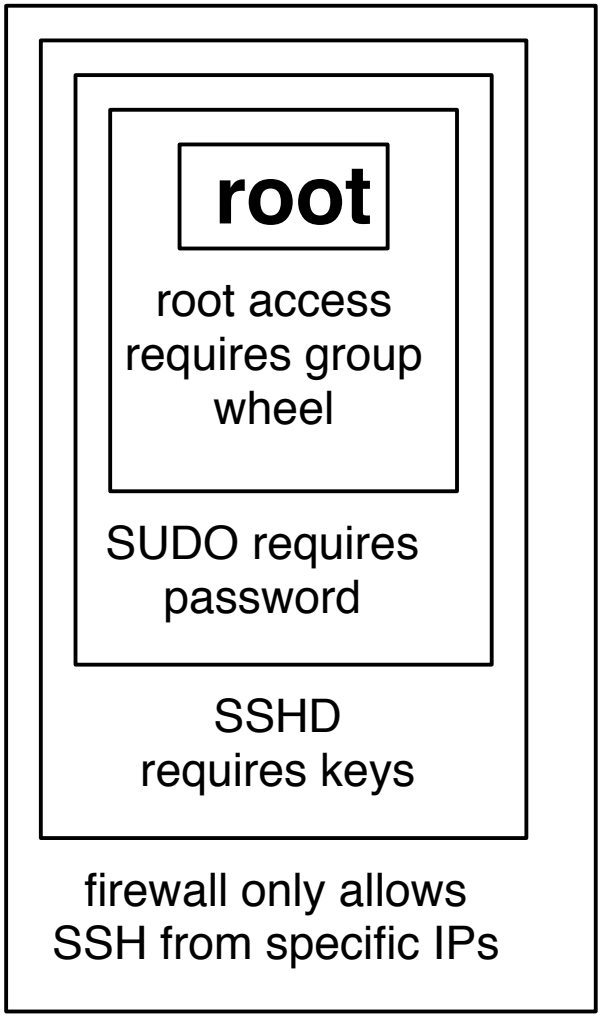
Note: these still have errors and bugs, but are better than older versions

OpenBSD has shown the way in many cases
`http://www.openbsd.org/papers/`

Always try to make life worse and more costly for attackers

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Defense in depth



Defense using multiple layers is stronger!

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Kryptografiske principper

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et successfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid
`http://www.interhack.net/people/cmcurtin/snake-oil-faq.html`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Formålet med kryptering

kryptering er den eneste måde at sikre:

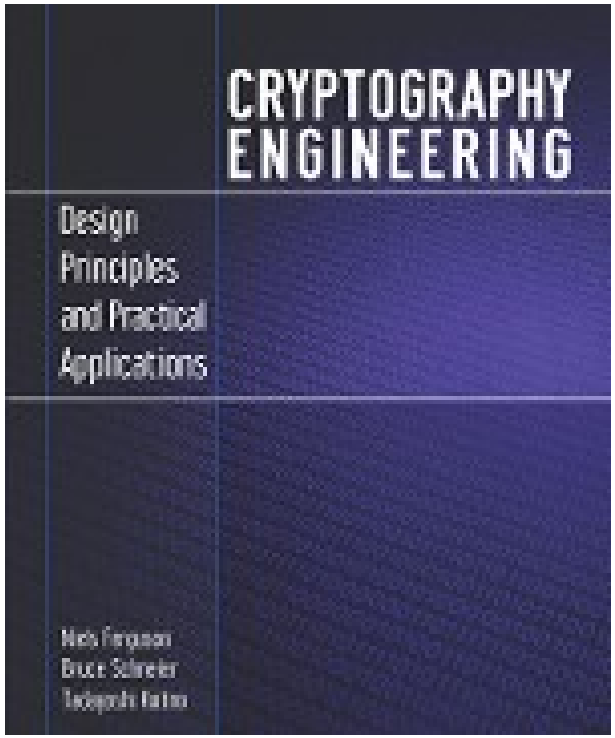
fortrolighed

autenticitet / integritet

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Cryptography Engineering

SOLIDO NETWORKS



Cryptography Engineering by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno

`https://www.schneier.com/book-ce.html`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Sorry, none

> The 'S' in HTTPS stands for 'secure' and the security is provided by SSL/TLS. SSL/TLS is a standard network protocol which is implemented in every browser and web server to provide confidentiality and integrity for HTTPS traffic.

OpenSSL, LibreSSL, Apple SSL flaw exit exit exit!, Android SSL, certs certs cert!!!111, SSLv3, Heartbleed

Sorry, brain overflow from SSL/TLS vulnerabilities

Sources: see my blog posts about heartbleed for more links and tools

`http://www.version2.dk/blog/openssl-er-doed-laenge-leve-libressl-57640`

`http://www.version2.dk/blog/opdater-openssl-og-dit-os-nu-57202`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Heartbleed CVE-2014-0160

The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Source: `http://heartbleed.com/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Heartbleed is yet another bug in SSL products

SOLIDO NETWORKS

What versions of the OpenSSL are affected?
Status of different versions:

* OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
* OpenSSL 1.0.1g is NOT vulnerable
* OpenSSL 1.0.0 branch is NOT vulnerable
* OpenSSL 0.9.8 branch is NOT vulnerable

Bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Why is heartbleed different?

Great PR, name, web site, logo

OpenSSL is very widespread

OpenSSL has been criticized before

The spotlight is now on a lot of products, infrastructure

BOTH Open Source products and Proprietary products hurt by this

TL;DR
OpenSSL is everywhere and an example of our dependency on weak components

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Key points after heartbleed

Source: picture source

`https://www.duosecurity.com/blog/heartbleed-defense-in-depth-part-2`

- Writing SSL software and other secure crypto software is hard
- Configuring SSL is hard
  check you own site `https://www.ssllabs.com/ssltest/`
- SSL is hard, finding bugs ”all the time” `http://armoredbarista.blogspot.dk/2013/01/a-brief-chronology-of-ssltls-attacks.html`
- Rekeying is hard - slow, error prone, manual proces - Automate!
- Proof of concept programs exist - god or bad?

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Proof of concept programs exist - god or bad?

SOLIDO NETWORKS

Some of the tools released shortly after Heartbleed announcement

- https://github.com/FiloSottile/Heartbleed tool i Go
  site http://filippo.io/Heartbleed/
- https://github.com/titanous/heartbleeder tool i Go
- http://s3.jspenguin.org/ssltest.py PoC
- https://gist.github.com/takeshixx/10107280 test tool med STARTTLS support
- http://possible.lv/tools/hb/ test site
- https://twitter.com/richinseattle/status/453717235379355649 Practical Heartbleed attack against session keys links til, https://www.mattslifebytes.com/?p=533 og "Fully automated here "
  https://www.michael-p-davis.com/using-heartbleed-for-hijacking-user-sessio
- Metasploit er også opdateret på master repo
  https://twitter.com/firefart/status/453758091658792960
  https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliar
  scanner/ssl/openssl_heartbleed.rb

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Heartbleed hacking

```
06b0: 2D 63 61 63 68 65 0D 0A 43 61 63 68 65 2D 43 6F  -cache..Cache-Co
06c0: 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D  ntrol: no-cache.
06d0: 0A 0D 0A 61 63 74 69 6F 6E 3D 67 63 5F 69 6E 73  ...action=gc_ins
06e0: 65 72 74 5F 6F 72 64 65 72 26 62 69 6C 6C 6E 6F  ert_order&billno
06f0: 3D 50 5A 4B 31 31 30 31 26 70 61 79 6D 65 6E 74  =PZK1101&payment
0700: 5F 69 64 3D 31 26 63 61 72 64 5F 6E 75 6D 62 65  _id=1& card_numbe
0710: XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX   r=4060xxxx413xxx
0720: 39 36 26 63 61 72 64 5F 65 78 70 5F 6D 6F 6E 74  96&card_exp_mont
0730: 68 3D 30 32 26 63 61 72 64 5F 65 78 70 5F 79 65  h=02&card_exp_ye
0740: 61 72 3D 31 37 26 63 61 72 64 5F 63 76 6E 3D 31  ar=17&card_cvn=1
0750: 30 39 F8 6C 1B E5 72 CA 61 4D 06 4E B3 54 BC DA  09.l..r.aM.N.T..
```

- Obtained using Heartbleed proof of concepts - Gave full credit card details
- ”can XXX be exploited” - yes, clearly! PoCs ARE needed
  without PoCs even Akamai wouldn’t have repaired completely!
- The internet was ALMOST fooled into thinking getting private keys
  from Heartbleed was not possible - scary indeed.

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Analysis of the heartbleed bug

SOLIDO NETWORKS

- analyse af problemet i koden
  `http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html`
- IDS regler Detecting OpenSSL Heartbleed with Suricata
  `http://blog.inliniac.net/2014/04/08/detecting-openssl-heartbleed-with-suricata/`
- god beskrivelse af hvordan man kan fixe hurtigere hvis man har automatiseret infrastruktur
  `https://www.getpantheon.com/heartbleed-fix`
- Mange blogindlæg om emnet - eksempelvis
  `http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/`
- ”nse script ssl-heartbleed.nse committed to nmap as rev 32798. ”
- You can now use Masscan to scan the whole internet for the Hearbleed vulnerability in under 6 minutes `https://twitter.com/jedisct1/status/453679529710460928`
  `https://github.com/robertdavidgraham/masscan/commit/23497c448b0a1c7058e8443e5202e7bffcab47`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

```
ssl_prefer_server_ciphers on;
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive
ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+\
  \aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!\
  \eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256\
  \-SHA:CAMELLIA128-SHA:AES128-SHA';
add_header Strict-Transport-Security max-age=15768000; # six months
# use this only if all subdomains support HTTPS!
# add_header Strict-Transport-Security "max-age=15768000; includeSubDomains";
```

Listing 2.6: *SSL settings for nginx*
[configuration/Webservers/nginx/default]

Overview

This whitepaper arose out of the need for system administrators to have an updated, solid, well researched and thought-through guide for configuring SSL, PGP, SSH and other cryptographic tools in the post-Snowden age. ... This guide is specifically written for these system administrators.

`https://bettercrypto.org/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Heartbleed Conclusions

Nothing new, but more focus on problems?
Really is there something new in this?

Software has bugs - stay vigilant, implement defense in depth

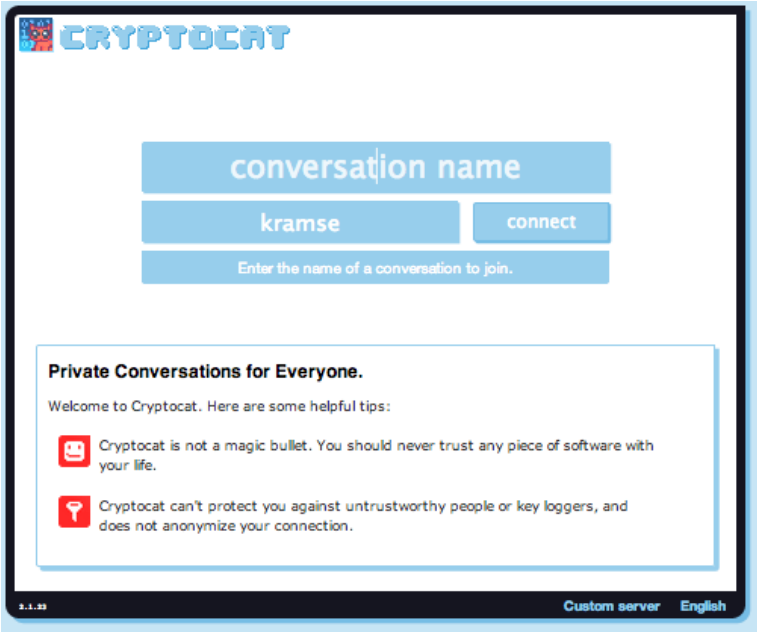
Software need funding - especially software used in our critical systems

Security needs proof of concepts and open communication
Akamai fix that wasn't good enough!

TL;DR Fund more security audits, stop using untested/unaudited software

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Audits



Truecrypt audit

`https://isecpartners.github.io/news/2014/04/14/iSEC-Completes-Truecrypt-Audit.html`

Cryptocat audit

`https://blog.crypto.cat/2013/02/cryptocat-passes-security-audit-with-flying-colors/`

Secure products need funding! Donate to multiple including OpenBSD

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Compare SSL

SOLIDO NETWORKS

```
/* Read type and payload length first */
  if (1 + 2 + 16 > s->s3->rrec.length)
      return 0; /* silently discard */
  hbtype = *p++;
  n2s(p, payload);
  if (1 + 2 + payload + 16 > s->s3->rrec.length)
      return 0; /* silently discard per RFC 6520 sec. 4 */
  pl = p;
```

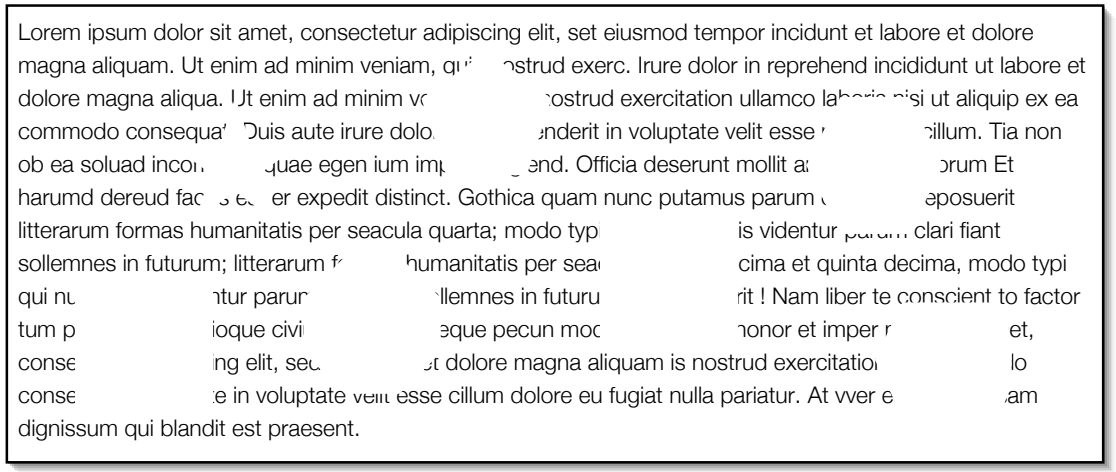
Ditch OpenSSL - write our own?

SSL implementations compared - above code from OpenSSL copied from this:
`http://tstarling.com/blog/2014/04/ssl-implementations-compared/`

LibreSSL announced, OpenBSD people
`http://www.libressl.org/` and `http://opensslrampage.org/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Are your data secure



Stolen laptop, tablet, phone - can anybody read your data?

Do you trust ”remote wipe”

How do you in fact wipe data securely off devices, and SSDs?

Encrypt disk and storage devices before using them in the first place!

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Circumvent security - single user mode boot

Unix systems often allows boot into singleuser mode
press command-s when booting Mac OS X

Laptops can often be booted using PXE network or CD boot

Mac computers can become a Firewire disk
hold t when booting - firewire target mode

Unrestricted access to un-encrypted data

Moving hard drive to another computer is also easy

Physical access is often - **game over**

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Mac OS X

Firewire target mode: Macbook disken kan tilgås fra en anden Mac

Press t to enter firewire target mode ☺

`http://support.apple.com/kb/ht1661`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Encrypting hard disk

Becoming available in the most popular client operating systems

- Microsoft Windows Bitlocker - requires Ultimate or Enterprise
- Apple Mac OS X - FileVault og FileVault2
- FreeBSD GEOM og GBDE/GELI - encryption framework
- Linux distributions like Ubuntu ask to encrypt home dir during installation
- PGP disk - Pretty Good Privacy - makes a virtuel krypteret disk
- TrueCrypt - similar to PGP disk, a virtual drive with data, cross platform *Let's audit Truecrypt!* Note: truecrypt halted and insecure? who knows?
  `http://blog.cryptographyengineering.com/2013/10/lets-audit-truecrypt.html`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Attacks on disk encryption

SOLIDO NETWORKS

Firewire, DMA & Windows, Winlockpwn via FireWire
Hit by a Bus: Physical Access Attacks with Firewire Ruxcon 2006

Removing memory from live system - data is not immediately lost, and can be read under some circumstances
Lest We Remember: Cold Boot Attacks on Encryption Keys
`http://citp.princeton.edu/memory/`

This is very CSI or Hollywoord like - but a real threat

VileFault decrypts encrypted Mac OS X disk image files
`https://code.google.com/p/vilefault/`

FileVault Drive Encryption (FVDE) (or FileVault2) encrypted volumes
`https://code.google.com/p/libfvde/`

So perhaps use both hard drive encryption AND turn off computer after use?

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Theft - kindergarten and airports

Many parents are in a hurry when they are picking up their kids

Many people can easily be distracted around crowds

Many people let their laptops stay out in the open - even at conferences

... making theft likely/easy

Stolen for the value of the hardware - or for the data?

Industrial espionage, economic espionage or corporate espionage is real

Security breaches happens any day of the week

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Kom igang!

- Skriv på DVD - DVD brændere i mange laptops idag
- Gem på netværket - Dropbox, husk en yderligere backup!
- Brug Duplicity på egen server, eller tilsvarende services

Mat Honan epic hacking :-(

`http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

What is it?

Duplicity backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because duplicity uses **GnuPG** to encrypt and/or sign these archives, they will be safe from spying and/or modification by the server.

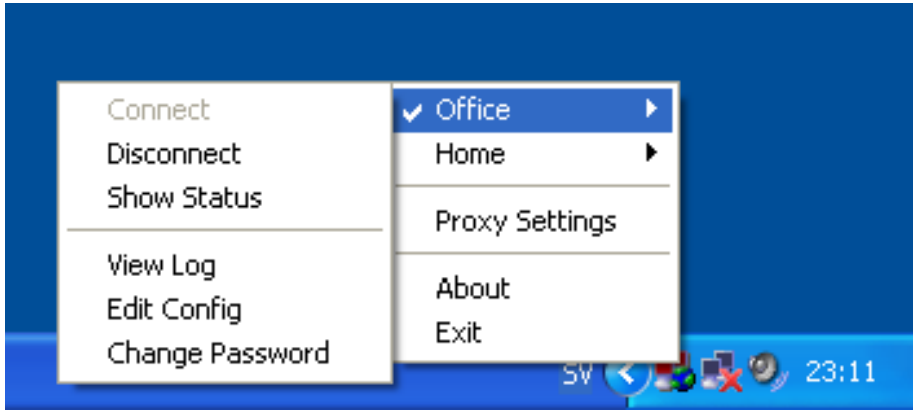
`http://duplicity.nongnu.org/` duplicity home page

`http://www.gnupg.org/` The GNU Privacy Guard

Dont forget to DELETE data also, write over or physically destroy

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Use VPN!



Virtual Private Networks are **useful** - or even **required when traveling**

VPN `http://en.wikipedia.org/wiki/Virtual_private_network`

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

IETF IPsec does work cross-vendors - sometimes, and is also increasingly becoming blocked or unusable due to NAT :-(

Note: your VPN provider may be forced to give up your identity and traffic, beware!

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Multiple browsers

- Strict Security settings in the general browser, Firefox or Chrome?
- More lax security settings for ”trusted sites” - like home banking
- Security plugins like HTTPS Everywhere and NoScripts for generic browsing

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

HTTPS Everywhere

HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`http://www.eff.org/https-everywhere`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Objective:

Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name.

DNS-based Authentication of Named Entities (dane)

`https://datatracker.ietf.org/wg/dane/charter/`

`http://googleonlinesecurity.blogspot.dk/2011/04/improving-ssl-certificate-security.html`

DNSSEC er ved at være godt udbredt - undtagen i DK

(findes på .dk zonen, men næsten ingen resolvere)

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Censurfridns.dk uncensoredDNS

```
http://www.censurfridns.dk

www.censurfridns.dk

Welcome to www.censurfridns.dk. You are welcome to use:

anycast.censurfridns.dk / 91.239.100.100 / 2001:67c:28a4::
ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::
as a resolver to avoid DNS censorship.
Please see blog.censurfridns.dk/en for more information.
```

Det er uacceptabelt at pille ved DNS - punktum!

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

DNSSEC trigger

Der findes mange DNSSEC programmer, blandt andet DNSSEC-trigger som er en navneserver til din lokale PC

- DNSSEC Validator for firefox
  `https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/`
- OARC tools `https://www.dns-oarc.net/oarc/services/odvr`
- `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Tor project

`https://www.torproject.org/`

Der findes alternativer, men Tor er mest kendt

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Turkey: Erdogan bans Twitter

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Censorship on the internet - lol

The Net interprets censorship as damage and routes around it.

John Gilmore

John Gilmore is an American computer science innovator, Libertarian, Internet activist, and one of the founders of Electronic Frontier Foundation. He created the alt.* hierarchy in Usenet and is a major contributor to the GNU project.

*This **scientist** article is a stub. You can help Wikiquote by expanding it.*

Sourced [edit]

- **The Net interprets censorship as damage and routes around it.**
  - As quoted in *TIME* magazine (6 December 1993)
  - Unsourced variant:

    The Net treats censorship as a defect and routes around it.
- How many of you have broken no laws this month?
  - As quoted in a speech to the First Conference on Computers, Freedom, and Privacy in 1991
- If you're watching everybody, you're watching nobody.
  - As quoted in Subject: [IP] John Gilmore on government trustworthiness and spy gear
- **When the X500 revolution comes, your name will be lined against the wall and shot.**
  - As quoted in Peter Gutmann's X509 style guide

The Net interprets censorship as damage and routes around it.

http://en.wikiquote.org/wiki/John_Gilmore
http://en.wikipedia.org/wiki/John_Gilmore_(activist)

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Directly connection Tor Users from Turkey

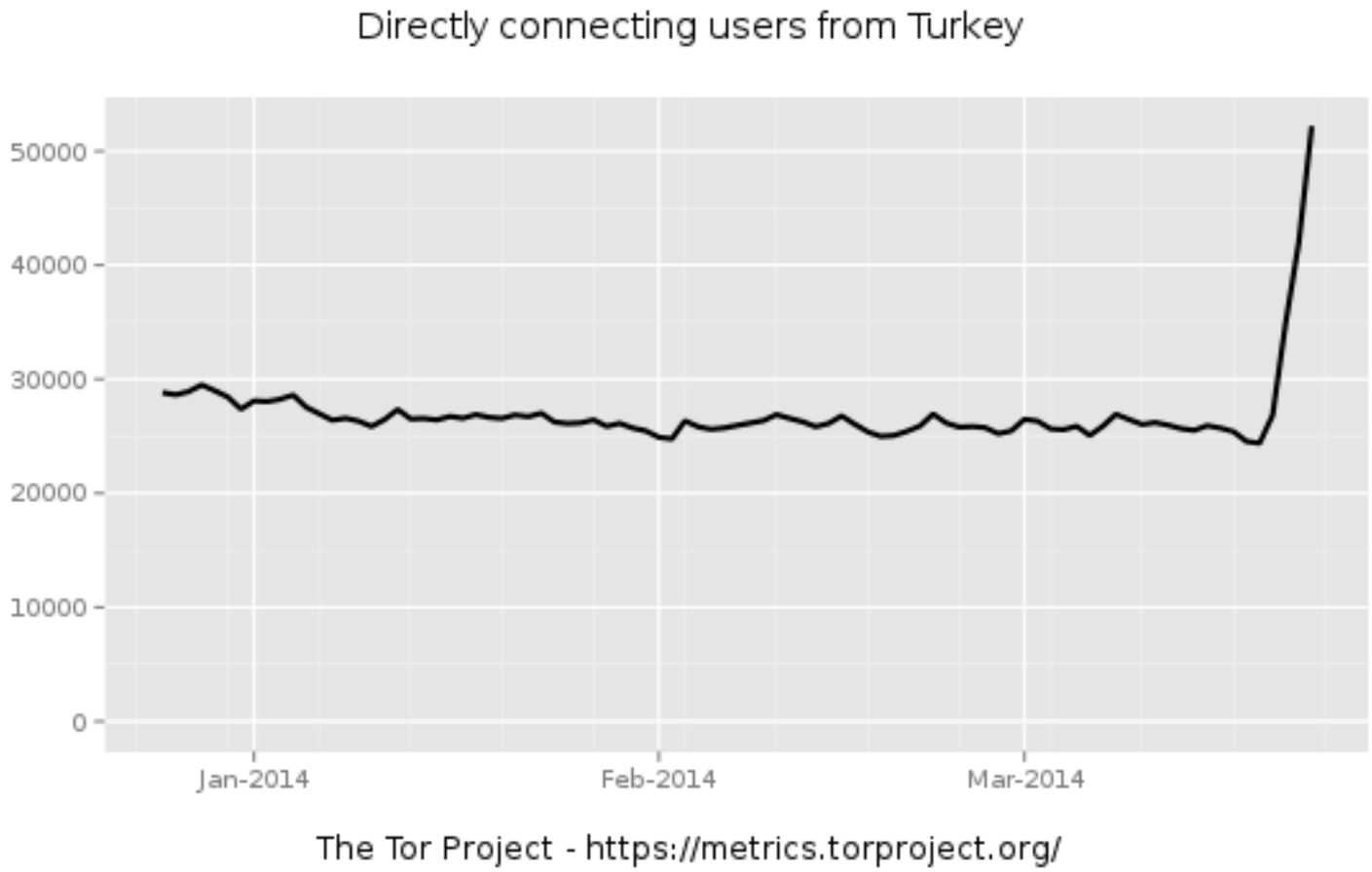


Image from `https://metrics.torproject.org`
via `https://twitter.com/runasand`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Directly connection Tor Users from Turkey +10.000

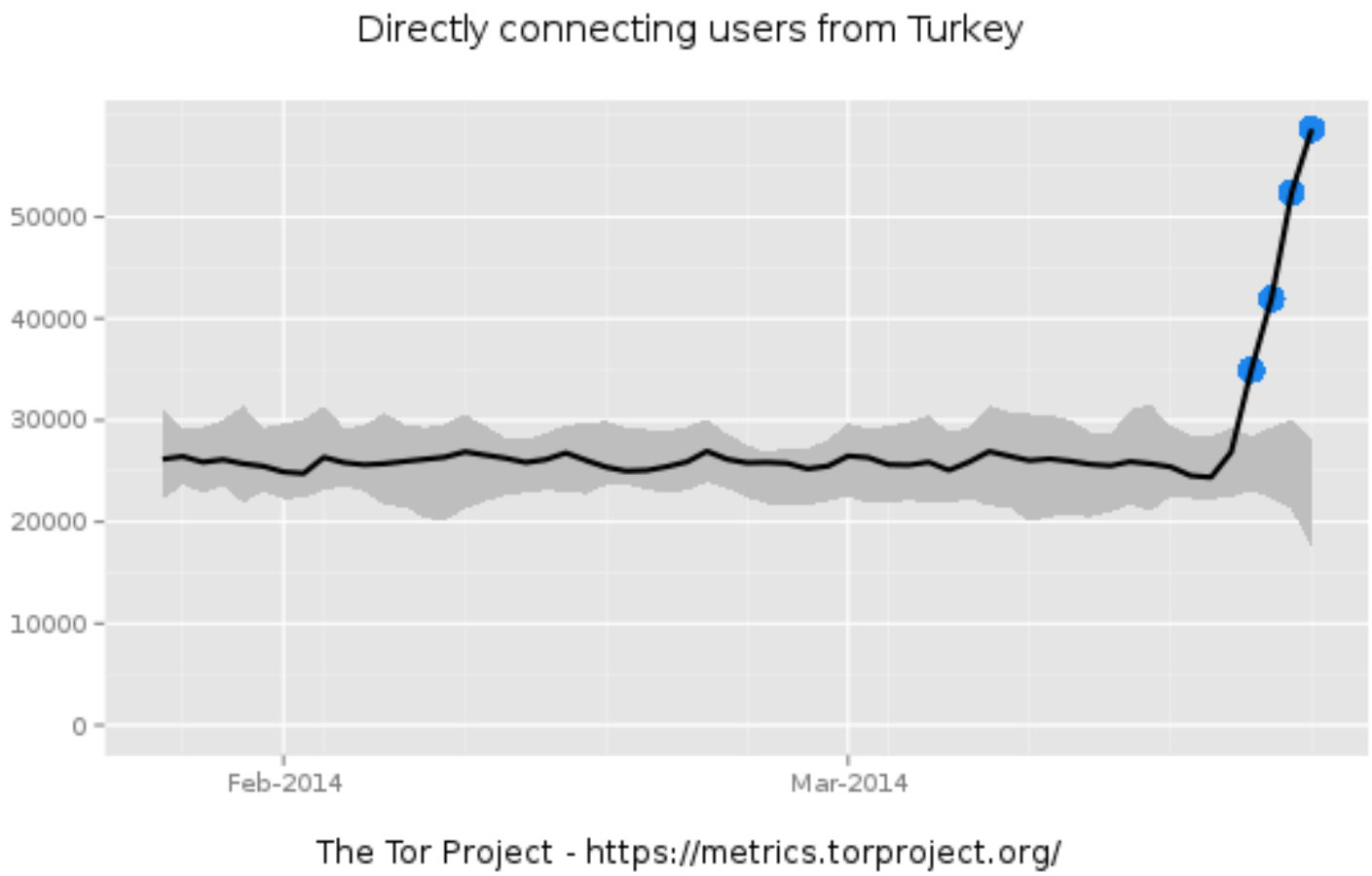
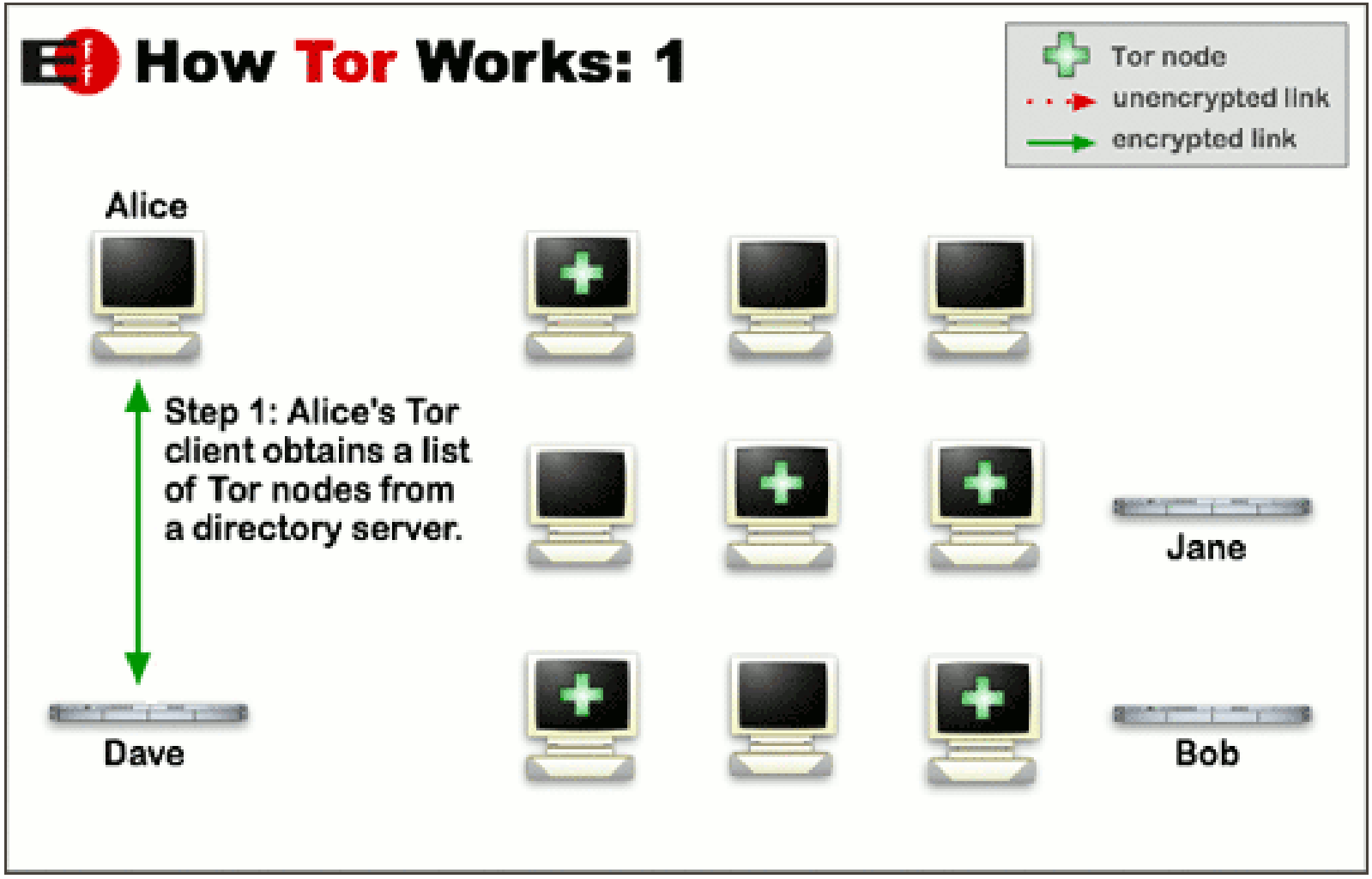


Image from `https://metrics.torproject.org` via `https://twitter.com/ioc32/status/448791582423408640`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

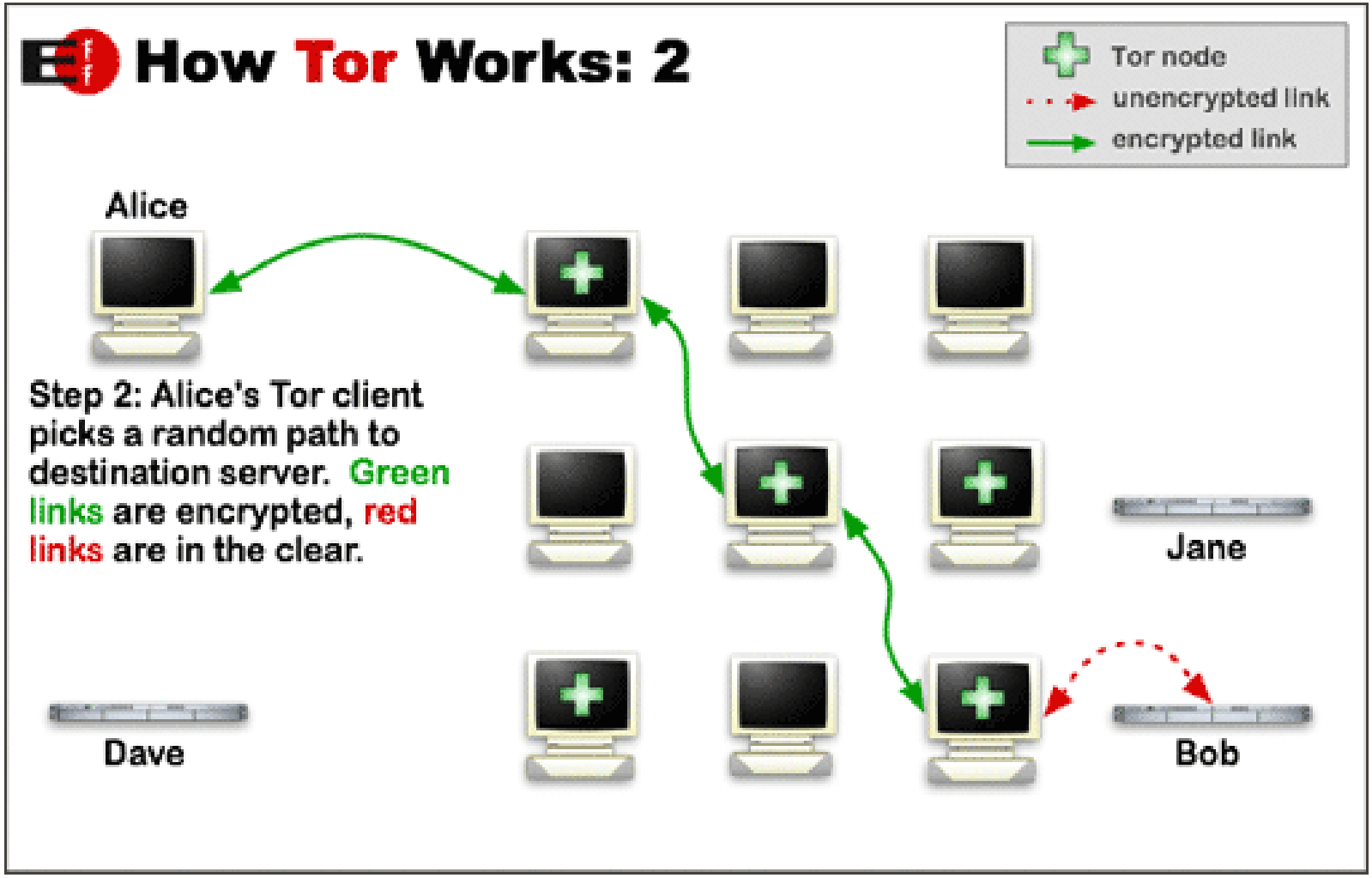
Tor project - how it works 1



pictures from `https://www.torproject.org/about/overview.html.en`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

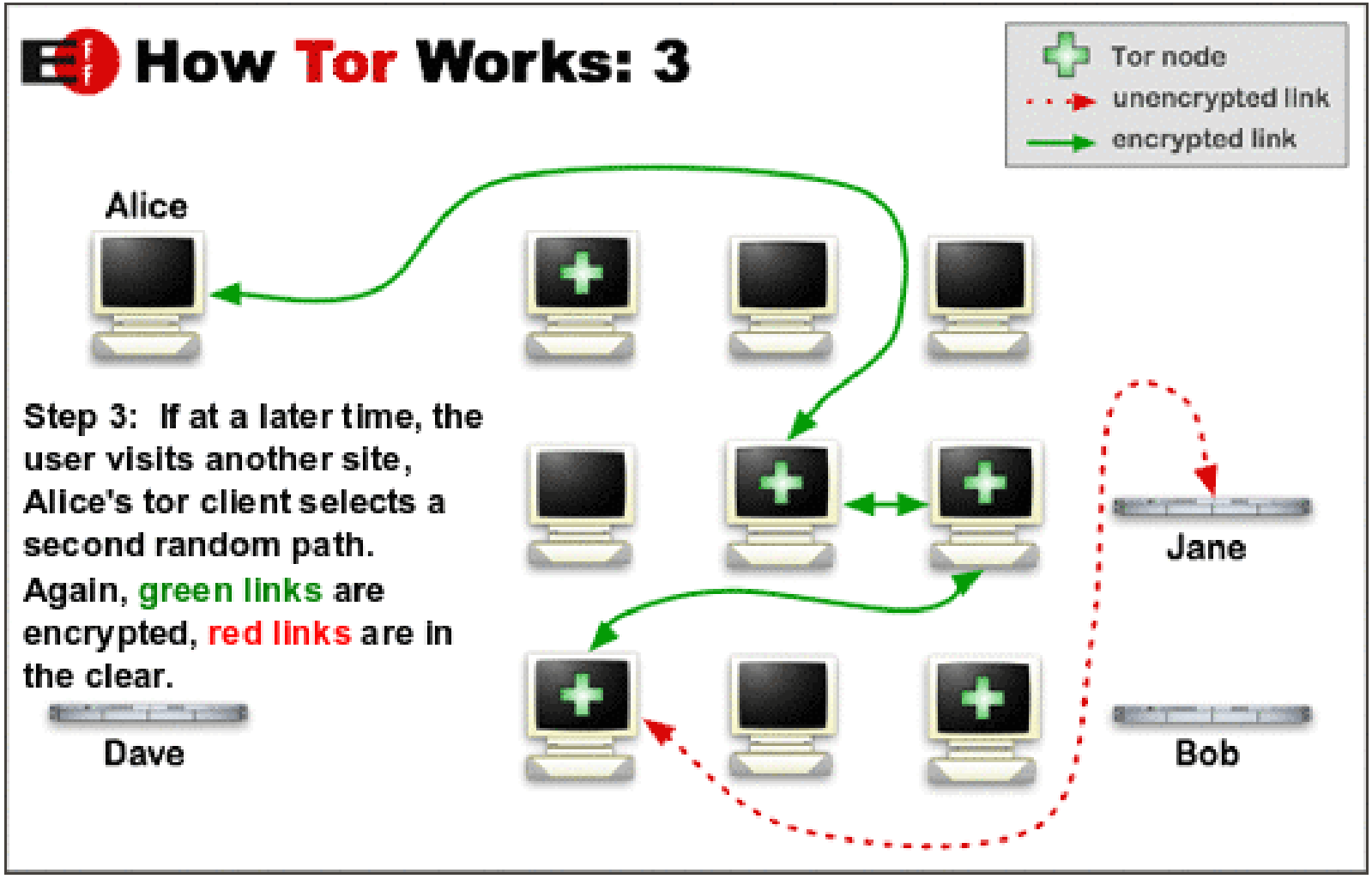
Tor project - how it works 2



pictures from `https://www.torproject.org/about/overview.html.en`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Tor project - how it works 3



pictures from `https://www.torproject.org/about/overview.html.en`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

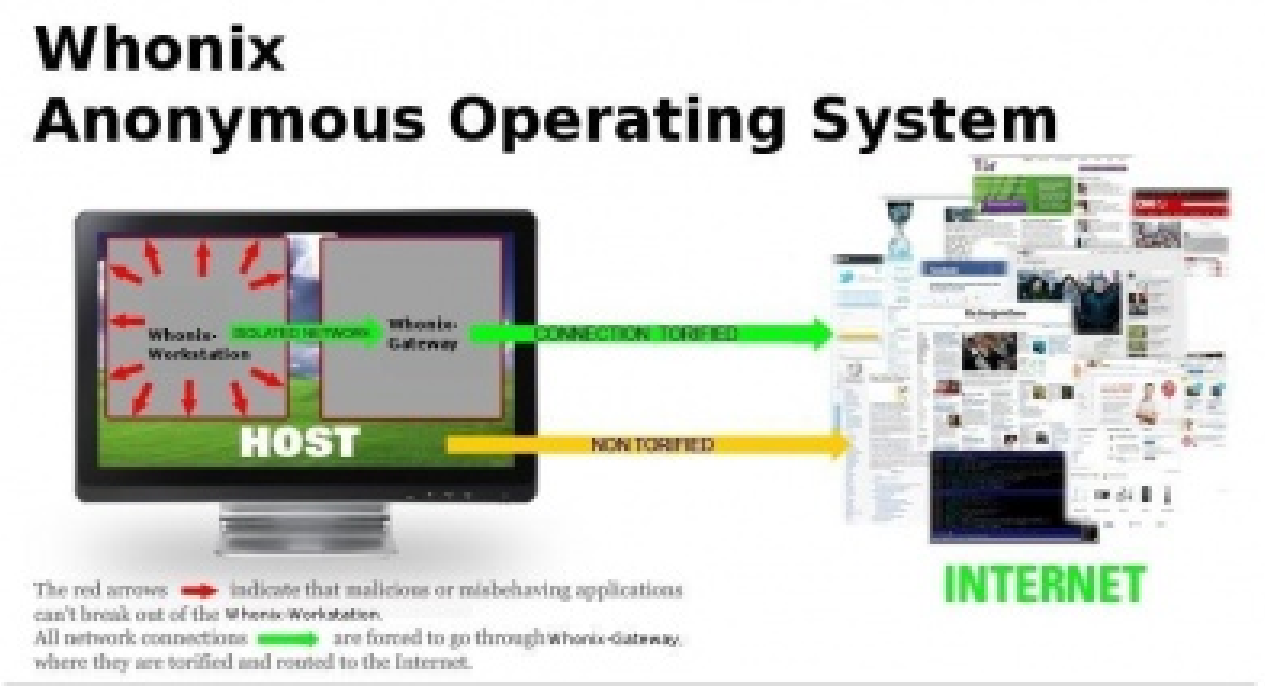
Tor project install

Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

Det anbefales at bruge bundles fra `https://www.torproject.org/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Whonix



Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find out the user's real IP.

`https://www.whonix.org/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Secure your mobile

Orbot:
Proxy With Tor

Orweb:
Private Web Browser

ChatSecure:
Private and Secure Messaging

ObscuraCam:
The Privacy Camera

Ostel:
Encrypted Phone Calls

CSipSimple:
Encrypted Voice Over IP (VOIP)

K-9 and APG:
Encrypted E-mail

KeySync:
Syncing Trusted Identities

TextSecure:
Short Messaging Service (SMS)

Pixelknot:
Hidden Messages

Dont forget your mobile platforms `https://guardianproject.info/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

How to become secure

Dont use computers at all, data about you is still processed by computers :-(

Dont use a single device for all types of data

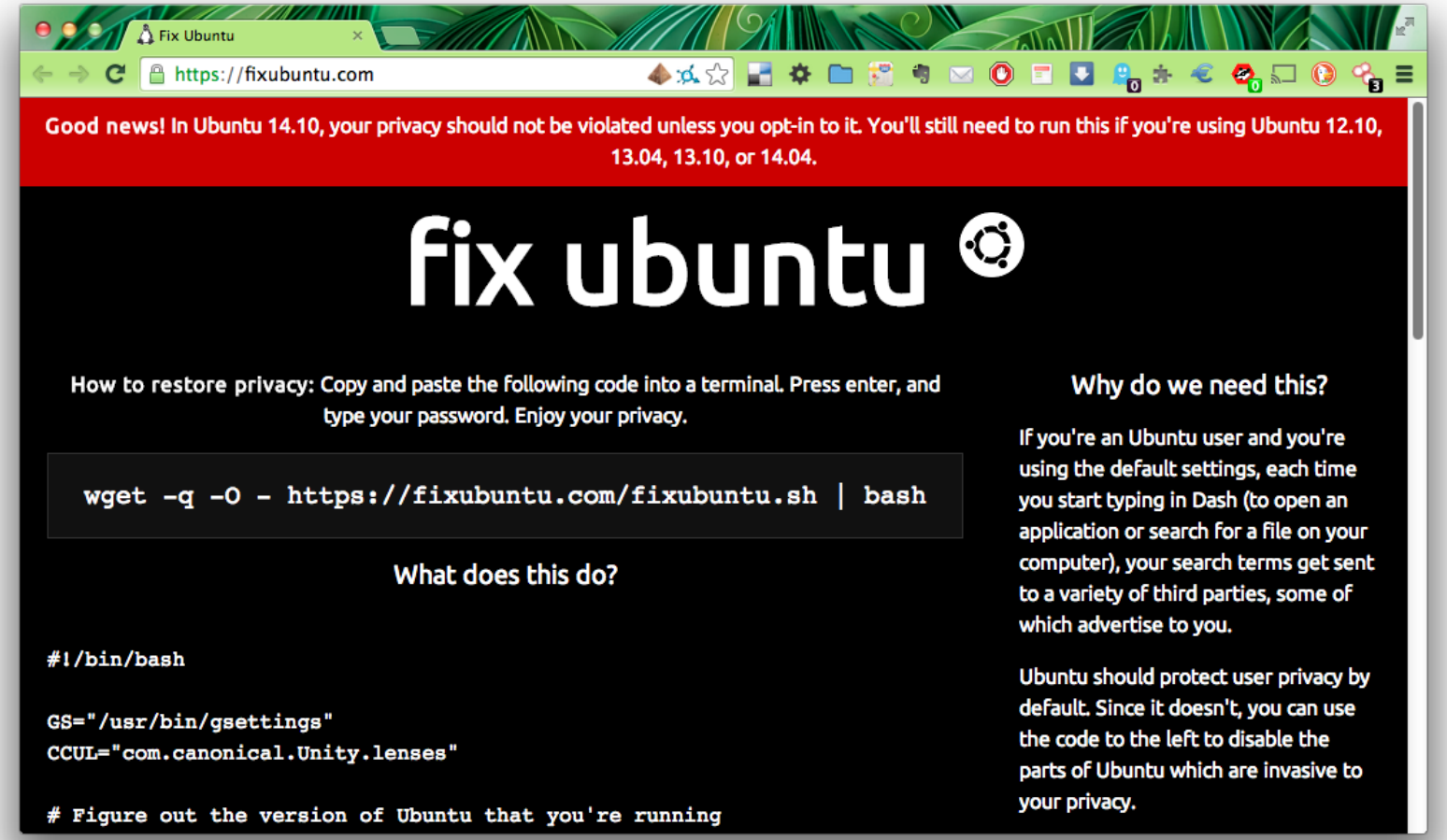
Dont use a single server for all types of data, mail server != web server

Configure systems to be secure by default, or change defaults

Use secure protocols and VPN solutions

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

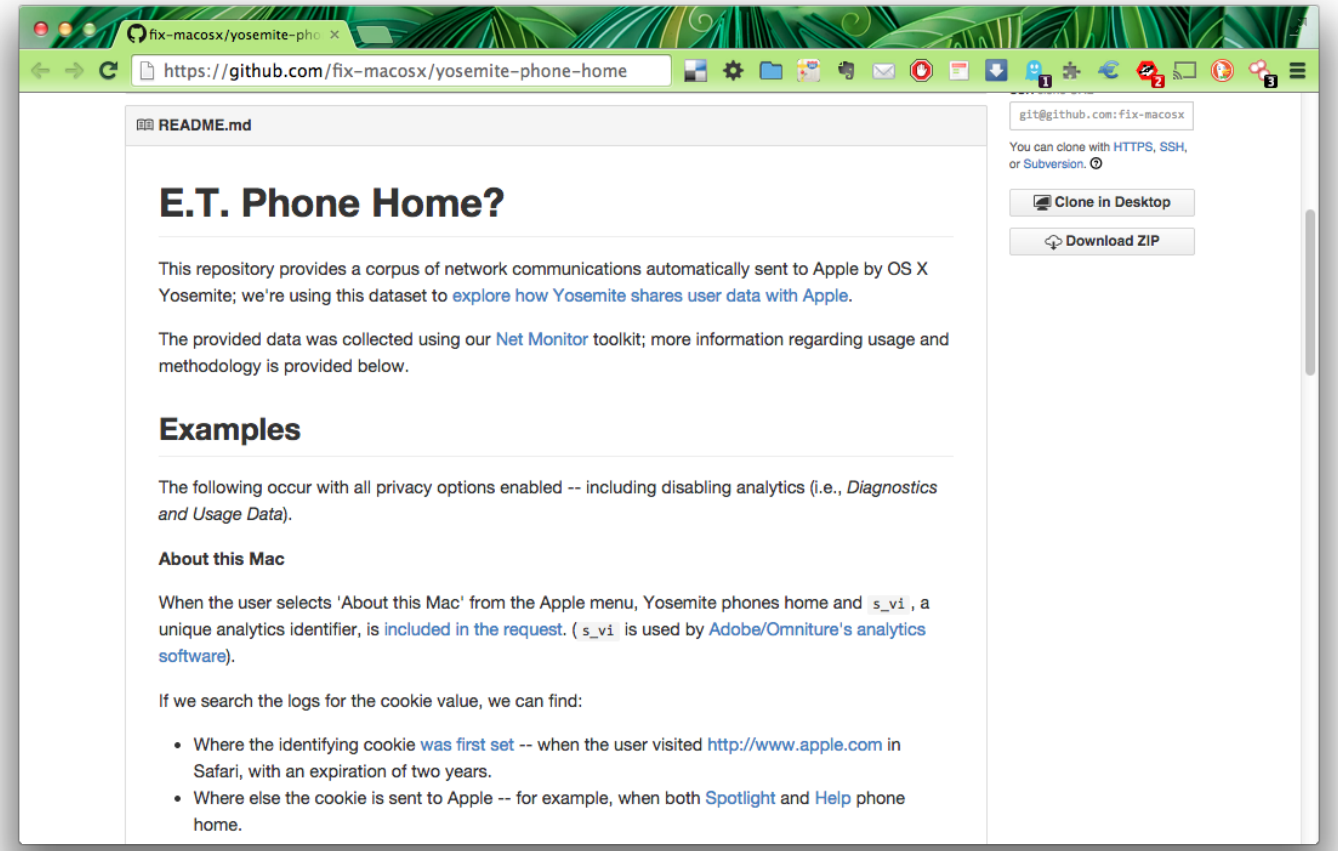
Ubuntu Unity Privacy problems



Source: `https://fixubuntu.com/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Mac OS X Yosemite - E.T. Phone Home



Source: https://github.com/fix-macosx/yosemite-phone-home

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Surveillance Self-Defense EFF

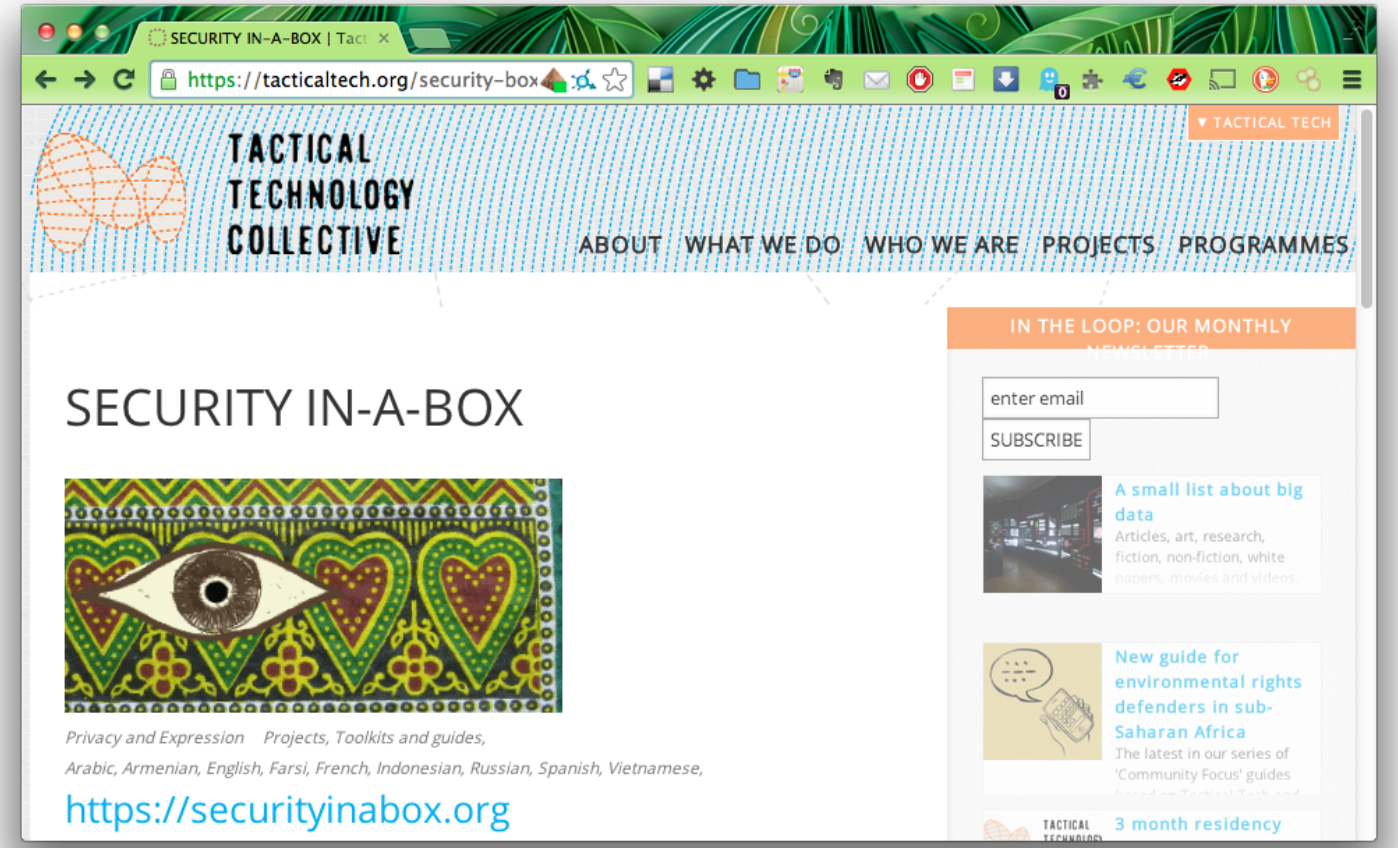
Tips, Tools and How-tos For Safer Online Communications

Modern technology has given the powerful new abilities to eavesdrop and collect data on innocent people. Surveillance Self-Defense is EFF's guide to defending yourself and your friends from surveillance by using secure technology and developing careful practices.

Source: `https://ssd.eff.org/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Ononymous robot, formerly ONO robot



Source: `https://tacticaltech.org/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Følg med Twitter news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

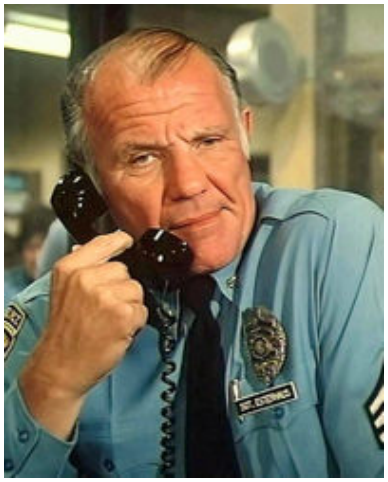
© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Checklisten

- BIOS kodeord, lock-codes for mobile devices
- Firewall - specifically for laptops
- Two browser strategy, one with paranoid settings
- Use OpenPGP for email
- Use a password safe for storing passwords
- Use hard drive encryption
- Keep systems updated
- Backup your data
- Dispose of data securely

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Source: Michael Conrad `http://www.hillstreetblues.tv/`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

PROSA CTF

PROSA afholder CTF konkurrence fredag den 28. november 2014 til lørdag

Capture the Flag er en mulighed for at afprøve sine hackerskillz

Distribueret CTF med hold Sjovt og lærerigt

Kilde: `http://prosa-ctf.the-playground.dk/`

Get ready! Lær debuggere, perl, java at kende, start på at hacke

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Hacker - cracker

Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

Idag er en hacker stadig en der bryder ind i systemer!

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj

Definition af hacking, oprindeligt

Eric Raymond, der vedligeholder en ordbog over computer-slang (The Jargon File) har blandt andet følgende forklaringer på ordet hacker:

- En person, der nyder at undersøge detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modsætning til de fleste brugere, der bare lærer det mest nødvendige
- En som programmerer lidenskabligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofter arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makholm, `http://hacking.dk`

Benyttes stadig i visse sammenhænge se `http://labitat.dk`

© license CC BY 3.0. 2014 Solido Networks, Henrik Lund Kramshøj