Welcome to

Paranoia and government hacking

PROSA Stud Svendborg2013

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Agenda and goal - workshop

Kl 10:00-12:30 and Kl 13:30-16:30

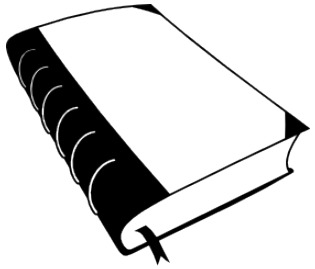
Paranoia defined

What are the vulnerabilities and threats

Reduce risk and mitigate impact

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Kursusmateriale



Dette materiale består af flere dele:

- Kursusmaterialet - præsentationen til undervisning - dette sæt
- Øvelseshæfte med øvelser
- Hertil kommer diverse ressourcer fra internet

Øvelserne er valgfrie ☺

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Bjarne Jess Hansen - Vi voksne kan også være bange

https://www.youtube.com/watch?v=ApRPz9FzkQM

Kilde: teksten fundet på
http://www.fredsakademiet.dk/abase/sange/sang29.htm

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Syria: Protest singer Ibrahim Kashoush had his throat cut

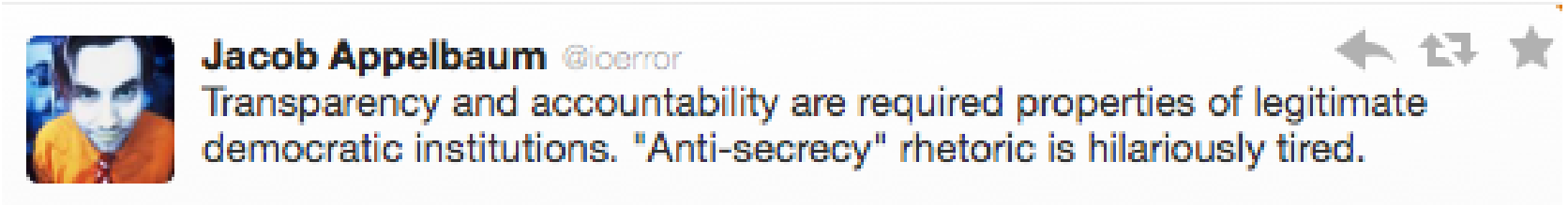
> Four days later, his body was found dumped in the Assi River (also spelled: Isa River), with a big, open and bloody wound in his neck where his adam's apple and voice chord had been removed. A clear message to those who dare to raise their voice against the Syrian President Bashar al-Assad.

'Yalla Erhal Ya Bashar' (It's time to leave, Bashar), demanding an end to President Bashar al-Assads regime.

`https://www.youtube.com/watch?v=nox6sVyhBYk`
`http://freemuse.org/archives/5054`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Formål: Hvorfor gør vi det her?



Et 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. 2013 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.

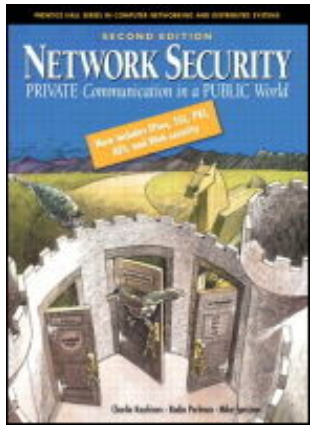
Derudover stalking, ekskærester, arbejdsgivere, forældre, ...

Du bestemmer - det er demokrati

© license CC BY 3.0. 2013 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. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Security is not magic

.

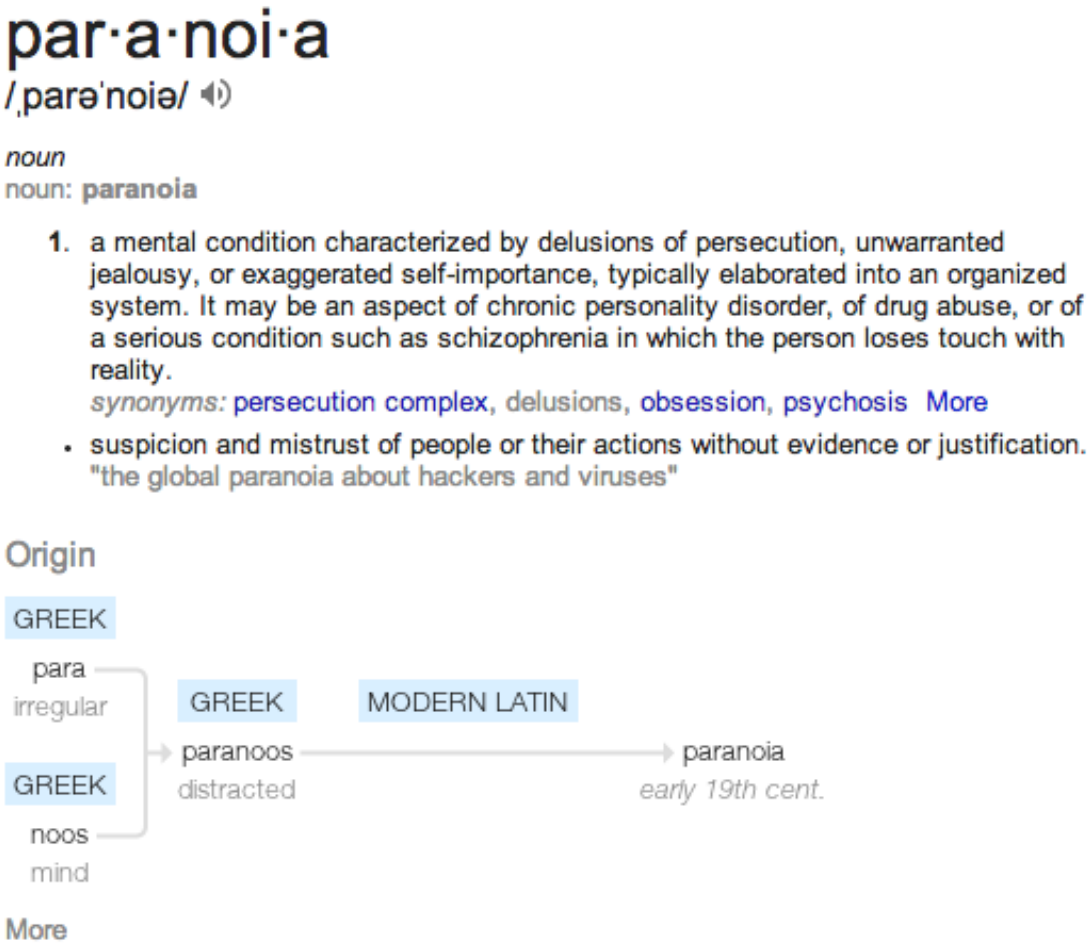
Think security, it may seem like magic - but it is not

Follow news about security

Support communities, join and learn

© license CC BY 3.0. 2013 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

GREEK para — irregular

GREEK noos — mind

GREEK paranoos — distracted

MODERN LATIN paranoia — *early 19th cent.*

More

Source: google paranoia definition

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Face reality

From the definition:

> 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
- 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

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

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Credit card fraud and identity theft statistics

Credit Card Fraud Statistics

Share This

Statistic Verification
Source: Consumer Sentinel Network, U.S. Department of Justice
Date Verified: 7.23.2012

Credit Card Fraud Statistics Statistics	Data
Percent of Americans who have been victims of credit card fraud	10 %
Percent of Americans who have been victims of debit or ATM card fraud	7 %
Median amount reported on credit card fraud	$399
Percent of all financial fraud related to credit cards	40 %
Total amount of credit card fraud worldwide	$5.55 Billion

Source: `http://www.statisticbrain.com/credit-card-fraud-statistics/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Identity theft statistics

Identity Theft / Fraud Statistics

Share This

Statistic Verification
Source: U.S. Department of Justice, Javelin Strategy & Research
Research Date: 6.18.2013
Identity theft is defined as the unauthorized use or attempted misuse of an existing credit card or other existing account, the misuse of personal information to open a new account or for another fraudulent purpose, or a combination of these types of misuse.

Identity Theft / Fraud Statistics	Data
Average number of U.S. identity fraud victims annually	11,571,900
Percent of U.S. households that reported some type of identity fraud	7 %
Average financial loss per identity theft incident	$4,930
Total financial loss attributed to identity theft in 2013	$21 billion
Total financial loss attributed to identity theft in 2010	$13.2 billion
Percent of Reported Identity Thefts by Type of Fraud	**Percent Reported**
Misuse of Existing Credit Card	64.1 %
Misuse of Other Existing Bank Account	35 %
Misuse of Personal Information	14.2 %

Source: `http://www.statisticbrain.com/identity-theft-fraud-statistics/`

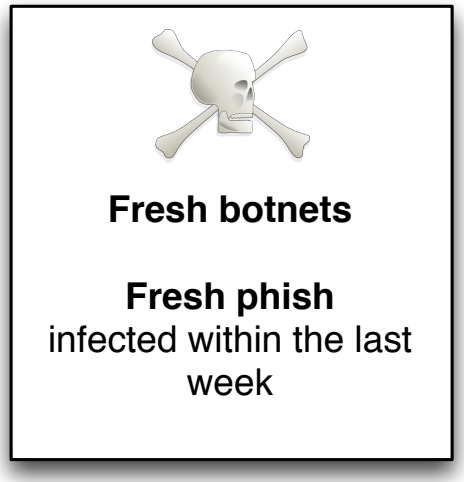
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Trading in infected computers

Botnets and malware today sold as SaaS with support contracts and updates

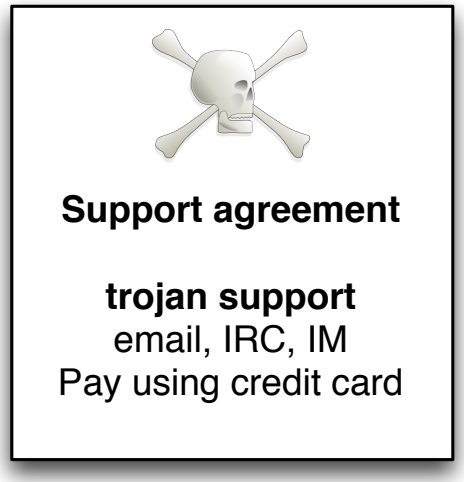
Todays offer trojans

Buy 2 pay for one



Fresh botnets

Fresh phish
infected within the last week



Support agreement

trojan support
email, IRC, IM
Pay using credit card

Malware programmers do better support than regular software companies

”Buy this version and get a year of updates free”

Rent our botnet with 100,000 by the hour

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

What if I told you:

Governments will introduce back-doors

Intercepting encrypted communications with fake certificates - check

May 5, 2011 A Syrian Man-In-The-Middle Attack against Facebook
”Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-middle attack against the HTTPS version of the Facebook site.”
Source:
`https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook`

Mapping out social media and finding connections - check

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Infecting activist machines

Infecting activist machines - check

Tibet activists are repeatedly being targeted with virus and malware, such as malicious apps for Android like KakaoTalk

Tor-users infected with malicious code to reveal their real IPs

`https://blog.torproject.org/blog/hidden-services-current-events-and-freedom-hosting`

Copying journalist data in airports - check

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Spearphishing - targetted attacks

Spearphishing - targetted attacks directed at specific individuals or companies

- Use 0-day vulnerabilities only in a few places
- Create backdoors and mangle them until not recognized by Anti-virus software
- Research and send to those most likely to activate program, open file, visit page
- Stuxnet is an example of a targeted attack using multiple 0-day vulns

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Client side: Flash, PDF, Facebook

Drive-by download

From Wikipedia, the free encyclopedia

Drive-by download means three things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). This is usually caused by poor security design[*clarification needed*]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any download that happens without a person's knowledge.
3. Download of spyware, a computer virus or any kind of malware that happens without a person's knowledge.

Kan vi undvære Flash og PDF?

Kilde: `http://en.wikipedia.org/wiki/Drive-by_download`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Flash blockers

Safari `http://clicktoflash.com/`

Firefox Extension Flashblock

Chrome extension called FlashBlock

Internet Explorer 8: IE has the Flash block functionality built-in so you don't need to install any additional plugins to be able to block flash on IE 8.

FlashBlock for Opera 9 - bruger nogen Opera mere?

FlashBlockere til iPad? iPhone? Android? - hvorfor er det ikke default?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

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. 2013 Solido Networks, Henrik Lund Kramshøj

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. 2013 Solido Networks, Henrik Lund Kramshøj

Skype is insecure

SOLIDO NETWORKS

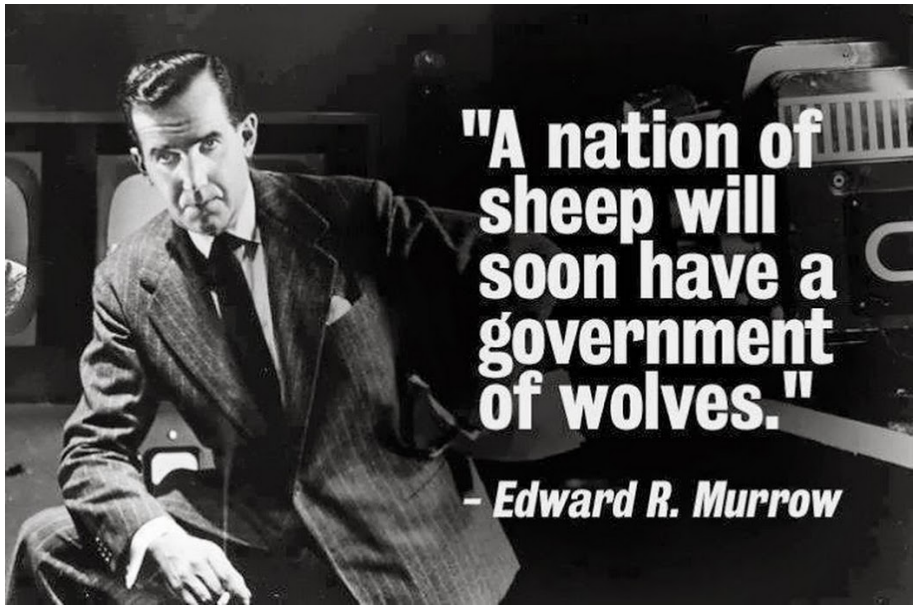
> August 7, 2013 Restoring Trust in Government and the Internet In July 2012, responding to allegations that the video-chat service Skype – owned by Microsoft – was changing its protocols to make it possible for the government to eavesdrop on users, Corporate Vice President Mark Gillett took to the company's blog to deny it.
>
> Turns out that wasn't quite true.
>
> **So Skype owned by Microsoft is not trustworthy - stop the presses!**

Source:

`http://www.schneier.com/blog/archives/2013/08/restoring_trust.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Government backdoors is not news



Nothing new really, see for example D.I.R.T and Magic Lantern

D.I.R.T - Data Interception by Remote Transmission since the late 1990s
`http://cryptome.org/fbi-dirt.htm`
`http://cryptome.org/dirty-secrets2.htm`

They will always use *Le mal du jour* to increase monitoring

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Government monitoring is not news

FBI Carnivore
"... that was designed to monitor email and electronic communications. It used a customizable packet sniffer that can monitor all of a target user's Internet traffic." `http://en.wikipedia.org/wiki/Carnivore_(software)`

NarusInsight "Narus provided Egypt Telecom with Deep Packet Inspection equipment, a content-filtering technology that allows network managers to inspect, track and target content from users of the Internet and mobile phones, as it passes through routers on the information superhighway. Other Narus global customers include the national telecommunications authorities in Pakistan and Saudi Arabia, ..."
`http://en.wikipedia.org/wiki/NarusInsight`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Denmark

Even Denmark which is considered a peaceful democracy has allowed this to go TO FAR

Danish police and TAX authorities have the legals means, even for small tax-avoidance cases, see *Rockerloven*

Danish TAX authorities have legal means to go into your property to catch builders working for cash and not reporting tax income

In both criminal and piracy cases we see a lot of extraneous equipment seized

Danish prime minister Helle Thorning-Schmidt does NOT criticize the USA

In fact the party Social Democrats are often pushing further surveillance

© license CC BY 3.0. 2013 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

Outlaw and/or discredit crypto

Go after Tor exit nodes

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Use protection - always

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

A vulnerability can and will be abused

SOLIDO NETWORKS

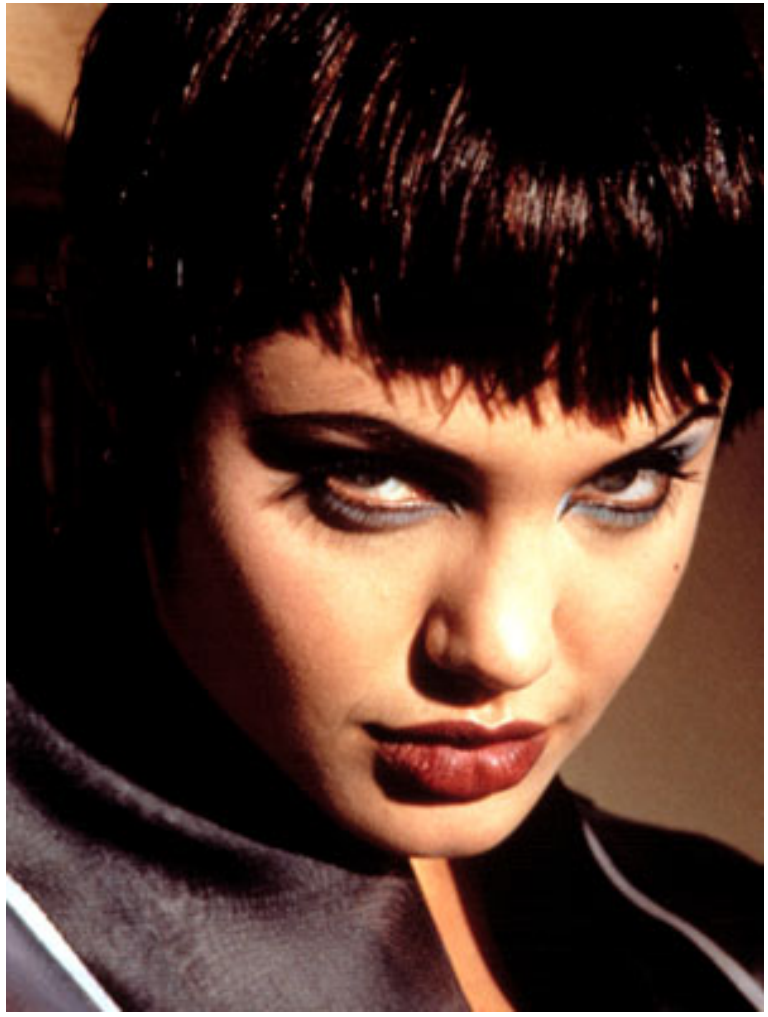
What if I told you:

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.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hackertyper anno 1995



Lad os lige gå tilbage til hackerne

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hacker types anno 2008

Lisbeth Salander from the Stieg Larsson's award-winning Millennium series does research about people using hacking as a method to gain access

How can you find information about people?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

From search patterns to persons

SOLIDO NETWORKS

First identify some basic information

Use search patterns like from email to full name

Some will give direct information about target

Others will point to intermediary information, domain names

Pivot and redo searching when new information bits are found

What information is public? (googledorks!)

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Example patterns - for a Dane

Name, fullname, aliases

IDs and membership information, CPR (kind a like social security number)

Computerrelated information: IP, Whois, Handles, IRC nicks

Nick names

Writing style, specific use of words, common speling mistakes

Be creative

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Google for it

Google as a hacker tools?

Concept named googledorks when google indexes information not supposed to be public `http://johnny.ihackstuff.com/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Fra mønstre til person

Først vil vi finde nogle mønstre

Derefter vil vi søge med de mønstre

Nogle giver direkte information

Andre giver baggrundsinformation

Hvad er offentligt og hvad er privat? (googledorks!)

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Eksempler på mønstre

Navn, fulde navn, fornavne, efternavne, alias'es

Diverse idnumre, som CPR - tør du søge på dit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

Øgenavne, kendenavne

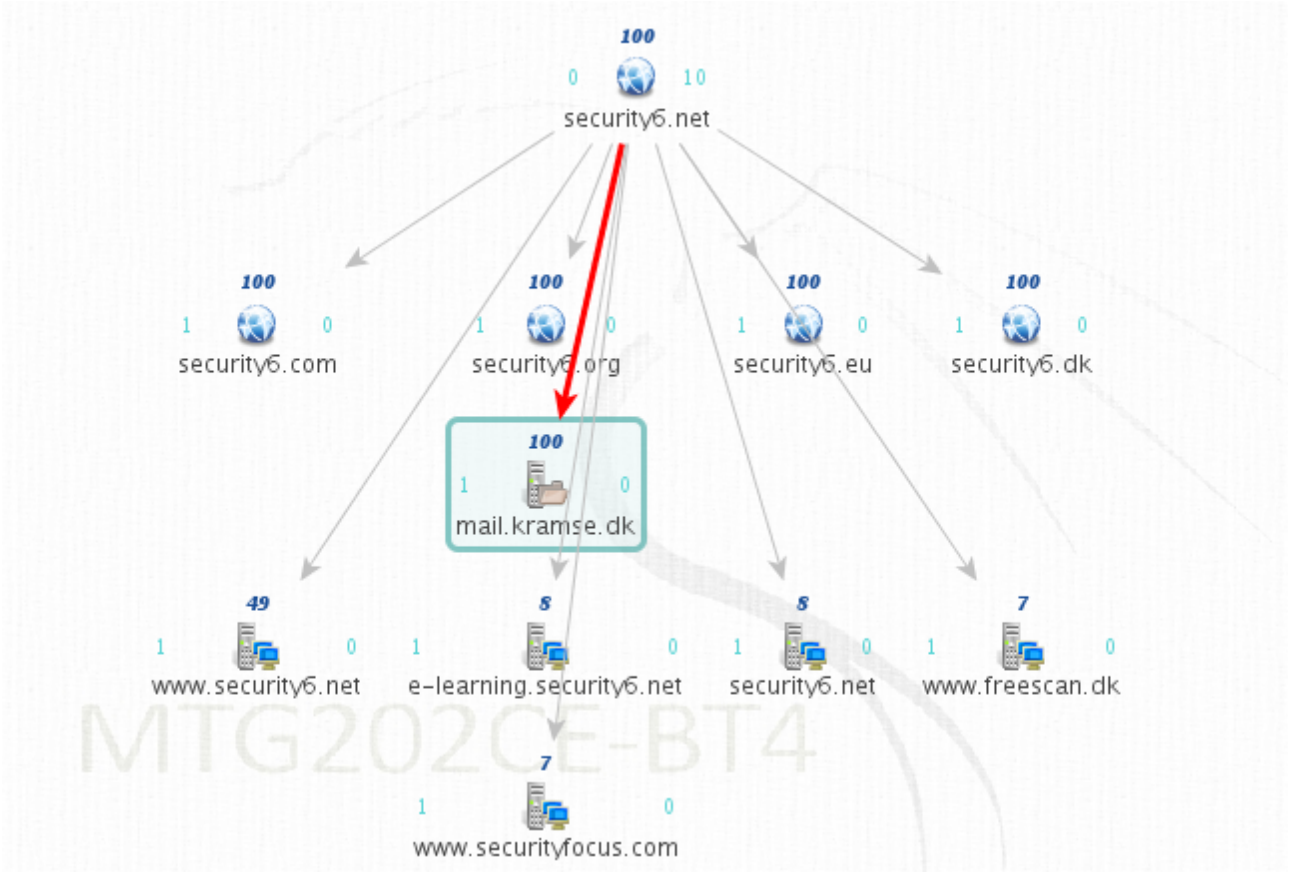
Skrivestil, ordbrug mv.

Tiden på din computer?

Tænk kreativt ☺

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Lisbeth in a box?



Maltego can automate the mining and gathering of information
uses the concept of transformations

`http://www.paterva.com/maltego/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hvor finder du informationerne

Email

DNS

Gætter

Google

Alt hvad du ellers har adgang til - eller som Lisbeth tilraner sig adgang til

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Er du passende paranoid?

Vær på vagt

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hvordan bliver du sikker

Lad være med at bruge computere

Lad være med at bruge een computer til alt - en privat bærbar ER mere privat end en firmacomputer

Forskellige computere til forskellige formål, en server er mail-server en anden er web-server

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. Tor

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- `http://csrc.nist.gov/publications/PubsSPs.html`
- `http://www.nsa.gov/research/publications/index.shtml`
- `http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml`

© license CC BY 3.0. 2013 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

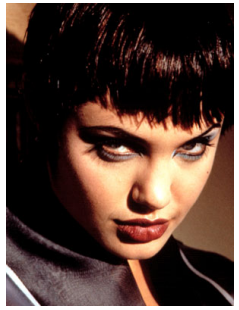
Vi skal bruge ånden fra hacking til forskning, udvikling

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. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Kali Linux the new backtrack

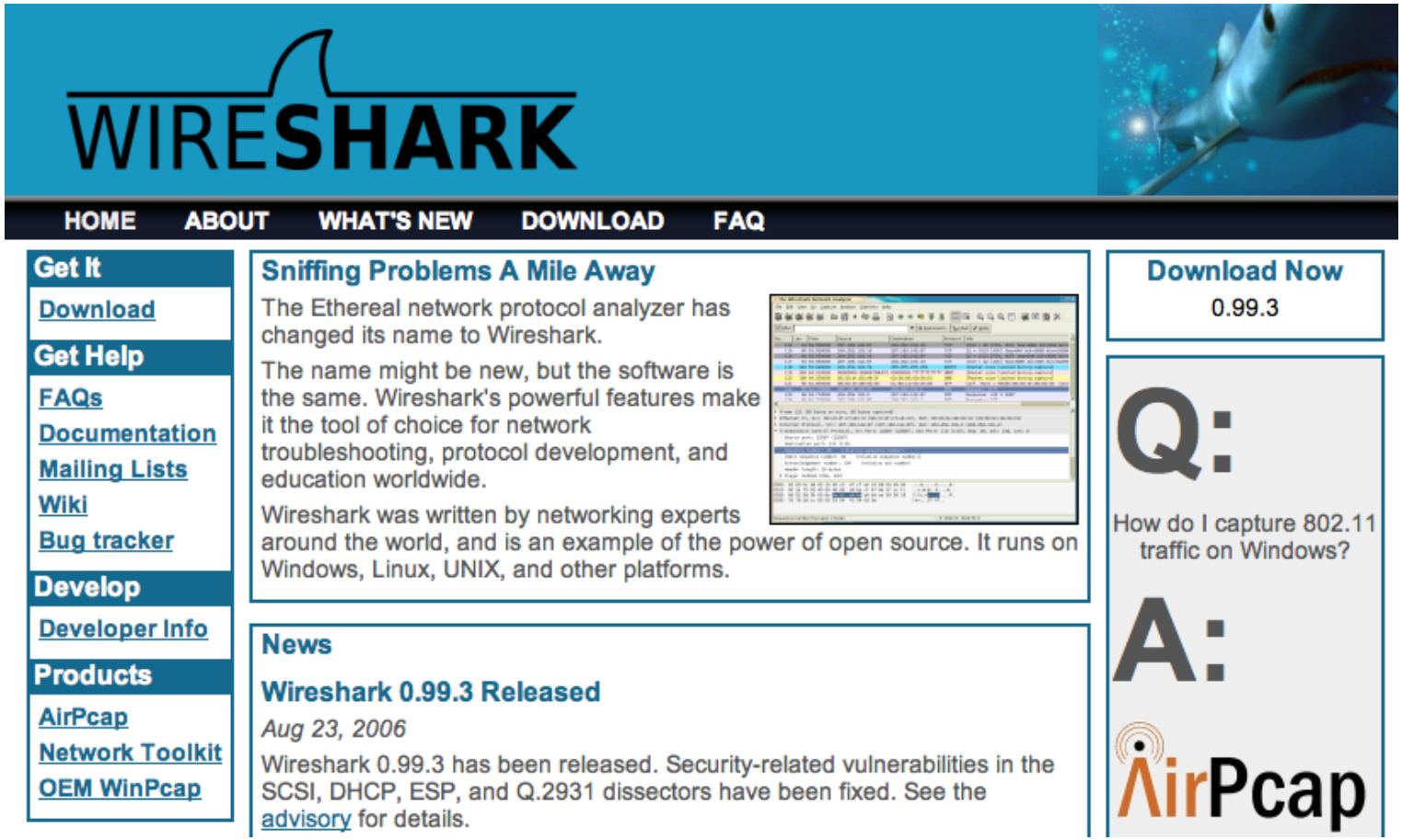
BackTrack `http://www.backtrack-linux.org`

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

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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Wireshark - grafisk pakkesniffer

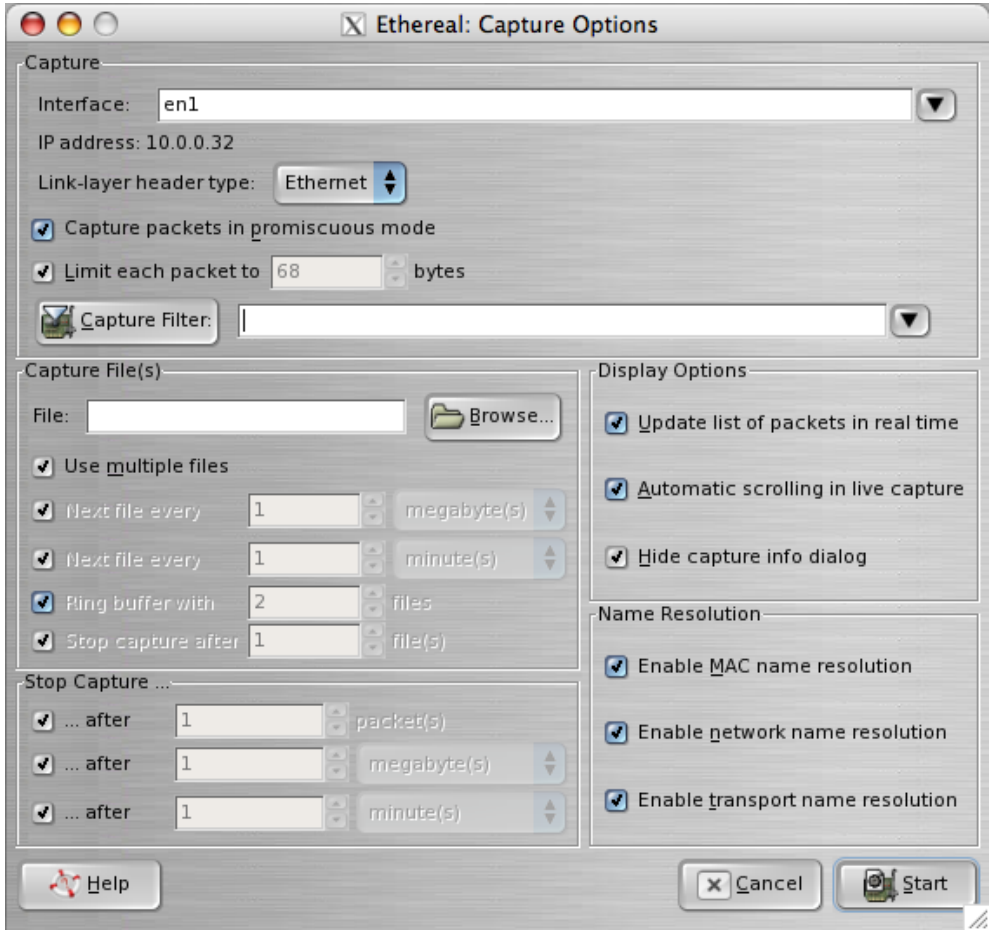


`http://www.wireshark.org`

både til Windows og UNIX, tidligere kendt som Ethereal

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

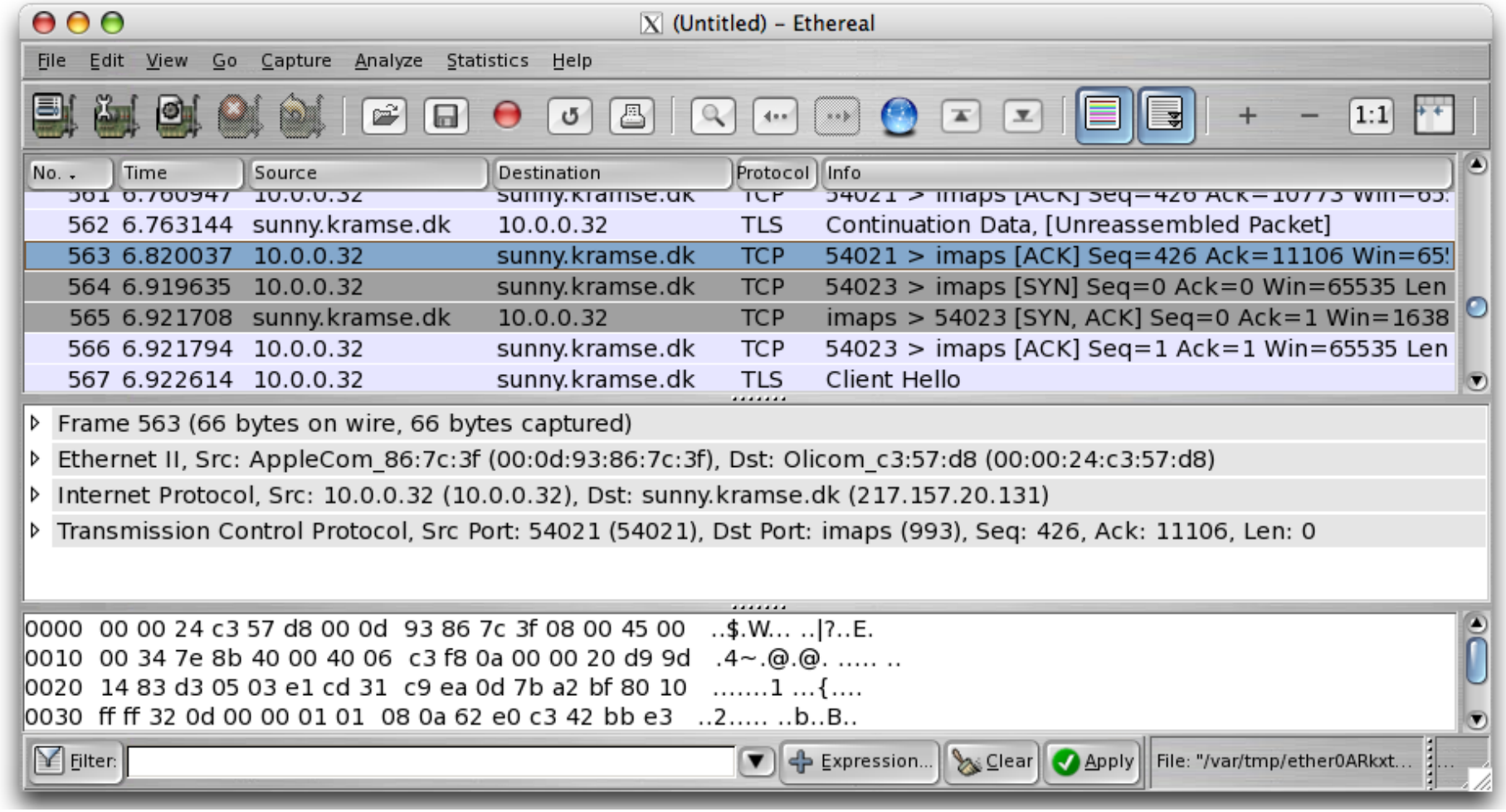
Brug af Wireshark



Man starter med Capture - Options

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

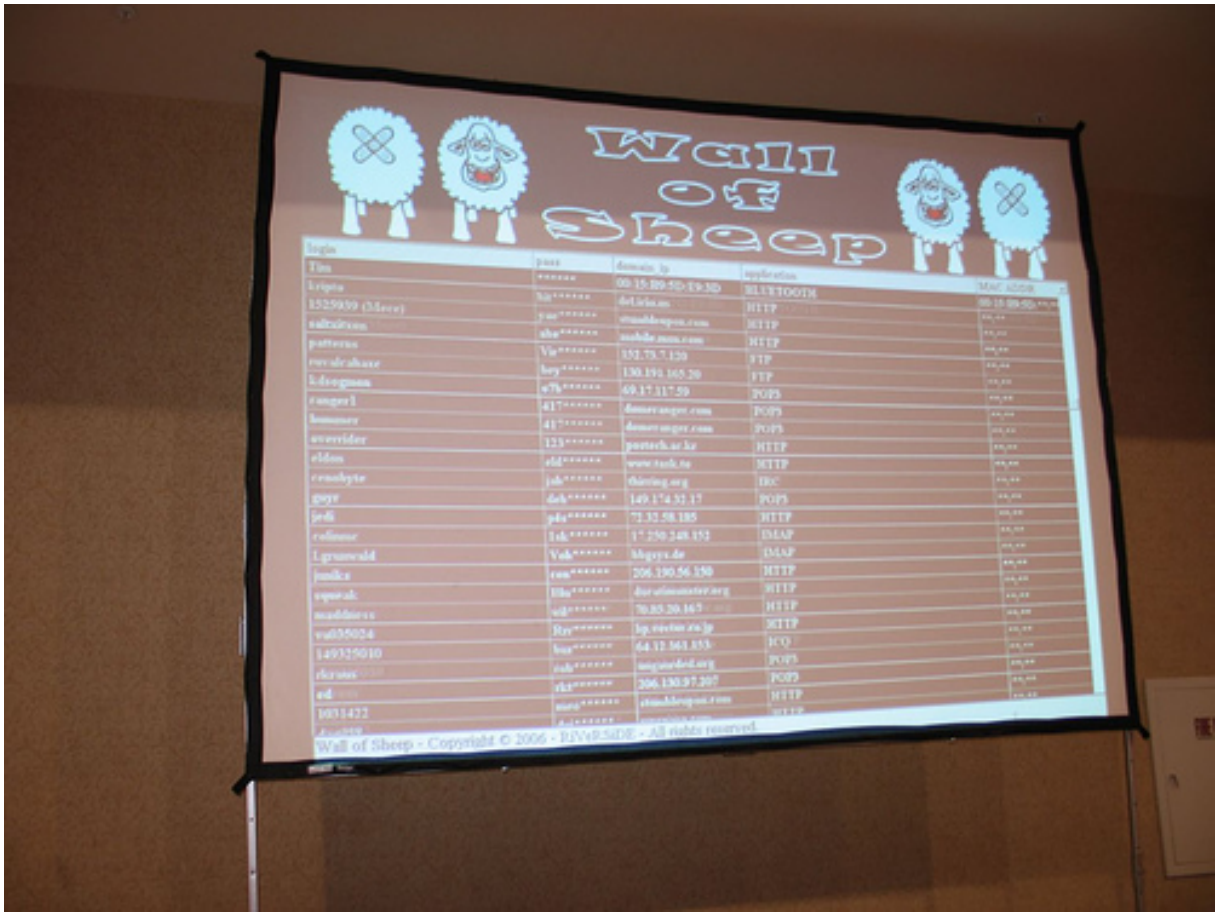
Brug af Wireshark



Læg mærke til filtermulighederne

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Wireshark installation

som er øvelse 1 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Vi laver nu øvelsen

Sniffing network packets

som er øvelse 2 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

dsniff

SOLIDO NETWORKS

en sniffer til mange usikre protokoller

inkluderer **arpspoof**

Lavet af Dug Song, dugsong@monkey.org

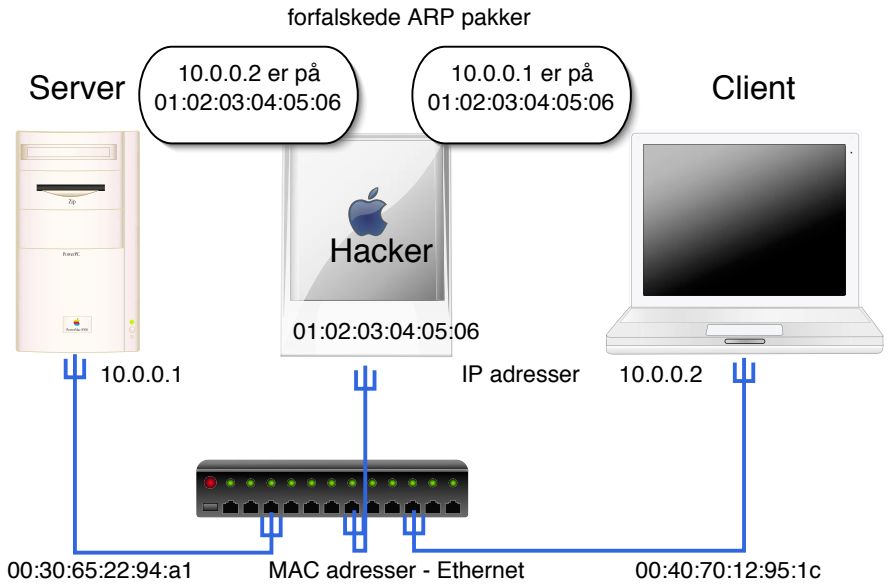
```
dsniff is a password sniffer which handles FTP, Telnet,
SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin,
RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11,
CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft
SMB, Oracle SQL*Net,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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

dsniff forudsætninger

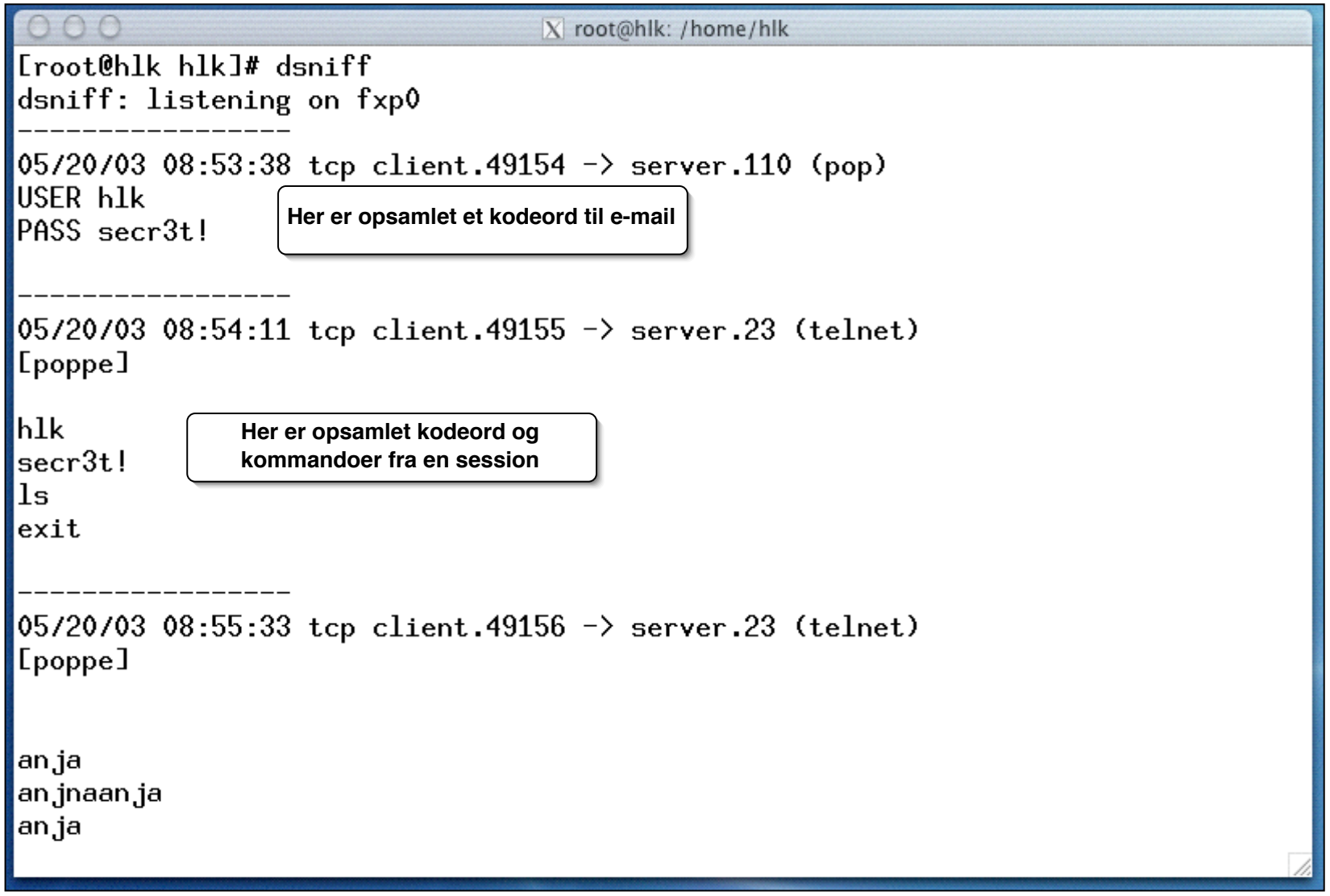
Der er visse forudsætninger der skal være opfyldt

- Man skal have trafikken
- Det kan gøres gennem arp spoofing eller ved at hacke ind i et system/router på netværksvejen



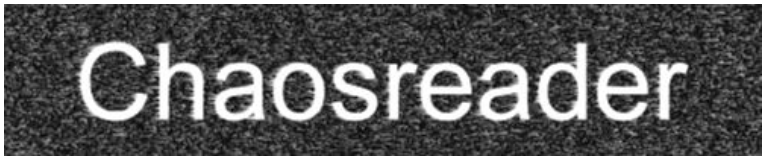
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Kommenteret dsniff



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Chaosreader



Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

Image Report - Click here for a report on captured images.
GET/POST Report (Empty) - Click here for a report on HTTP GETs and POSTs.
HTTP Proxy Log - Click here for a generated proxy style HTTP log.

TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• as_html
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• as_html

Med adgang til et netværksdump kan man læse det med chaosreader

Output er HTML med oversigter over sessioner, billeder fra datastrømmen osv.

`http://chaosreader.sourceforge.net/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Suricata IDS/IPS/NSM

Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is developed by the OISF and its supporting vendors.

- `http://suricata-ids.org/`
- `http://openinfosecfoundation.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Netflow

Netflow is getting more important, more data share the same links

Accounting is important

Detecting DoS/DDoS and problems is essential

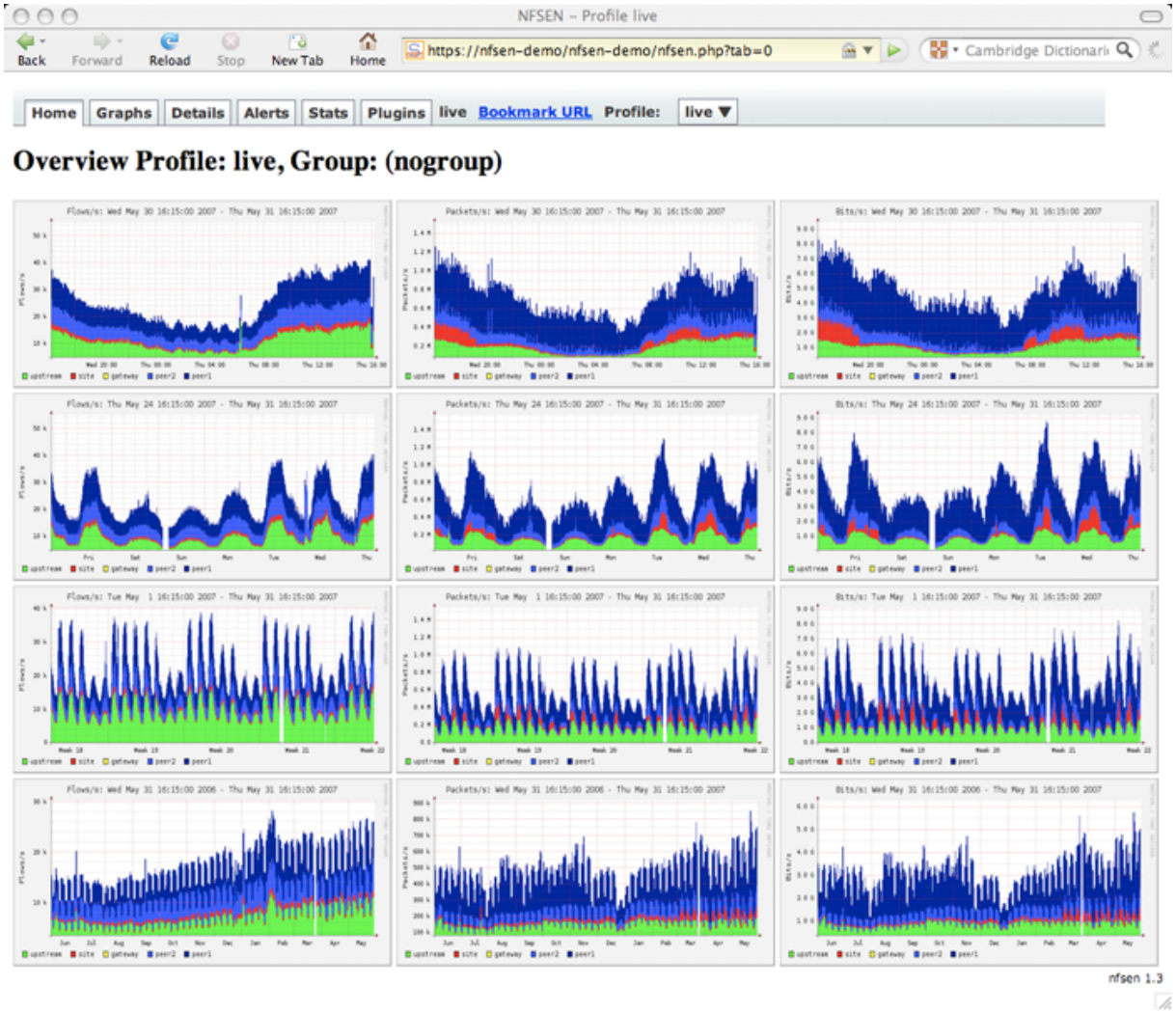
Netflow sampling is vital information - 123Mbit, but what kind of traffic

We use mostly NFSen, but are looking at various software packages
`http://nfsen.sourceforge.net/`

Currently also investigating sFlow - hopefully more fine grained

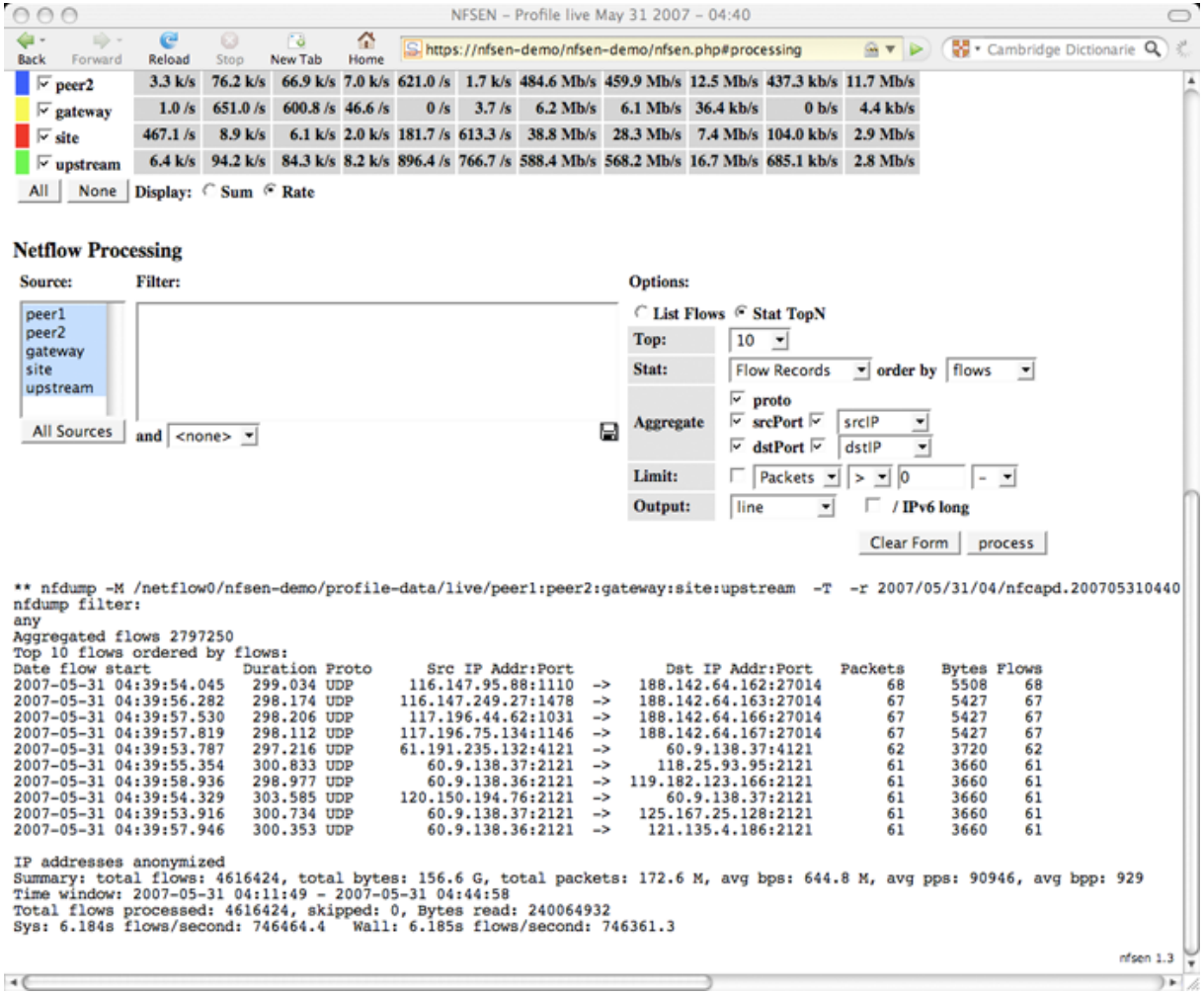
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Netflow using NFSen



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

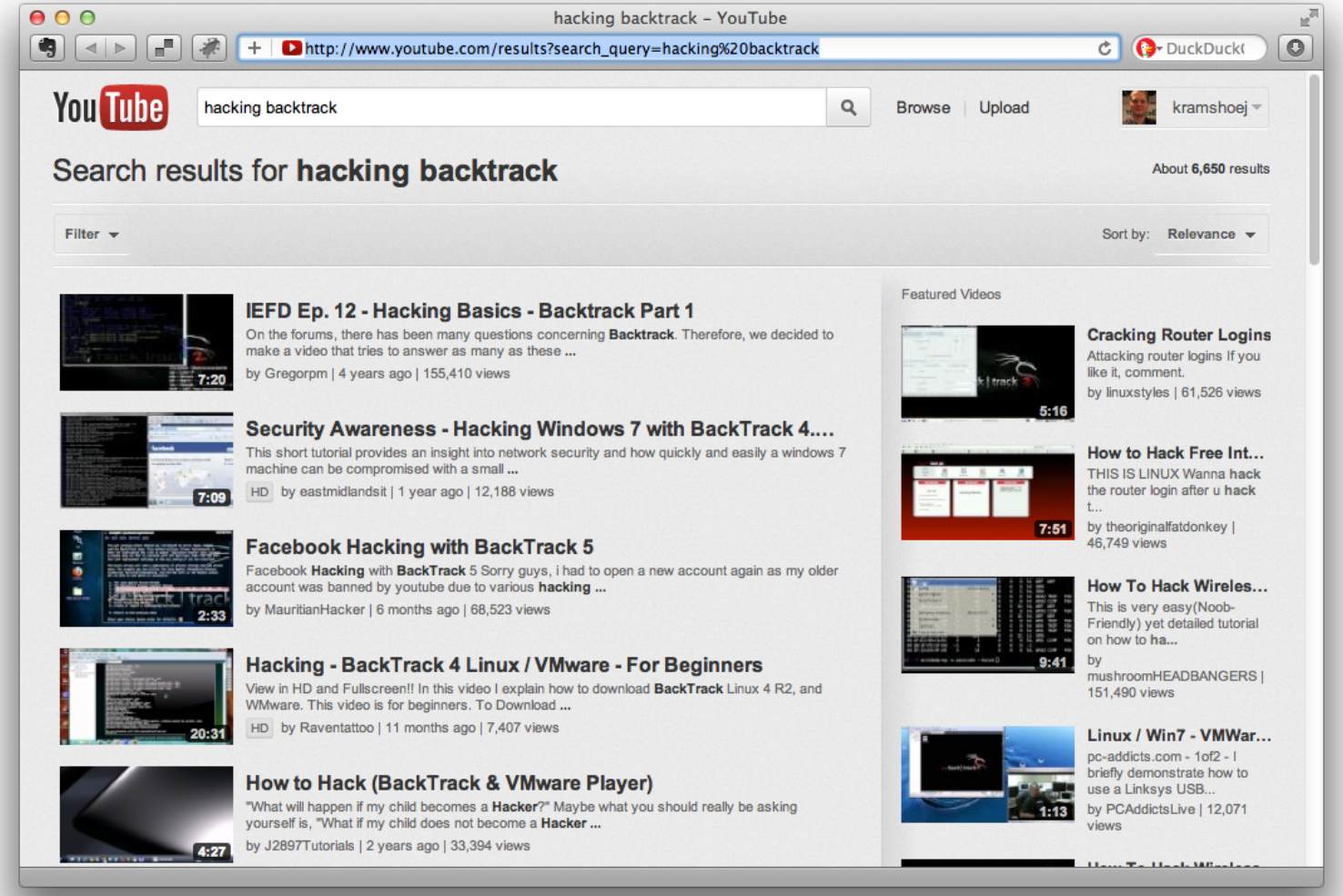
Netflow processing from the web interface



Bringing the power of the command line forward

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Status idag på internet



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Moderne botnets

Botnets spreder sig ved at inficere så mange systemer som muligt

Botnets idag vokser gerne langsommere - ingen ny Code Red hastighedsrekord

Spreder sig via SMTP, HTTP, SMB, ... alle protokoller der kan overføre data

Bannerkampagner og 3. parts kilder til elementer på din side?!

Når først der er kommet malware på systemet udvides med moduler

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Malware idag

Malware idag er sofistikeret

Modulært opbygget

Benytter stærk kryptering til at sikre administrationen af inficerede computere

Benytter seneste sikkerhedshuller - 0 days til at sprede sig

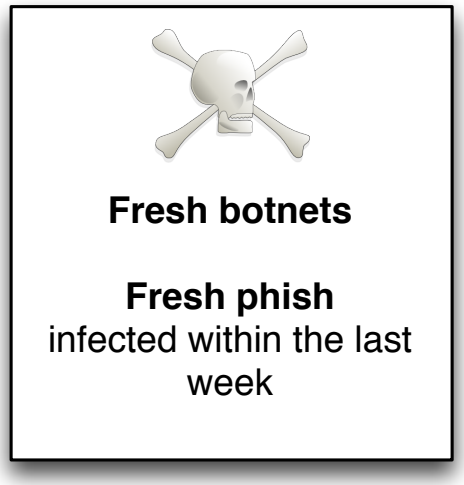
Benytter de seneste rootkit metoder til at holde sig skjult

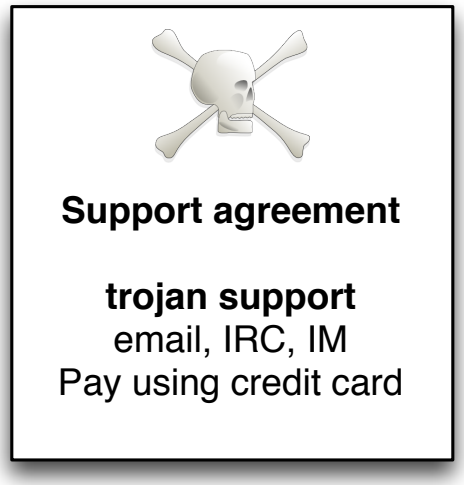
Muterer efter alle kendte metoder for at undgå opdagelse

Larmer mindre end tidligere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Botnets og malware sælges med support





Malware programmører har lært kundepleje

”Køb denne version og få gratis opdateringer”

Lej vores botnet med 100.000 computere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Phishing - Receipt for Your Payment to mark561@bt....com

Mark Willson
145 Church Lane East
Aldershot, Hampshire, GU11 3ST
United Kingdom

Important Note: Mark Willson has provided an Unconfirmed Address. If you are planning on shipping items to Mark Willson, please check the Transaction Details page of this payment to find out whether you will be covered by the PayPal Seller Protection Policy.

Note:

If you haven't authorized this charge ,click the link below to cancel transaction

Cancel Transaction:

https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

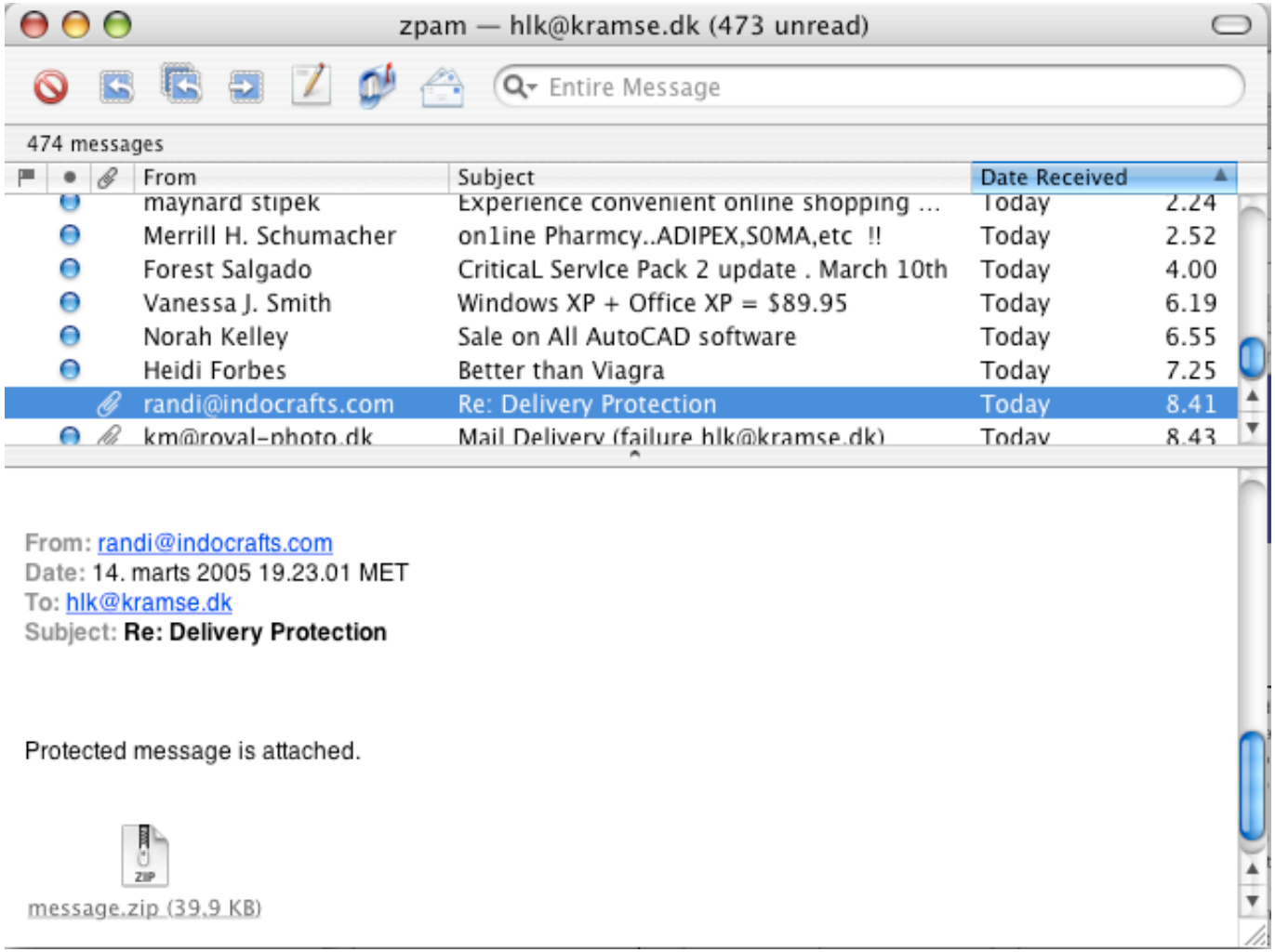
*SSL connection:
PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)
---

http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

Kan du selv genkende Phishing

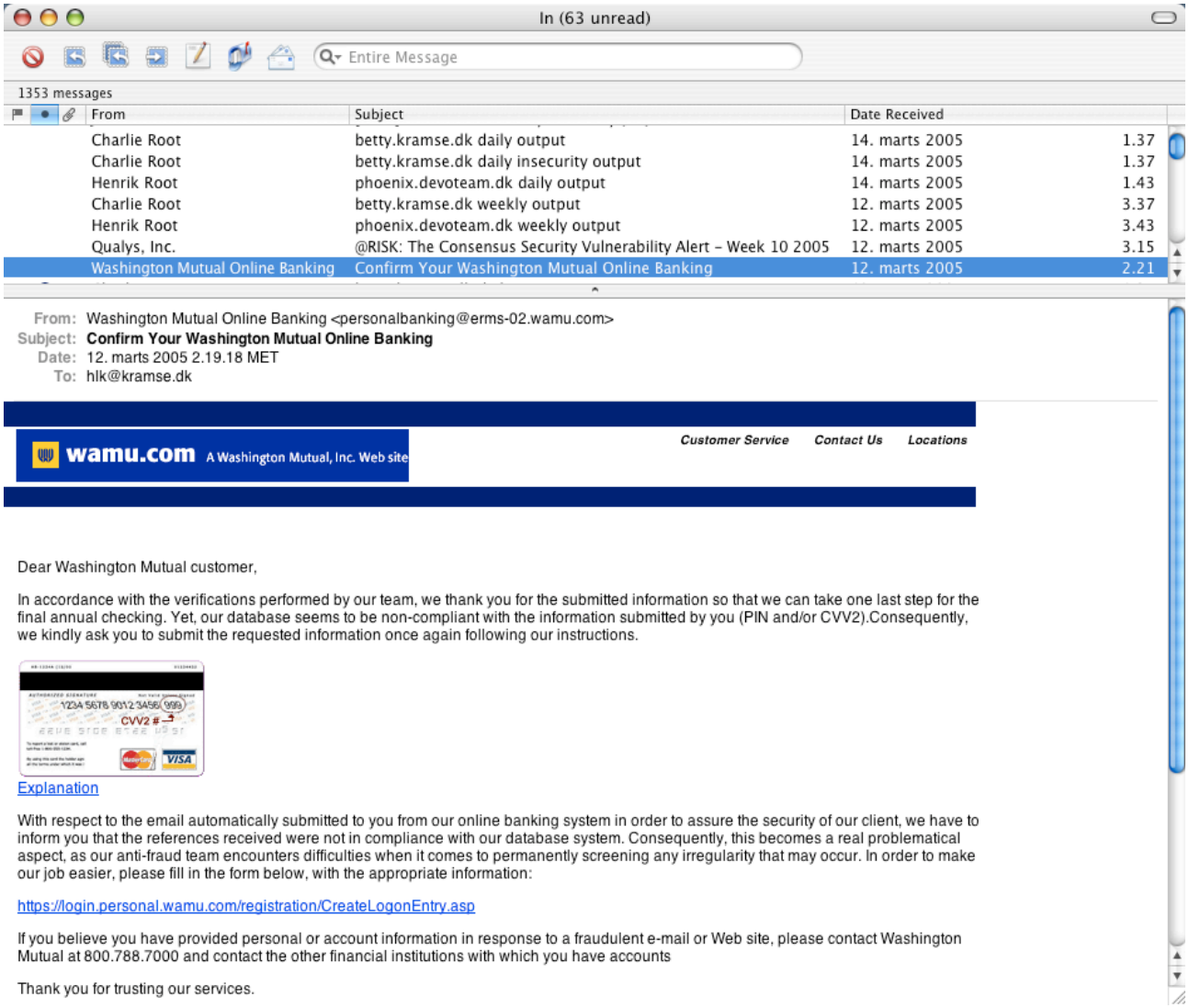
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Zip files?

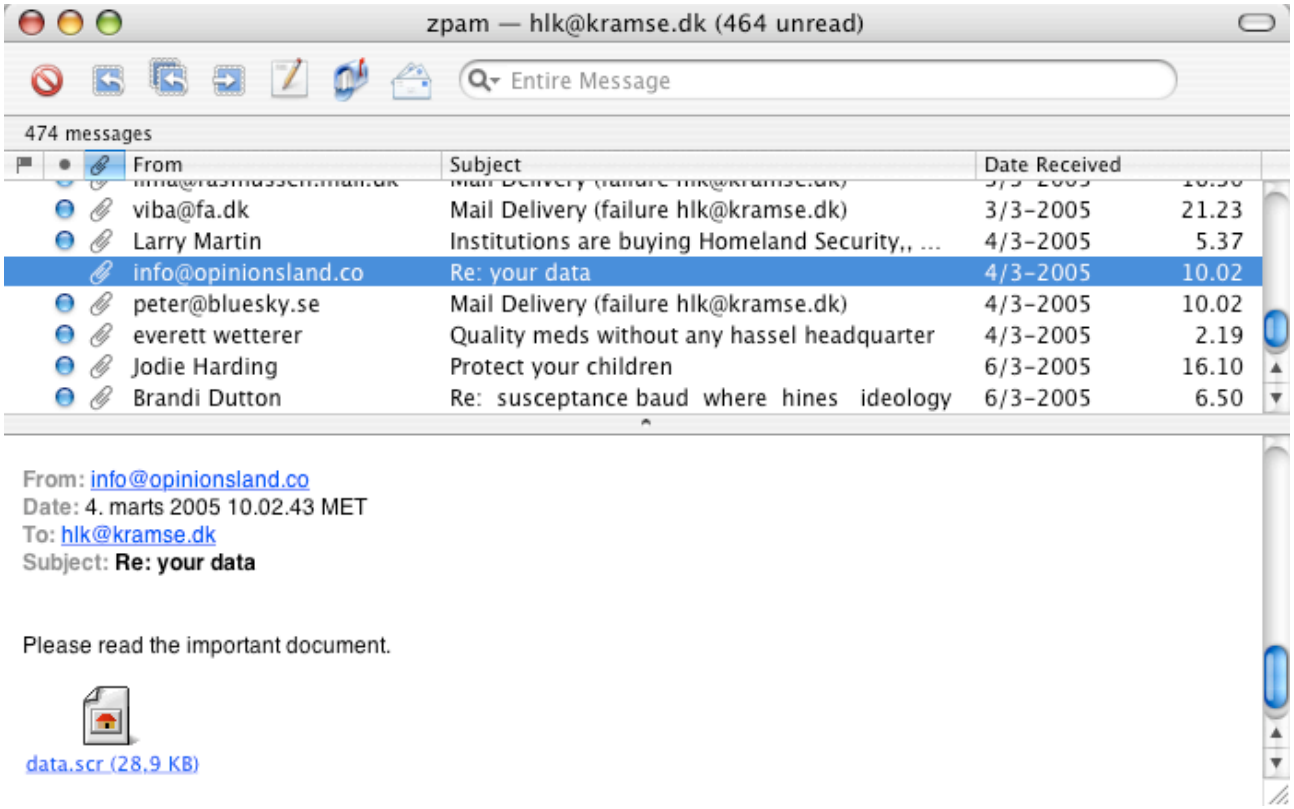


© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Money!



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

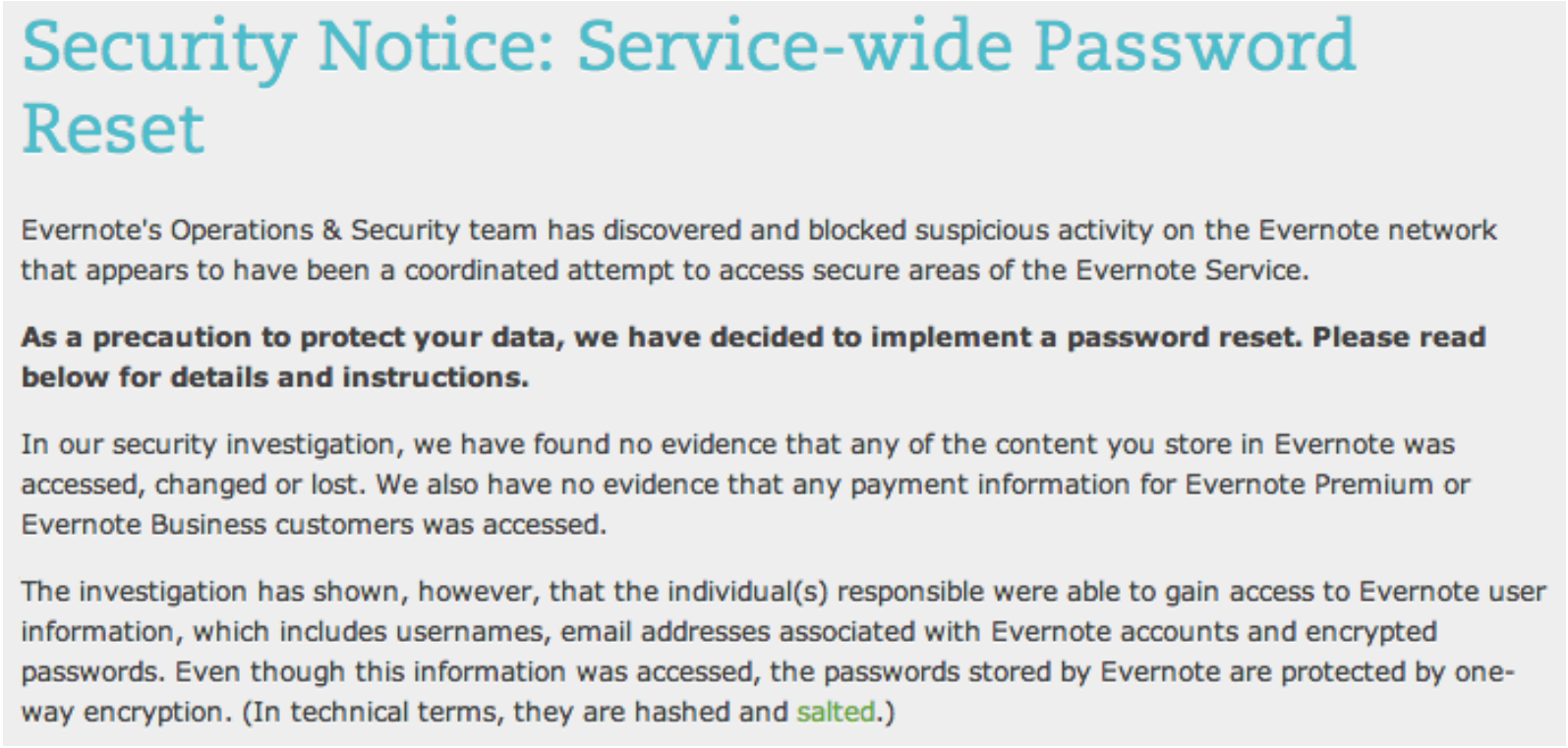


SCR er screensaver files - programmer

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Evernote password reset

What happens when security breaks?



Security Notice: Service-wide Password Reset

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed.

The investigation has shown, however, that the individual(s) responsible were able to gain access to Evernote user information, which includes usernames, email addresses associated with Evernote accounts and encrypted passwords. Even though this information was accessed, the passwords stored by Evernote are protected by one-way encryption. (In technical terms, they are hashed and salted.)

Sources:

`http://evernote.com/corp/news/password_reset.php`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Twitter password reset

Blog

Keeping our users secure

Friday, February 01, 2013

As you may have read, there's been a recent uptick in large-scale security attacks aimed at U.S. technology and media companies. Within the last two weeks, the *New York Times* and *Wall Street Journal* have chronicled breaches of their systems, and Apple and Mozilla have turned off Java by default in their browsers.

This week, we detected unusual access patterns that led to us identifying unauthorized access attempts to Twitter user data. We discovered one live attack and were able to shut it down in process moments later. However, our investigation has thus far indicated that the attackers may have had access to limited user information – usernames, email addresses, session tokens and encrypted/salted versions of passwords – for approximately 250,000 users.

Sources:

`http://blog.twitter.com/2013/02/keeping-our-users-secure.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Are passwords dead?

google: passwords are dead
About 6,580,000 results (0.22 seconds)

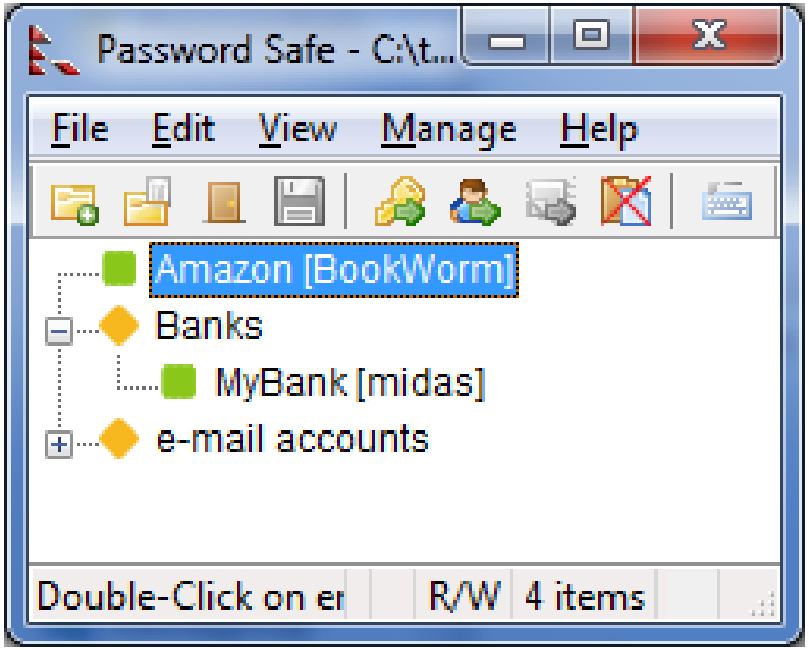
Can we stop using passwords?

Muffett on Passwords has a long list of password related information, from the author of crack `http://en.wikipedia.org/wiki/Crack_(password_software)`

`http://dropsafe.crypticide.com/muffett-passwords`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Storing passwords



PasswordSafe `http://passwordsafe.sourceforge.net/`

Apple Keychain provides an encrypted storage

Browsere, Firefox Master Password, Chrome passwords, ... who do YOU trust

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Google looks to ditch passwords for good

”Google is currently running a pilot that uses a YubiKey cryptographic card developed by Yubico

The YubiKey NEO can be tapped on an NFC-enabled smartphone, which reads an encrypted one-time password emitted from the key fob.”

Source: `http://www.zdnet.com/google-looks-to-ditch-passwords-for-good-with-nfc-based-replacement`

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

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`

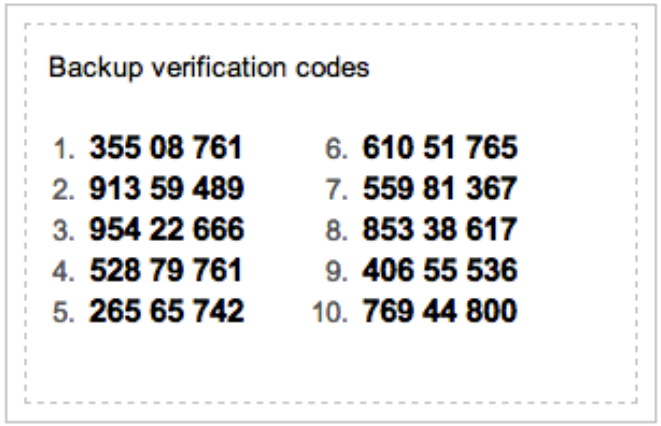
`https://www.duosecurity.com/`

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Integrate or develop?

From previous slide:

Conclusion passwords: integrate with authentication, not reinvent

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. 2013 Solido Networks, Henrik Lund Kramshøj

Cisco IOS password

Title: Cisco's new password hashing scheme easily cracked

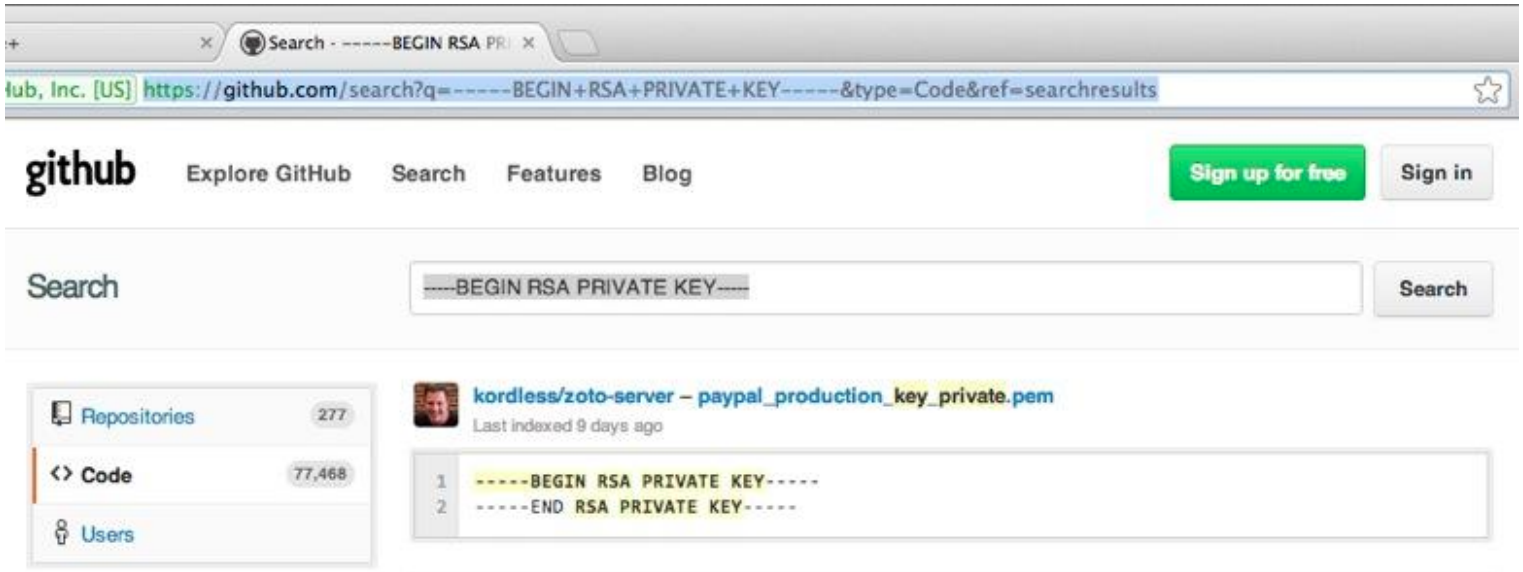
Description: In an astonishing decision that has left crytographic experts scratching their heads, engineer's for Cisco's IOS operating system chose to switch to a **one-time SHA256 encoding - without salt** - for storing passwords on the device. This decision leaves password hashes vulnerable to high-speed cracking - modern graphics cards can compute over **2 billion SHA256 hashes in a second - and is actually considerably less secure than Cisco's previous implementation.** As users cannot downgrade their version of IOS without a complete reinstall, and no fix is yet available, security experts are urging users to avoid upgrades to IOS version 15 at this time.

Reference: via SANS @RISK newsletter

`http://arstechnica.com/security/2013/03/cisco-switches-to-weaker-h`

© license CC BY 3.0. 2013 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

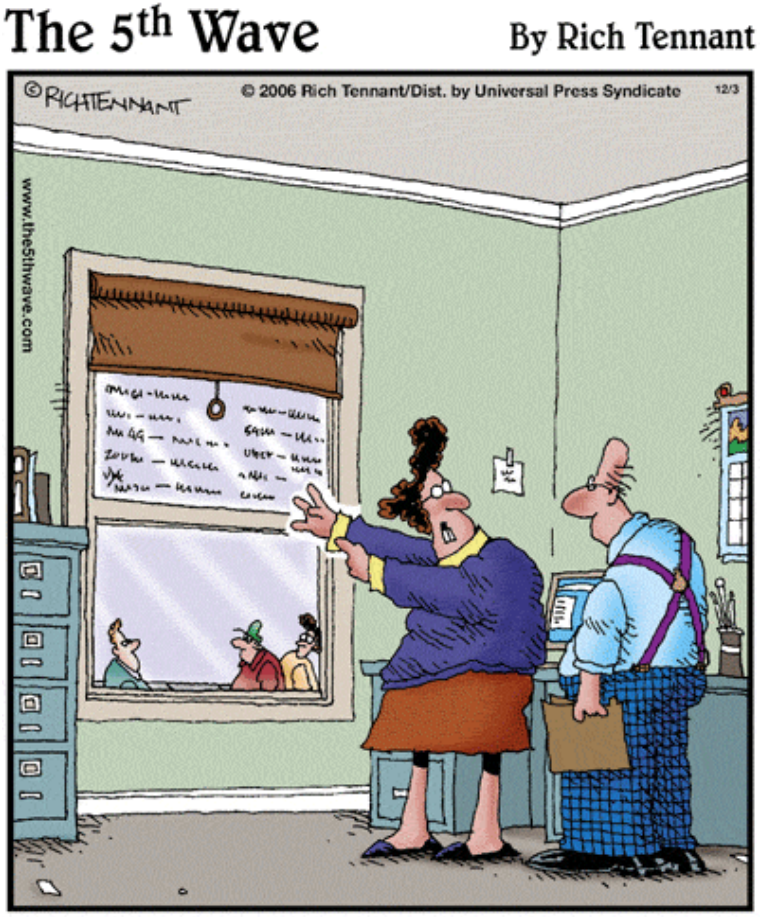
http://www.leakedin.com/

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

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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Opbevaring af passwords

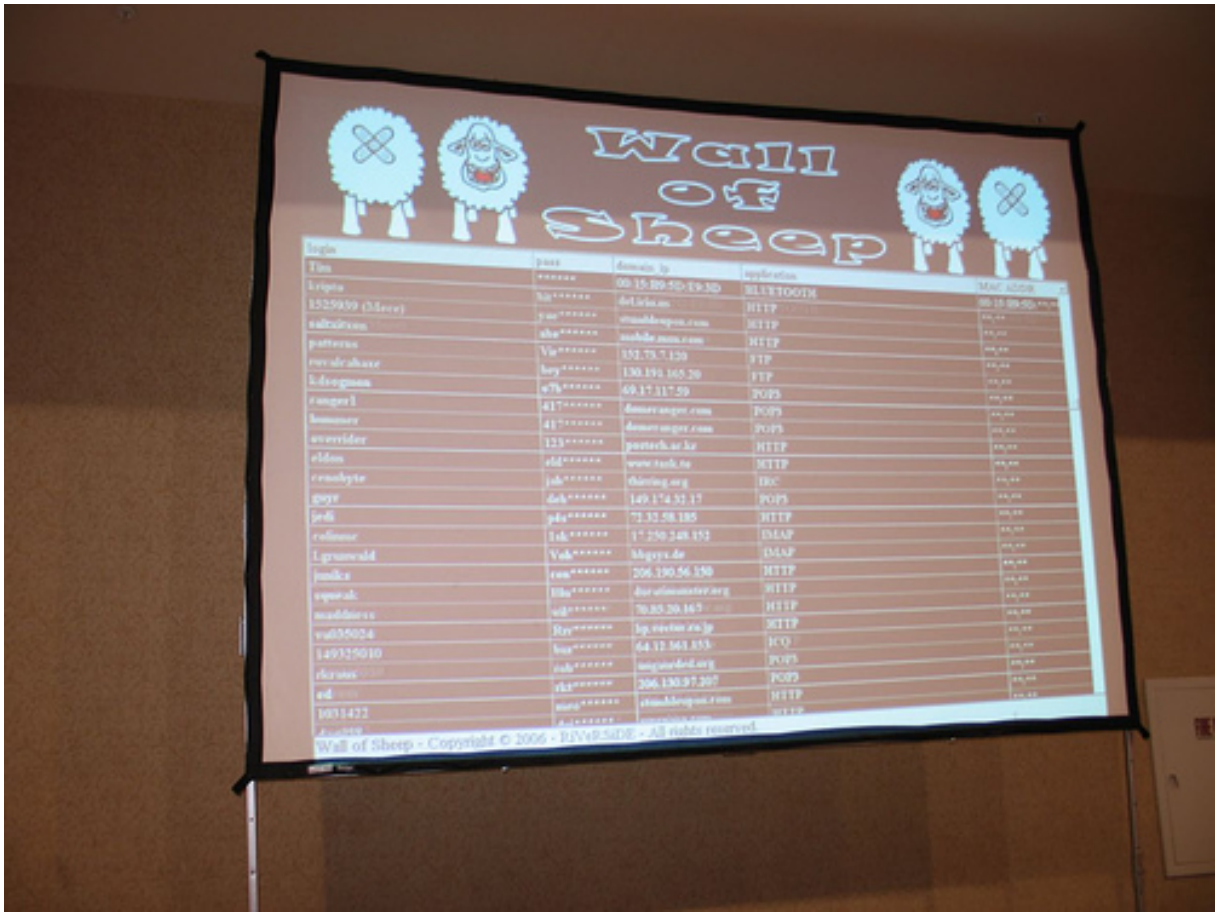


"Don't be silly — of course my passwords are safe. I keep them written on my window, but then I pull the shade if anyone walks in the room."

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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

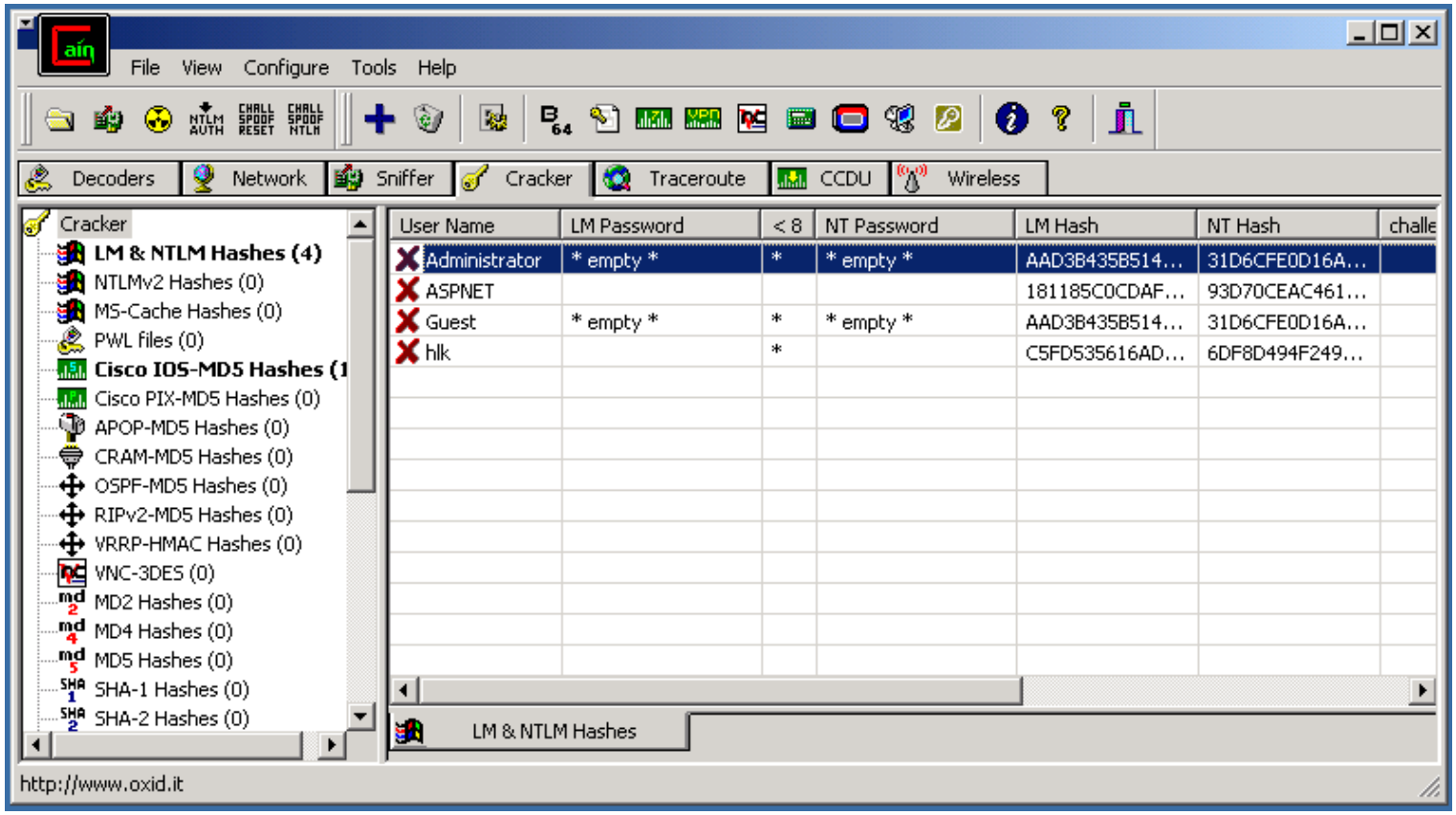
Wall of sheep



Defcon Wall of Sheep

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Cain & Abel



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

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Pause

Er det tid til en lille pause?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hackers do not discriminate

We have seen lots of hacker stories, and we learn:

We are all targets of hacking

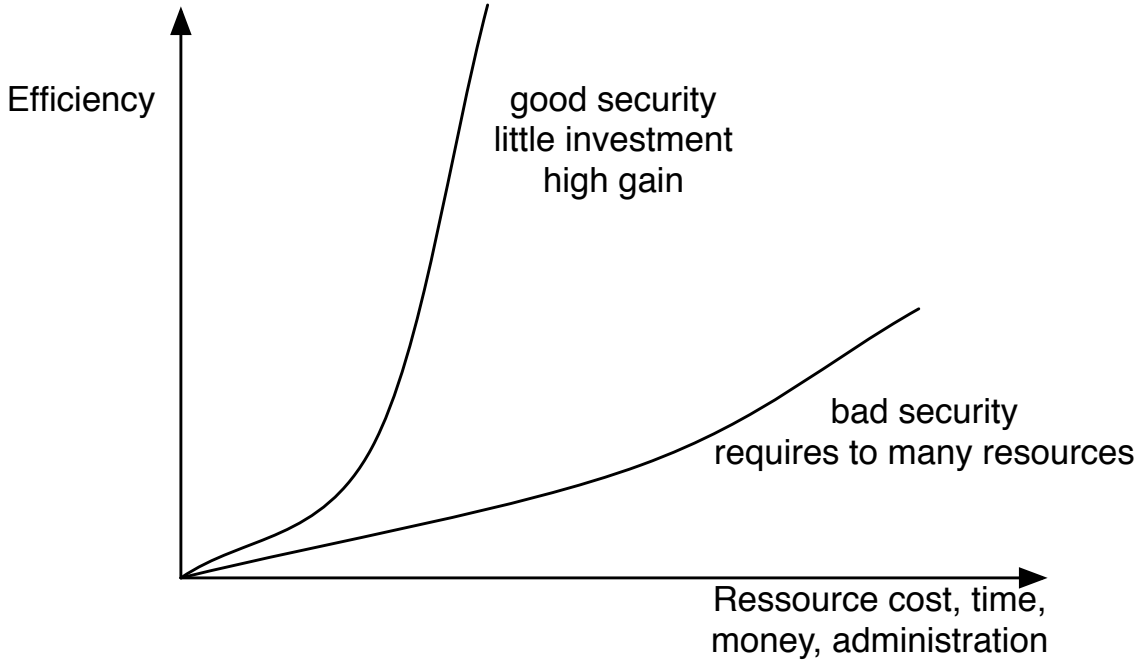
Social Engineering rockz! Phishing works.

Anyone can be hacked - resources used to protect vs attackers resources

Hacking is not cool

© license CC BY 3.0. 2013 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. 2013 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. 2013 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.

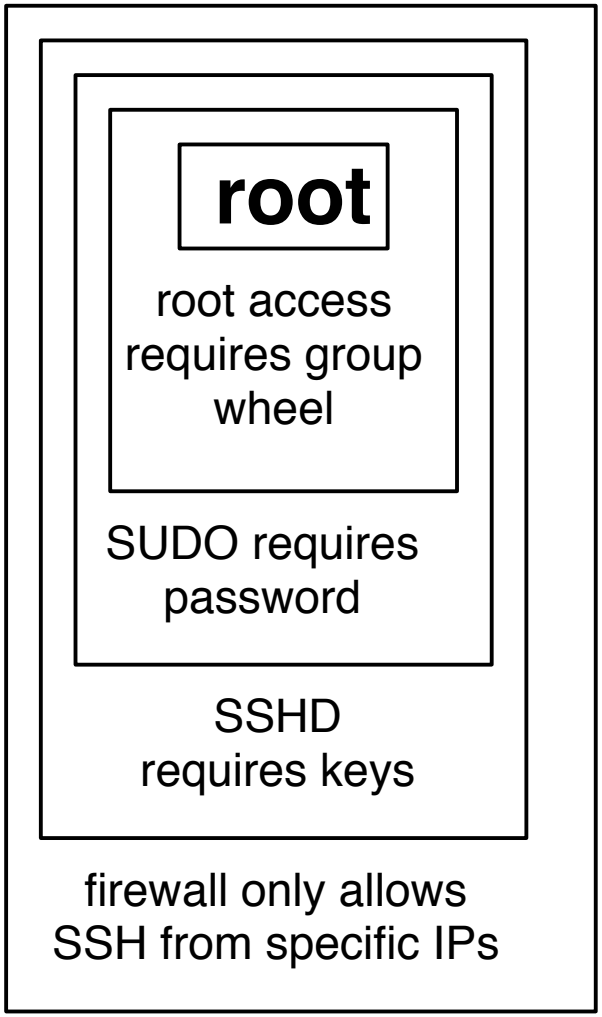
Note: these still have errors and bugs, but are better than older versions

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. 2013 Solido Networks, Henrik Lund Kramshøj

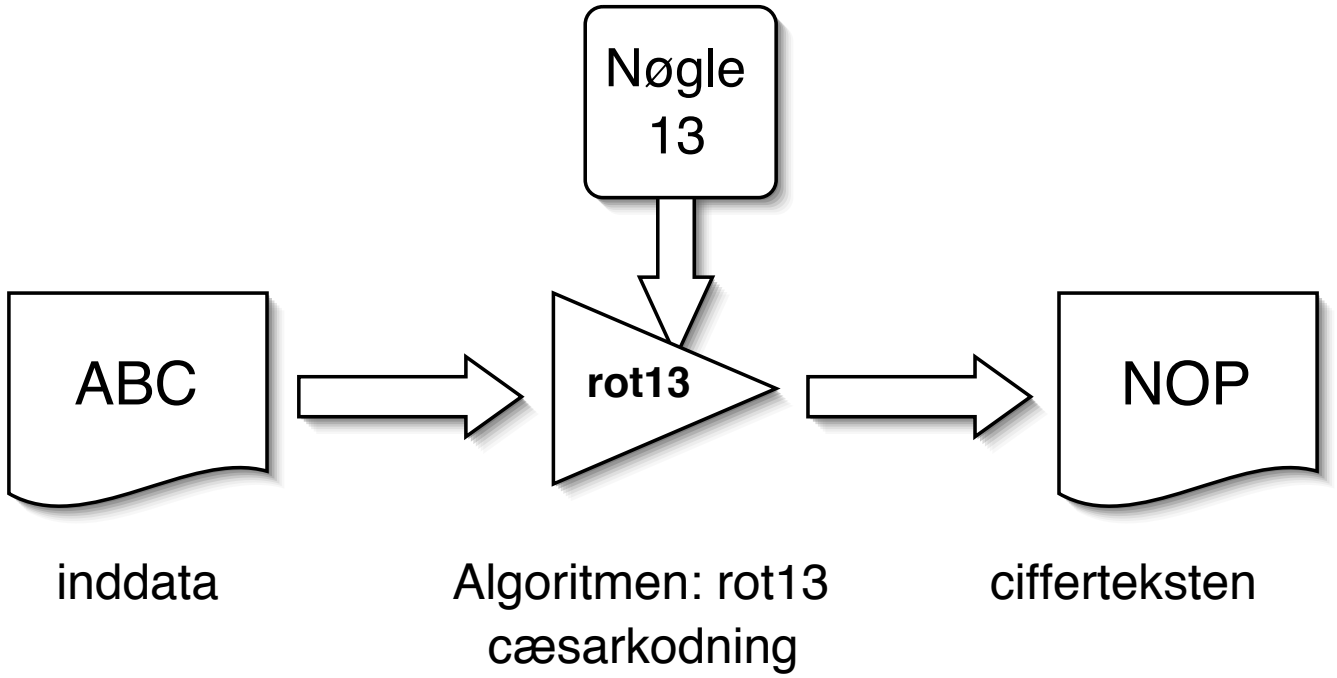
Defense in depth



Defense using multiple layers is stronger!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Kryptografi

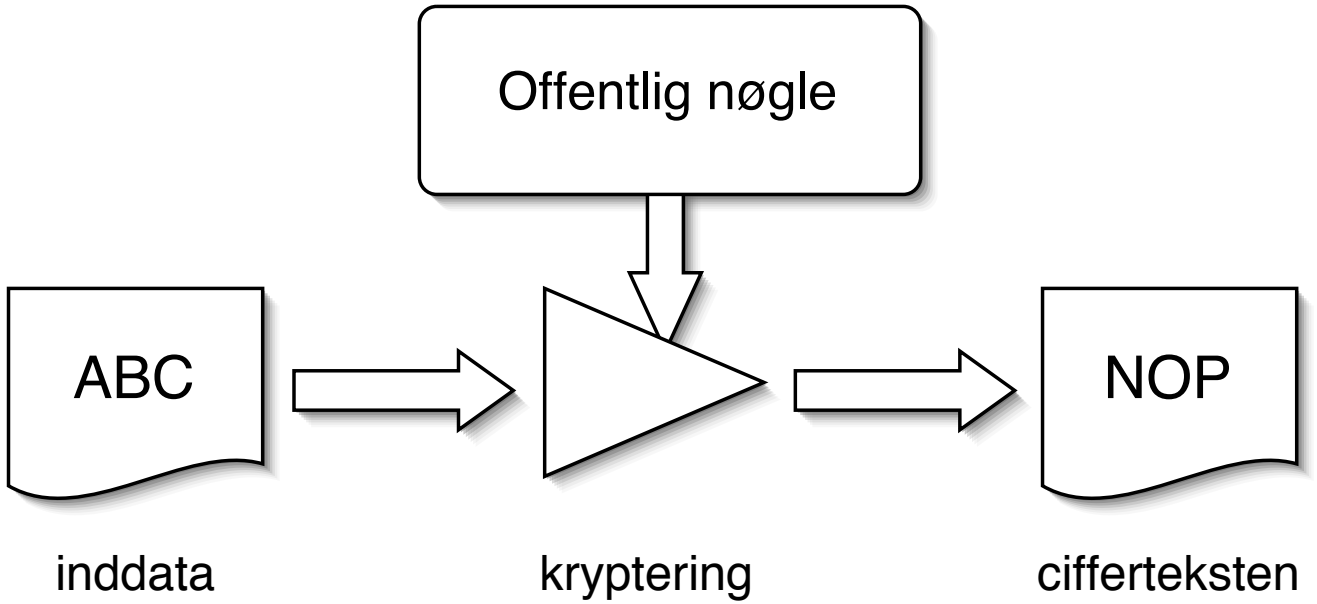


Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en ciffertekst - der kun kan læses ved hjælp af den tilhørende nøgle

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Public key kryptografi - 1

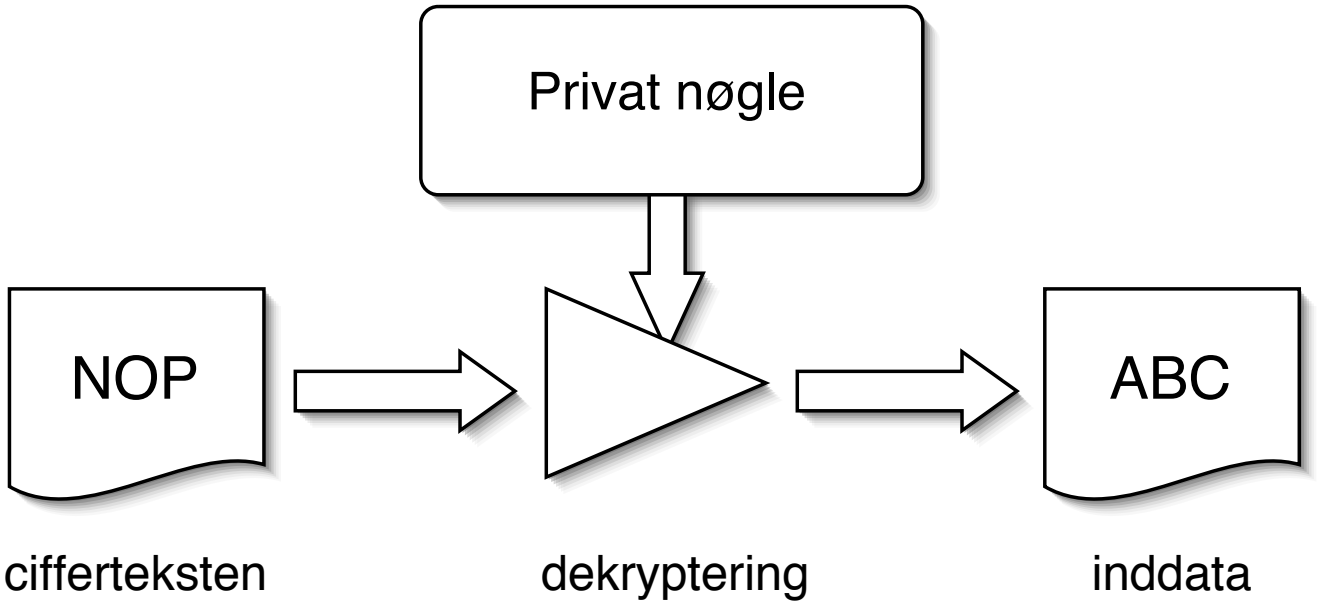


privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

offentlig-nøgle kryptografi (eksempelvis RSA) benytter to separate nøgler til kryptering og dekryptering

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Public key kryptografi - 2



offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere

man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter - som så verificeres med den offentlige nøgle

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Formålet med kryptering

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

DES, Triple DES og AES

AES

Advanced Encryption Standard

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

`http://www.cs.bc.edu/~straubin/cs381-05/blockciphers/rijndael_ingl`
`swf?utm_content=bufferfabef&utm_source=buffer&utm_medium=twitter&u`
`campaign=Buffer`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

hashing algoritmer

NIST announced a public competition in a Federal Register Notice on November 2, 2007 to develop a new cryptographic hash algorithm called SHA-3. The competition is NIST's response to advances made in the cryptanalysis of hash algorithms.

...

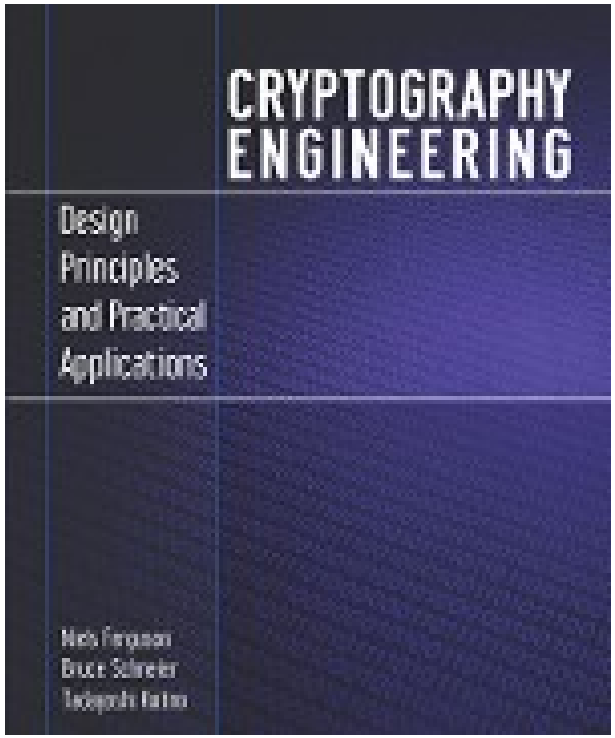
Based on the public comments and internal review of the candidates, NIST announced **Keccak** as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012, and ended the five-year competition.

`http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Sikre protokoller som bruger crypto

Kryptering af e-mail

- Pretty Good Privacy - Phil Zimmermann
- PGP = mail sikkerhed

Kryptering af sessioner SSL/TLS

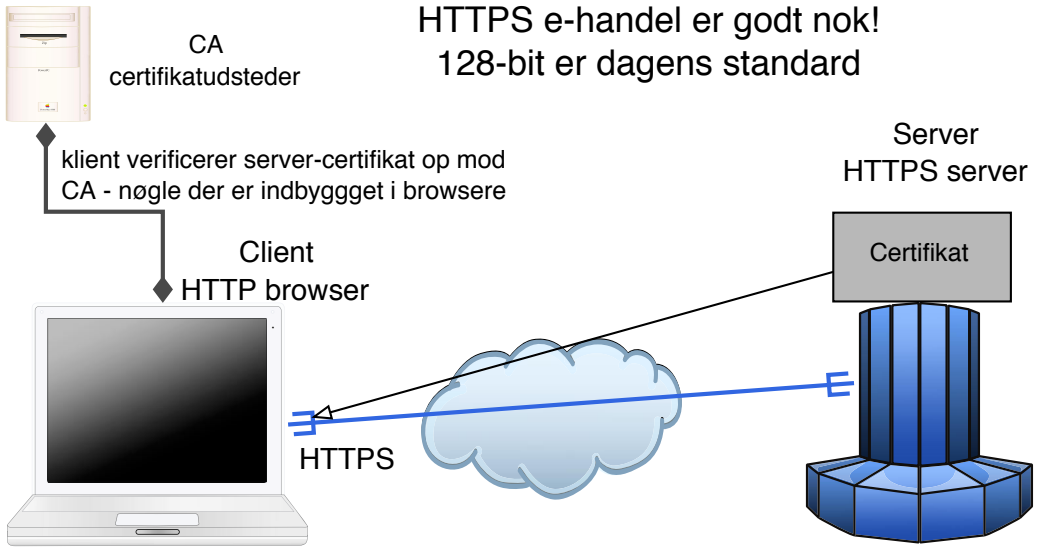
- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Kryptering af netværkstrafik - Virtual Private Networks VPN

- VPN IPsec IP Security Framework, se også L2TP
- VPN PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- SSL VPN, OpenVPN m.fl.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SSL og TLS



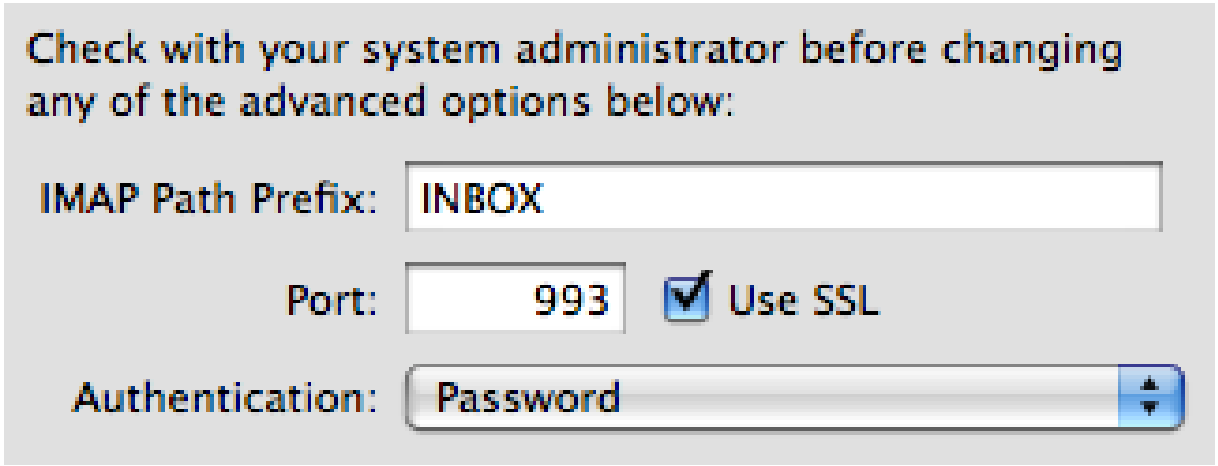
Oprindeligt udviklet af Netscape Communications Inc.

Secure Sockets Layer SSL er idag blevet adopteret af IETF og kaldes derfor også for Transport Layer Security TLS TLS er baseret på SSL Version 3.0

RFC-2246 The TLS Protocol Version 1.0 fra Januar 1999

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SSL/TLS udgaver af protokoller



Mange protokoller findes i udgaver hvor der benyttes SSL

HTTPS vs HTTP

IMAPS, POP3S, osv.

Bemærk: nogle protokoller benytter to porte IMAP 143/tcp vs IMAPS 993/tcp

Andre benytter den samme port men en kommando som starter:

SMTP STARTTLS RFC-3207

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SSL

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.

Nu vi snakker om kryptering - SSL overalt?

Kan vi klare det på vores servere?

Google kan:
`http://www.imperialviolet.org/2010/06/25/overclocking-ssl.html`

Men alt for få gør det

Næste spørgsmål er så hvilke rod-certifikater man stoler på ...

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Secure Shell - SSH og SCP

Hvad er Secure Shell SSH?

Oprindeligt udviklet af Tatu YlÃ¶nen i Finland,
se `http://www.ssh.com`

SSH afløser en række protokoller som er usikre:

- Telnet til terminal adgang
- r* programmerne, rsh, rcp, rlogin, ...
- FTP med brugerid/password

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Postservere til klienter

Når vi skal hente post sker det typisk med POP3 eller IMAP

- POP3 Post Office Protocol version 3 RFC-1939
- Internet Message Access Protocol (typisk IMAPv4) RFC-3501

Forskellen mellem de to er at man typisk med POP3 henter posten, hvor man med IMAP lader den ligge på serveren

POP3 er bedst hvis kun en klient skal hente

IMAP er bedst hvis du vil tilgå din post fra flere systemer

Jeg bruger selv IMAPS, IMAP over SSL kryptering - idet kodeord ellers sendes i klartekst

SMTP bruges til at sende mail mellem servere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

POP3 - e-mail i Danmark

POP3 sender brugernavn og kodeord i klartekst - ligesom FTP

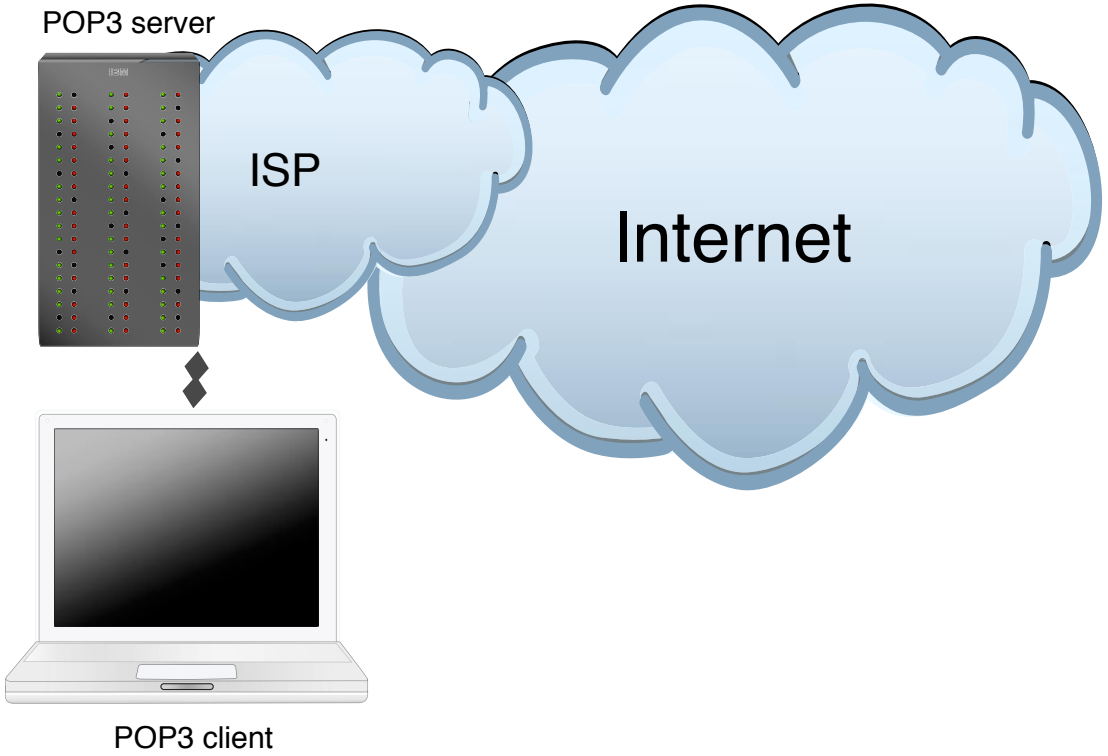
bruges dagligt af næsten alle privatkunder

alle internetudbydere og postudbydere tilbyder POP3

der findes en variant, POP3 over SSL/TLS

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

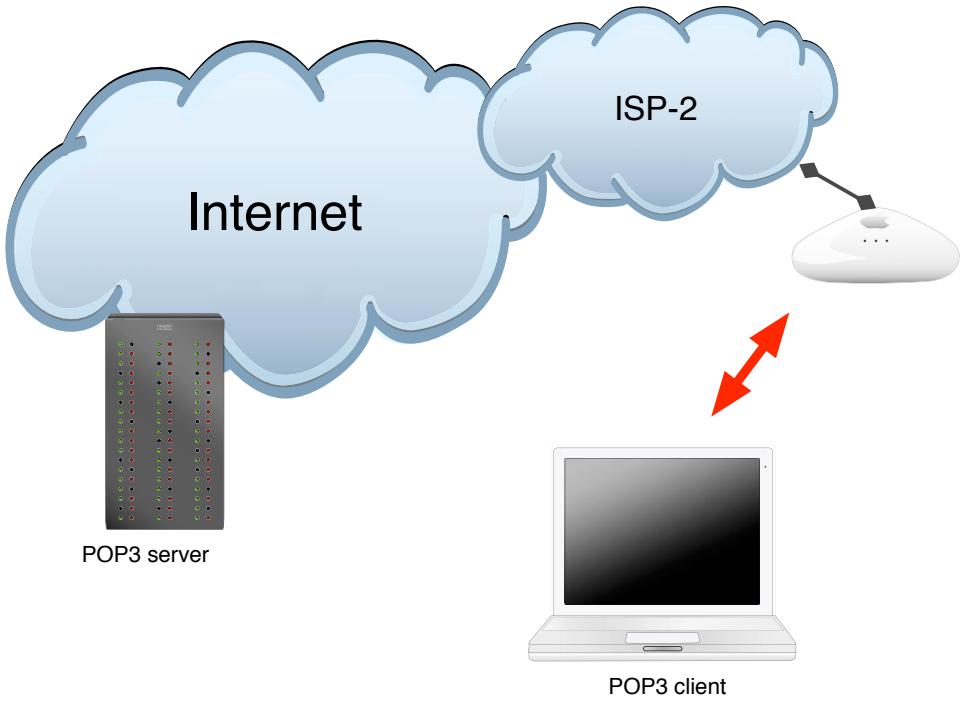
POP3 i Danmark



Man har tillid til sin ISP - der administrerer såvel net som server

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

POP3 i Danmark - trådløst



Har man tillid til andre ISP'er? Alle ISP'er?

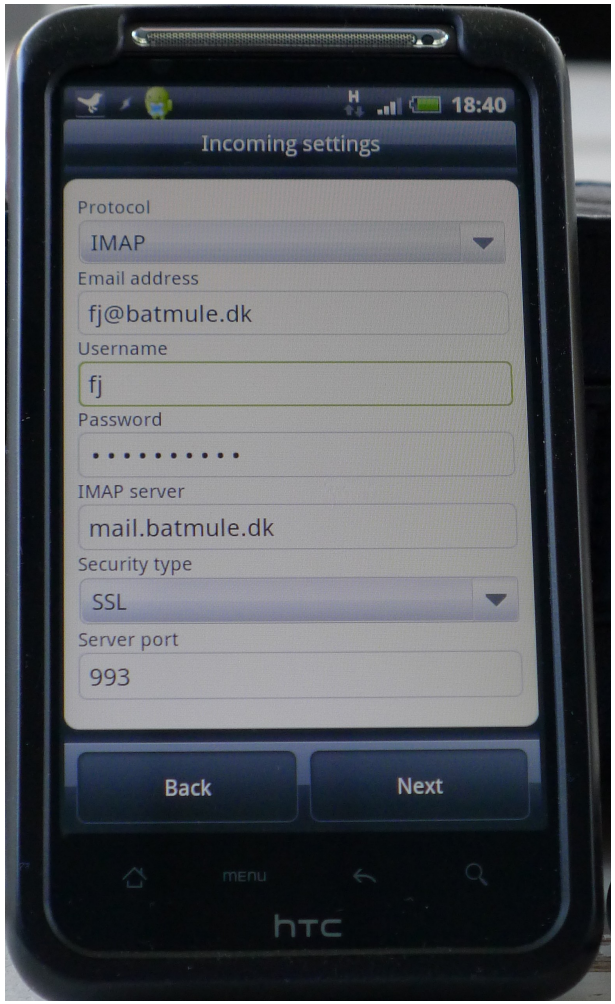
Deler man et netværksmedium med andre?

Brug de rigtige protokoller!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

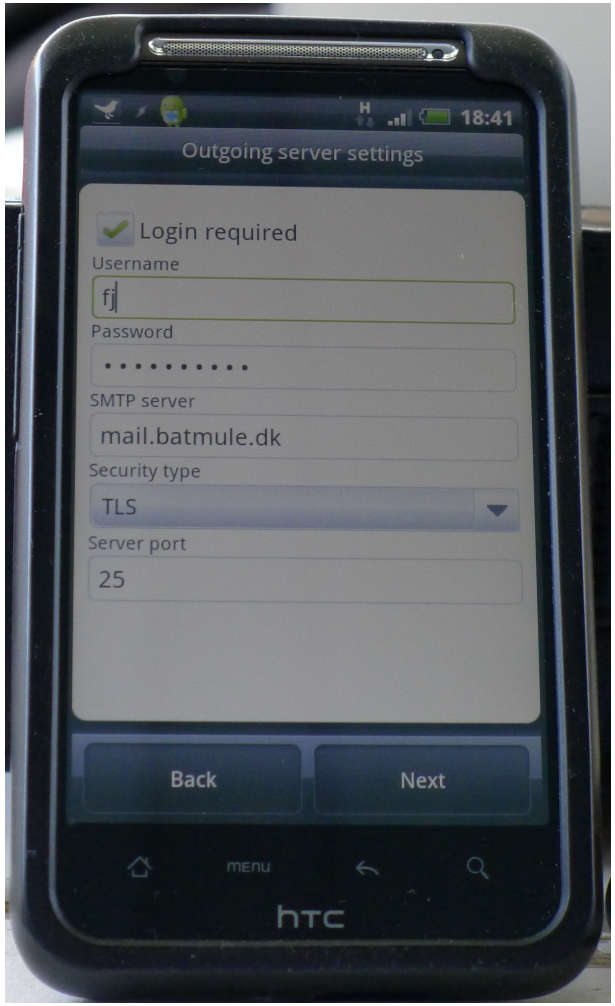
POP3 og IMAP - SSL/TLS (1)

Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SMTP kan erstattes med SMTP+TLS



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Vi laver nu øvelsen

Installation af alternativ browser

som er øvelse 3 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Installation af Thunderbird

som er øvelse 4 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

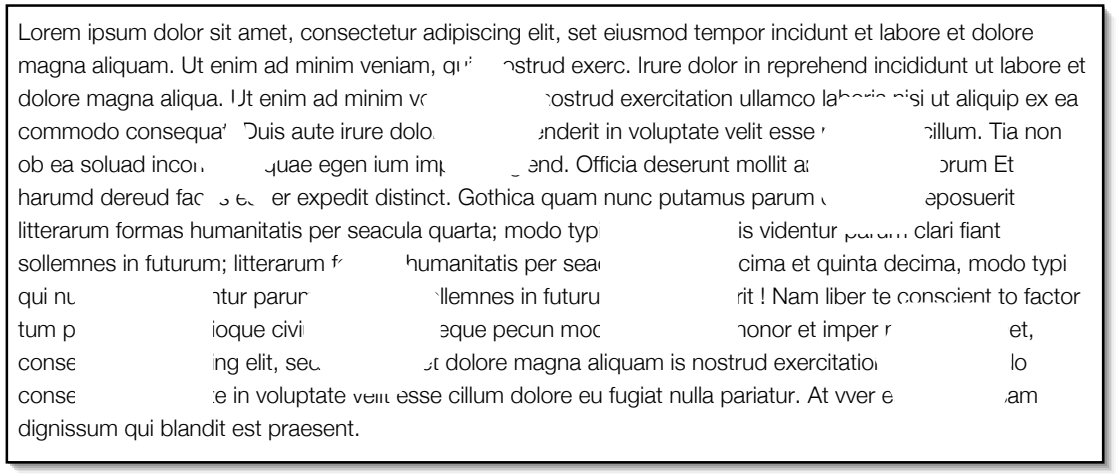
Vi laver nu øvelsen

Installation af GPG GNU Privacy Guard

som er øvelse **5** fra øvelseshæftet.

© license CC BY 3.0. 2013 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. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

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. 2013 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

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

What is it?

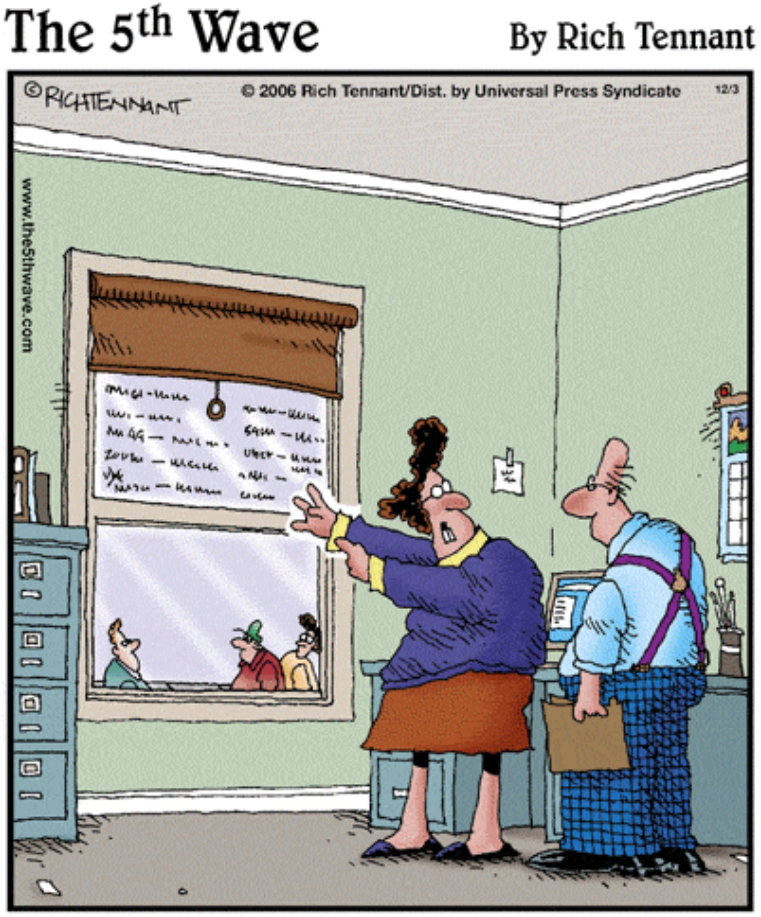
Duplicity backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because duplicity uses **GnuPG**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

© license CC BY 3.0. 2013 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."

© license CC BY 3.0. 2013 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 - 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
- Some vendors have BIOS passwords, or disk passwords

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Vi laver nu øvelsen

Installation af Truecrypt

som er øvelse **6** fra øvelseshæftet.

NB: Der er startet et projekt *Let's audit Truecrypt!*

`http://blog.cryptographyengineering.com/2013/10/lets-audit-truecrypt.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Email sikkerhed

Selvom du kommunikerer sikkert med din mail server sendes email som postkort over internet.

En måde at beskytte data er at bruge PGP, pretty good privacy

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Basale tools - PGP

- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommercielt, men der findes altid en freeware version `http://www.pgp.com`
- Eksporteret fra USA på papir og scannet igen - det var lovligt
- I dag kan en masse information om PGP findes gennem: `http://www.pgpi.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Basale tools - GPG

Gnu Privacy Guard, forkortes GnuPG eller GPG

brug linket: `http://www.gnupg.org/`

Open Source med GPL licens.

Kan bruges på alle de gængse operativsystemer

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

GnuPG - verifikation af downloads

```
$ cd /userdata/download/src/postfix/
$ ls -l *.sig
-rw-r--r--  1 hlk  admin  152 13 Sep  2003 postfix-2.0.16.tar.gz.sig
-rw-r--r--  1 hlk  admin  152  3 May 13:34 postfix-2.1.1.tar.gz.sig
$  gpg --verify postfix-2.1.1.tar.gz.sig
gpg: Signature made Mon May  3 19:34:08 2004 CEST using RSA key ID D5327CB9
gpg:  Good signature from "wietse venema <wietse@porcupine.org>"
gpg:                 aka "wietse venema <wietse@wzv.win.tue.nl>"
$
```

Det er nødvendigt at verificere arkiver med kildekode!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Generering af keys 1

SOLIDO NETWORKS

Generering af key

```
$ gpg --gen-key
```

- Vælg ”DSA and Elgamal”
- Vælg passende keysize - 4096 skader næppe
- Vælg passende udløbsdato - ”no expire” vil virke for de fleste
- Brug din officielle mailaddresse i forbindelse med dit navn, så Email klienter kan finde din key aytomatisk
- Brug en god passphrase.
  En lang sætning som du kan huske, og som ikke kan gættes udfra kendskab til dig.
- Når nøglen genereres, så hjælp med at generere ”randomness” i systemet. Det får genereringen til at gå hurtigere, og det giver en bedre key.

samme spørgsmål i GUI programmerne, **og husk at lave et revoke certifikat!**

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Generering af keys 2

Du har nu en GnuPG key klar til at blive signeret

Er du **sikker** på at du kan huske din passphrase?

Når nøglen er genereret bliver der vist et kort sammendrag af indholdet
Dette *fingerprint* kan også fås frem med:

```
$ gpg --fingerprint addr@domain.dk
pub   1024D/D1EFBAA6 2003-01-20
      Key fingerprint = 0FAE F19D DB46 DF2E D93D  9B05 21A6 469B D1EF BAA6
uid                  Henrik Lund Kramshoej (work email) <hlk@security6.net>
uid                  Henrik Lund Kramshoej (Kramse) <hlk@kramse.dk>
uid                  [jpeg image of size 14412]
sub   2048g/6D08E6E6 2003-01-20
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Opsætning af defaults

Vi sætter defaults der sikrer:

- Ingen brok over usikker brug af hukommelsen (at låse sider kræver root, dvs. SUID på UNIX)
- Valg af default keyserver
- Valg af default key (hvis du har flere)
- Valg af karaktersæt

```
$ tail ~/.gnupg/gpg.conf
no-secmem-warning
keyserver hkp://pgp.mit.edu/
default-key D1EFBAA6
charset ISO-8859-1
```

Det gør livet lidt lettere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Signering af keys

Keys signeres med:

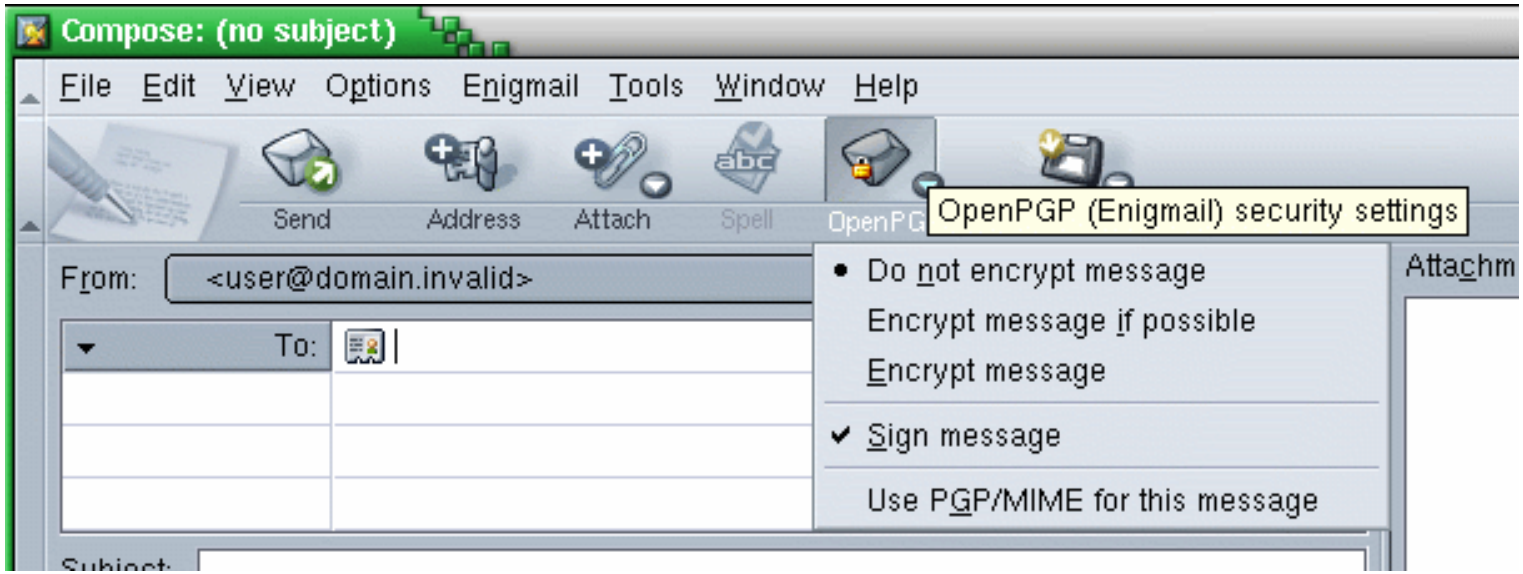
```
gpg --sign-key addr@domain.dk  # Eller keyid
```

Husk at sikre at det nu også er den korrekte key i signerer
Kontroller med:

```
gpg --fingerprint addr@domain.dk
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

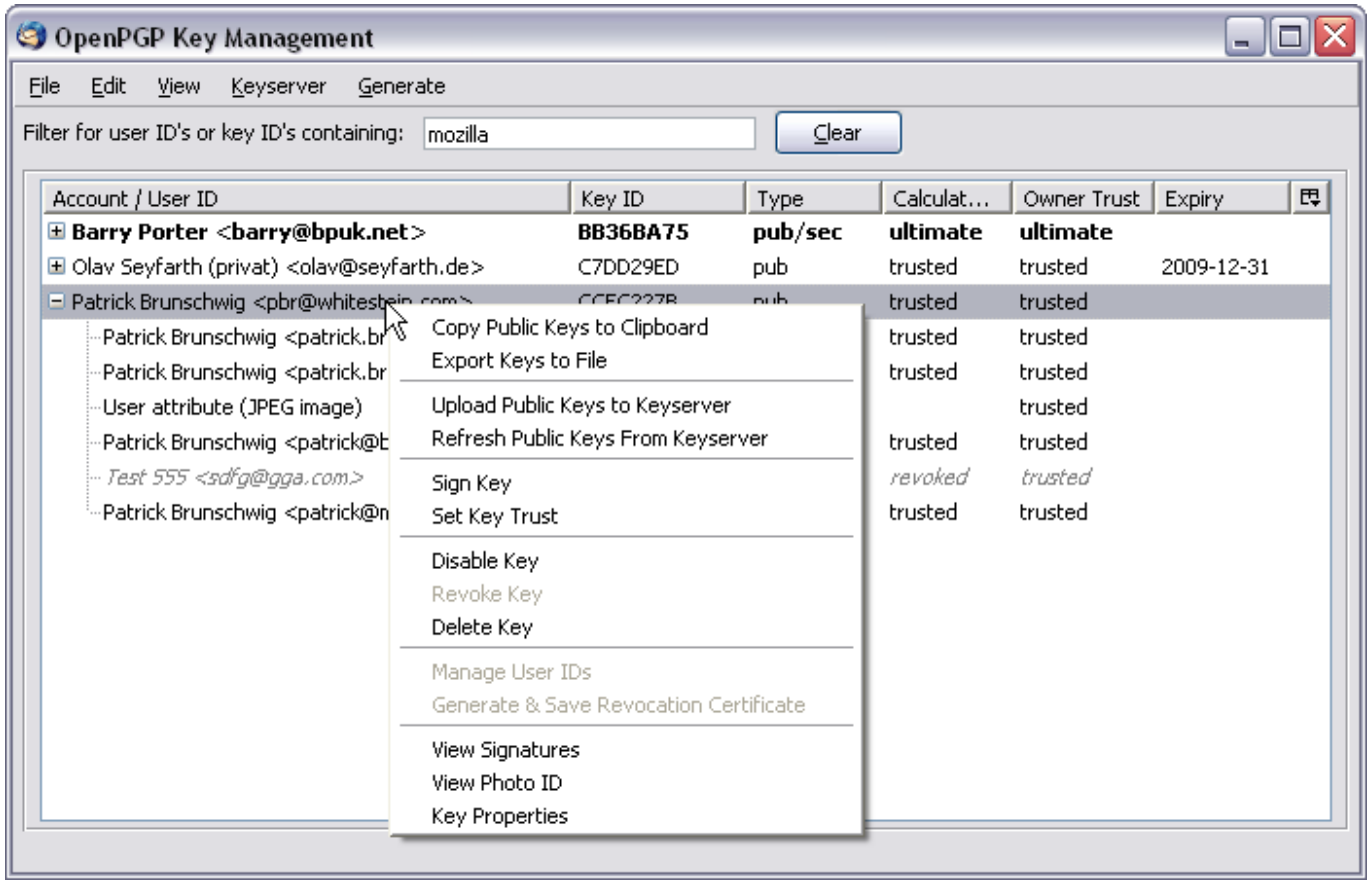
Enigmail - GPG plugin til Mail



- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra `http://enigmail.mozdev.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

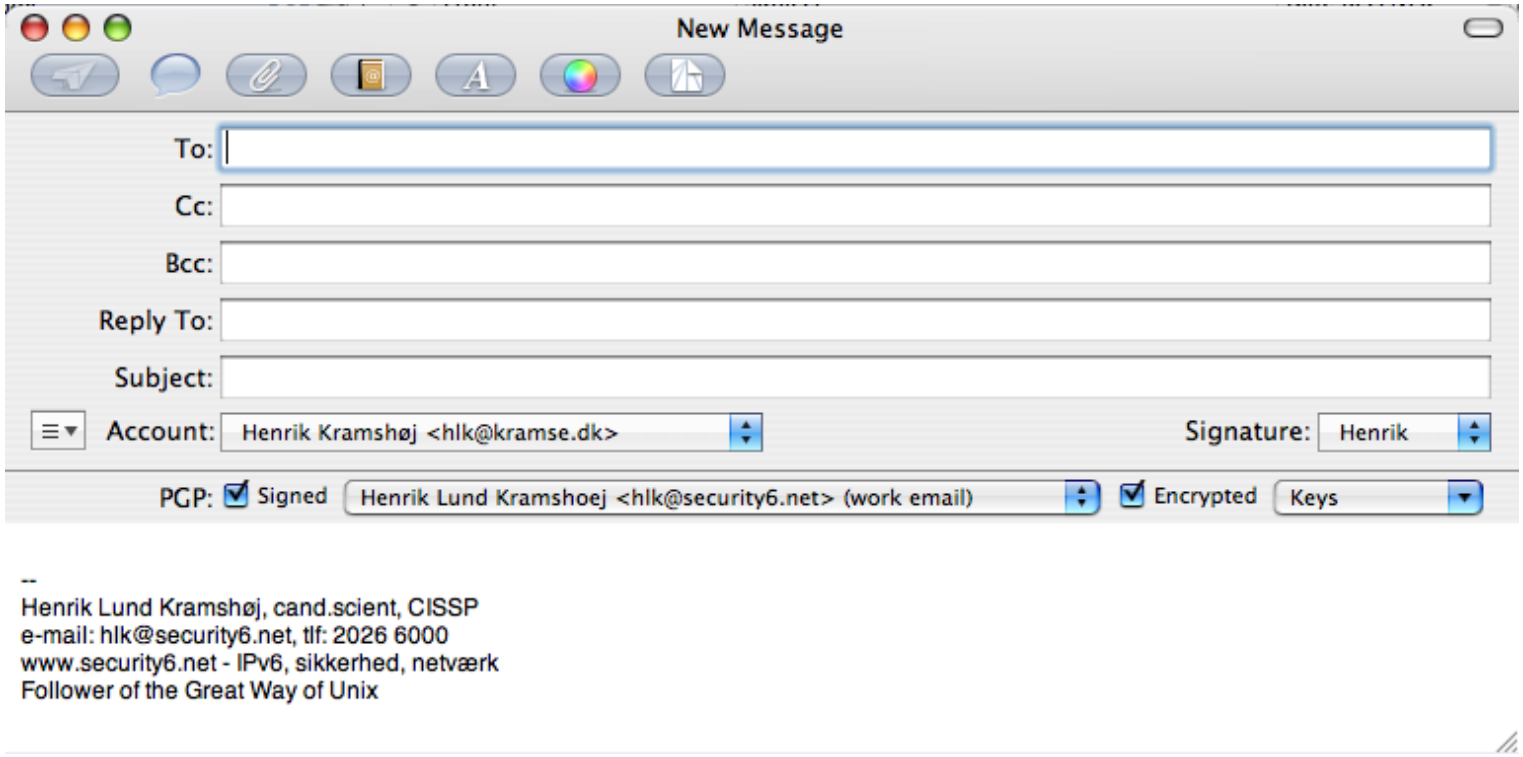
Enigmail - OpenGPG Key Manager



Key Manager funktionaliteten i Enigmail kan anbefales

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

GPGMail plugin til Mac OS X Mail.app



- Bruger GPG
- kilde: `http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Installation af Enigmail plugin

som er øvelse 7 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Lav en PGP-kompatibel nøgle

som er øvelse 8 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Hent en nøgle fra en anden

som er øvelse 9 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Send en krypteret mail

som er øvelse 10 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Signer en nøgle

som er øvelse 11 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Do NOT USE FTP

File Transfer Protocol - filoverførsler

FTP bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- Opdatering af websites
- Overførsel af data mellem virksomheder
- Serveren er indbygget i de fleste serveroperativsystemer

FTP sender i klartekst
USER brugernavn og
PASS hemmeligt-kodeord

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

FileZilla - understøtter SFTP

FileZilla Features

Overview

FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features

Features

Among others, the features of FileZilla include the following:

- Easy to use
- Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, *BSD, Mac OS X and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files >4GB
- Tabbed user interface
- Powerful Site Manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits

http://filezilla-project.org/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

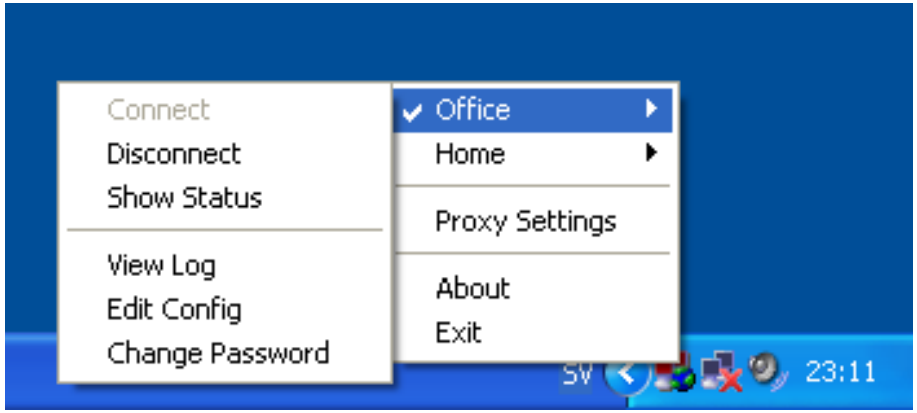
Vi laver nu øvelsen

Installation af FileZilla

som er øvelse **12** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

VPN



Virtual Private Networks are useful - or even required when travelling

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 :-(

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Internet sniffing by government

Ægypten, Sudan, Tunesien, ...

Den der kontrollerer ISPerne kontrollerer trafikken

Facebook revolutionerne

Blokering er umulig, men det forsøges

Spredning af falsk information

Diginotar Dutch Certificate Authority

Kilde: `http://irevolution.net/2011/02/10/facebook-for-repressive-regimes/`

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

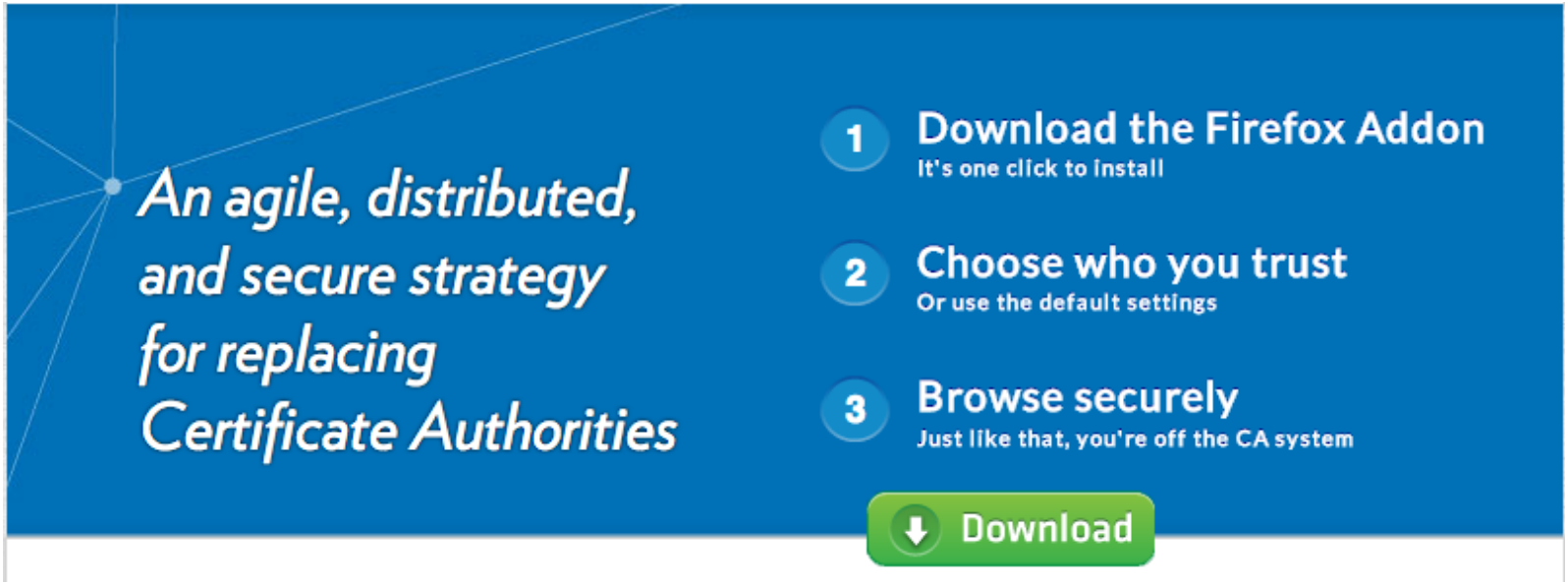
CertPatrol - which site uses which certificate

An add-on formerly considered paranoid: CertPatrol implements ”pinning” for Firefox/Mozilla/SeaMonkey roughly as now recommended in the User Interface Guidelines of the World Wide Web Consortium (W3C).

`http://patrol.psyced.org/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Convergence - who do you trust



`http://convergence.io/`

Warning: radical change to how certificates work

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Censurfridns.dk uncensoredDNS

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

Velkommen til www.censurfridns.dk.

Du er velkommen til at benytte:

ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::
ns2.censurfridns.dk / 89.104.194.142 / 2002:5968:c28e::53
som DNS server for at undgå DNS censur.
Se venligst blog.censurfridns.dk for mere info.
```

Det er uacceptabelt at pille ved DNS - punktum!

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

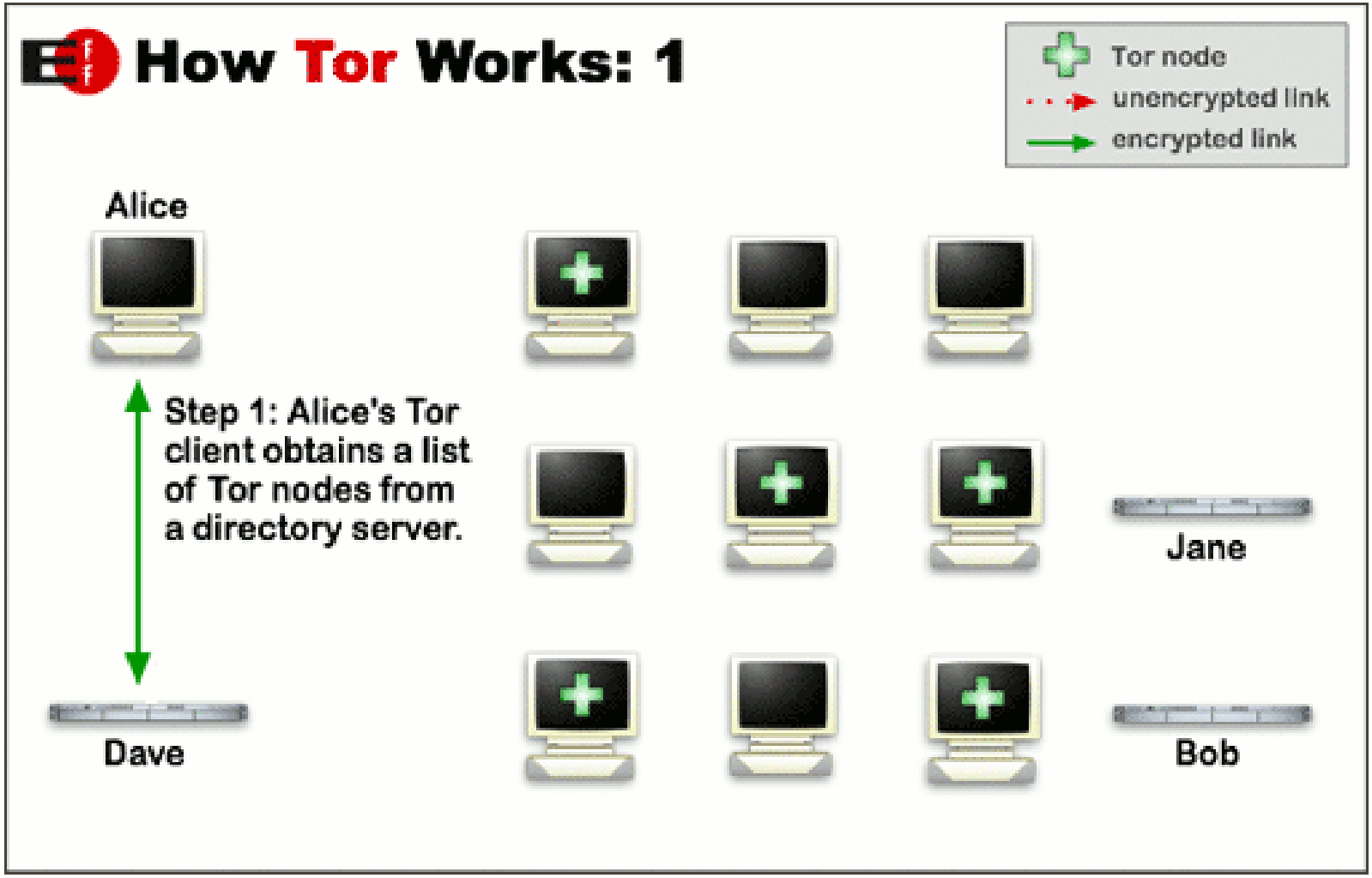
Tor project

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

Der findes alternativer, men Tor er mest kendt

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

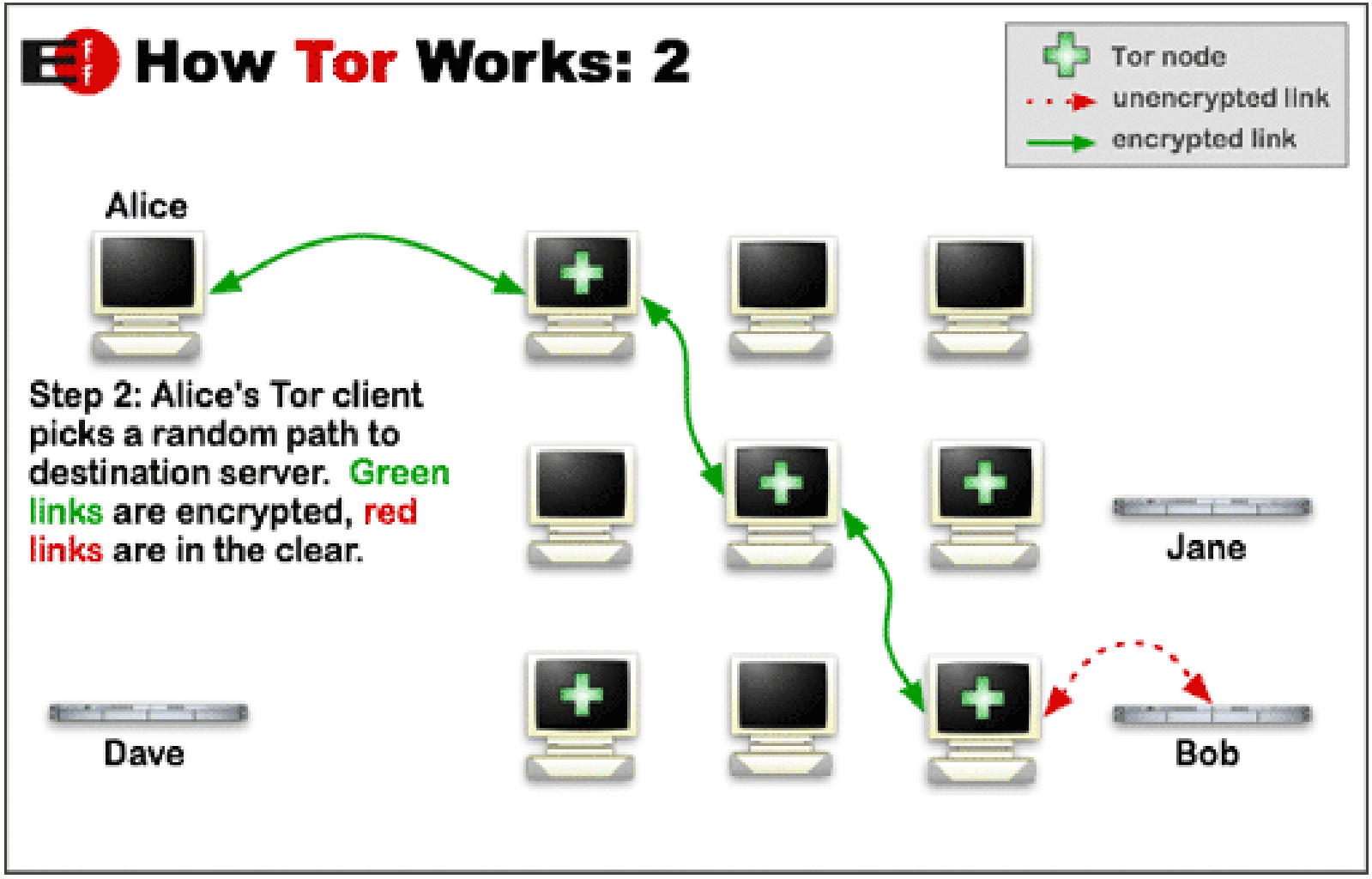
Tor project - how it works 1



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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

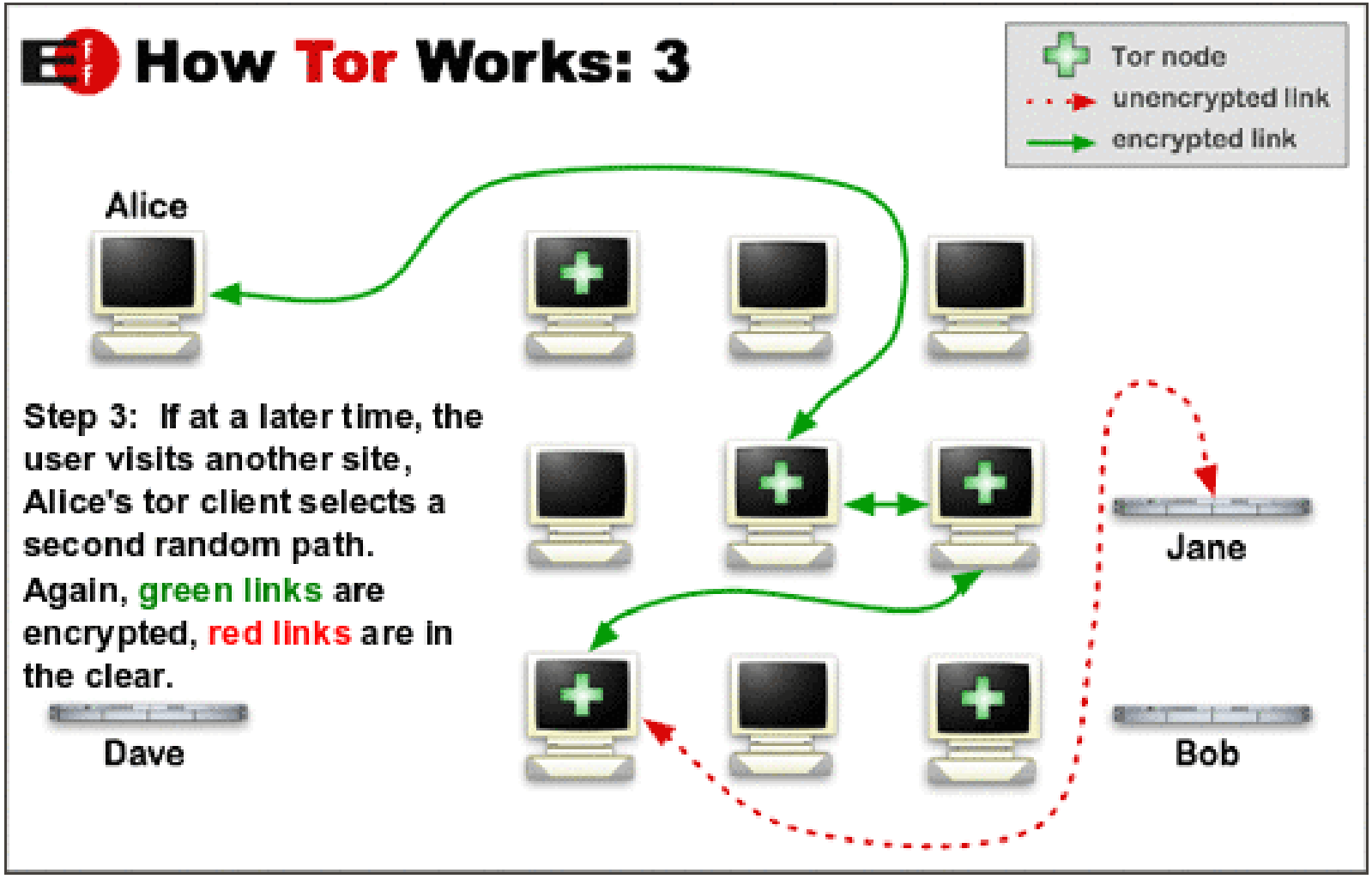
Tor project - how it works 2



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

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Tor project install

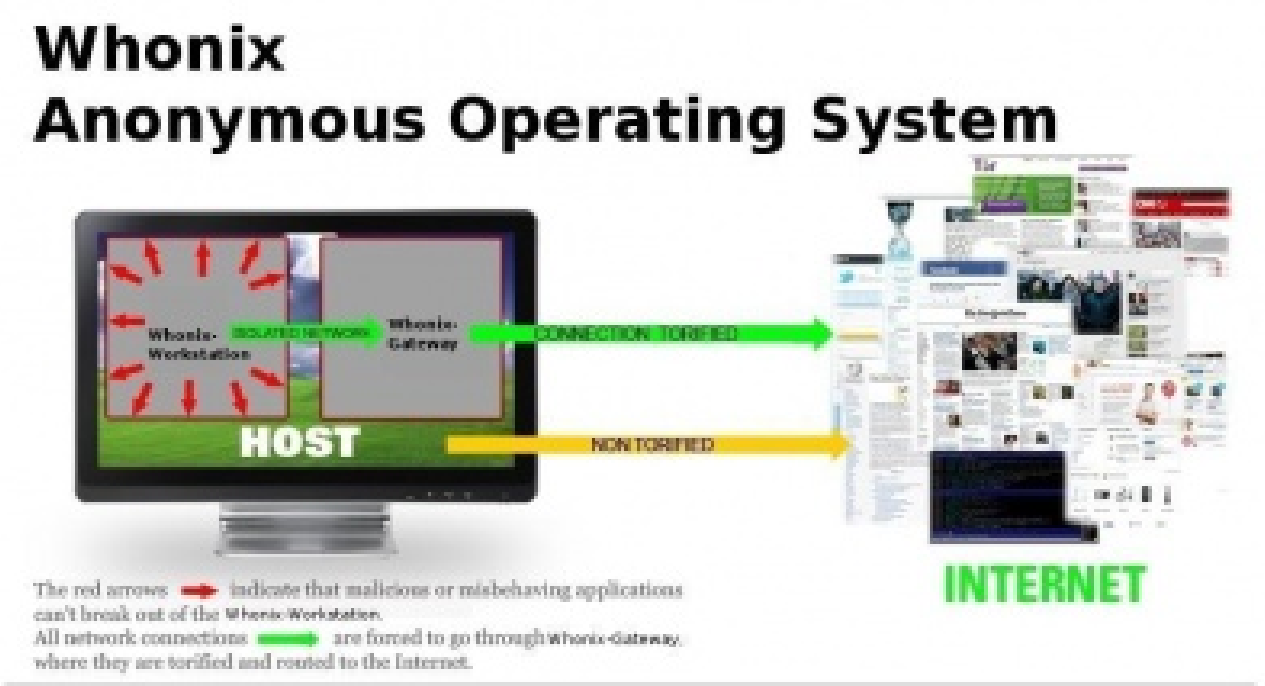
Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

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

Pause mens dem som vil installere gør det

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Bonus: brug Bitcoins?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Definition

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.

Computer Forensics: Incident Response Essentials, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

TASK og Autopsy

Inspireret af TCT har Brian Carrier fra Atstake lavet flere værktøjer til forensics analyse

Det officielle hjem for TASK og autopsy er nu: `www.sleuthkit.org`

TASK kan betragtes som en erstatning for TCT the coroners toolkit lavet af Dan Farmer og Wietse Venema

Autopsy er en Forensic Browser - et interface til TASK

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hvordan slettes data

- Filsystemer skal være hurtige - skal ikke lave unødvendige operationer
- En harddisk er en fysisk disk med en arm der skal bevæges og et læse/skrivehoved som skal tændes og slukkes
- Hvis man kan undgå at skulle skrive over hele filen ved sletning er det hurtigere
- De fleste operativsystemer sletter derfor kun metadata og overskriver derfor ikke alle datablokke for filer
- Eksempel DOS FAT
  Når man slettede en fil på MS-DOS fjernede man reelt kun det første bogstav i filnavnet
  undelete bestod i at skrive det første bogstav i filnavnet - og håbe på at alle datablokke der hørte til filen stadig var at finde på disken

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Guttman paper - analyse af diske

Secure Deletion of Data from Magnetic and Solid-State Memory Peter Gutmann, 1996

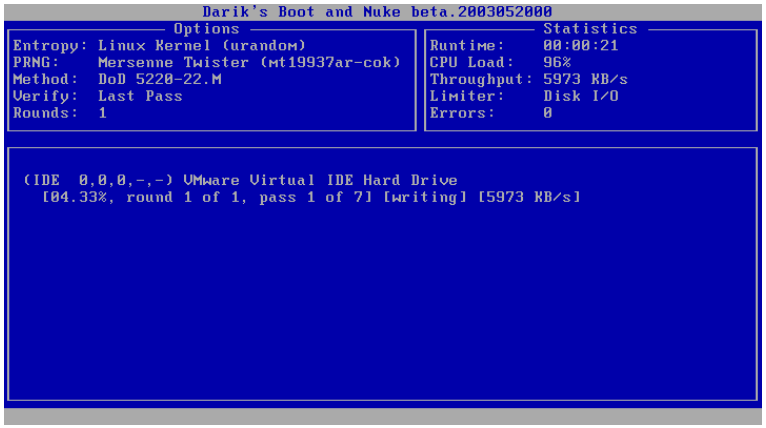
Det er et klassisk paper om sletning af data som man bør læse
`http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html`

Der findes mange kommercielle værktøjer til sletning og en del Open Source - baseret på Guttman's dokument

DBAN er efter min mening et af de bedste
`http://dban.sourceforge.net/` USB

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

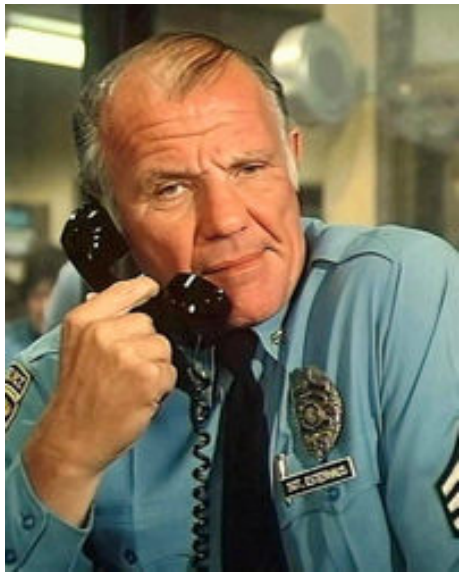
Darik's Boot and Nuke



- ad-hoc oprydning, formatering og sletning af filer giver ingen sikkerhed!
- Free. Fast. Rapid deployment in emergency situations.
- Easy. Start the computer with DBAN and press the ENTER key.
- Safe. Irrecoverable data destruction. Prevents most forensic data recovery techniques.
- `http://dban.sourceforge.net/`
- NB: Brug `http://unetbootin.sourceforge.net/` til at skrive CD-image til

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Be careful



Hey, Lets be careful out there!

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

Nødvendigt eller er det ekstreme teknikker vi har diskuteret?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Pause

Er det tid til en lille pause?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Part III: Mere Hacking, Hackerværktøjer

Teknisk hvad er hacking - og værktøjer
Mere frit - vi undersøger diverse emner som hackere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Målet for denne del

Don’t Panic!

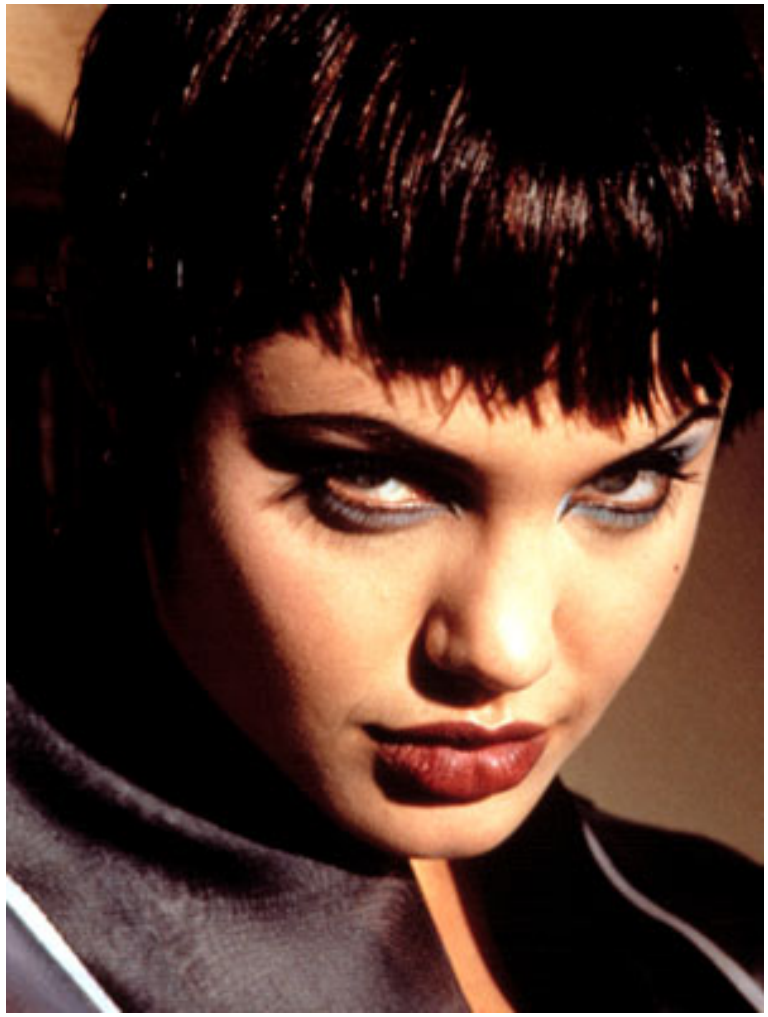
Introduce hacking and a couple of hacker tools

List some tools that can be used to protect your computer and data

PS Sorry about the many TLAs ... og danglish

præsentationen er meget teknisk, men foredraget behøver ikke at blive det ☺

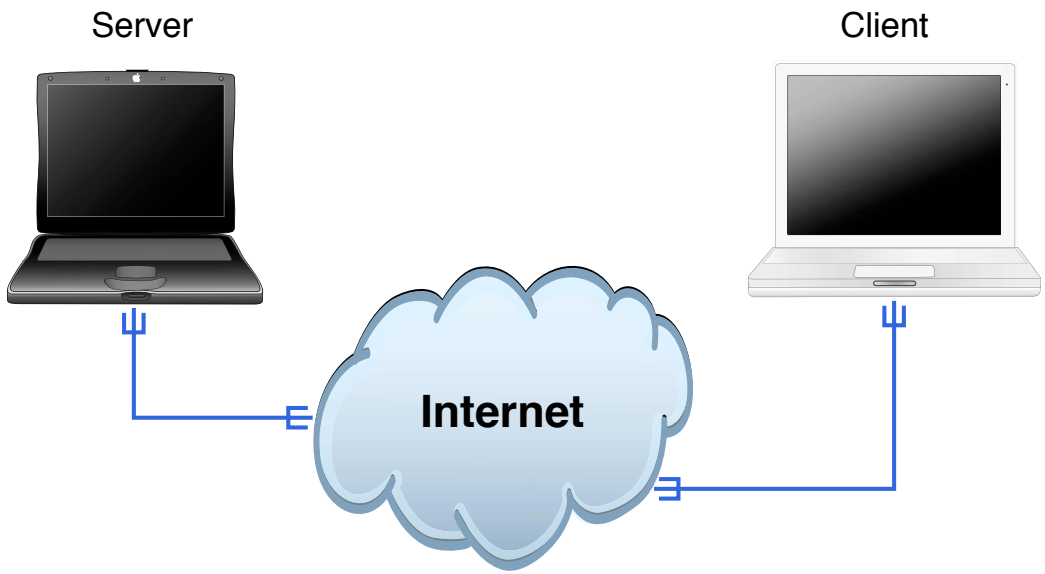
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj



http://www.imdb.com/title/tt0113243/ Hackers (1995)

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Internet today



Clients and servers

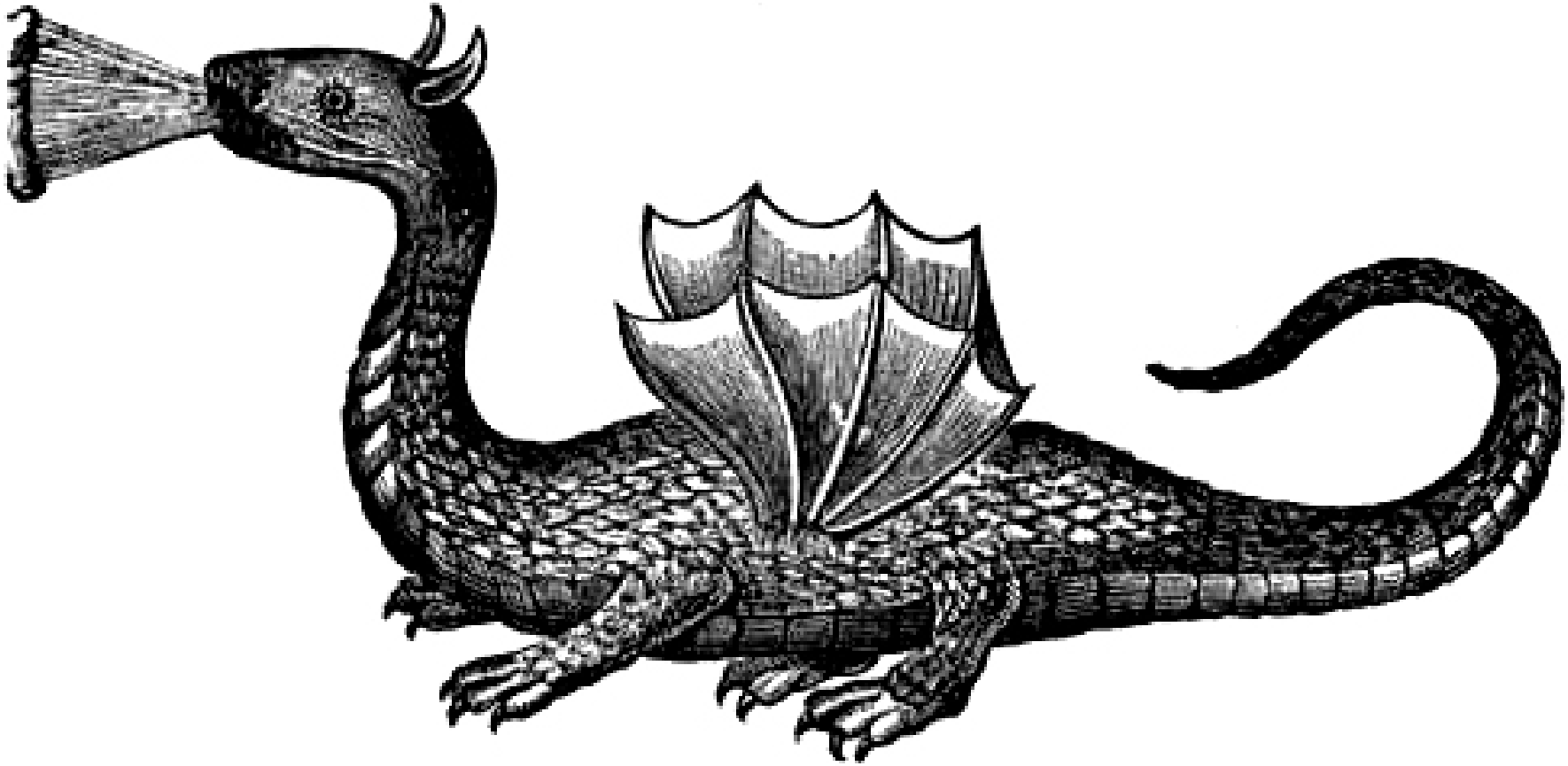
Rooted in academic networks

Protocols which are more than 20 years old, moved to TCP/IP in 1981

Trying to migrate to IPv6 - a lot of hacking opportunities here

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Internet - Here be dragons



© license CC BY 3.0. 2013 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. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

Internet er åbne standarder!

SOLIDO NETWORKS

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

RFC, BCP, FYI, informational
de første stammer tilbage fra 1969

Ændres ikke, men får status Obsoleted når der udkommer en nyere version af en standard

Standards track:
Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

The Internet Worm 2. nov 1988

SOLIDO NETWORKS

Udnyttede følgende sårbarheder

- buffer overflow i fingerd - VAX kode
- Sendmail - DEBUG
- Tillid mellem systemer: rsh, rexec, ...
- dårlige passwords

Avanceret + camouflage!

- Programnavnet sat til 'sh'
- Brugte fork() til at skifte PID jævnligt
- password cracking med intern liste med 432 ord og /usr/dict/words
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...

Lavet af Robert T. Morris, Jr.

Medførte dannelsen af CERT, `http://www.cert.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder
- At man får konfiskeret sit udstyr af politiet
- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde - eller fængselsstraf i alvorlige tilfælde
- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien
- Frit efter: `http://www.stophacking.dk` lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

DDoS udviklingen, januar 2010 rapporten

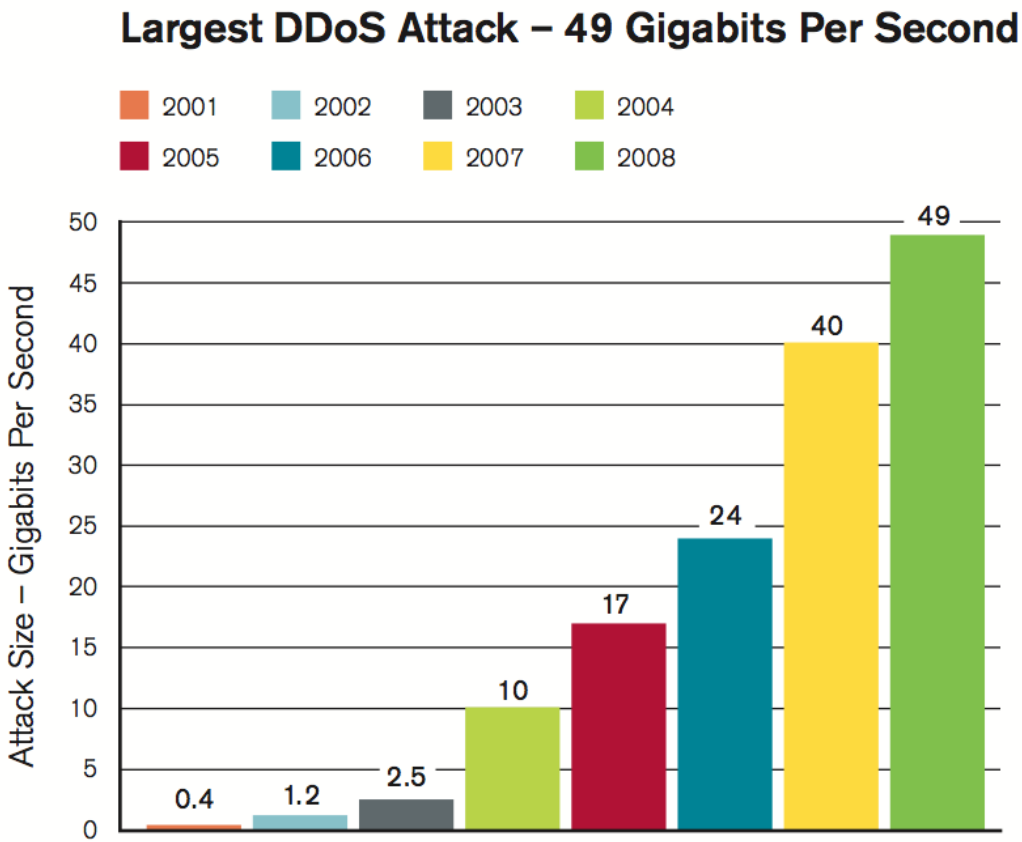


Figure 1: *Largest DDoS Attack – 49 Gigabits Per Second*

Source: Arbor Networks, Inc.

Kilde: `http://www.arbornetworks.com/report` 2009 rapporten

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

DDoS udviklingen, februar 2011

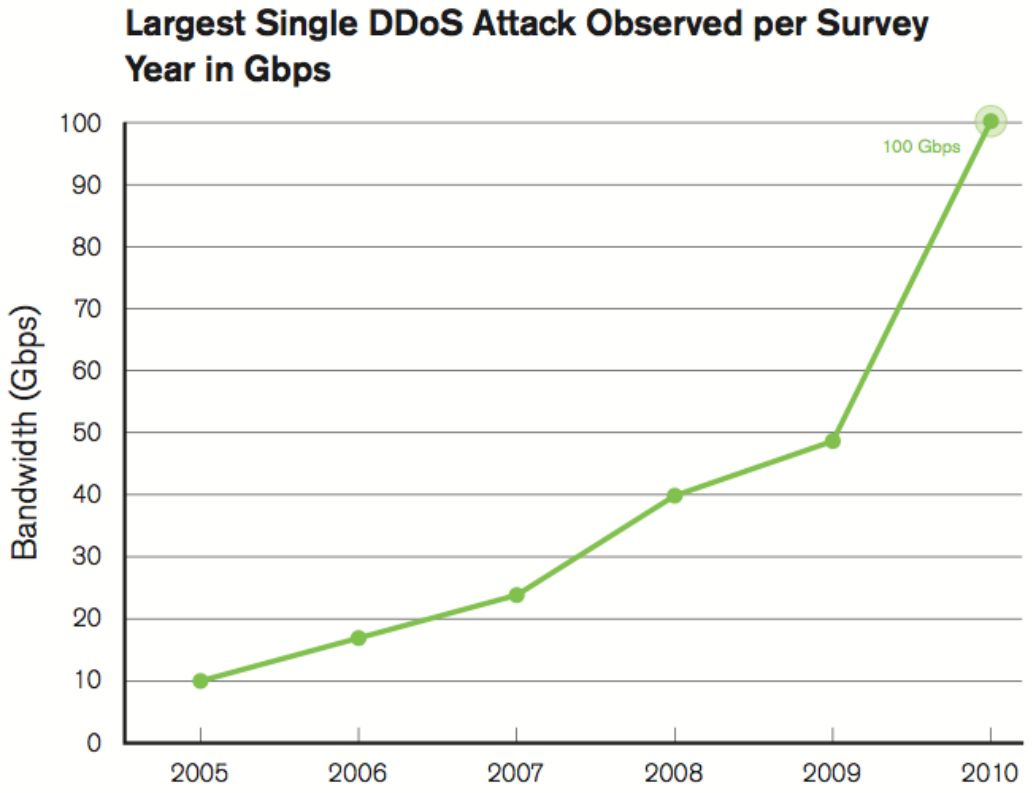


Figure 1
Source: Arbor Networks, Inc.

Kilde: `http://www.arbornetworks.com/report` 2010 rapporten

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

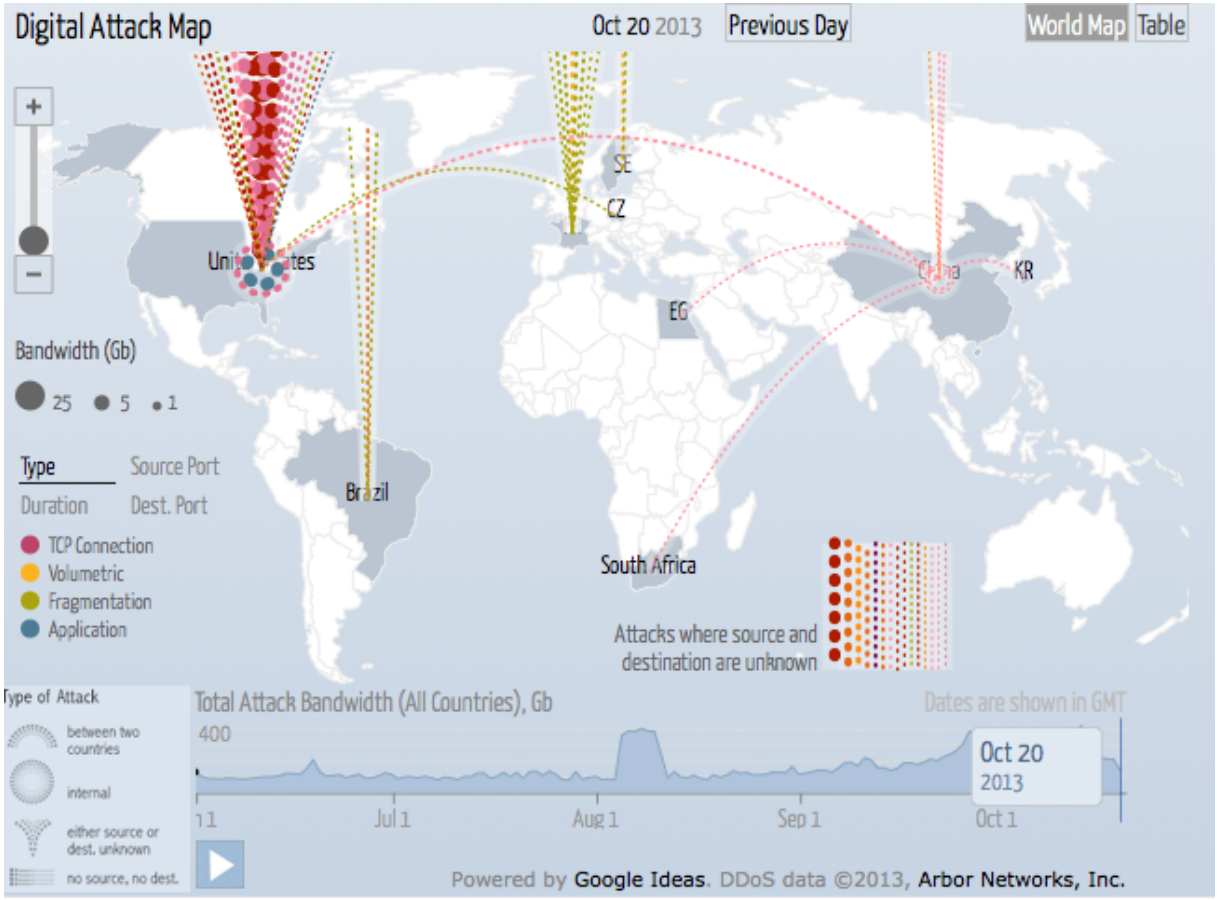
Key findings 2011

- Application-Layer DDoS Attacks Are Increasing in Sophistication and Operational Impact
- Mobile/Fixed Wireless Operators Are Facing Serious Challenges to Maintaining Availability in the Face of Attacks
- Firewalls and IPS Devices Are Falling Short on DDoS Protection
- DNS Has Broadly Emerged as an Attack Target and Enabler
- Lack of Visibility into and Control over IPv6 Traffic Is a Significant Challenge
- Chronic Underfunding of Operational Security Teams
- Operators Continue to Express Low Confidence in the Efficacy of Law Enforcement
- Operators Have Little Confidence in Government Efforts to Protect Critical Infrastructure

Kilde: `http://www.arbornetworks.com/report` februar 2011

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

DDoS udviklingen 2013 rapporter



Source: Arbor Networks `http://www.digitalattackmap.com/`

Also see Prolexic reports and Akamai state of the internet

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hacking er magi

Hacking ligner indimellem magi

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hacking eksempel - det er ikke magi

MAC filtrering på trådløse netværk

Alle netkort har en MAC adresse - BRÆNDT ind i kortet fra fabrikken

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket

Det virker dog ikke ☺

De fleste netkort tillader at man overskriver denne adresse midlertidigt

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Myten om MAC filtrering

Eksemplet med MAC filtrering er en af de mange myter

Hvorfor sker det?

Marketing - producenterne sætter store mærkater på æskerne

Manglende indsigt - forbrugerne kender reelt ikke koncepterne

Hvad *er* en MAC adresse egentlig

Relativt få har forudsætningerne for at gennemskue dårlig sikkerhed

Løsninger?

Udbrede viden om usikre metoder til at sikre data og computere

Udbrede viden om sikre metoder til at sikre data og computere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

MAC filtrering

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

buffer overflows is a C problem

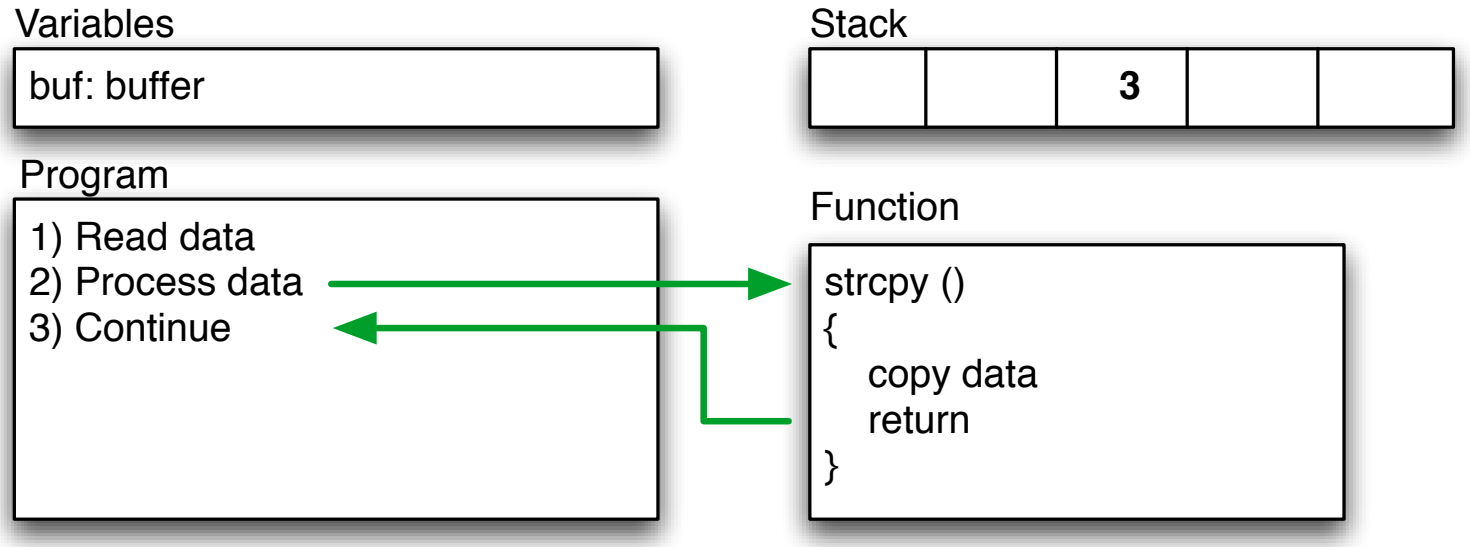
SOLIDO NETWORKS

Et buffer overflow is what happens if some internal structure in programs are modified by an attacker for the purpose of taking control of the application and system. Often a program will crash, but if the attacker can input specific data it might be possible to point to their own **shell code** containing instructions to be executed.

Stack protection today both a specific technique and generic term for adding protection to operating systems and programs to reduce the likelihood of buffer overflows succeeding. The main features are protecting areas in memory by making them non-writeable and non-executable. StackGuard and Propolice are some popular choices

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

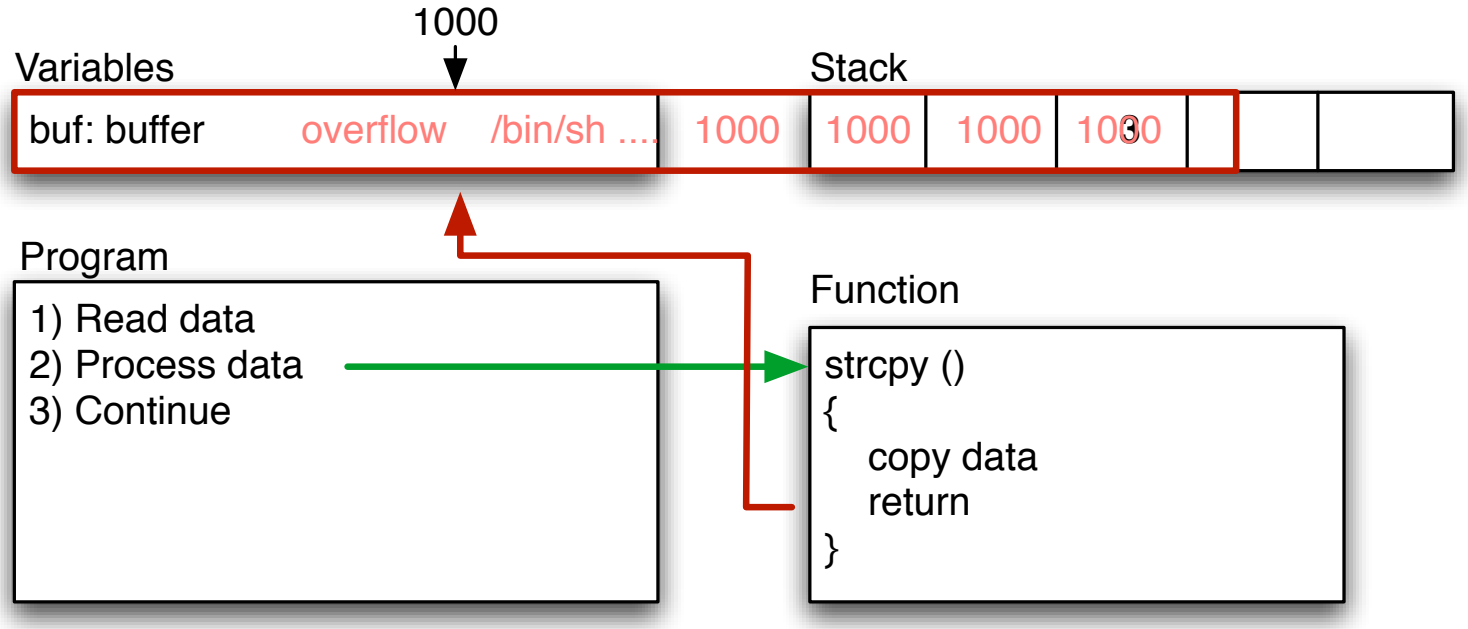
Buffer og stacks




```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\n",buf);
}
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Exploits - exploiting vulnerabilities

an exploit is a program designed to abuse some weakness or vulnerability

- Usually the expliot will demonstrate the weakness found, proof-of-concept (PoC)
- Usually the exploit will only include one vulnerability and is targeted at specific versions of the vulnerable program
- Exploits can be a few lines of code or multiple pages
- Used to be written using Perl and C, but today popular choices include Ruby and Python
- Can often be plugged into the Metasploit framework for direct execution

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Exploit sample

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

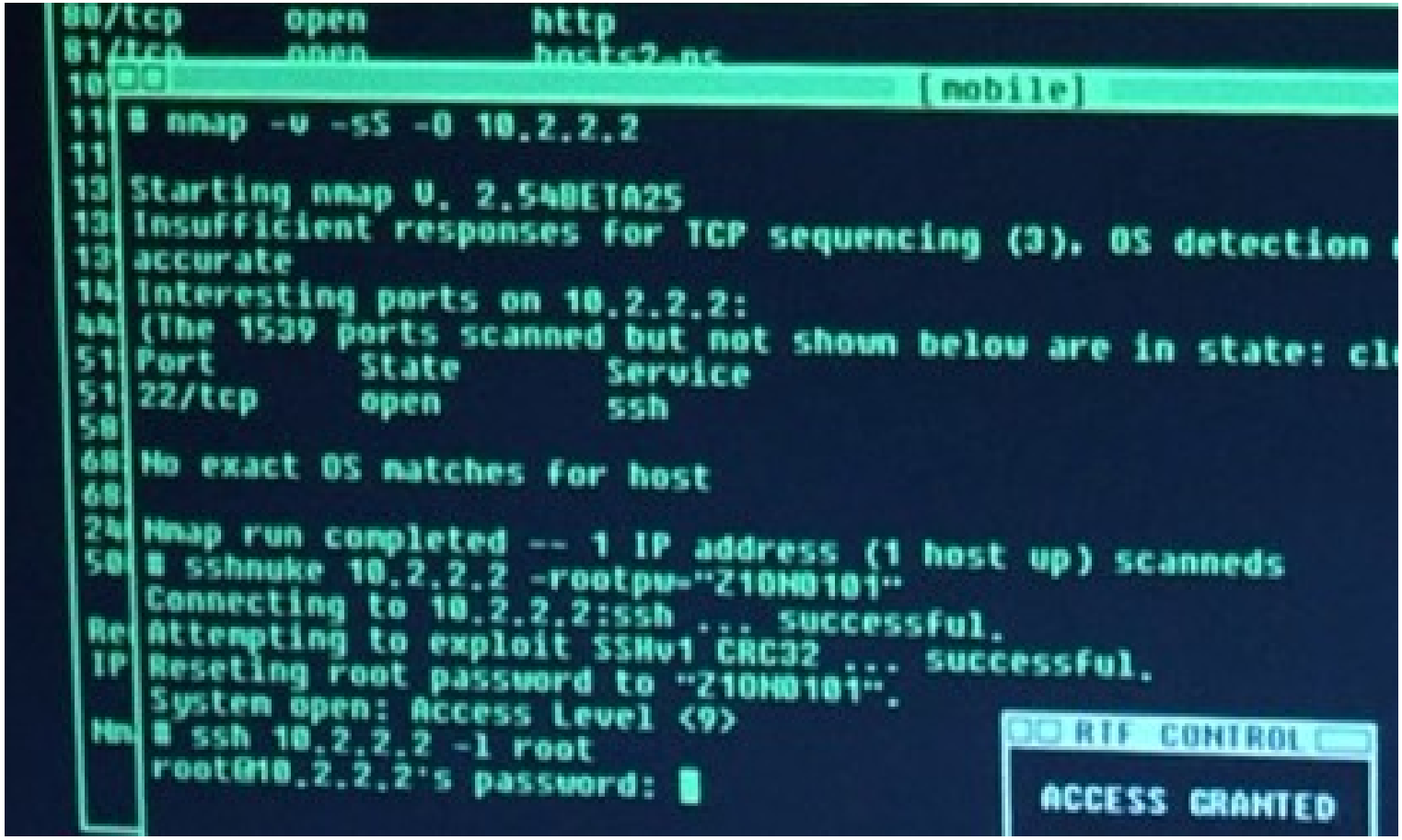
Demo exploit in Perl

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Matrix style hacking anno 2003

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Trinity breaking in



http://nmap.org/movies.html

Meget realistisk http://www.youtube.com/watch?v=51lGCTgqE_w

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hvordan finder man buffer overflow, og andre fejl

SOLIDO NETWORKS

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Principle of least privilege

Why execute applications with administrative rights - if they only need to read from a database

principle of least privilege execute code only with the most restrictive set of permissions required to perform a task

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Privilege escalation

privilege escalation is what an attacker aims to perform

Trying to get from an authenticated user to a higher privileged administrative user id

Some functions in operating systems require higher privileges, and they can sometimes be persuaded to fail in spectacular ways

When an attacker can execute commands they can often find a way to exploit software and escalate privileges

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

local vs. remote exploits

SOLIDO NETWORKS

local vs. remote signifies if the specific attack exploited is done from the operating system using a local command/feature or if this is done remotely across some network connection

remote root exploit - feared because it would grant administrative rights across a network connection

More often an attacker will combine a remote exploit with a privilege escalation exploit

zero-day exploits 0-days are not made public, but kept in small groups and suddenly can be found in use on the internet, or in specific use for a targeted attack

Since nobody is aware of the problem, there is no fix readily available from the vendors/programmers

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

The Exploit Database - dagens buffer overflow

http://www.exploit-db.com/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Create your own exploits and spearphishing?

SOLIDO NETWORKS

Metasploit Still rocking the internet
`http://www.metasploit.com/`

Armitage GUI fast and easy hacking for Metasploit
`http://www.fastandeasyhacking.com/`

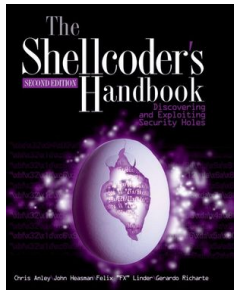
Metasploit Unleashed
`http://www.offensive-security.com/metasploit-unleashed/Main_Page`

Social-Engineer Toolkit
`https://www.trustedsec.com/downloads/social-engineer-toolkit/`

You can get these easily on `http://www.kali.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Buffer overflows



Hvis man vil lære at lave buffer overflows og exploit programmer er følgende dokumenter et godt sted at starte

Smashing The Stack For Fun And Profit Aleph One

Writing Buffer Overflow Exploits with Perl - anno 2000

Følgende bog kan ligeledes anbefales: *The Shellcoder's Handbook : Discovering and Exploiting Security Holes* af Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan "noir" Eren, Neel Mehta, Riley Hassell, John Wiley & Sons, 2004

NB: bogen er avanceret og således IKKE for begyndere!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Code quality

SOLIDO NETWORKS

Why are programs still insecure?

Programs are complex!

Try implementing tools to improve quality

Hudson Extensible continuous integration server `http://hudson-ci.org/`

Sonar `http://www.sonarsource.org/`

Yasca can scan source code written in Java, C/C++, HTML, JavaScript, ASP, ColdFusion, PHP, COBOL, .NET, and other languages. Yasca can integrate easily with other tools
`http://www.scovetta.com/yasca.html`

Software analysis can help
`http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html`

NB: you still have to think ☺

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Stack protection

Stack protection er mere almindeligt
- med i OpenBSD current fra 2. dec 2002

Buffer overflows er almindeligt kendte

- Selv OpenSSH har haft buffer overflows
- Stack protection prøver at modvirke/fjerne muligheden for buffer overflows. arbitrary code execution bliver til ude af drift for berørte services

Propolice
`http://www.openbsd.org`
`http://www.trl.ibm.com/projects/security/ssp/`

StackGuard
`http://www.immunix.org/stackguard.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

We must allow open hacker tools

I 1993 skrev Dan Farmer og Wietse Venema artiklen
Improving the Security of Your Site by Breaking Into it

I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

> We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se `http://sectools.org` og `http://www.packetstormsecurity.org/`

Kilde: `http://www.fish2.com/security/admin-guide-to-cracking.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

OWASP top ten

> The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

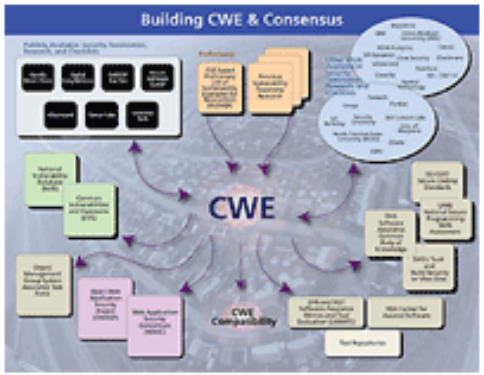
The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

`http://www.owasp.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

CWE Common Weakness Enumeration



Enlarge

CWE™ International in scope and free for public use, CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

CWE in the Enterprise

- Software Assurance
- Application Security
- Supply Chain Risk Management
- System Assessment
- Training
- Code Analysis
- Remediation & Mitigation
- NVD (National Vulnerability Database)
- *Recommendation ITU-T X.1524 CWE,* ITU-T CYBEX Series

http://cwe.mitre.org/

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

CWE/SANS Monster mitigations

SOLIDO NETWORKS

Monster Mitigations

These mitigations will be effective in eliminating or reducing the severity of the Top 25. These mitigations will also address many weaknesses that are not even on the Top 25. If you adopt these mitigations, you are well on your way to making more secure software.

A Monster Mitigation Matrix is also available to show how these mitigations apply to weaknesses in the Top 25.

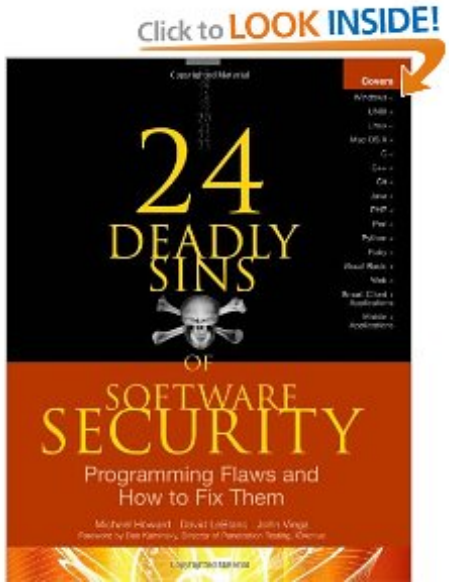
ID	Description
M1	Establish and maintain control over all of your inputs.
M2	Establish and maintain control over all of your outputs.
M3	Lock down your environment.
M4	Assume that external components can be subverted, and your code can be read by anyone.
M5	Use industry-accepted security features instead of inventing your own.
GP1	(general) Use libraries and frameworks that make it easier to avoid introducing weaknesses.
GP2	(general) Integrate security into the entire software development lifecycle.
GP3	(general) Use a broad mix of methods to comprehensively find and prevent weaknesses.
GP4	(general) Allow locked-down clients to interact with your software.

See the Monster Mitigation Matrix that maps these mitigations to Top 25 weaknesses.

Source: `http://cwe.mitre.org/top25/index.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

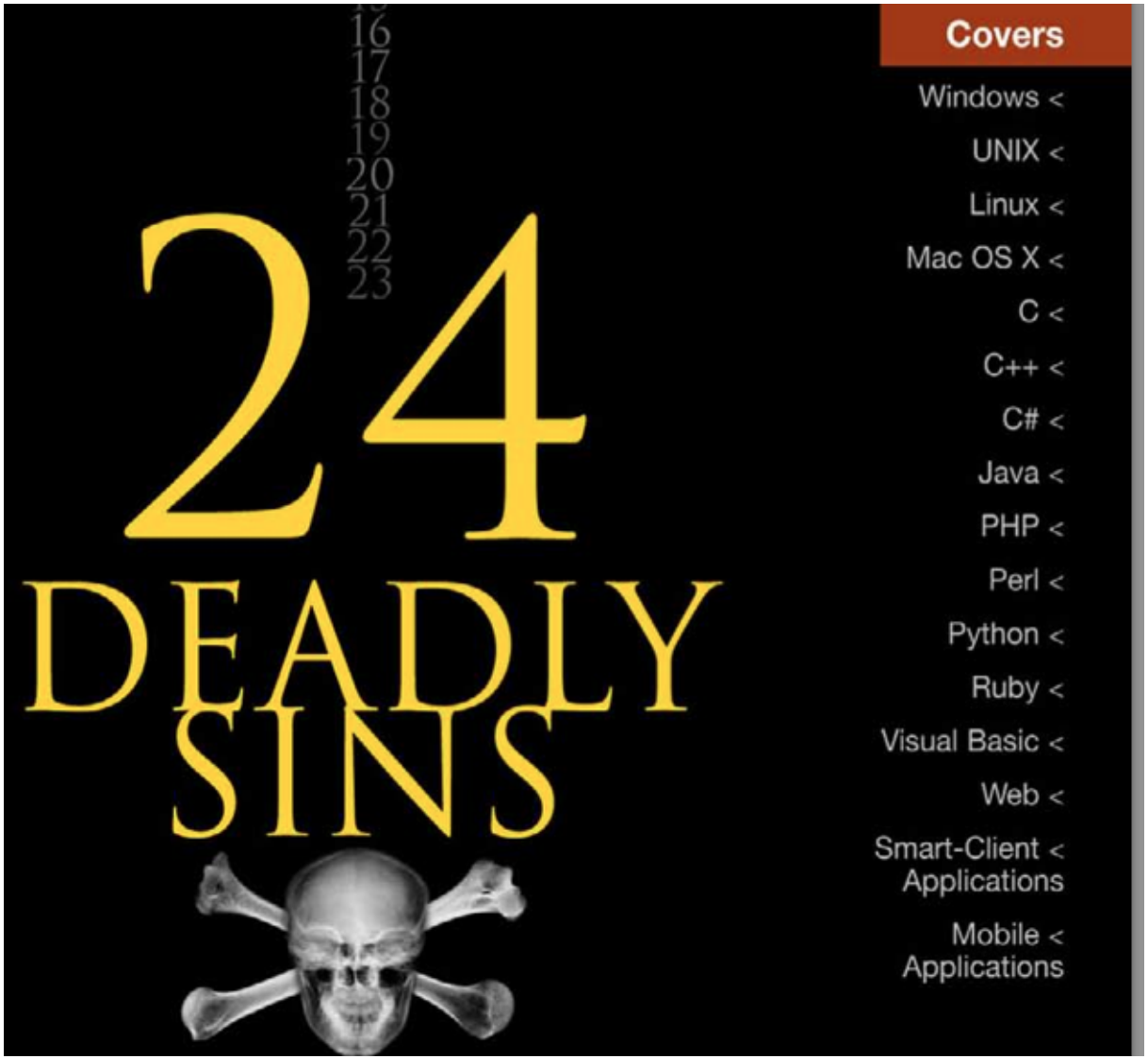
Deadly sins bogen



24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Deadly sins bogen - close up



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Deadly Sins 1/2

SOLIDO NETWORKS

Part I Web Application Sins 1-4

- 1) SQL Injection
- 2) Web Server-Related Vulnerabilities
- 3) Web Client-Related Vulnerabilities (XSS)
- 4) Use of Magic URLs, Predictable Cookies, and Hidden Form Fields

Part II Implementation Sins 5-18
5) Buffer Overruns, 6) Format String, 7) Integer Overflows, 8) C++ Catastrophes, 9) Catching Exceptions, 10) Command Injection 11) Failure to Handle Errors Correctly 12) Information Leakage 13) Race Conditions 14) Poor Usability 15) Not Updating Easily 16) Executing Code with Too Much Privilege 17) Failure to Protect Stored Data 18) The Sins of Mobile Code

Still want to program in C?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Deadly Sins 2/2

SOLIDO NETWORKS

Part III Cryptographic Sins 19-21

- 19) Use of Weak Password-Based System
- 20) Weak Random Numbers
- 21) Using Cryptography Incorrectly

Part IV Networking Sins 22-24

- 22) Failing to Protect Network Traffic,
- 23) Improper use of PKI, Especially SSL,
- 24) Trusting Network Name Resolution

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Forudsætninger

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Eksempler på forudsætninger

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

Executable heap

Fejl i programmet

alle programmer har fejl

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Use cases for BackTrack and Kali

Det anbefales at afvikle BackTrack i en virtuel maskine, på klient med VMware Player, Virtualbox eller tilsvarende

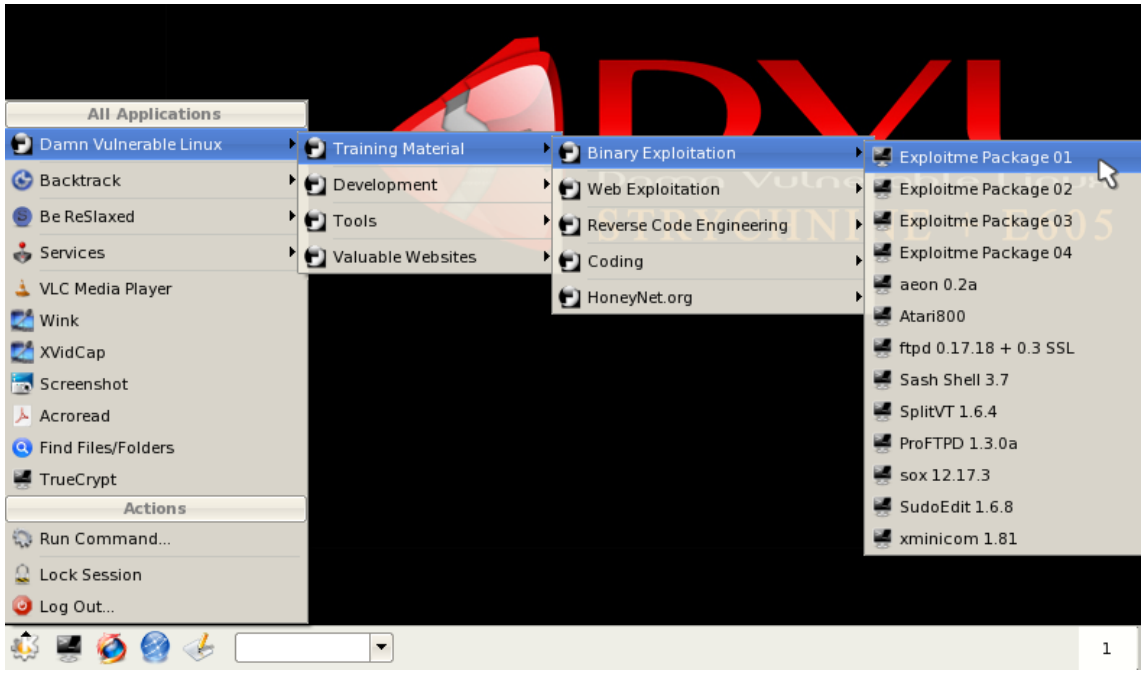
BackTrack kan også benyttes som pentest server i netværket, med eller uden virtualisering

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

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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Damn Vulnerable Linux boot CD'er



Damn Vulnerable Linux `http://www.damnvulnerablelinux.org/`
DVL er baseret på Linux og må kopieres frit :-)

Brug DVD'en eller VMware player til den

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

OWASP WebGoat

WebGoat fra OWASP, `http://www.owasp.org`

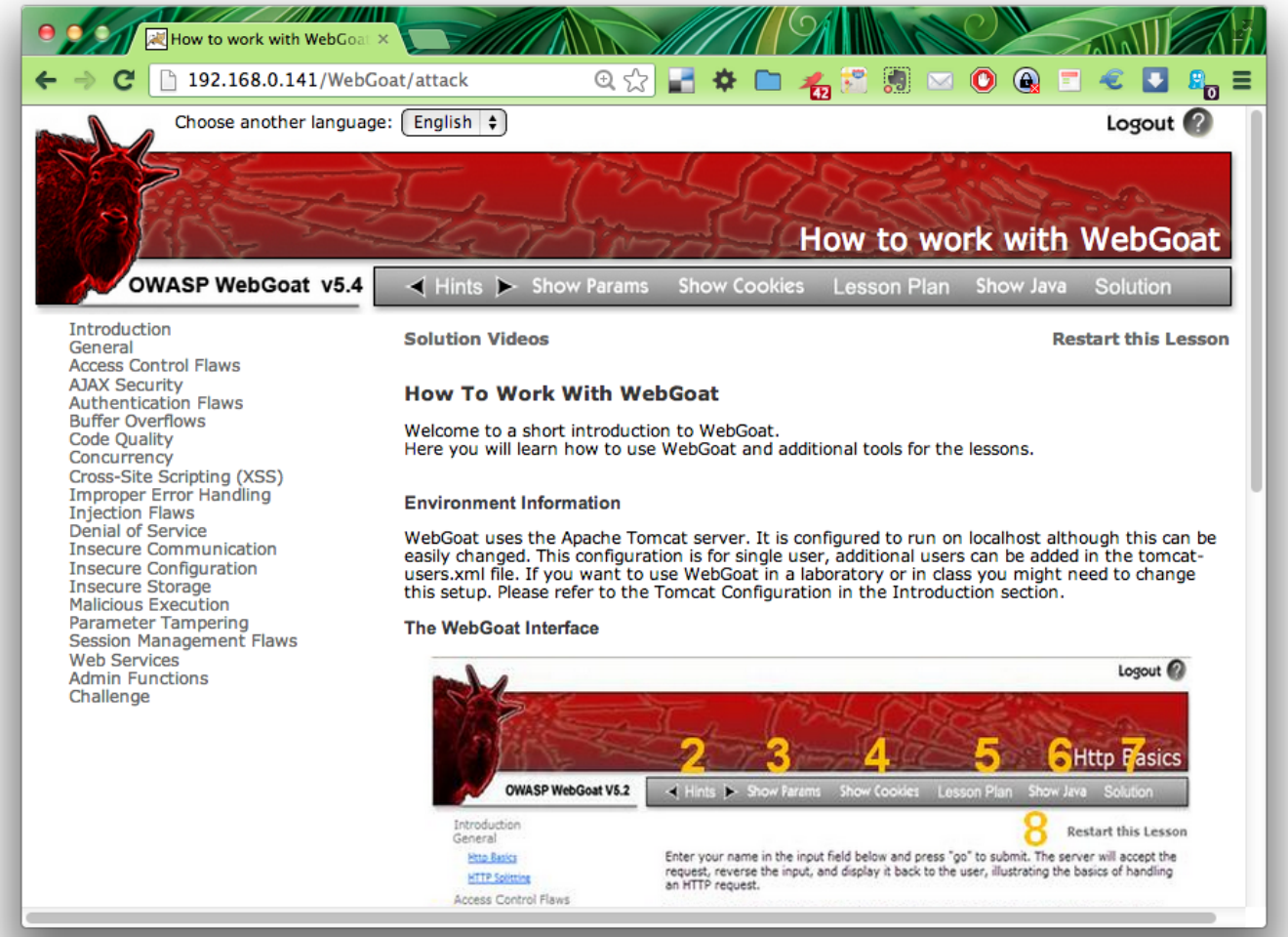
Træningsmiljø til webhacking

Downloades som Zipfil og kan afvikles direkte på en Windows laptop

`https://www.owasp.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Demo: WebGoat og Kali



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Pause

Er det tid til en lille pause?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hvad skal der ske?

Tænk som en hacker

Rekognoscering

- ping sweep, port scan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: nikto, exploit programs

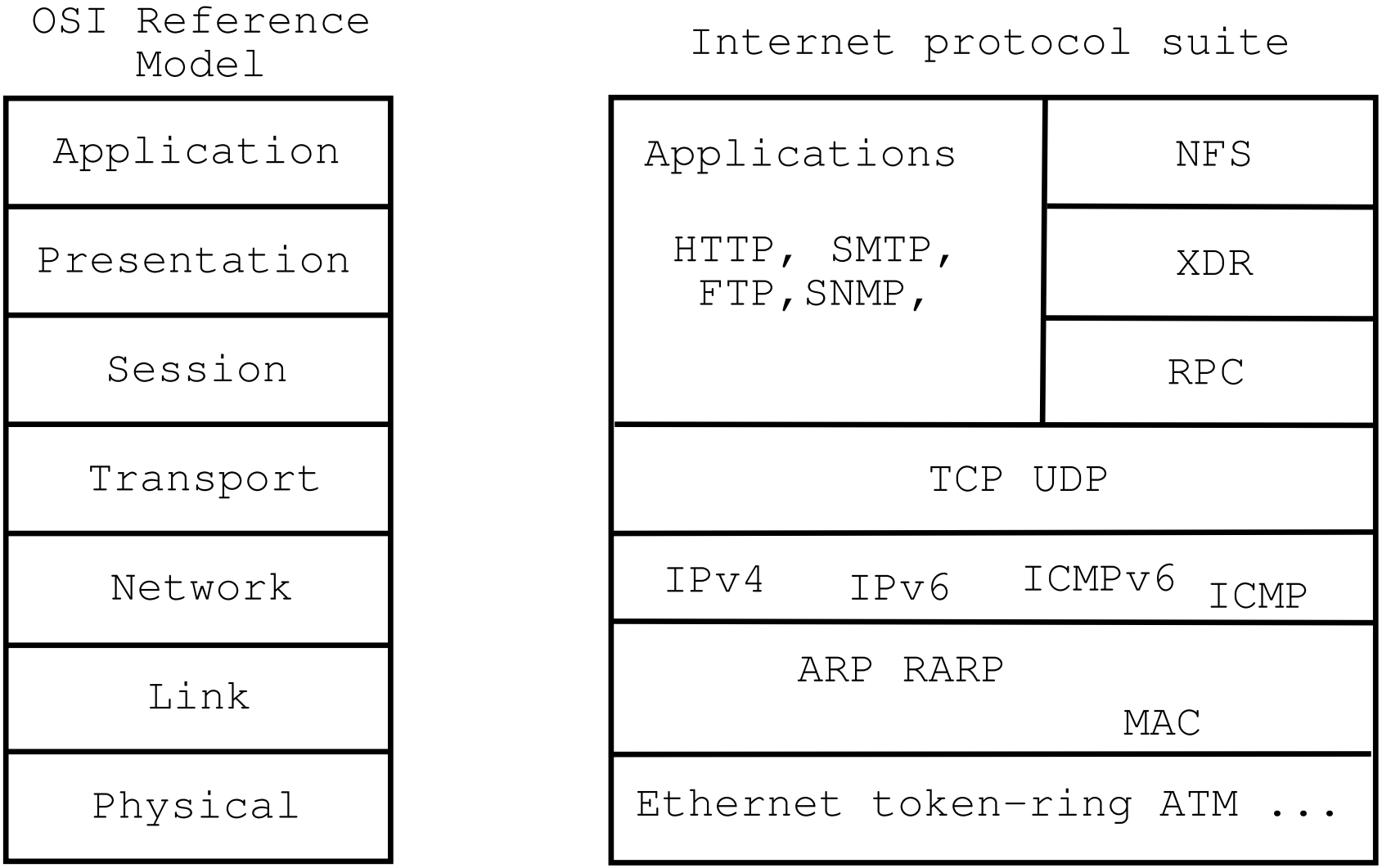
Oprydning vises ikke på kurset, men I bør i praksis:

- Lav en rapport
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo også VISE andre at I gør noget ved sikkerheden.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

OSI og Internet modellerne



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Informationsindsamling

Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet

passiv kunne være at lytte med på trafik eller søge i databaser på Internet

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar

© license CC BY 3.0. 2013 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

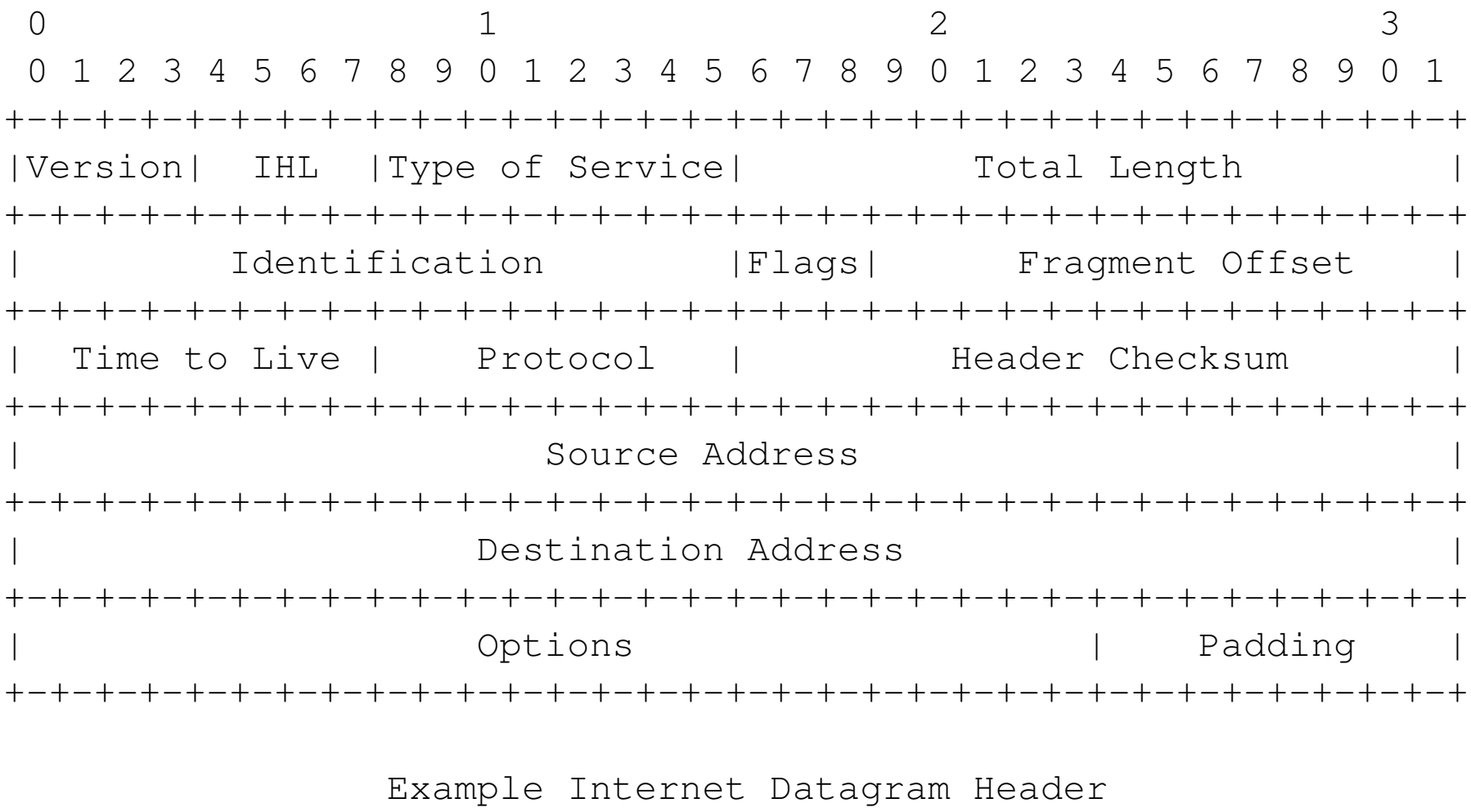
Første halvdel af adresserne er Organizationally Unique Identifier (OUI)

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. 2013 Solido Networks, Henrik Lund Kramshøj

IPv4 pakken - header - RFC-791



Example Internet Datagram Header

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Well-known port numbers

IANA vedligeholder en liste over magiske konstanter i IP

De har lister med hvilke protokoller har hvilke protokol ID m.v.

En liste af interesse er port numre, hvor et par eksempler er:

- Port 25 SMTP Simple Mail Transfer Protocol
- Port 53 DNS Domain Name System
- Port 80 HTTP Hyper Text Transfer Protocol over TLS/SSL
- Port 443 HTTP over TLS/SSL

Se flere på `http://www.iana.org`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Basal Portscanning

Hvad er portscanning

afprøvning af alle porte fra 0/1 og op til 65535

målet er at identificere åbne porte - sårbare services

typisk TCP og UDP scanning

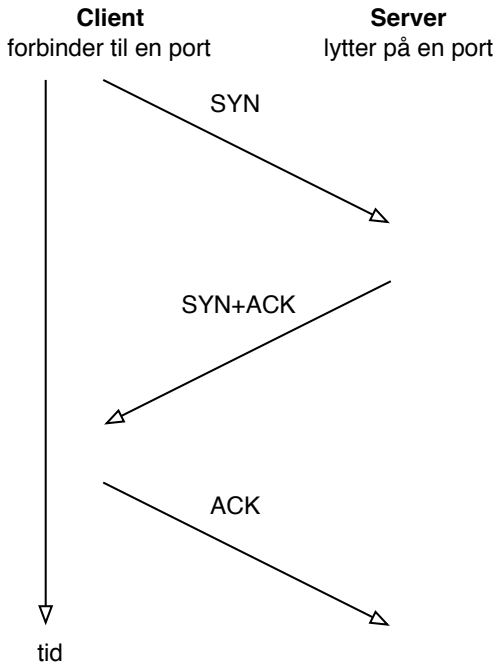
TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere

UDP applikationer svarer forskelligt - hvis overhovedet

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

TCP three way handshake



- **TCP SYN half-open** scans
- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse - dette kan/kunne udnyttes til *stealth*-scans
- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op - og derved afholde nye forbindelser fra at blive oprette - **SYN-flooding**

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Ping og port sweep

scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

- konfigurer en maskine med to IP-adresser som ikke er i brug
- hvis der kommer trafik til den ene eller anden er det portscan
- hvis der kommer trafik til begge IP-adresser er der nok foretaget et sweep - bedre hvis de to adresser ligger et stykke fra hinanden

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

nmap port sweep efter port 80/TCP

Port 80 TCP er webservere

```
 #  nmap  -p 80 217.157.20.130/28

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
Port       State       Service
80/tcp     filtered    http

Interesting ports on www.kramse.dk (217.157.20.131):
Port       State       Service
80/tcp     open        http

Interesting ports on  (217.157.20.139):
Port       State       Service
80/tcp     open        http
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

nmap port sweep efter port 161/UDP

Port 161 UDP er SNMP

```
 #  nmap -sU -p 161 217.157.20.130/28

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on router.kramse.dk (217.157.20.129):
Port       State       Service
161/udp    open        snmp

The 1 scanned port on mail.kramse.dk (217.157.20.130) is: closed

Interesting ports on www.kramse.dk (217.157.20.131):
Port       State       Service
161/udp    open        snmp

The 1 scanned port on  (217.157.20.132) is: closed
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

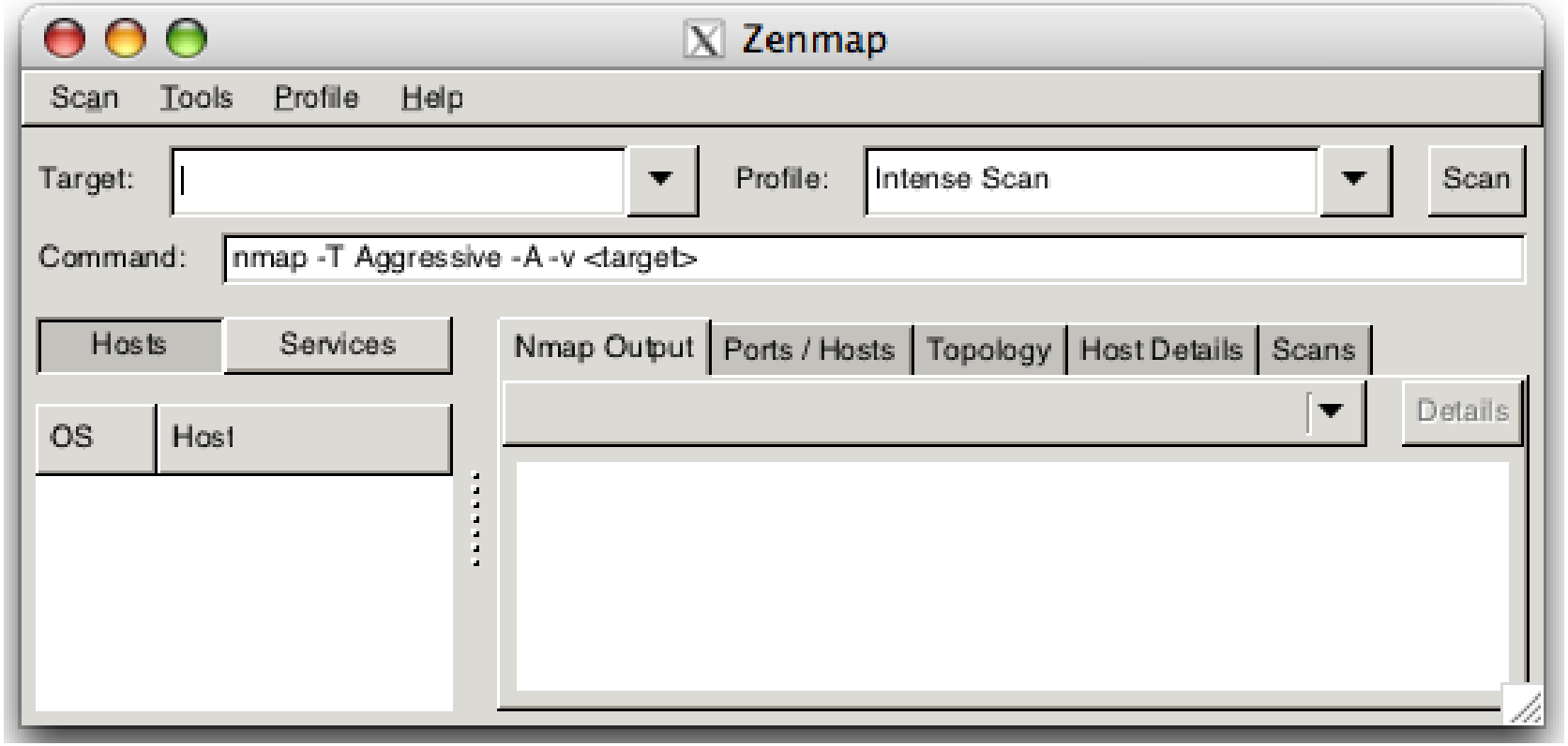
OS detection

```
# nmap -O ip.adresse.slet.tet scan af en gateway
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-12-03 11:31 CET
Interesting ports on gw-int.security6.net (ip.adresse.slet.tet):
(The 1653 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1080/tcp open  socks
5000/tcp open  UPnP
Device type: general purpose
Running: FreeBSD 4.X
OS details: FreeBSD 4.8-STABLE
Uptime 21.178 days (since Wed Nov 12 07:14:49 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 7.540 seconds
```

- lavniveau måde at identificere operativsystemer på
- send pakker med *anderledes* indhold
- Reference: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin
  `http://www.sys-security.com/html/projects/icmp.html`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Zenmap



Vi bruger Zenmap til at scanne med, GUI til Nmap

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Discover active systems ping sweep

som er øvelse **13** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Execute nmap TCP and UDP port scan

som er øvelse **14** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Vi laver nu øvelsen

Perform nmap OS detection

som er øvelse **15** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Perform nmap service scan

som er øvelse **16** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Pause

Er det tid til en lille pause?

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Erfaringer hidtil

mange oplysninger

kan man stykke oplysningerne sammen kan man sige en hel del om netværket

en skabelon til registrering af maskiner er god

- svarer på ICMP: □ echo, □ mask, □ time
- svarer på traceroute: □ ICMP, □ UDP
- Åbne porte TCP og UDP:
- Operativsystem:
- ... (banner information m.v.)

Mange små pakker kan oversvømme store forbindelser og give problemer for netværk

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hvad er værdien af pentest?

hvor og hvordan kan I bruge penetrationstest

hvis man vil have et andet indblik i netværket, TCP, UDP, ICMP, portscannning og samle puslespil udfra få informationer

Netværksadministratorer kan bruge pentesting til at sikre egne netværk ved brug af samme teknikker som hackere

Pentesting er ikke kun til test af produktionsnetværk

man skal ofte vurdere nye produkter - sikkerhedsmæssigt og funktionalitetsmæssigt - yder det beskyttelse, forbedrer det sikkerheden m.v.

Man står med en server der er kompromitteret - hvordan skete det? - hvordan forhindrer vi det en anden gang.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Insecure programming - web

Problem:
Ønsker et simpelt CGI program, en web udgave af finger

Formål:
Vise oplysningerne om brugere på systemet

Vi bruger Web applikationer som eksempel!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Muligheder for web programmering

ASP, PHP, Ruby on Rails m.fl.

- server scripting, meget generelt - man kan alt

SQL

- databasesprog - meget kraftfuldt
- mange databasesystemer giver mulighed for specifik tildeling af privilegier ”grant”

JAVA

- generelt programmeringssprog
- bytecode verifikation
- indbygget sandbox funktionalitet

Perl og andre generelle programmeringssprog

Pas på shell escapes!!!

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Hello world of insecure web CGI

Demo af et sårbart system - badfinger

Løsning:

- Kalde finger kommandoen
- et Perl script
- afvikles som CGI
- standard Apache HTTPD 1.3 server

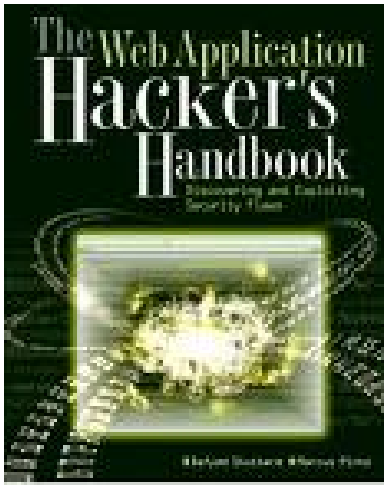
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

De vitale - og usikre dele

```
print "Content-type: text/html <html>";
print "<body bgcolor=#666666 leftmargin=20 topmargin=20";
print <<XX;
<h1>Bad finger command!</h1>
<HR COLOR=#000>
<form method="post" action="bad_finger.cgi">
Enter userid: <input type="text" size="40" name="command">
</form>
<HR COLOR=#000>
XX
if(&ReadForm(*input))
    print "<pre>";
    print "will execute: /usr/bin/finger $input{'command'}";
    print "<HR COLOR=#000>";
     print `/usr/bin/finger $input{'command'}`;
    print "<pre>";
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Mere Web application hacking



The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws
Dafydd Stuttard, Marcus Pinto, Wiley 2007 ISBN: 978-0470170779

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

WebScarab eller Firefox plugins

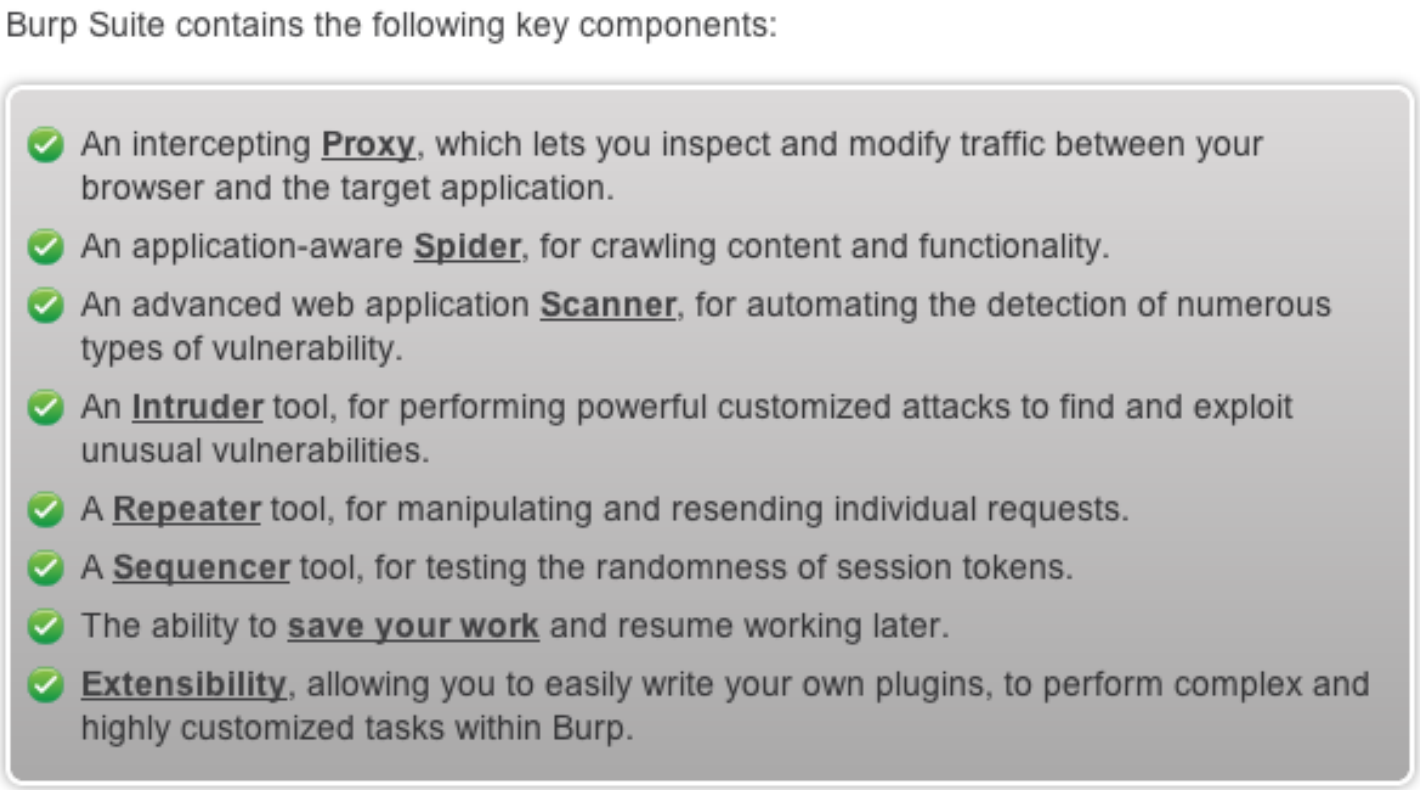
Form validation kan omgås med proxyprogrammer

Nogle af de mest kendte er:

- Burp proxy
- Tamper Data plugin til Firefox
- OWASP WebScarab

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Burp Suite



Burp Suite af Dafydd Stuttard `http://portswigger.net/burp/`

Twitter @PortSwigger

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Burpsuite

SOLIDO NETWORKS

> Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
>
> Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke - NB: EUR 249 per user per year.

`http://portswigger.net/burp/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

directory traversal- unicode dekodning

webroot er det sted på harddisken, hvorfra data der vises af webserveren hentes.

Unicode bug:

`http://10.0.43.10/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:`

Kilde:

`http://www.cgisecurity.com/archive/misc/unicode.txt` - rain forest puppy

`http://online.securityfocus.com/bid/1806/info/` - securityfocus info

Fundet i år 2000 - og idag mange produkter med tilsvarende problemer

Se også *Do you know who's watching you?: An in-depth examination of IP cameras attack surface* by Francisco Falcon and Nahuel Riva, Hack.lu 2013

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Nikto og W3af

Nikto web server scanner `http://cirt.net/nikto2`

W3af Web Application Attack and Audit Framework `http://w3af.sourceforge.net/`

Begge findes på BackTrack/Kali

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Skipfish

Skipfish fully automated, active web application security reconnaissance tool.

Af Michal Zalewski `http://code.google.com/p/skipfish/`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Simple Network Management Protocol

SNMP er en protokol der supporteres af de fleste professionelle netværksenheder, såsom switche, routere

hosts - skal slås til men følger som regel med

SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl - SNMP traps

sikkerheden baseres på community strings der sendes som klartekst ...

det er nemmere at brute-force en community string end en brugerid/kodeord kombination

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

brute force

SOLIDO NETWORKS

hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:
  -S         connect via SSL
  -s PORT    if the service is on a different default port, define it here
  -l LOGIN   or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS    or -P FILE try password PASS, or load several passwords from FILE
  -e ns      additional checks, "n" for null password, "s" try login as pass
  -C FILE    colon seperated "login:pass" format, instead of -L/-P option
  -M FILE    file containing server list (parallizes attacks, see -T)
  -o FILE    write found login/password pairs to FILE instead of stdout
...
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Find systems with SNMP

som er øvelse 17 fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Try Hydra brute force

som er øvelse **18** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Vi laver nu øvelsen

Try Cain brute force

som er øvelse **19** fra øvelseshæftet.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

Hvorfor ikke bare bruge JAVA?

JAVA karakteristik

- automatisk garbage collection
- bytecode verifikation på
- mulighed for signeret kode
- beskyldes for at være langsomt
- platformsuafhængigt

JAVA just in Time (JIT) er sammenligneligt med kompileret C

god sikkerhedsmodel - men problemer i implementationerne

JVM - den virtuelle maskine er udsat for hacking

NemID - aaaaaaaaaargggggggghhhhh

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

ASCII baserede protokoller

Diskussion:
I skal se/lære at mange protokoller i dag er *ASCII baserede* - dvs benytter kommandoer i klar tekst, GET, HEAD, QUIT osv. som gør det nemt at debugge.

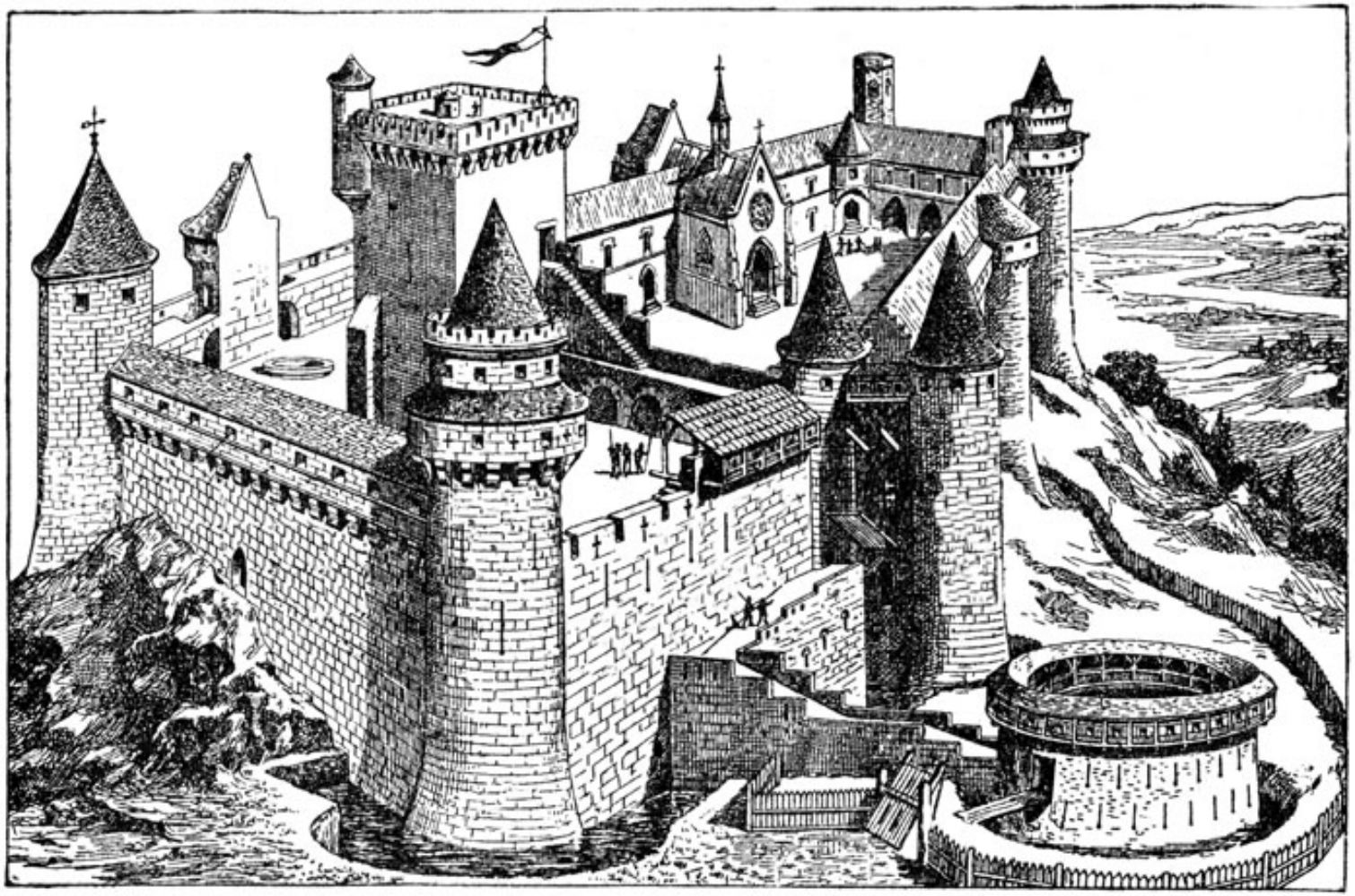
Det gælder eksempelvis for:

- SMTP
- POP3
- FTP
- HTTP

man kan altså forbinde til den pågældende service og interagere

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Enhance and secure runtime environment



Sidste chance er på afviklingstidspunktet

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Chroot, Jails and

Der findes mange typer *jails* på Unix

Ideer fra Unix chroot som ikke er en egentlig sikkerhedsfeature

- Unix chroot - bruges stadig, ofte i daemoner som OpenSSH
- FreeBSD Jails
- SELinux
- Solaris Containers og Zones - *jails på steroider*
- VMware virtuelle maskiner, er det et jail?

Hertil kommer et antal andre måder at adskille processer - sandkasser

Husk også de simple, database som `_postgresql`, Tomcat som `tomcat`, Postfix postsystem som `_postfix`, SSHD som `sshd` osv. - simple brugere, få rettigheder

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

SOLIDO NETWORKS

systrace - generate and enforce system call policies

```
EXAMPLES
   An excerpt from a sample ls(1) policy might look as follows:
     Policy: /bin/ls, Emulation: native
     [...]
        native-fsread: filename eq "$HOME" then permit
        native-fchdir: permit
     [...]
        native-fsread: filename eq "/tmp" then permit
        native-stat: permit
        native-fsread: filename match "$HOME/*" then permit
        native-fsread: filename eq "/etc/pwd.db" then permit
     [...]
        native-fsread: filename eq "/etc" then deny[eperm], if group != wheel

SEE ALSO
     systrace(4)
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Apache 6.0.18 catalina.policy (uddrag) - Java JVM

```
// ========== WEB APPLICATION PERMISSIONS ============================================
// These permissions are granted by default to all web applications
// In addition, a web application will be given a read FilePermission
// and JndiPermission for all files and directories in its document root.
grant {
    // Required for JNDI lookup of named JDBC DataSource's and
    // javamail named MimePart DataSource used to send mail
    permission java.util.PropertyPermission "java.home", "read";
    permission java.util.PropertyPermission "java.naming.*", "read";
    permission java.util.PropertyPermission "javax.sql.*", "read";
...
};
// The permission granted to your JDBC driver
// grant codeBase "jar:file:$catalina.home/webapps/examples/WEB-INF/lib/driver.jar!/-" {
//      permission java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
// };
```

Eksempel fra `apache-tomcat-6.0.18/conf/catalina.policy`

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Apple sandbox named generic rules

```
;; named - sandbox profile
;; Copyright (c) 2006-2007 Apple Inc.  All Rights reserved.
;;
;; WARNING: The sandbox rules in this file currently constitute
;; Apple System Private Interface and are subject to change at any time and
;; without notice. The contents of this file are also auto-generated and not
;; user editable; it may be overwritten at any time.
;;
(version 1)
(debug deny)

(import "bsd.sb")

(deny default)
(allow process*)
(deny signal)
(allow sysctl-read)
(allow network*)
```

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Apple sandbox named specific rules

```
;; Allow named-specific files
(allow file-write* file-read-data file-read-metadata
  (regex "^(/private)?/var/run/named\\.pid$"
         "^/Library/Logs/named\\.log$"))

(allow file-read-data file-read-metadata
  (regex "^(/private)?/etc/rndc\\.key$"
         "^(/private)?/etc/resolv\\.conf$"
         "^(/private)?/etc/named\\.conf$"
         "^(/private)?/var/named/"))
```

Eksempel fra `/usr/share/sandbox` på Mac OS X

© license CC BY 3.0. 2013 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

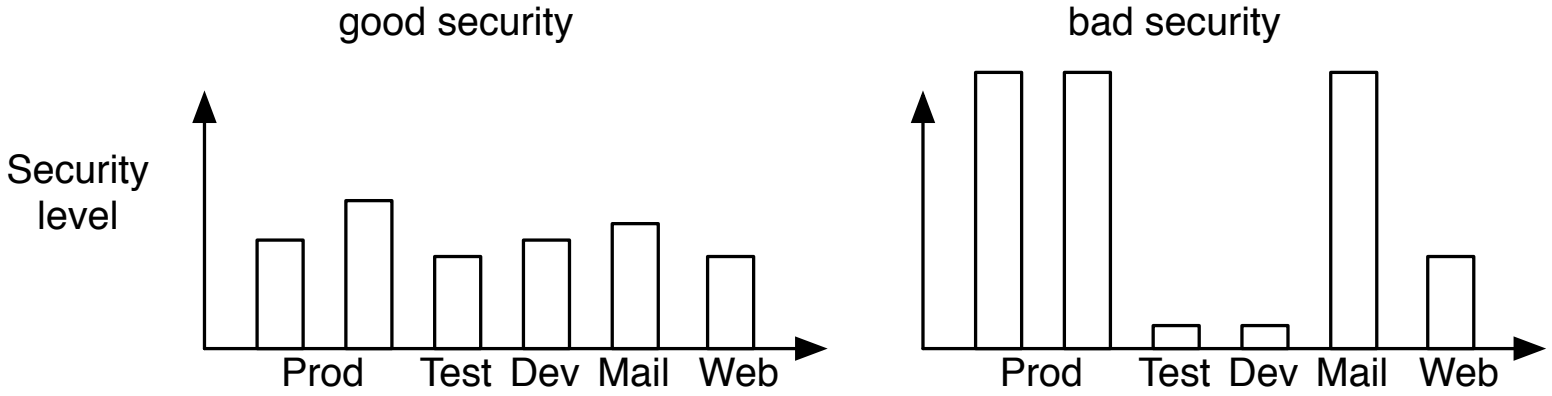
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Checklisten

- BIOS kodeord, pin-kode til telefon
- Firewall - specielt på laptops
- Installer anti-virus og anti-spyware hvis det er på Windows
- Brug to browsere med forskellige indstillinger
- Brug evt. PGP til mailkryptering
- Brug Password Safe, Keychain Access (OSX) eller tilsvarende
- Overvej at bruge harddisk eller filkryptering
- Opdatere alle programmer jævnligt
- **Backup af vigtige data - harddiske i bærbare kan også dø**
- Husk: sikker sletning af harddiske, medier osv.

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

Balanced security



Better to have the same level of security

If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

© license CC BY 3.0. 2013 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. 2013 Solido Networks, Henrik Lund Kramshøj

PROSA CTF

PROSA afholder CTF konkurrence fredag den 29. november 13 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. 2013 Solido Networks, Henrik Lund Kramshøj

Fri adgang til hackerværktøjer

I 1993 skrev Dan Farmer og Wietse Venema artiklen
Improving the Security of Your Site by Breaking Into it

I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

> We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se `http://sectools.org` og `http://www.packetstormsecurity.org/`

Kilde: `http://www.fish2.com/security/admin-guide-to-cracking.html`

© license CC BY 3.0. 2013 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

Some advice can be found in these places

- `http://csrc.nist.gov/publications/PubsSPs.html`
- `http://www.nsa.gov/research/publications/index.shtml`
- `http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml`

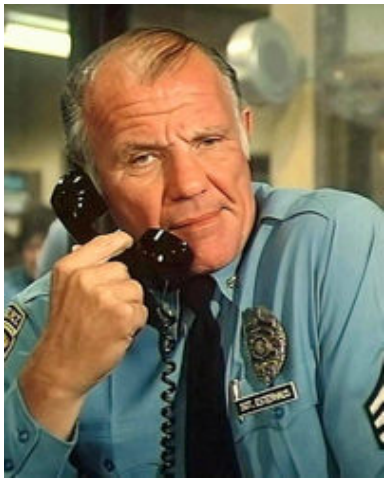
© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

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. 2013 Solido Networks, Henrik Lund Kramshøj

Be careful - questions?



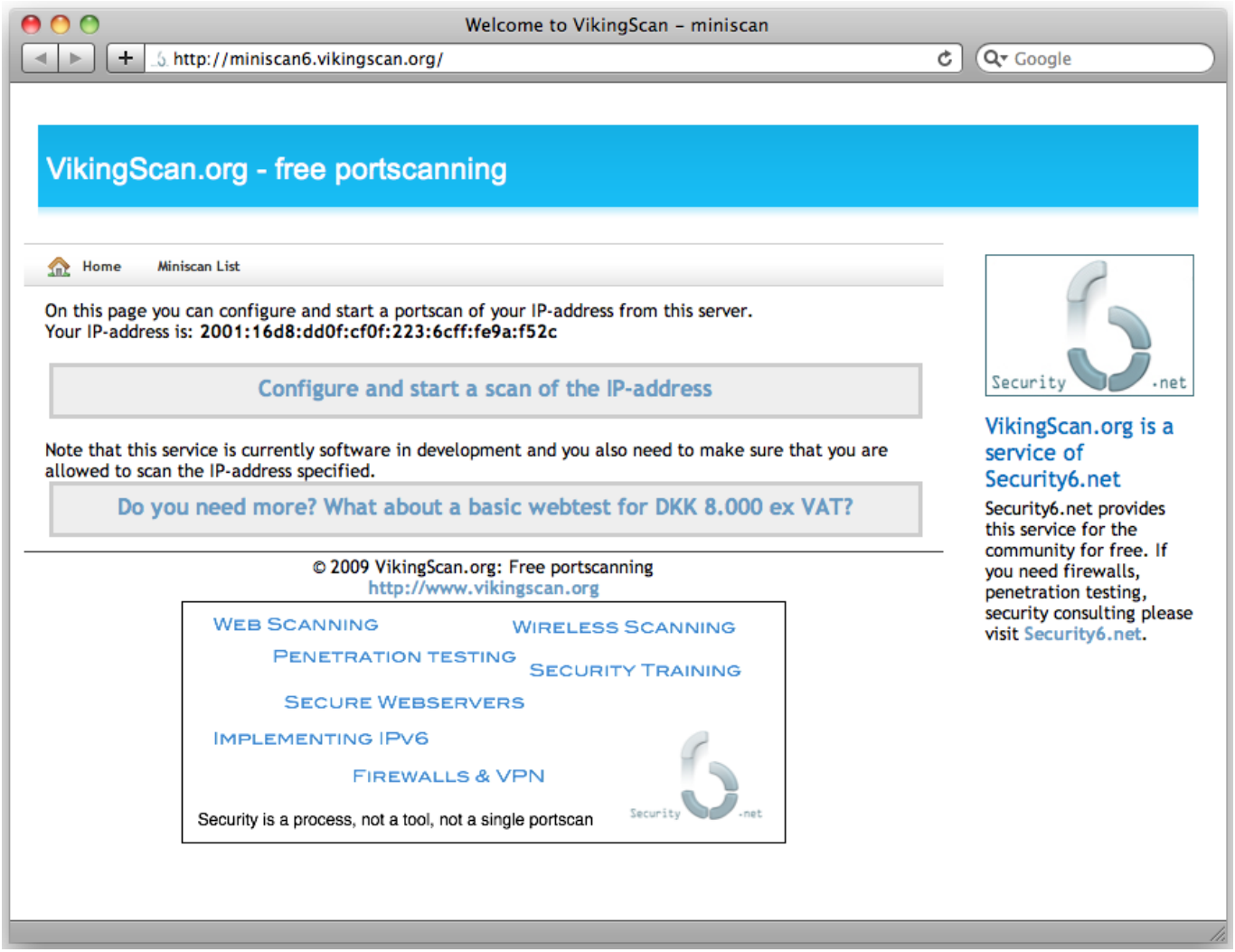
Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

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

© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj

VikingScan.org - free portscanning



© license CC BY 3.0. 2013 Solido Networks, Henrik Lund Kramshøj