Welcome to

Paranoia or RISK management

2013

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Agenda

Don’t Panic!

Kl 16:00-18:30 presentation

Less presentation, more social interaction, sharing information

You are welcome to email questions later

Goals: Increase Security Awareness

SOLIDO NETWORKS

Fact of life: Software has errors, hardware fails

Sometimes software can be made to fail in interesting ways

Humans can be social engineered

We are being attacked by criminals - including paranoid governments

Detailed agenda

Part I: Paranoia defined

Part II: What are the vulnerabilities and threats

Part III: Reduce risk and mitigate impact

Security is not magic

.

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

Follow news about security

Support communities, join and learn

Part I: Paranoia defined

SOLIDO NETWORKS

par·a·noi·a

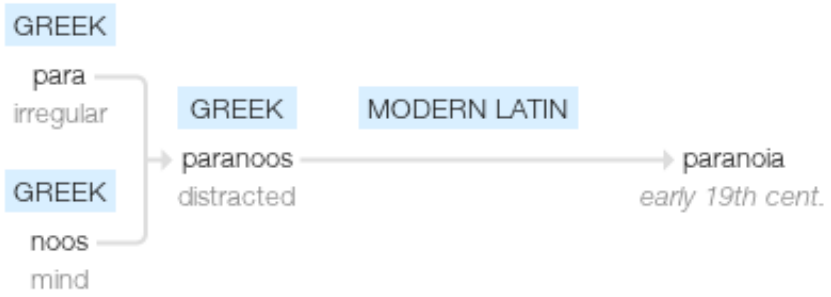
/ˌparəˈnoiə/

noun

noun: **paranoia**

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

Origin



More

Source: google paranoia definition

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!

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/`

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 %

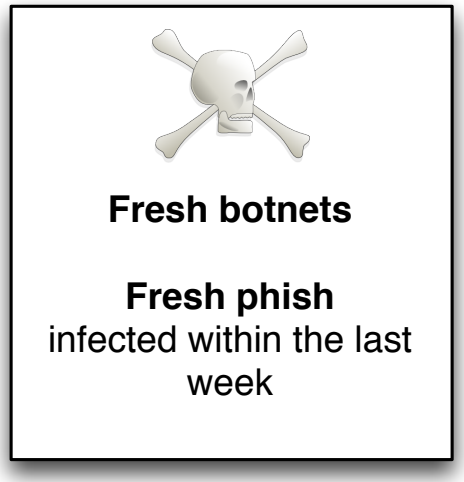
Source: `http://www.statisticbrain.com/identity-theft-fraud-statistics/`

Trading in infected computers

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

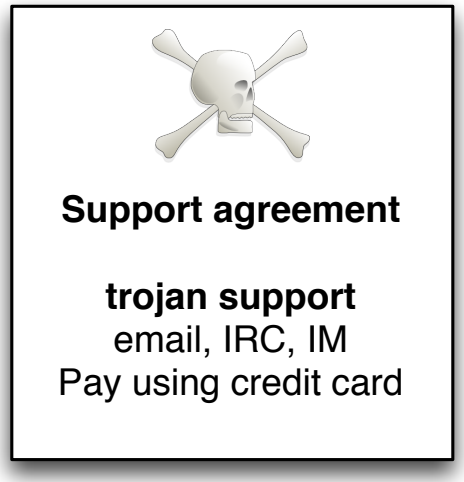
Todays offer trojans

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

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

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`

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

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

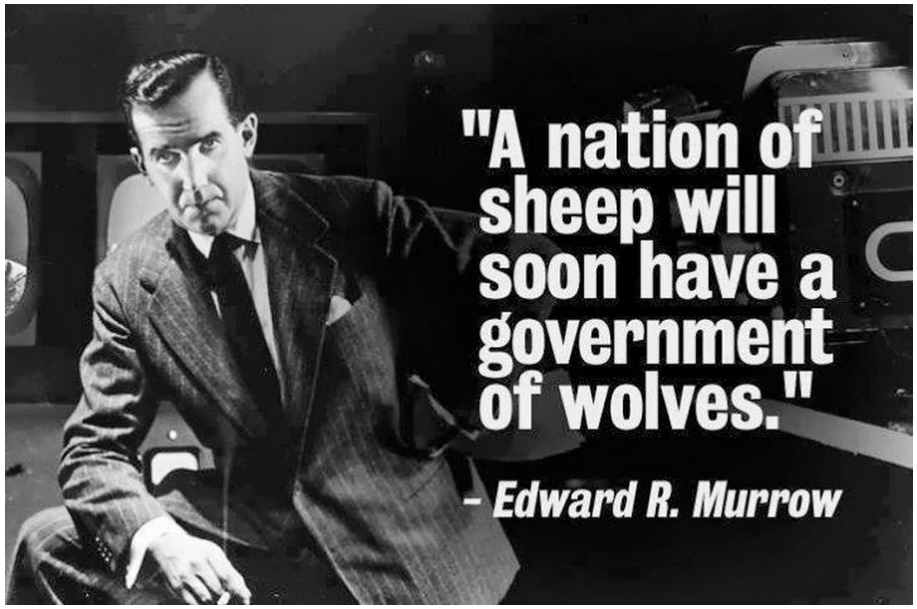
Skype is insecure

> 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`

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

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`

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

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

Use protection - always

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.

Hackers do not discriminate

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

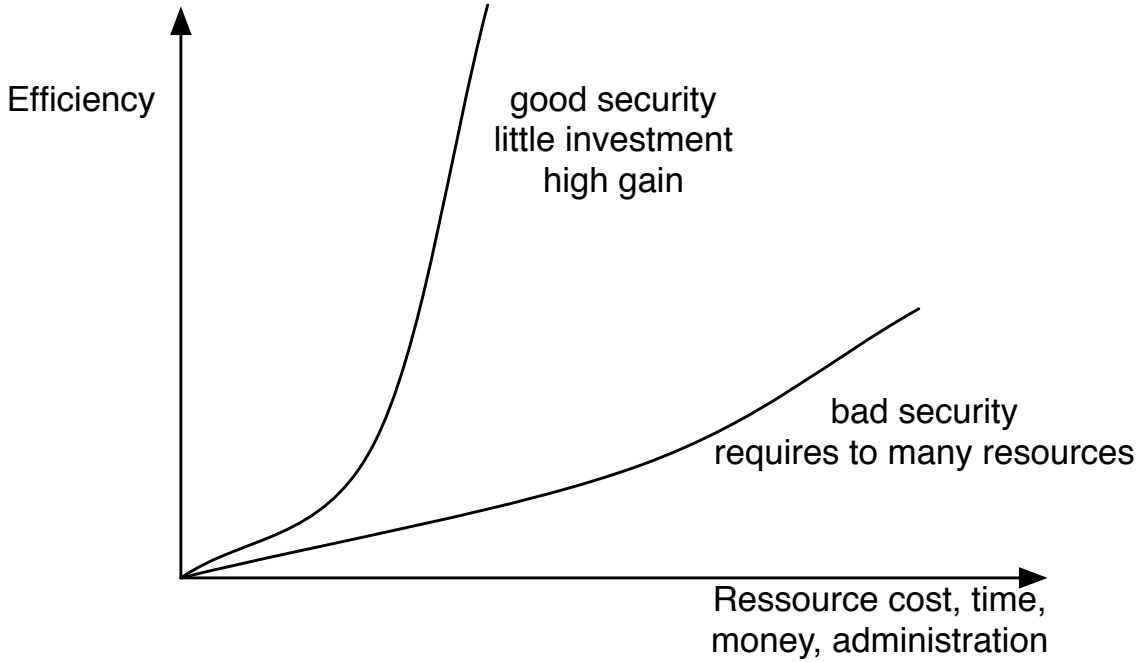
We are all targets of hacking

Social Engineering rockz! Phishing works.

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

Hacking is not cool

Good security



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

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

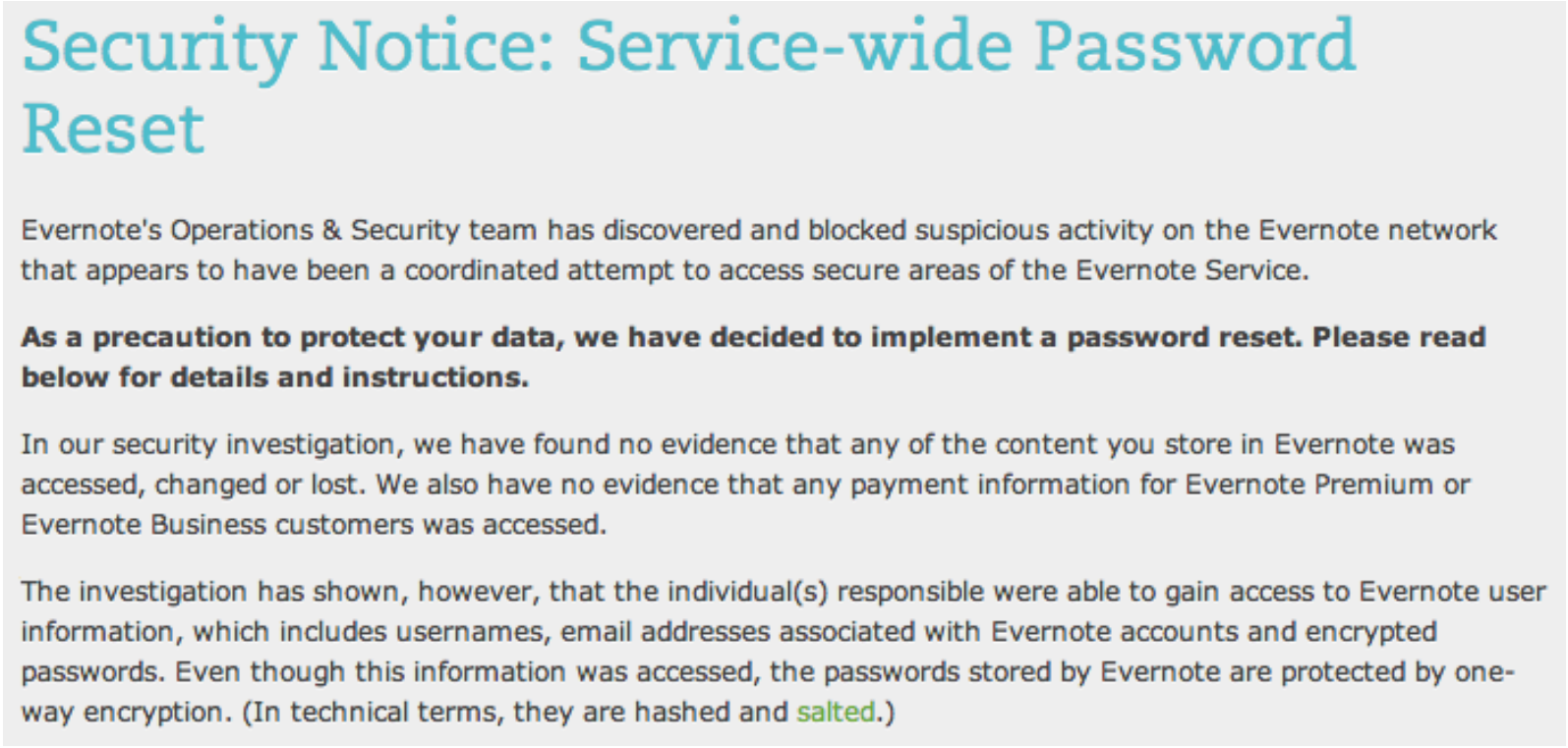
Why think of security?

> 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`

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`

Twitter password reset

Blog

Keeping our users secure

Friday, February 01, 2013

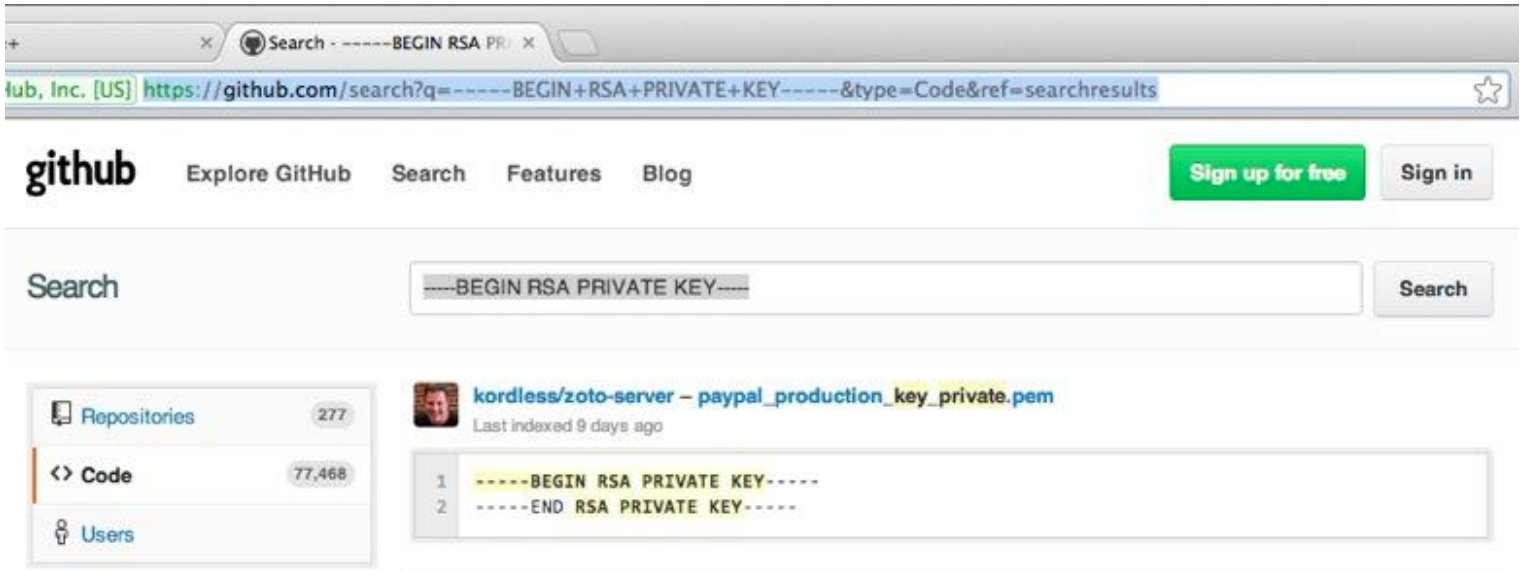
As you may have read, there's been a recent uptick in large-scale security attacks aimed at U.S. technology and media companies. Within the last two weeks, the *New York Times* and *Wall Street Journal* have chronicled breaches of their systems, and Apple and Mozilla have turned off Java by default in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

January 2013: Github Public passwords?



Sources:

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

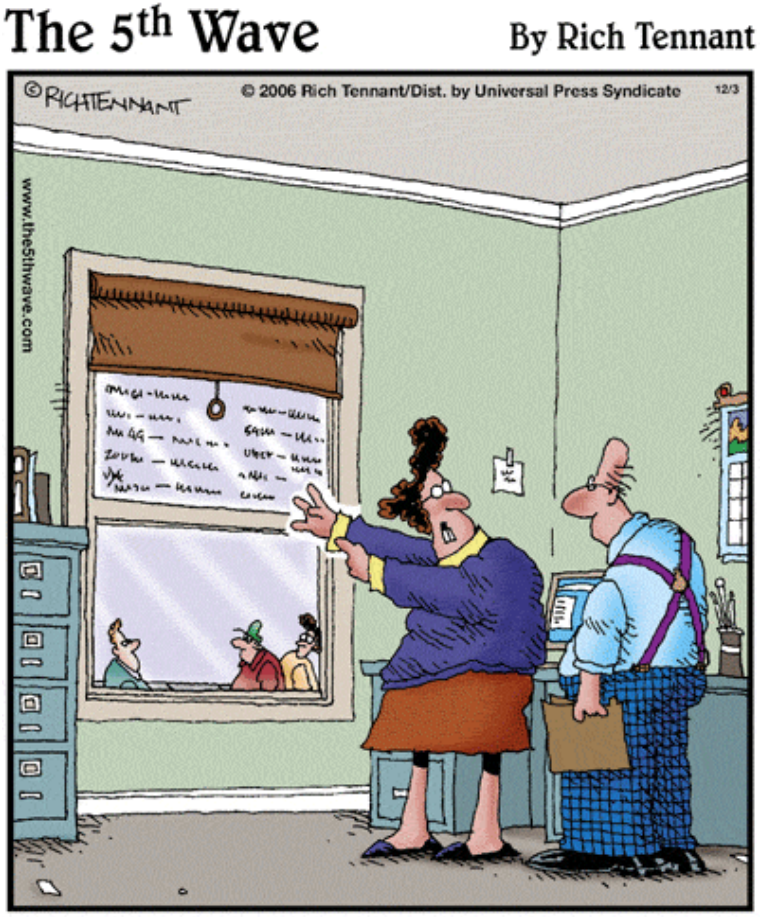
http://www.webmonkey.com/2013/01/users-scramble-as-github-search-exposes-passwords-security-de

http://www.leakedin.com/

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

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

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

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?

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!)

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

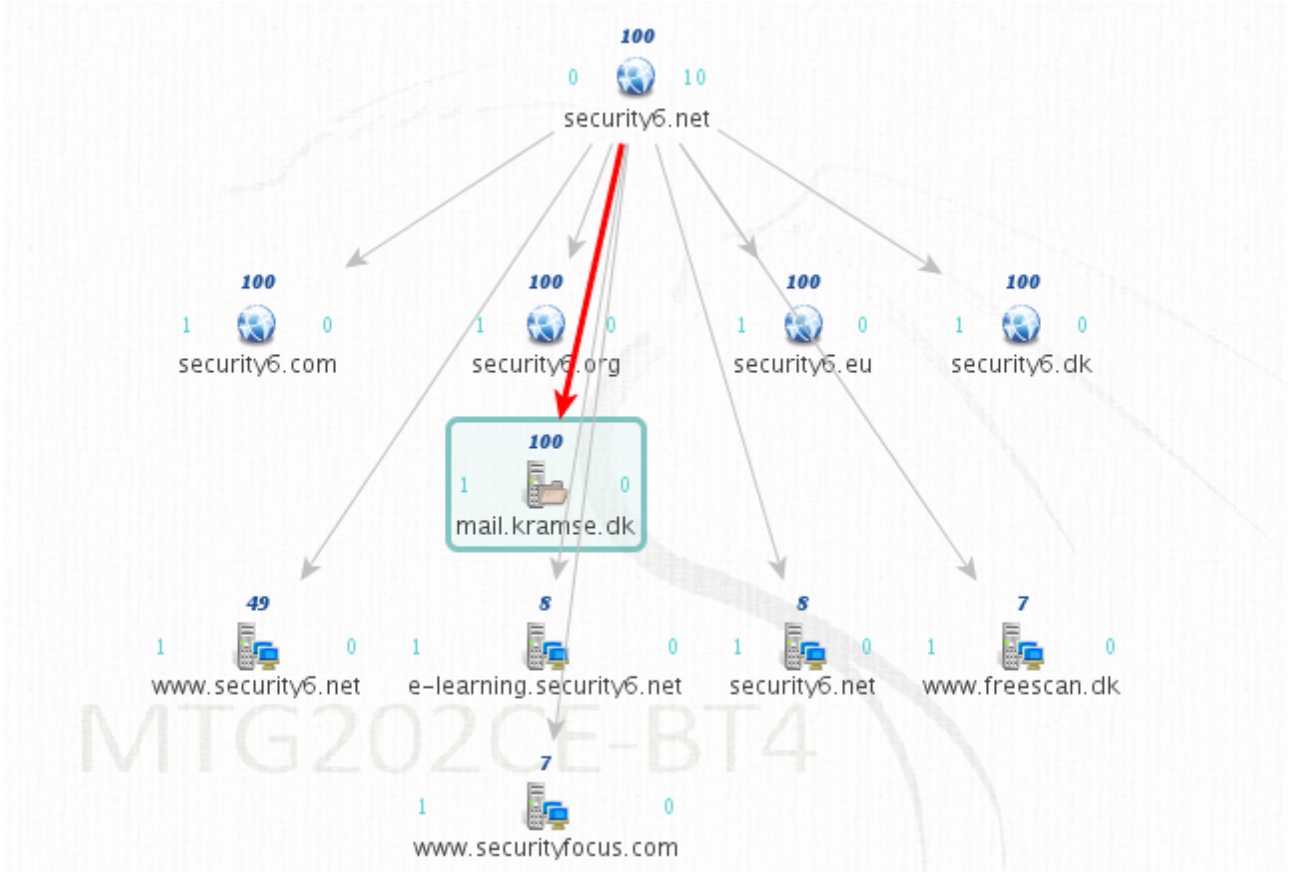
Be creative

Google for it

Google as a hacker tools?

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

Listbeth in a box?



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

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

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:

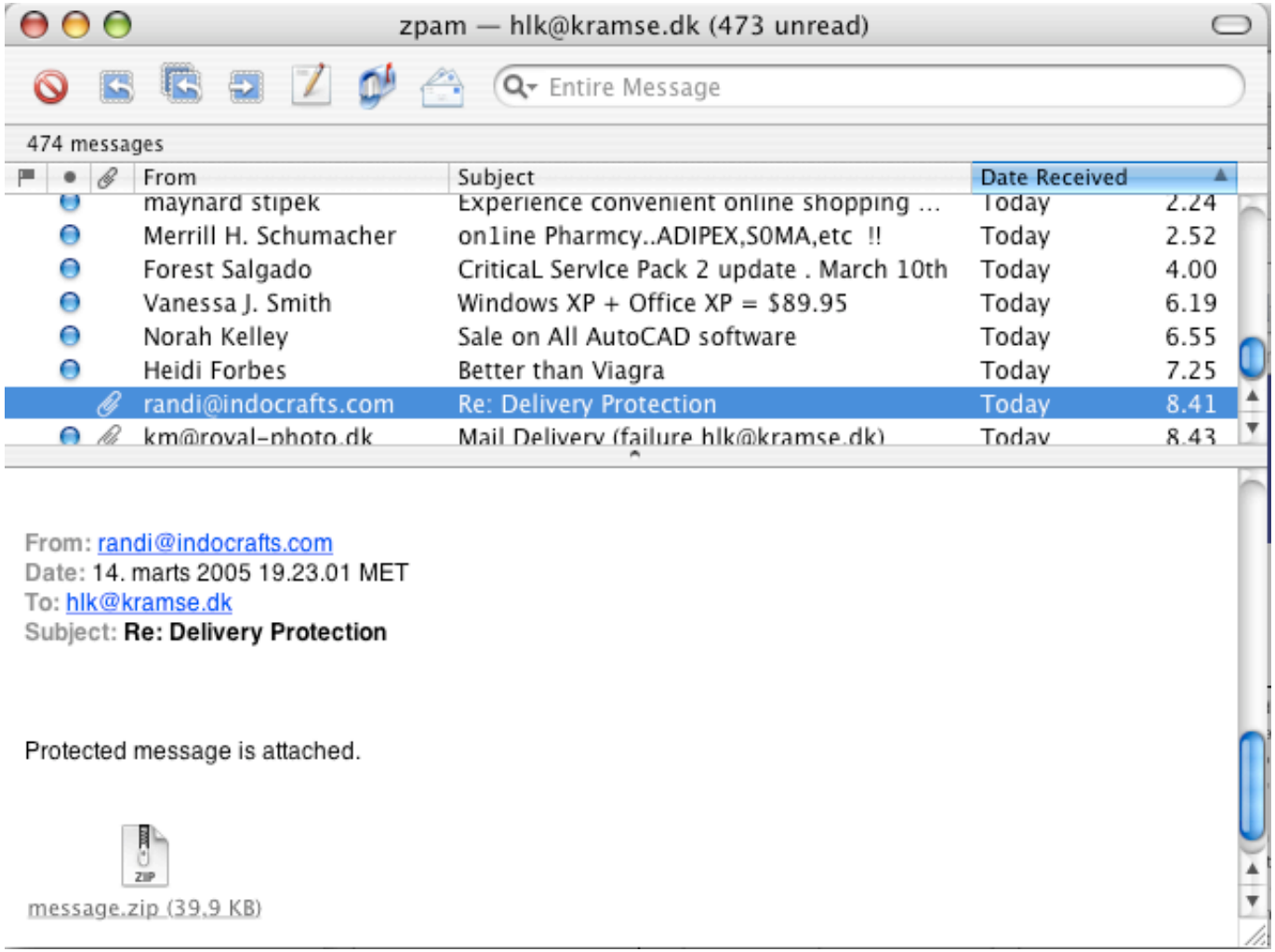
https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

*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)
---

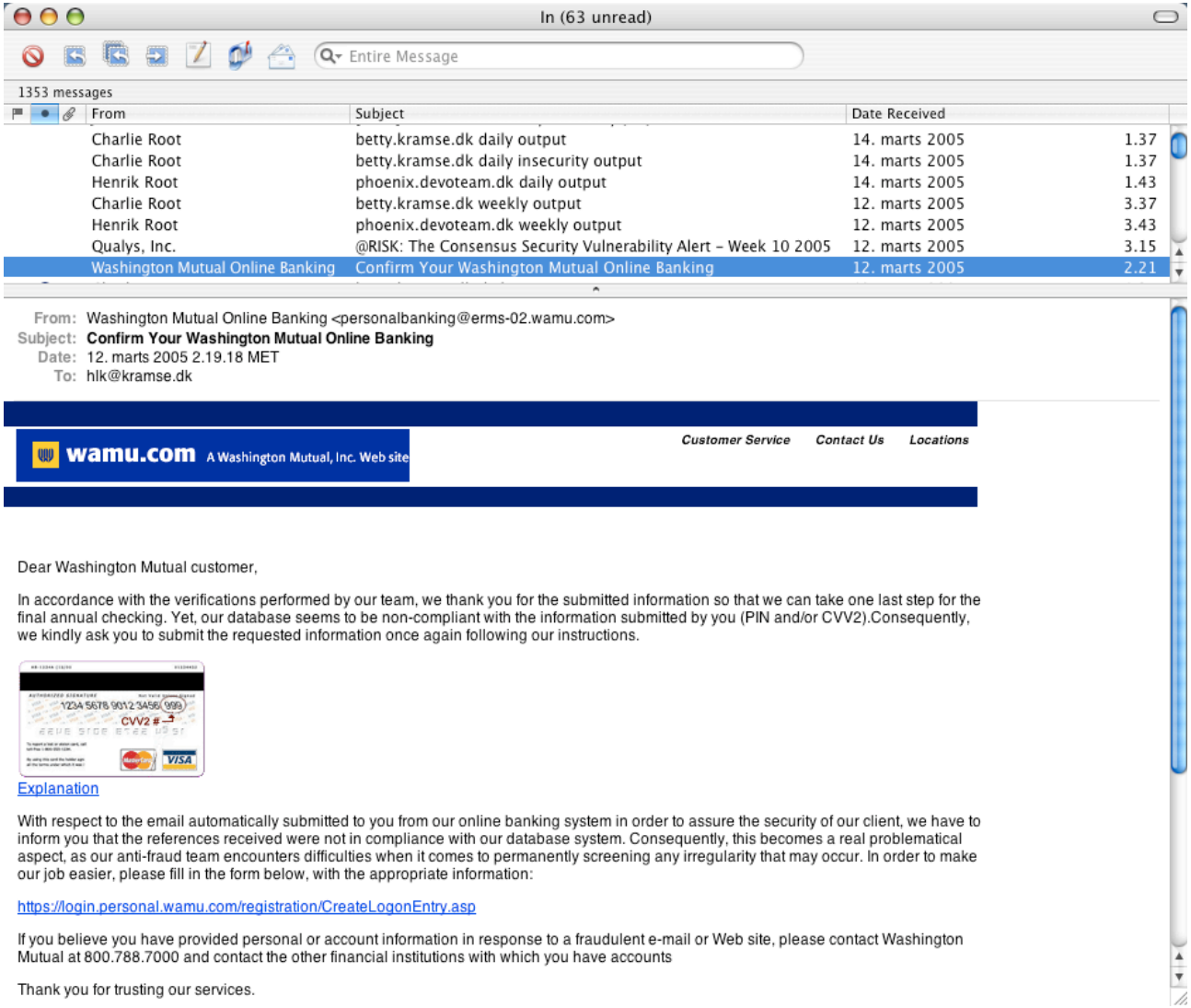
http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

Kan du selv genkende Phishing

Zip files?



Money!



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

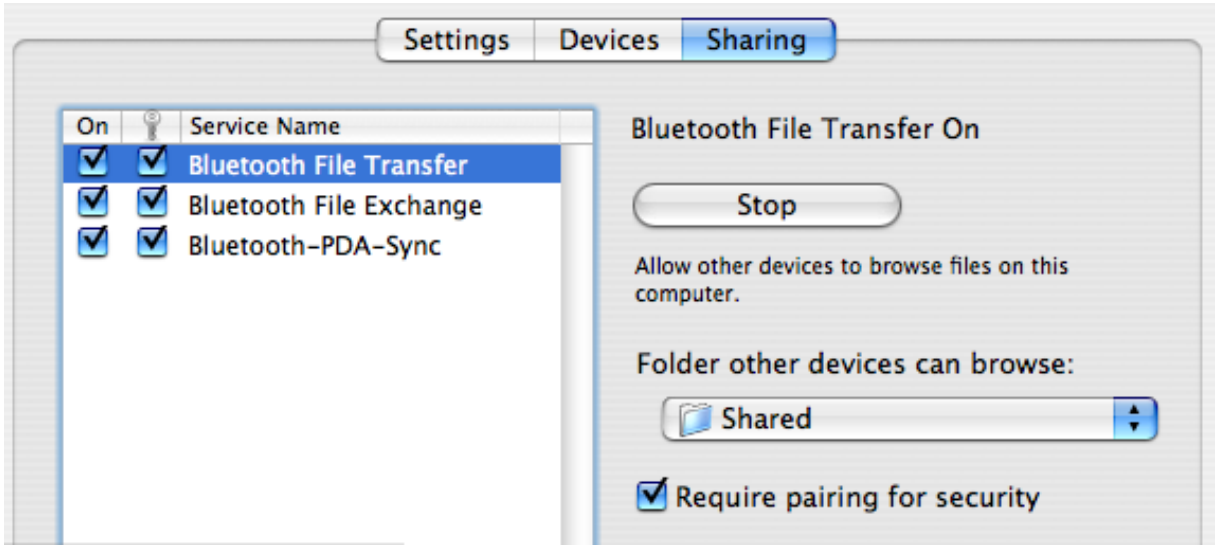
Mobile devices

SOLIDO NETWORKS

What characterizes mobile devices

- Small - sometimes can fit in a pocket
- Less resources, smaller CPU and memory than PC
- Limited functionality, limited control - can be rooted (sometimes)
- Synchronize with data from multiple sources
- Storage has increased to +32Gb
- Has *viewer programmer* for Word, Excel, PDF m.fl.
- Has browser built-in - often not changed
- Always on - mobile 3G/4G and Wifi - connected most of the day

Bluetooth security



- All small devices also have bluetooth
- Bluetooth - turn it off when not in use
- In your car - built-in bluetooth, GPS has bluetooth?
- Turn on security features for bluetooth allow access on to *paired* devices

Car Whisperer using bluetooth

Bluetooth kits for cars use passkey like ’0000’ or ’1234’

Sources:

`http://trifinite.org/blog/archives/2005/07/introducing_the.html`
`http://trifinite.org/trifinite_stuff_carwhisperer.html`

Problems with mobile devices

Can store a lot of data - sensitive data can be lost

Has microphone, camera, GPS location, tracking/stalking

- Calendar
- Contacts and email,
- Tasks - To Do listen

Easy access to data - easy to get the data

- Vendors make it easy to switch device, move data to new device
- Phones can often move data without inserting SIM card
- Backup of data to memory cards - copy all data in minutes

Access to the company network using VPN or wireless?

- Reuse some login data from mobile devices and connect laptop to the network

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

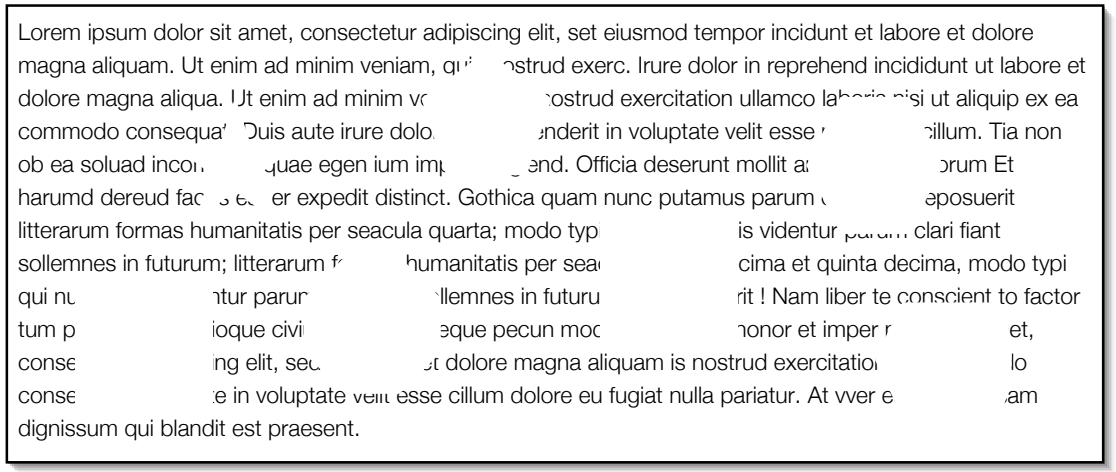
Many people let their laptops stay out in the open - even at conferences

... making theft likely/easy

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

Industrial espionage, economic espionage or corporate espionage is real

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!

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**

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

Firewire attacks

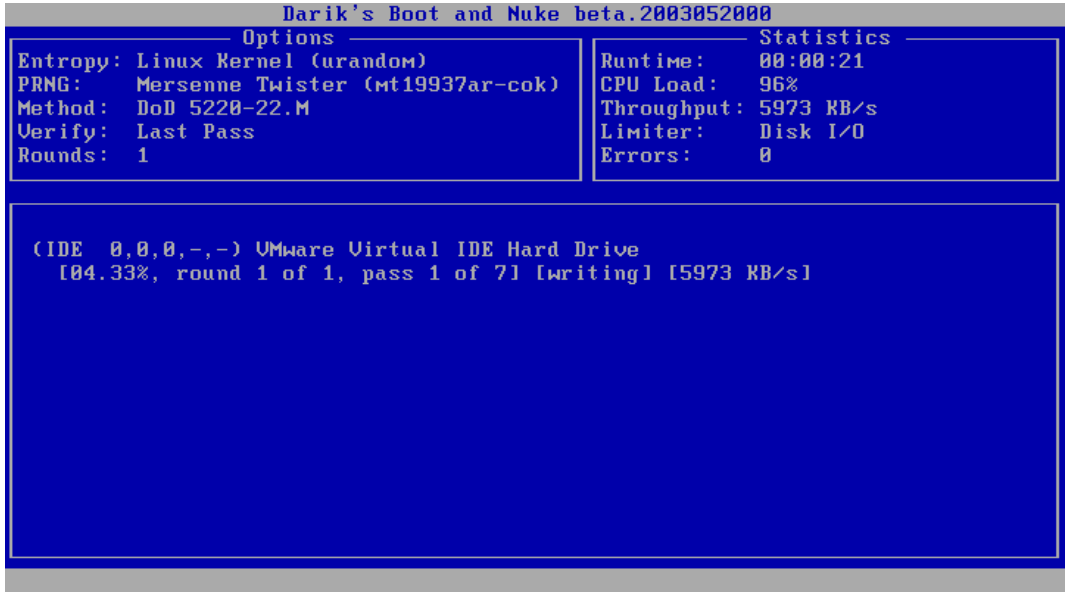
Firewire, DMA & Windows, Winlockpwn via FireWire
Hit by a Bus: Physical Access Attacks with Firewire Ruxcon 2006

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

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

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

... and deleting data



Getting rid of data from old devices is a pain

Some tools will not overwrite data, leaving it vulnerable to recovery

Even secure erase programs might not work on SSD - due to reallocation of blocks

I have used Darik's Boot and Nuke ("DBAN") `http://www.dban.org/`

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.

Can we avoid using Flash and PDF?

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

Flashback

SOLIDO NETWORKS

Adobe Flash problems, player security issues & exploits - 2011

Google Chrome offers to help stop Flash security problems - March 2011

Google have extended their flash security sandbox to allow Adobe flash to take advantage of it. Google have also enhanced plug-in security by notifying the user of out-of-date plug-ins that may cause vulnerabilities.

Flash security vulnerabilities affects Microsoft Excel - March 2011

A flash security issue is currently being exploited by hackers by embedding malicious SWF files into Microsoft Excel spreadsheets. These are then emailed to unsuspecting users. All major OS's are affected by this flash security flaw.

USB flash security compromized by major design flaw - February 2011

Secure flash drives manufactured by some of the big brand flash memory-makers can be sent an 'unlock' flag to the devices which makes them unlock without requiring the password. The system is inherently insecure because when the secure flash drive software authenticates the supplied password it sends an 'unlock' flag to the drive (a common 'conditional jump'), which can be patched to unlock the device.

Adobe flash security sandbox bypassed - January 2011

Adobe flash player security has been bypassed by a security researcher who used a file request to a network machine. Adobe flash problems were meant to be minimized by use of the sandbox but the security researcher detailed how this could be easily bypassed by a malicious person.

Source: `http://www.locklizard.com/adobe-flash-security.htm`

Flash blockers

Safari `http://clicktoflash.com/`

Firefox Extension Flashblock and NoScript

Chrome extension called FlashBlock and built-in configurable setting Click to play

Internet Explorer: 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.

FlashBlockere til iPad? iPhone? Android?

why aren't Flash blockers on by default?

Note it is easy to inject malicious javascript and flash when sharing a wireless network

Secure protocols

Securing e-mail

- Pretty Good Privacy - Phil Zimmermann
- OpenPGP = e-mail security

Network sessions use SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- Encrypting data sent and received
- SSL/TLS already used for many protocols as a wrapper: POP3S, IMAPS, SSH, SMTP+TLS m.fl.

Encrypting traffic at the network layer - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- OpenVPN uses SSL/TLS across TCP or UDP

Note: SSL/TLS is not trivial to implement, key management!

Basic tools - PGP

- Pretty Good Privacy - PGP
- Originally developed by Phil Zimmermann
- Now a commecrial entity `http://www.pgp.com`
- Source exported from USA on paper and scanned outside - which was legal
- `http://www.pgpi.org`

Basic tools - GPG

Gnu Privacy Guard, GnuPG or GPG

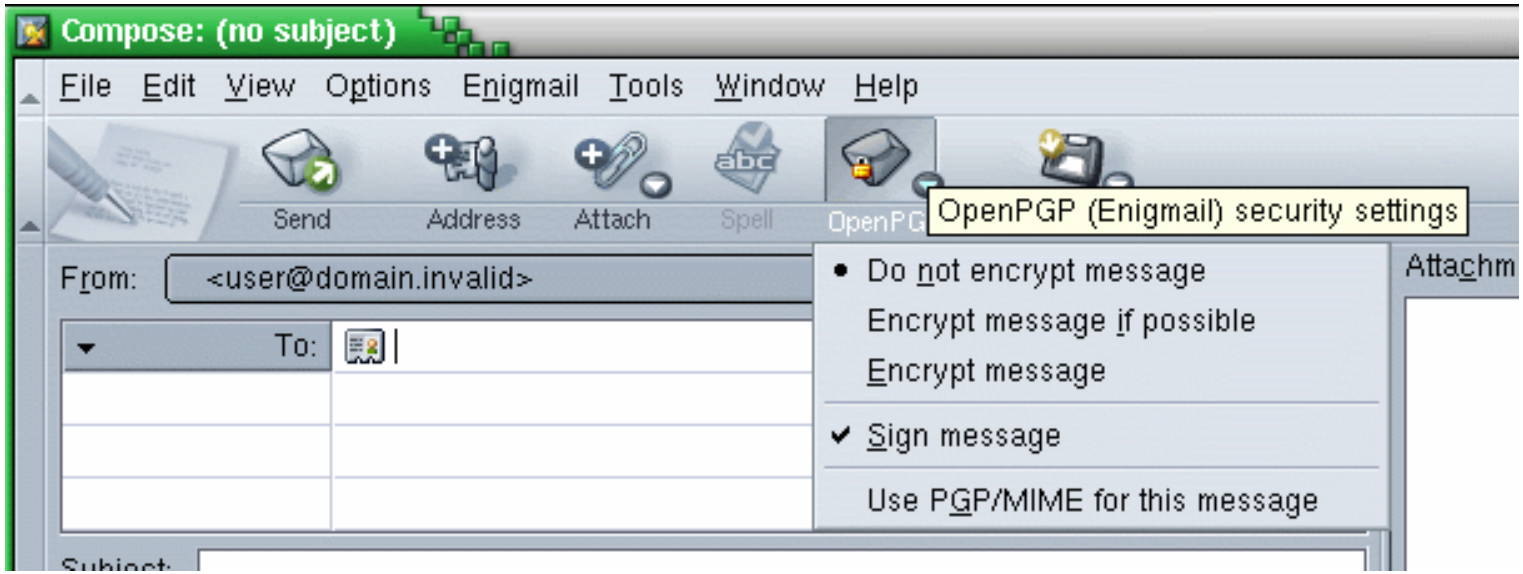
Web site: `http://www.gnupg.org/`

Open Source - GPL license

Available for most popular operating systems

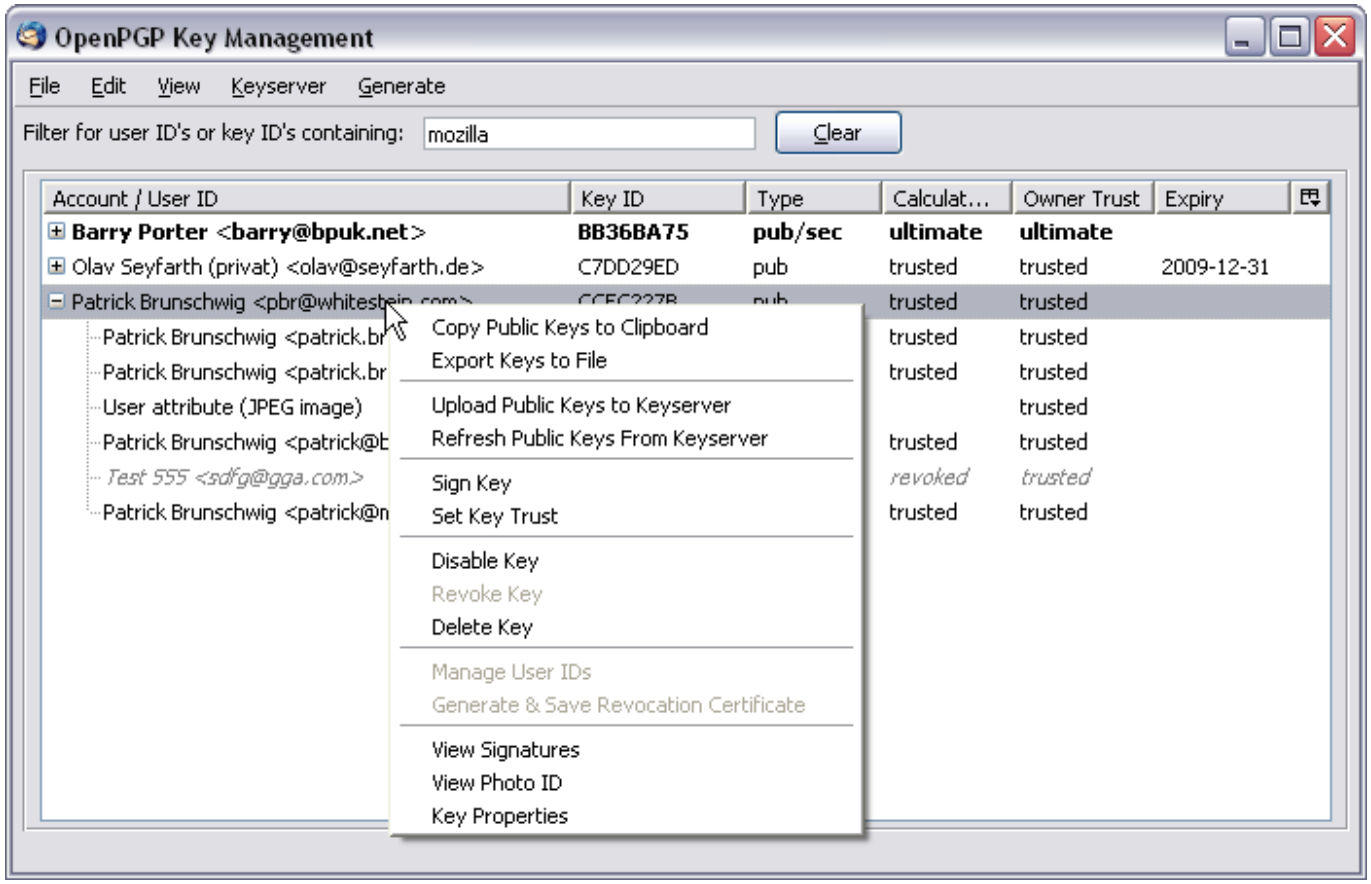
Highly recommended

Enigmail - GPG plugin til Mail



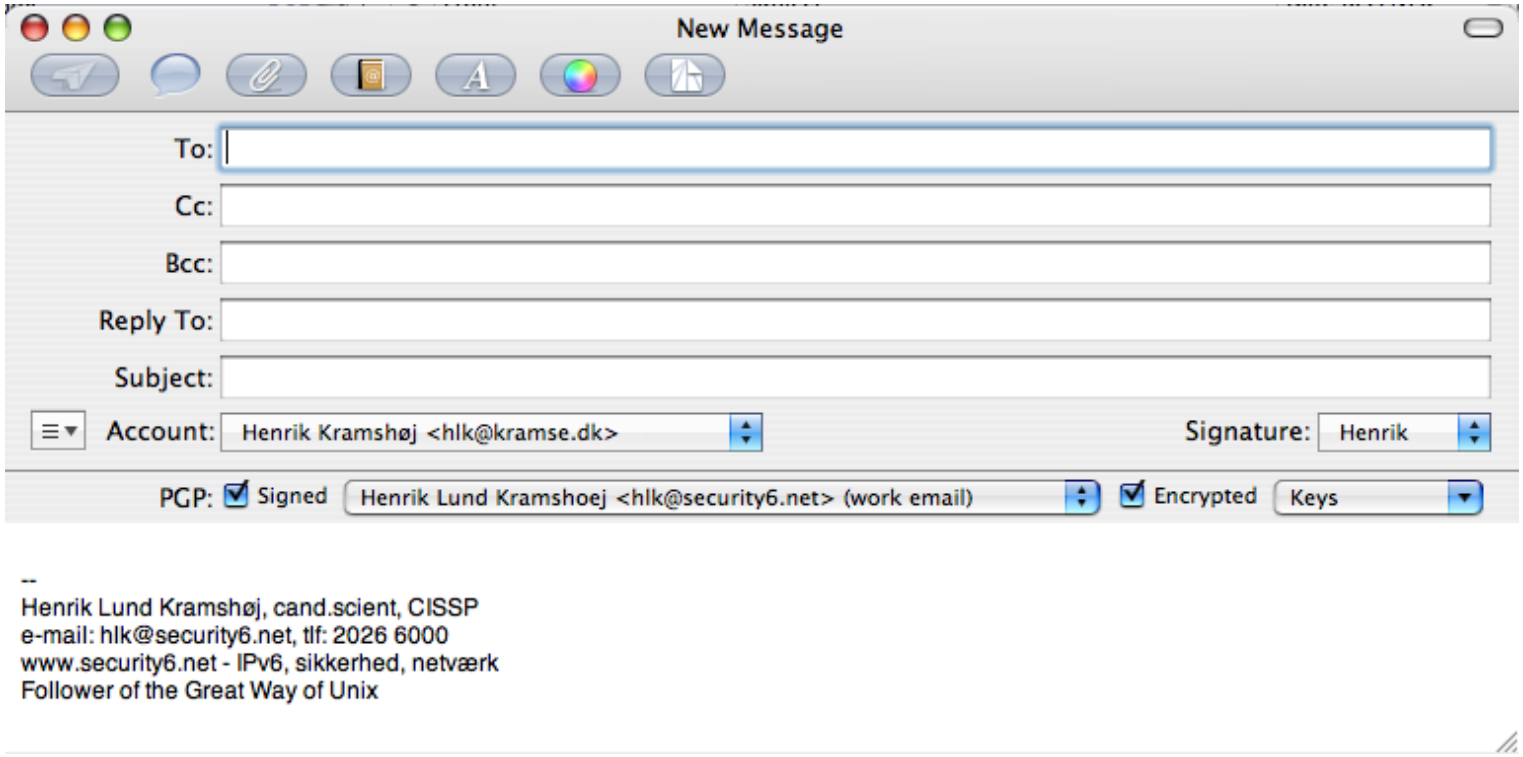
- Enigmail is a plugin for the Thunderbird mail client
- Screenshot from `http://enigmail.mozdev.org`

Enigmail - OpenGPG Key Manager



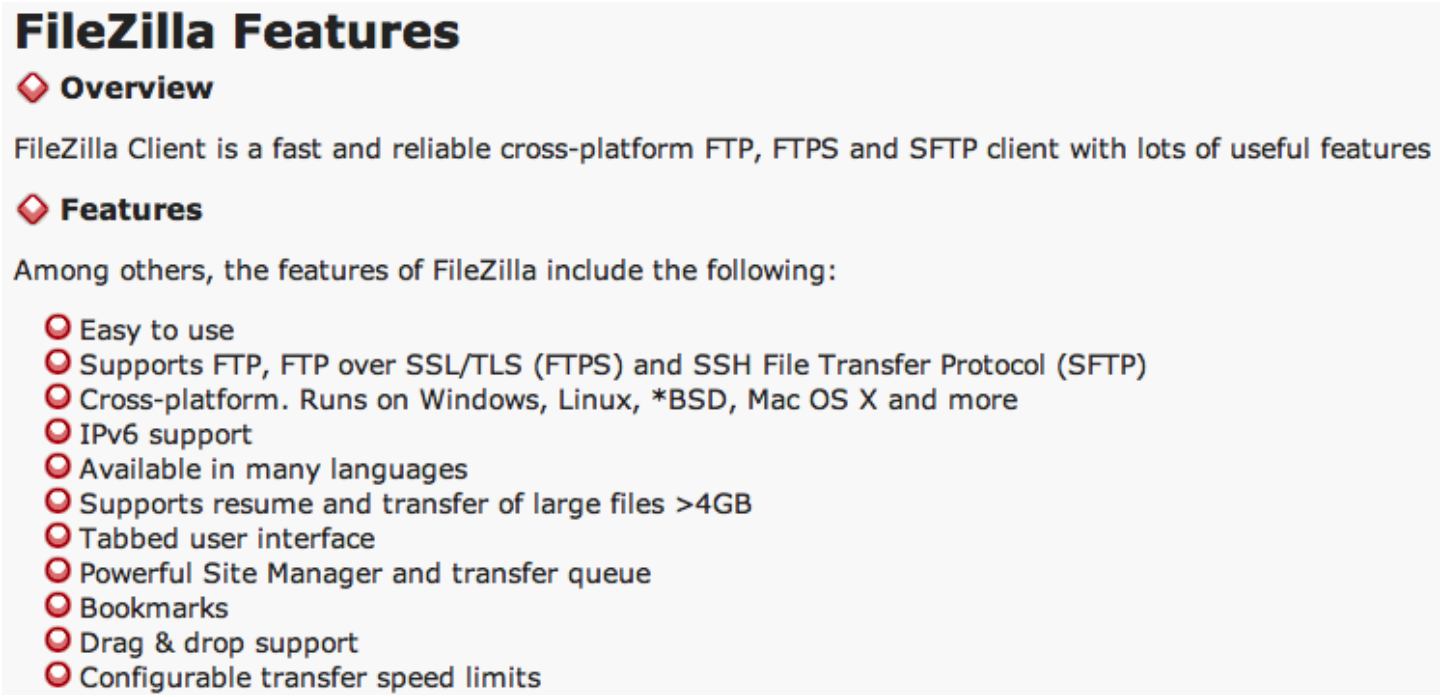
Key Manager built-int Enigmail is recommended

GPGMail plugin for Mac OS X Mail.app



- Uses GPG and is part of the GPGTools
- `https://gpgtools.org/`

Filetransfer programs FileZilla - 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

Stop using FTP! Dammit!

Lots of programs support SFTP and SCP for secure copying of data

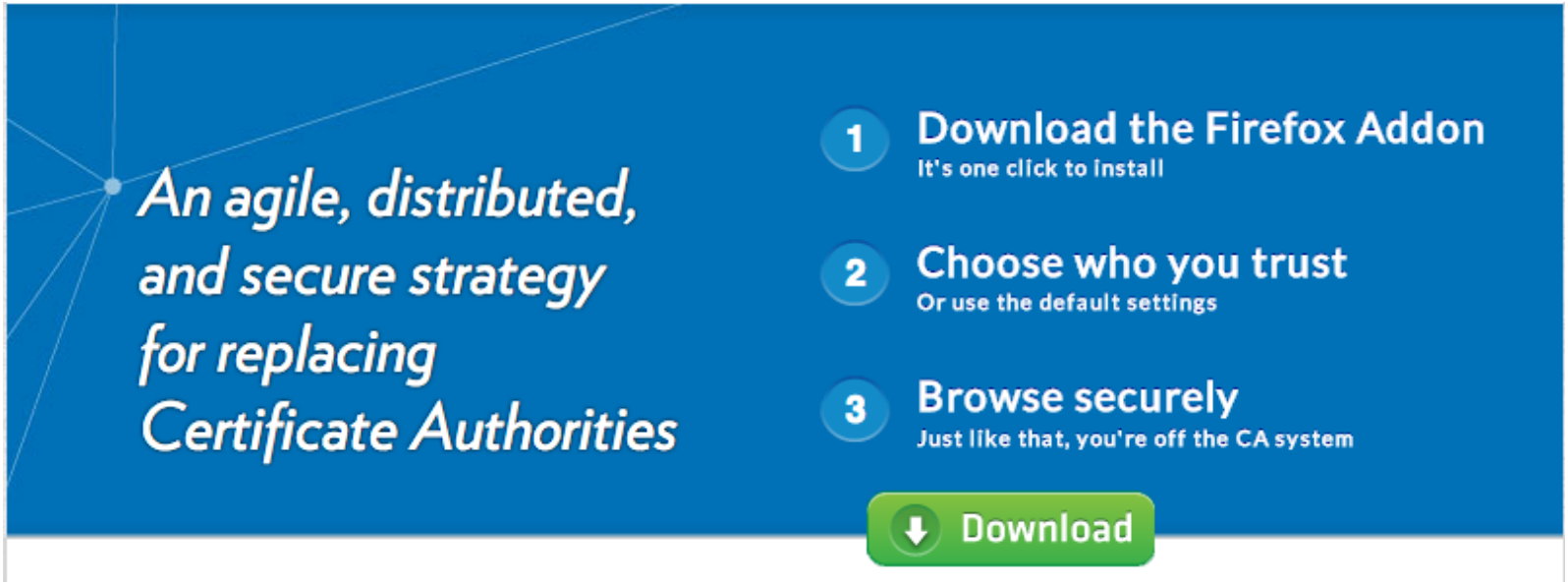
`http://filezilla-project.org/`

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`

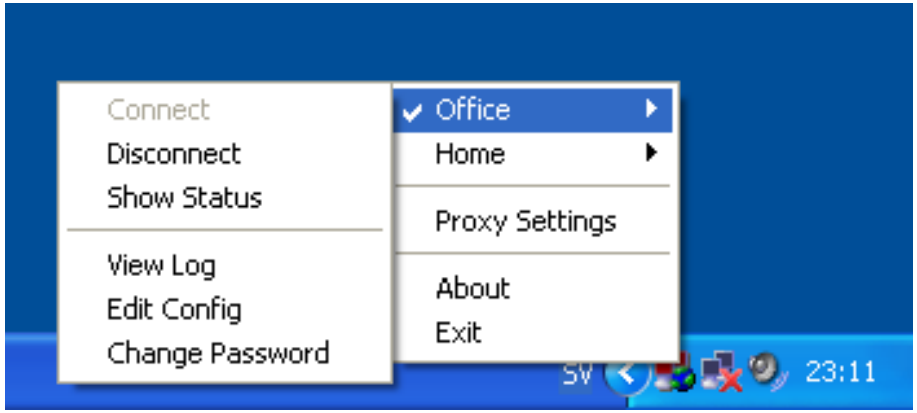
Convergence - who do you trust



`http://convergence.io/`

Warning: radical change to how certificates work

VPN



Virtual Private Networks are useful - or even required when travelling

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

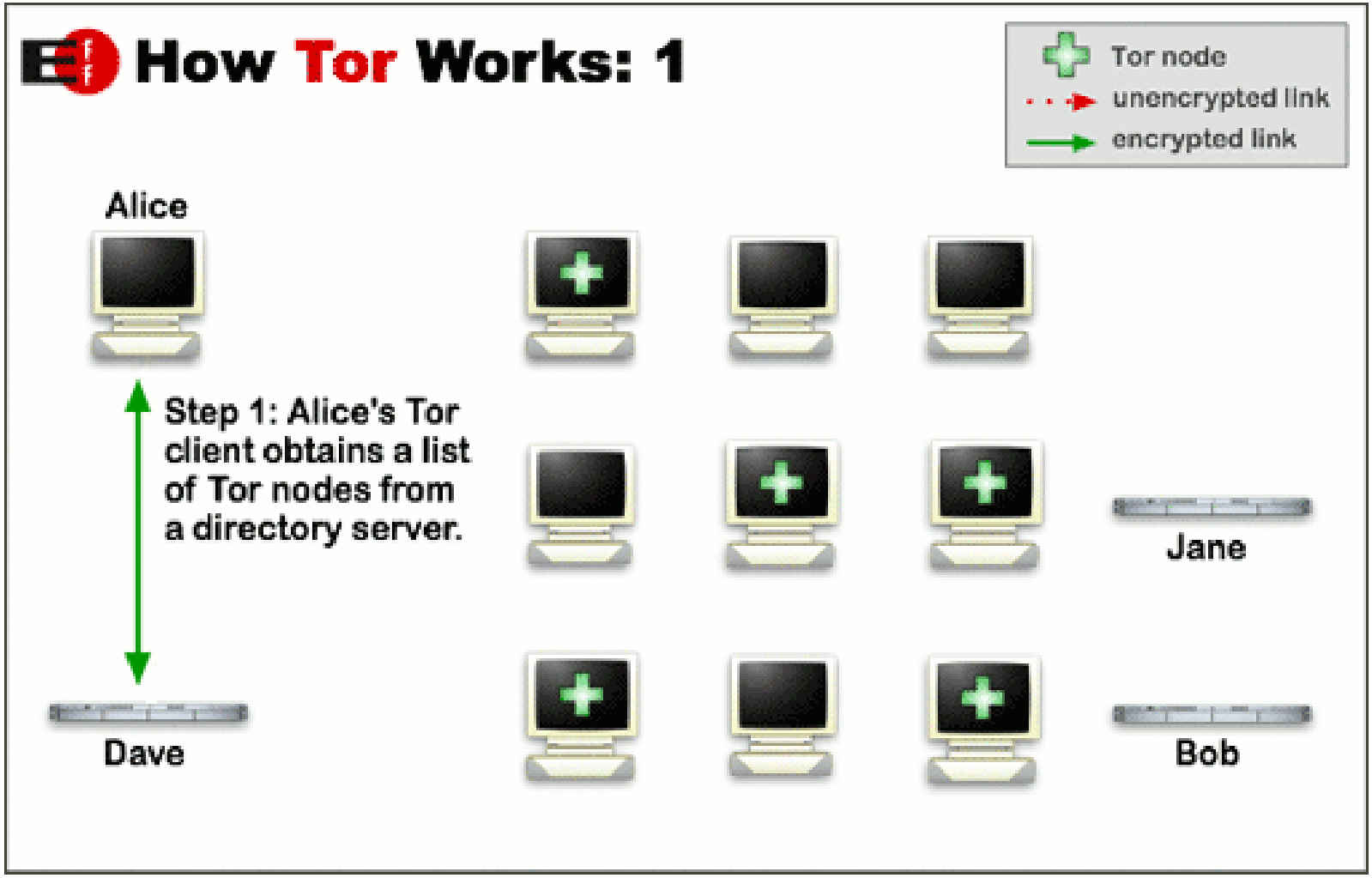
SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

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

Tor project

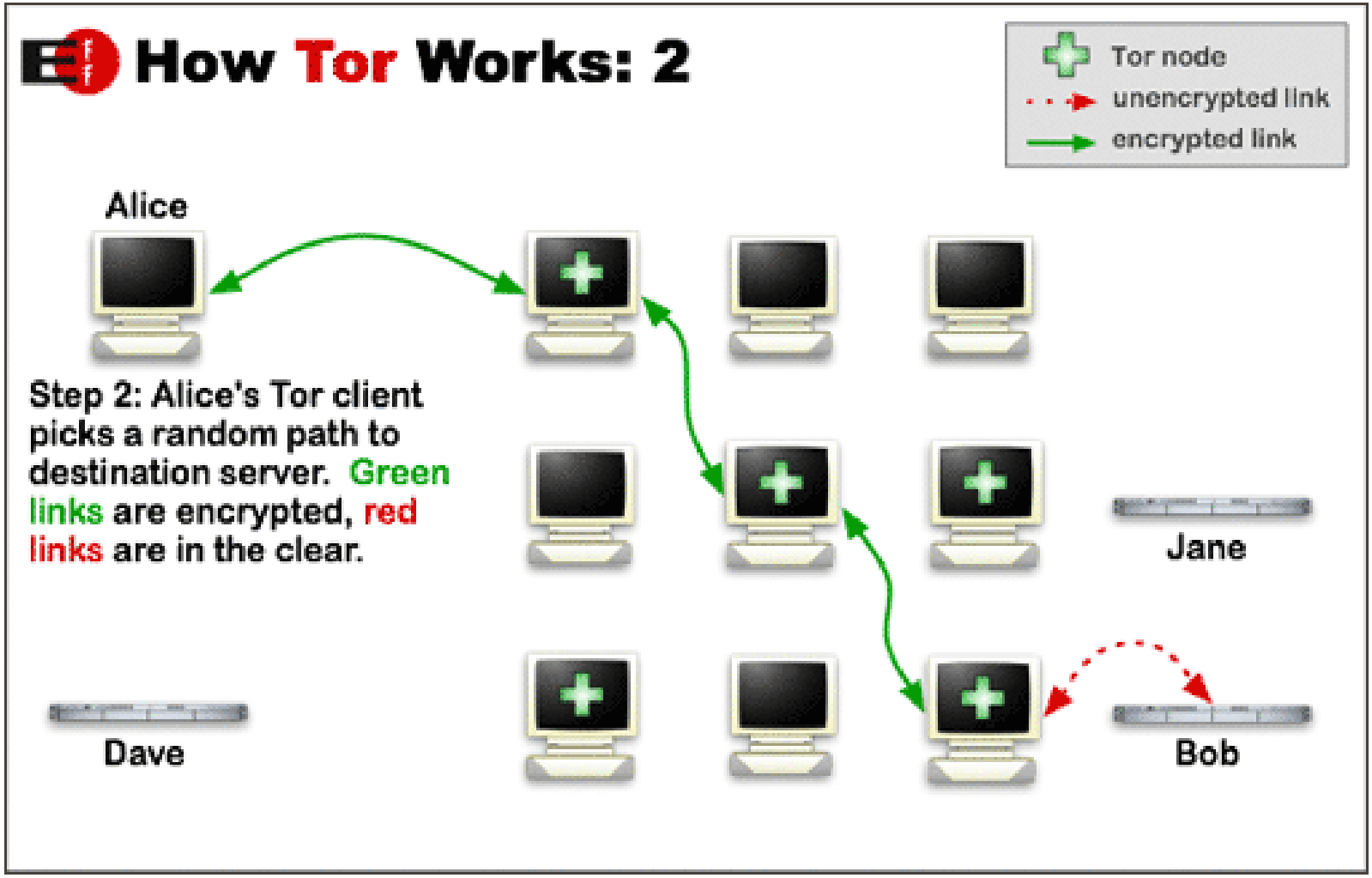
https://www.torproject.org/

Tor project - how it works 1



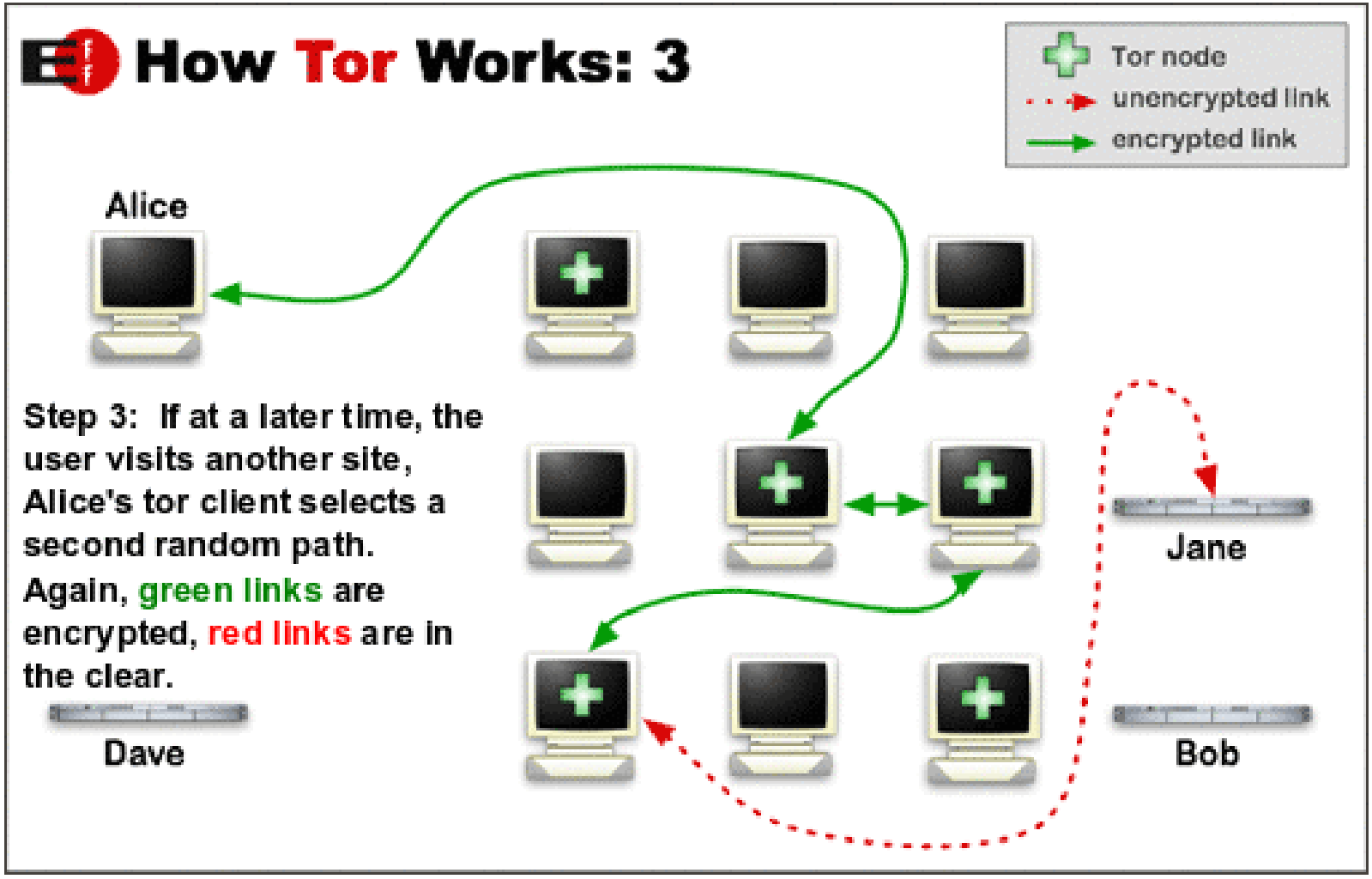
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project - how it works 2



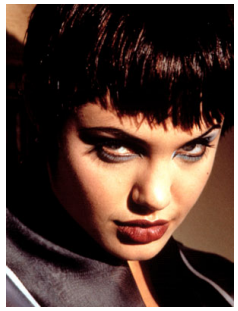
pictures from `https://www.torproject.org/about/overview.html.en`

Tor project - how it works 3



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

Hackers and ressources



Hackers work all the time to break stuff

Use hackertools:

- Nmap, Nping - test network ports `http://nmap.org`
- Wireshark advanced network analyzer - `http://http://www.wireshark.org/`
- Metasploit Framework exploit development and delivery `http://www.metasploit.com/`
- Burpsuite web scanner and proxy `http://portswigger.net/burp/`
- Skipfish web scanner `http://code.google.com/p/skipfish/`
- Kali Linux pentesting operating system `http://www.kali.org`
- Most used hacker tools `http://sectools.org/`

Picture: Angelina Jolie as *Kate Libby/Acid Burn* Hackers 1995

Part III: Reduce risk and mitigate impact

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*

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

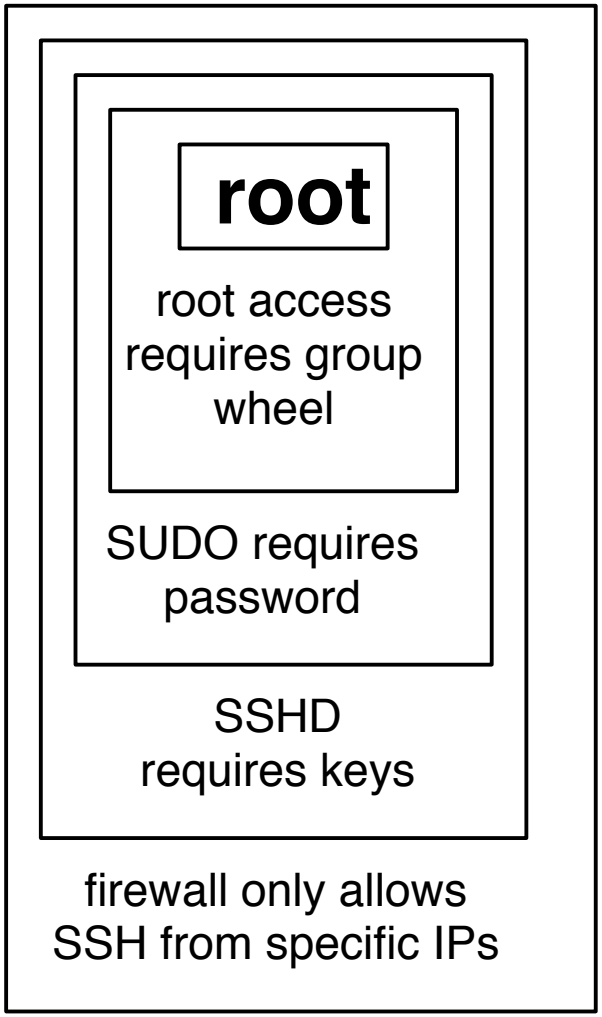
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

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

Defense in depth - flere lag af sikkerhed



Defense using multiple layers is stronger!

Are passwords dead?

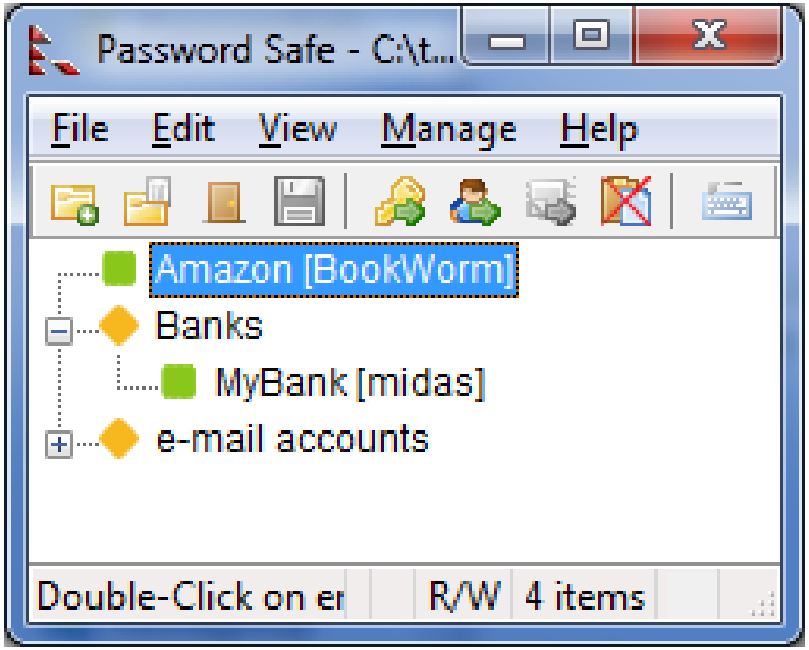
google: passwords are dead
About 6,580,000 results (0.22 seconds)

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`

Storing passwords



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

Apple Keychain provides an encrypted storage

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

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`

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.

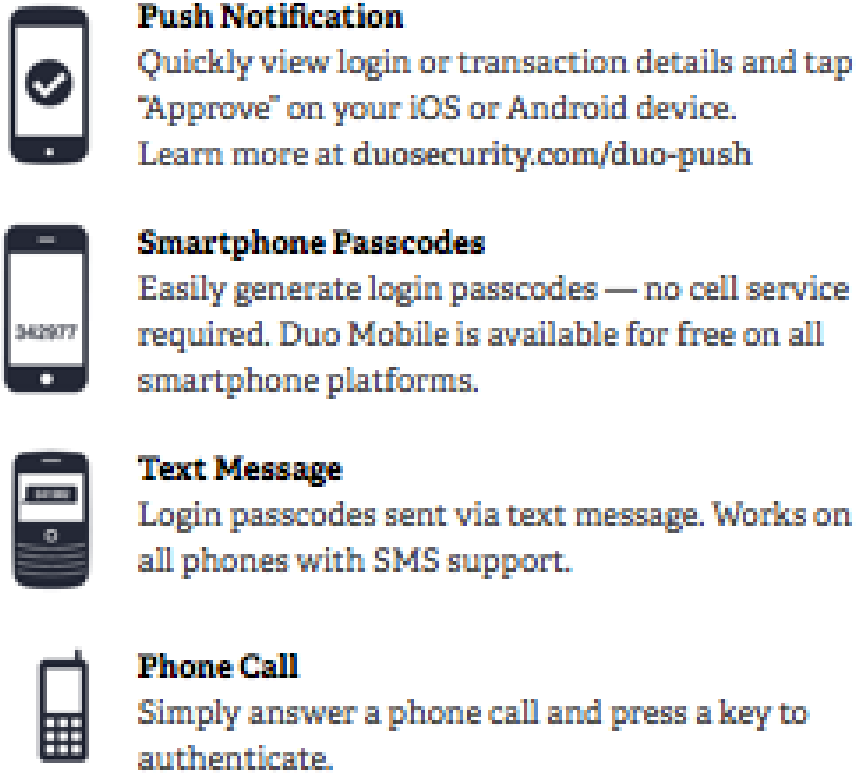
› Password Safe YubiKey

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/`

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.

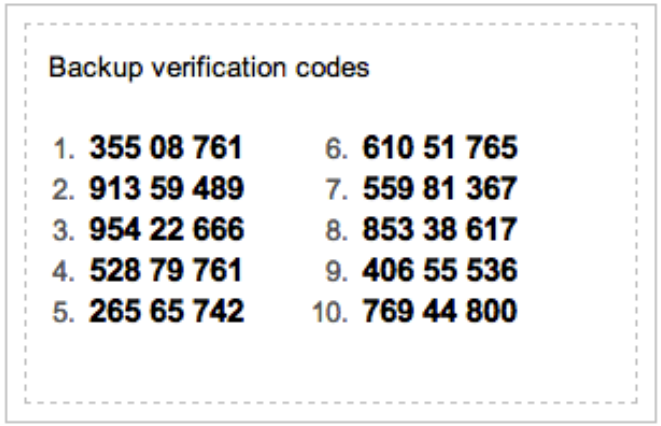
Video `https://www.duosecurity.com/duo-push`

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

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

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

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`

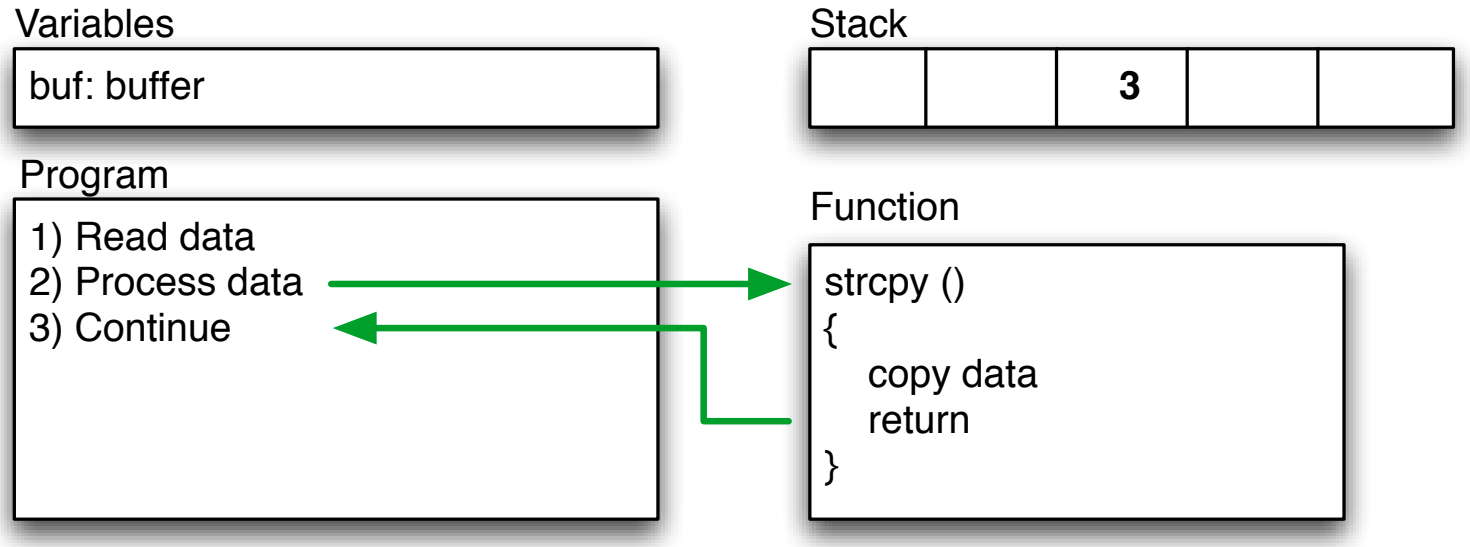
buffer overflows is a C problem

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.

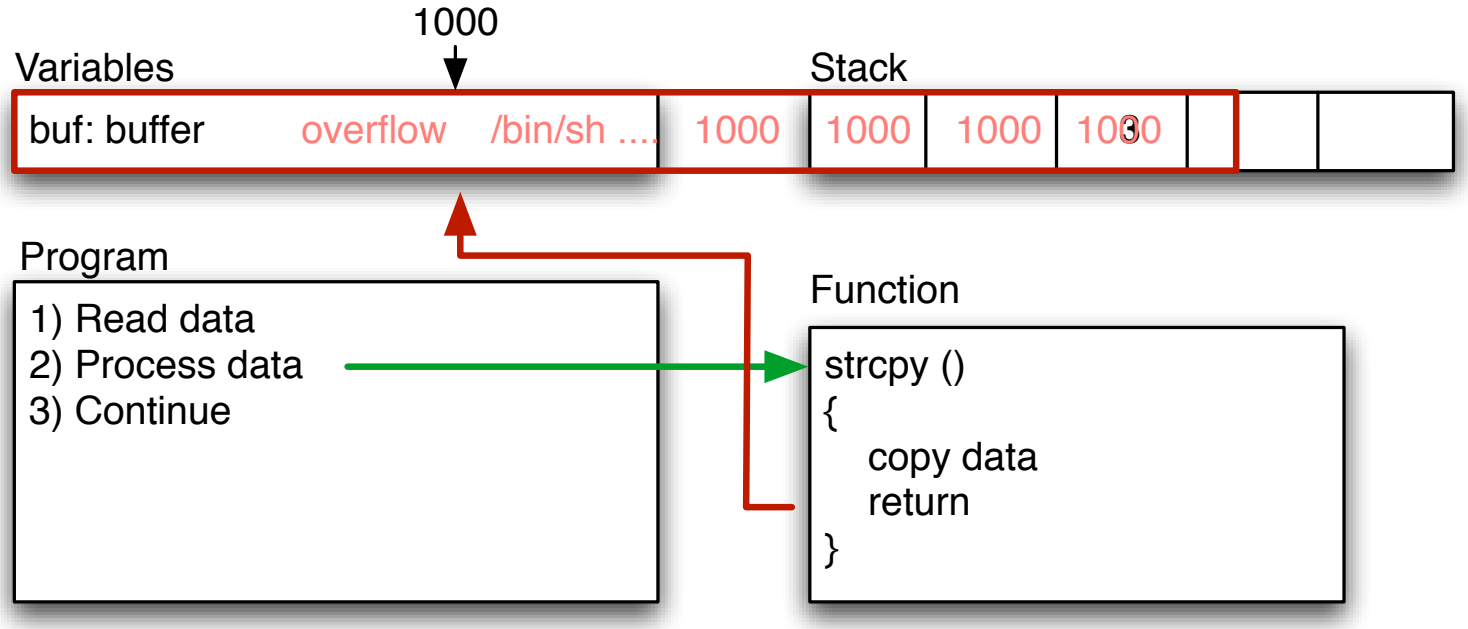
Stack protection today both a specific technique and generic term for adding protection to operating systems and programs to reduce the likelihood of buffer overflows succeeding. The main features are protecting areas in memory by making them non-writeable and non-executable. StackGuard and Propolice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

Buffer og stacks




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

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

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

Exploit sample

SOLIDO NETWORKS

```
$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

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

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

local vs. remote exploits

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

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 ☺

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`

Change management

Do people have focus on software in production

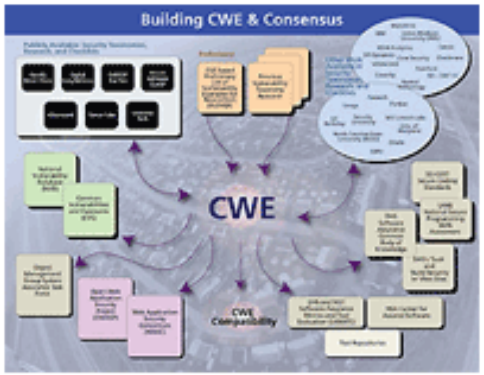
Can you re-install a server quickly, easily

Making changes to production systems

Fall back plan when updating that production database live

Good system administrators are hard to come by

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/

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.

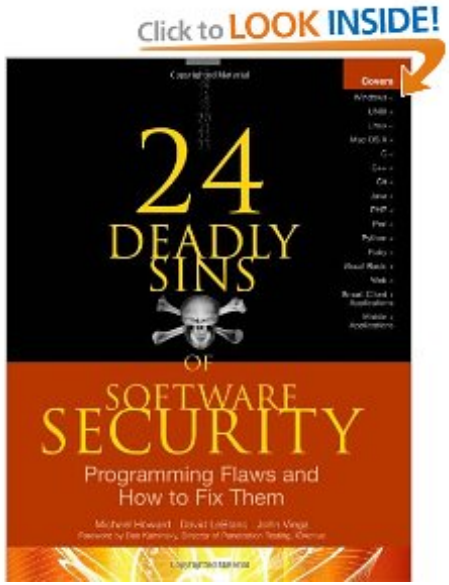
A Monster Mitigation Matrix is also available to show how these mitigations apply to weaknesses in the Top 25.

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.

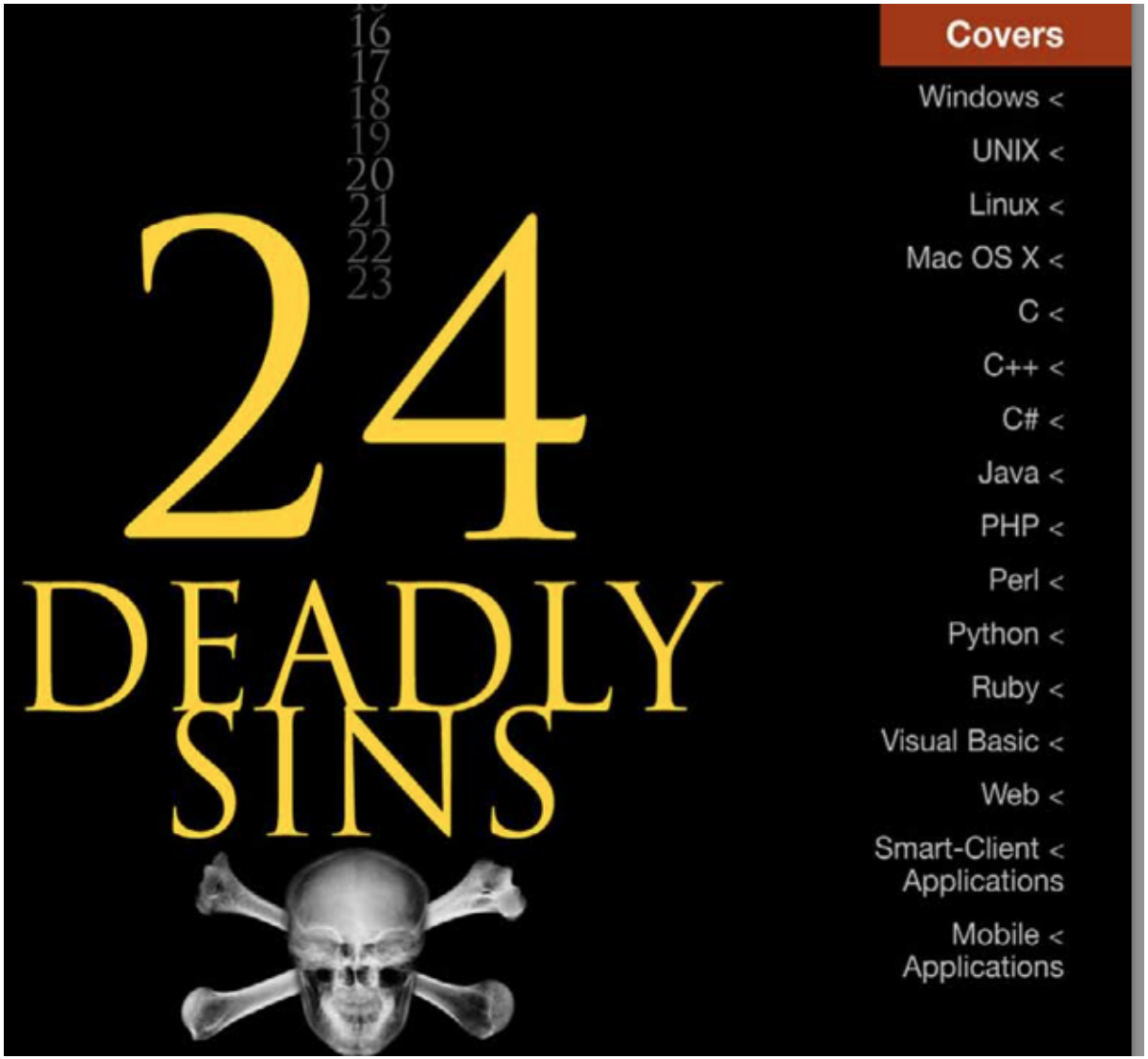
Source: `http://cwe.mitre.org/top25/index.html`

Deadly sins bogen



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

Deadly sins bogen - close up



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?

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

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`

Kilde:
`http://www.metasploit.com/redmine/projects/framework/wiki/Release_Notes_360`

Kali Linux the new backtrack

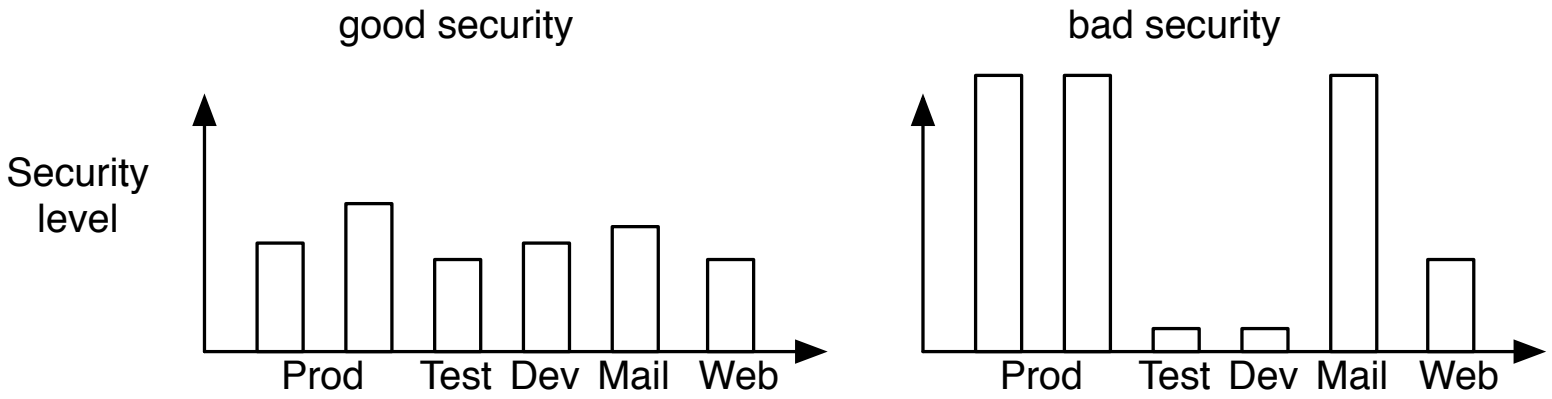
BackTrack `http://www.backtrack-linux.org`

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

The Exploit Database - dagens buffer overflow

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

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

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

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`

Twitter news

Twitter is one of the fastest newsfeeds in the world

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

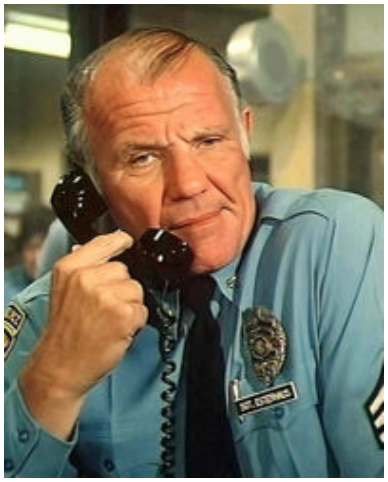
Some advice can be found in these places

- `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`

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

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

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