

Welcome to

IT-sikkerhed 2013

PROSA Superhelteseminar

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

<http://www.solidonetworks.com>



Don't Panic!

Kl 17:00-19:00

Mindre enetale, mere foredrag 2.0 med sociale medier, informationsdeling og interaktion

Send gerne spørgsmål senere

PS er her nogle timer efter foredraget til spørgsmål og snak



Vores passwords er overalt

Vi er afhængige af cloud services

Vi er afhængige af netværk

Vi er afhængige af andres computere - servere og services

The 5th Wave

By Rich Tennant



"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."

Opbevaring af passwords



.

Backup - jævnligt

Kryptografi og kryptoværktøjer Sikre protokoller

Tal frit - Lær og lær fra dig

Følg med i nyheder, støt det frie internet





- 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/>
- Kali Linux operativsystem med fokus på sikkerhedstest <http://www.kali.org>

Billede: Angelina Jolie fra Hackers 1995

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.

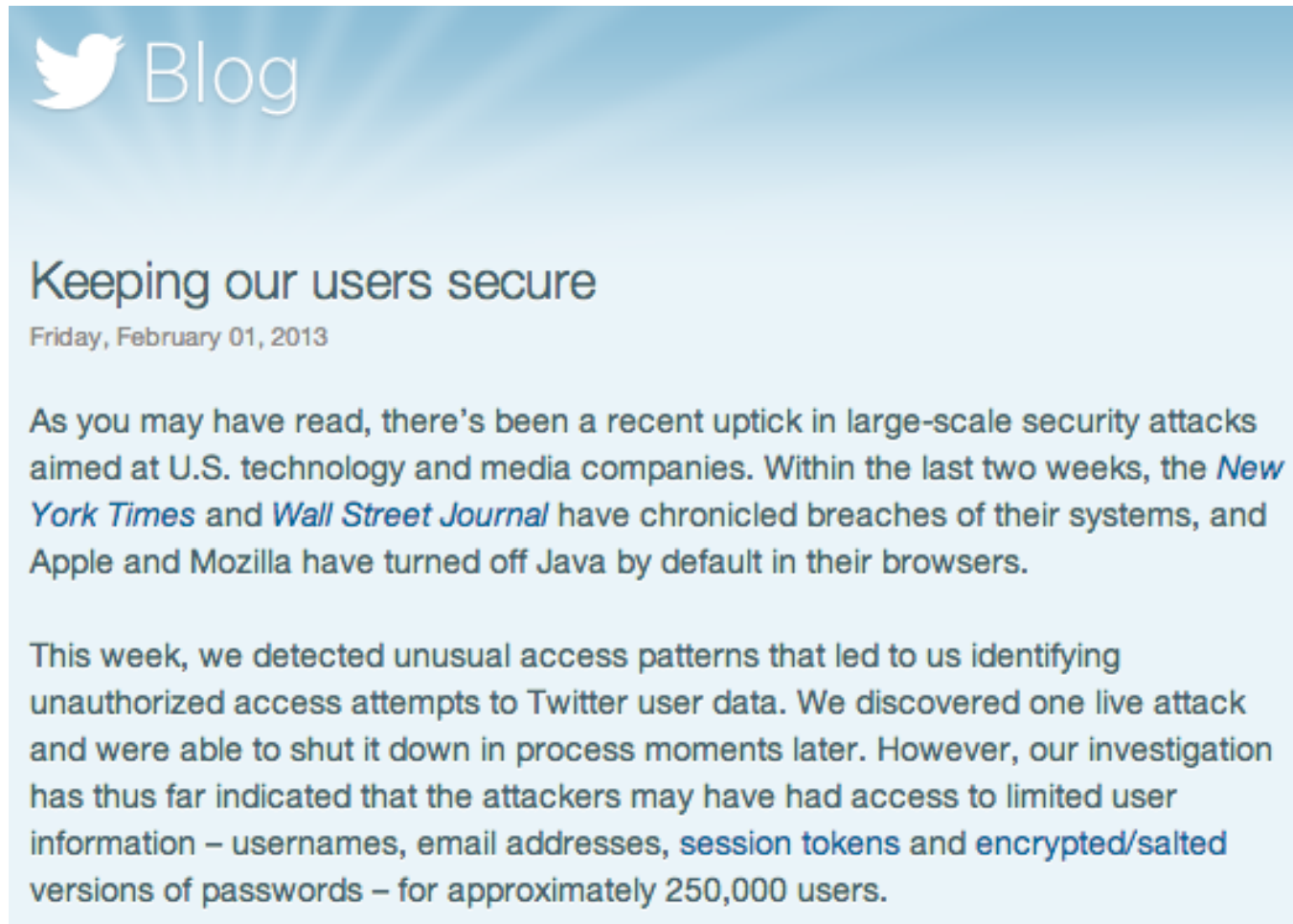
As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

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



Sources:

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

January: 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/>

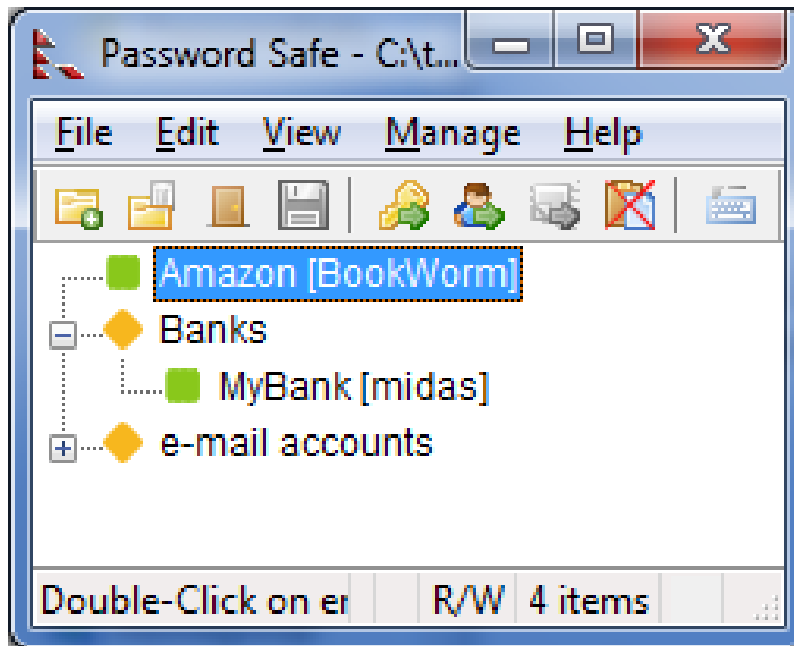
Are passwords dead?

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://en.wikipedia.org/wiki/Crack_(password_software))

<http://dropsafe.crypticide.com/muffett-passwords>



PasswordSafe <http://passwordsafe.sourceforge.net/>

Apple Keychain

Browsers, Firefox Master Password

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>



> 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

Passord 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/>



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.



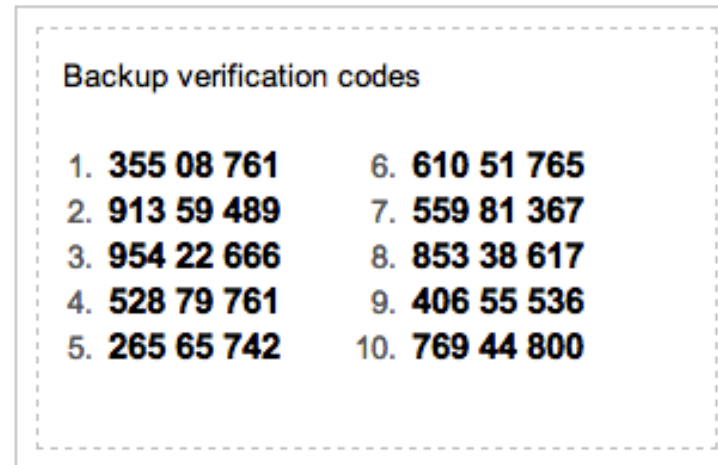
Phone Call

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

Video <https://www.duosecurity.com/duo-push>

<https://www.duosecurity.com/>

Print af koder, low level pragmatisk



Login fra nye enheder kræver ekstra sikkerhed

google 2-faktor auth. SMS med backup codes

Developed at Bellcore in the late 1980s <http://en.wikipedia.org/wiki/S/KEY>

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incididunt et labore et dolore magna aliqua. Ut enim ad minim veniam, qui nostrud exerc. Irure dolor in reprehenderit in voluptate velit esse cillum. Tia non ob ea soluta in corporis quae egestas impedit. Officia deserunt mollit anim id est laborum Et harumque corruptoribus expedit distinctio. Gothica quam nunc putamus parum claram, aperuerit litterarum formas humanitatis per seacula quarta; modo typi is videntur, clari fiant sollemnes in futurum; litterarum formas humanitatis per seacula prima et quinta decima, modo typi qui nunc solent parum sollemnes in futuro rit ! Nam liber te conscient to factor tum per idemque civili neque pecuniae modum honor et imperium et, consequentia elit, secundum ut dolore magna aliqua is nostrud exercitation ullamco laboris consequentia in voluptate velit esse cillum dolore eu fugiat nulla pariatur. At vero eos et accusamus et iusto odio dignissim dui dolorem ipsum veniam, qui blandit est praesent.

Stjålet laptop

Cloud services

Slettede eller ødelagte data

- og hvordan sletter man data? Huskede du mini SD kortet med dine private billeder?



Kryptering findes i alle de gængse klient operativsystemer

- Microsoft Windows Bitlocker - kryptering af disken Ultimate eller Enterprise
- Apple Mac OS X - krypterer nemt med FileVault og FileVault2
- FreeBSD GEOM og GBDE - giver mulighed for at kryptere enheder generelt
- PGP disk - Pretty Good Privacy - laver en virtuel krypteret disk
- Nogle producenter har kodeord på disken - IBM harddisk BIOS kodeord

Kryptering af e-mail

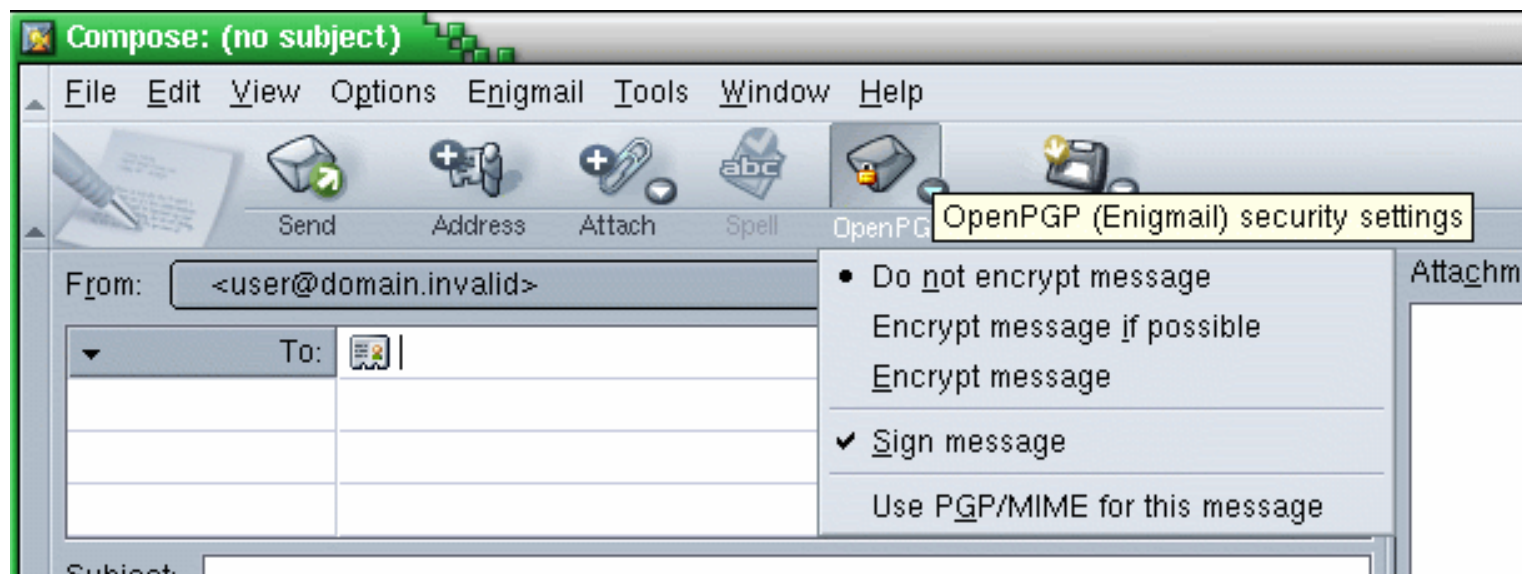
- Pretty Good Privacy - Phil Zimmermann
- PGP = mail sikkerhed

Kryptering af sessioner SSL/TLS

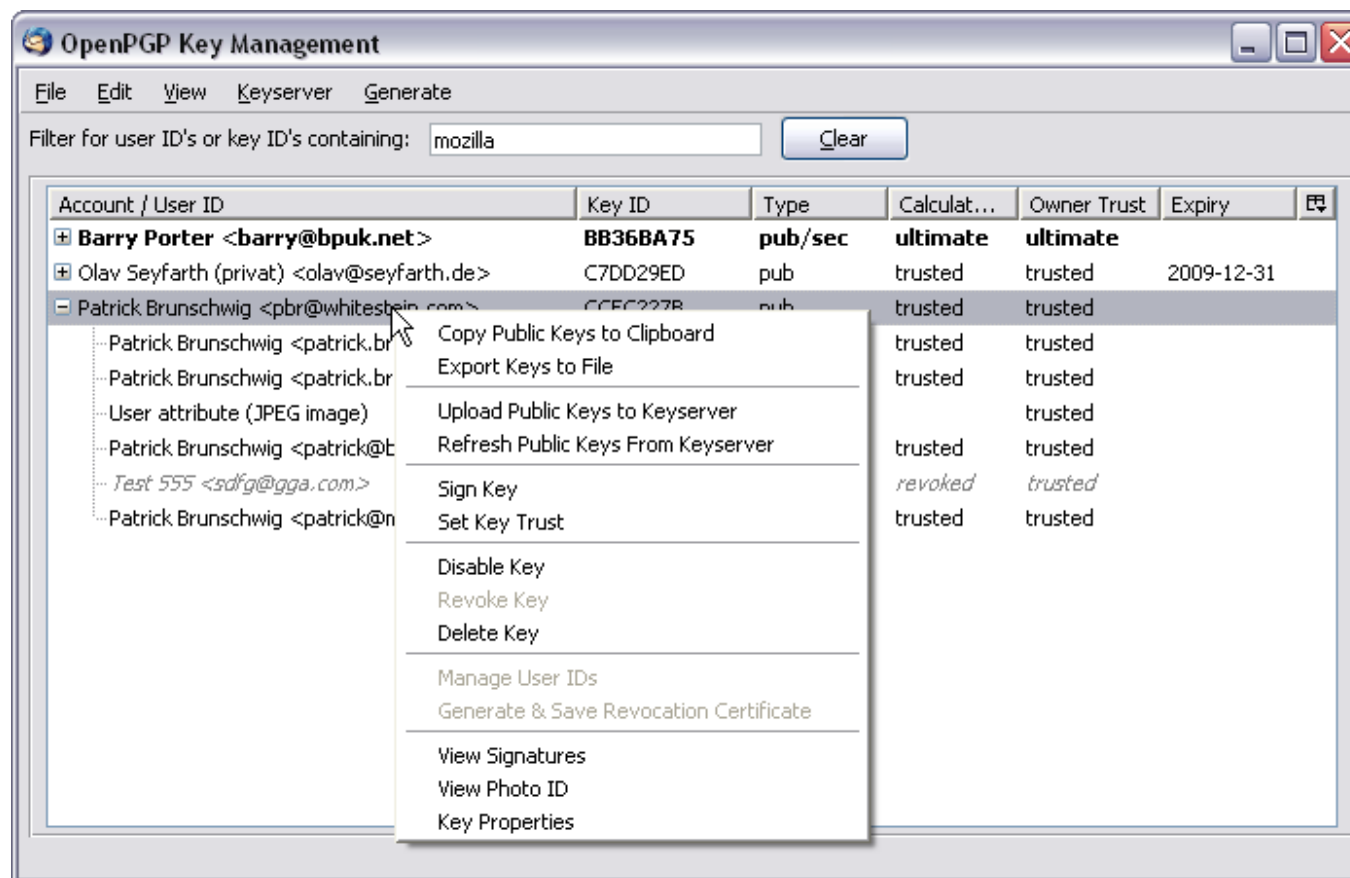
- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Kryptering af netværkstrafik - Virtual Private Networks VPN

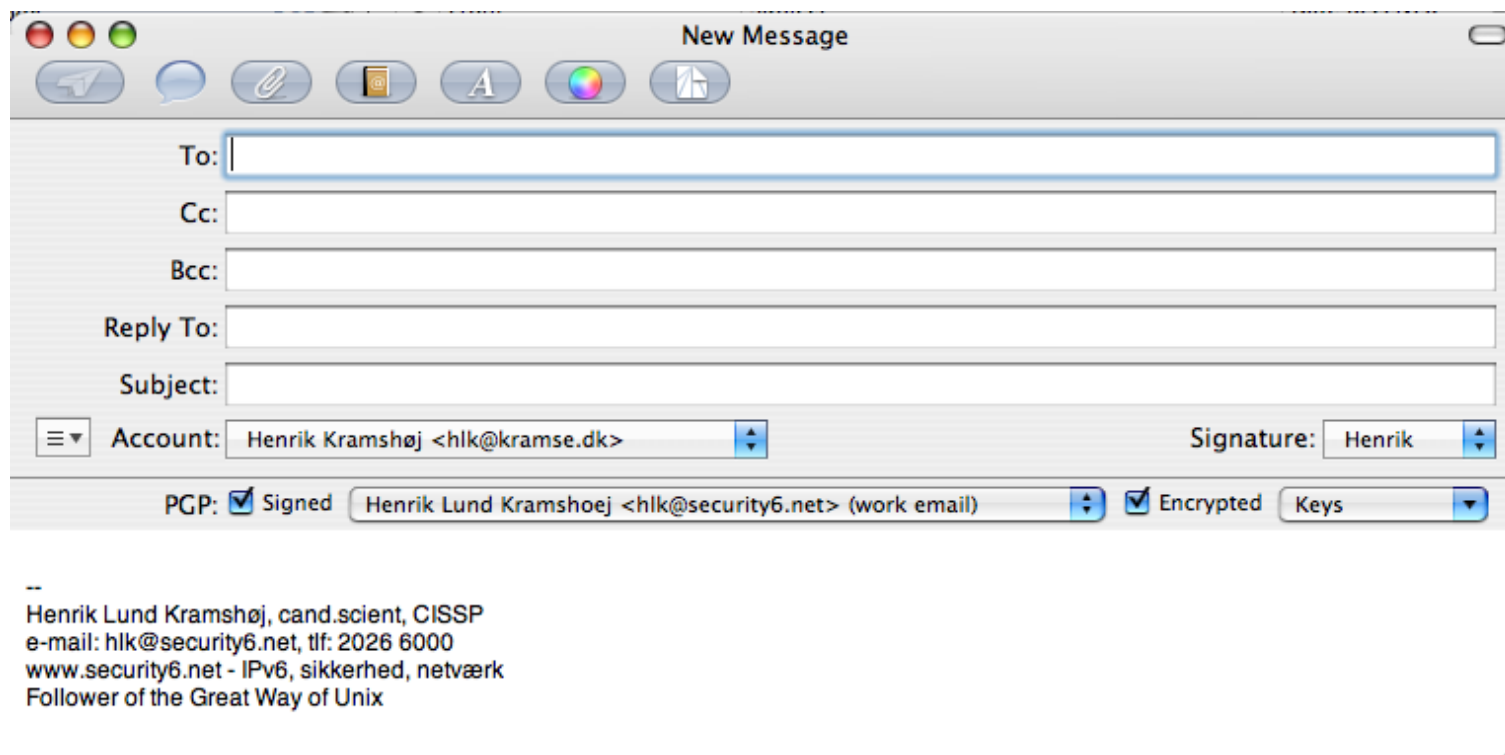
- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol - dårlig og usikker, brug den ikke mere!
- OpenVPN m.fl.



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



Key Manager funktionaliteten i Enigmail kan anbefales



- Bruger GPG
- kilde: <http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html>
- Mailserver udvidelser som <https://github.com/infertux/zeyple>

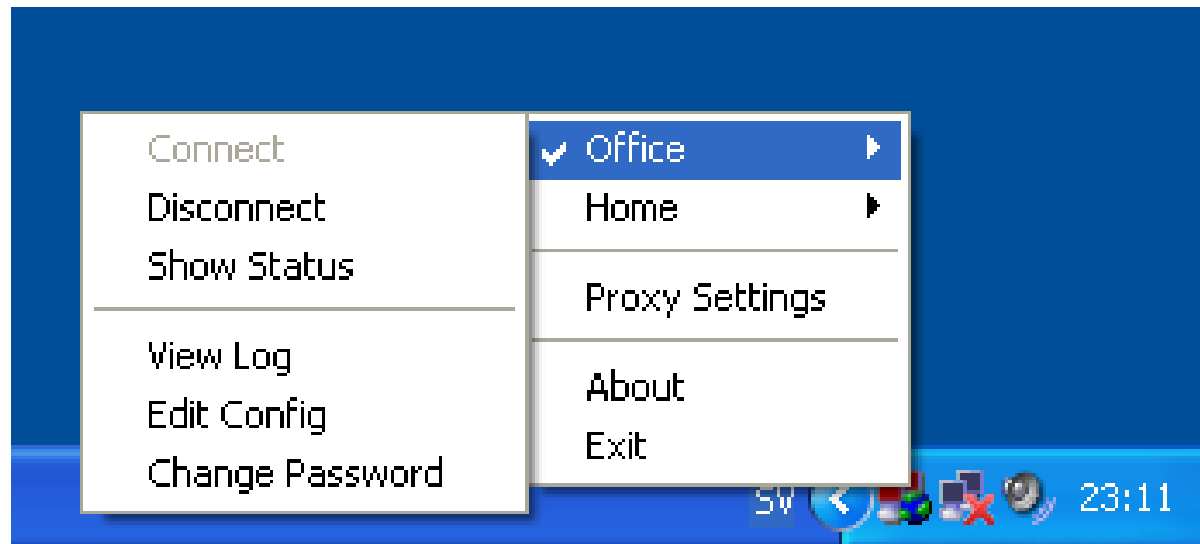
VPN http://en.wikipedia.org/wiki/Virtual_private_network

SSL/TLS VPN - Generelt koncept. Adskillige leverandører: Cisco, Juniper, F5 Big IP

De snakker ikke ret godt sammen på tværs. Brug IPSec for dette.

IPsec er desværre blokeret mange steder og man skal bruge en klient
(I praksis bruger SSL VPN ofte en klient, men den downloades fra web)

Open source variant: OpenVPN



OpenVPN GUI - easy to use

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/>



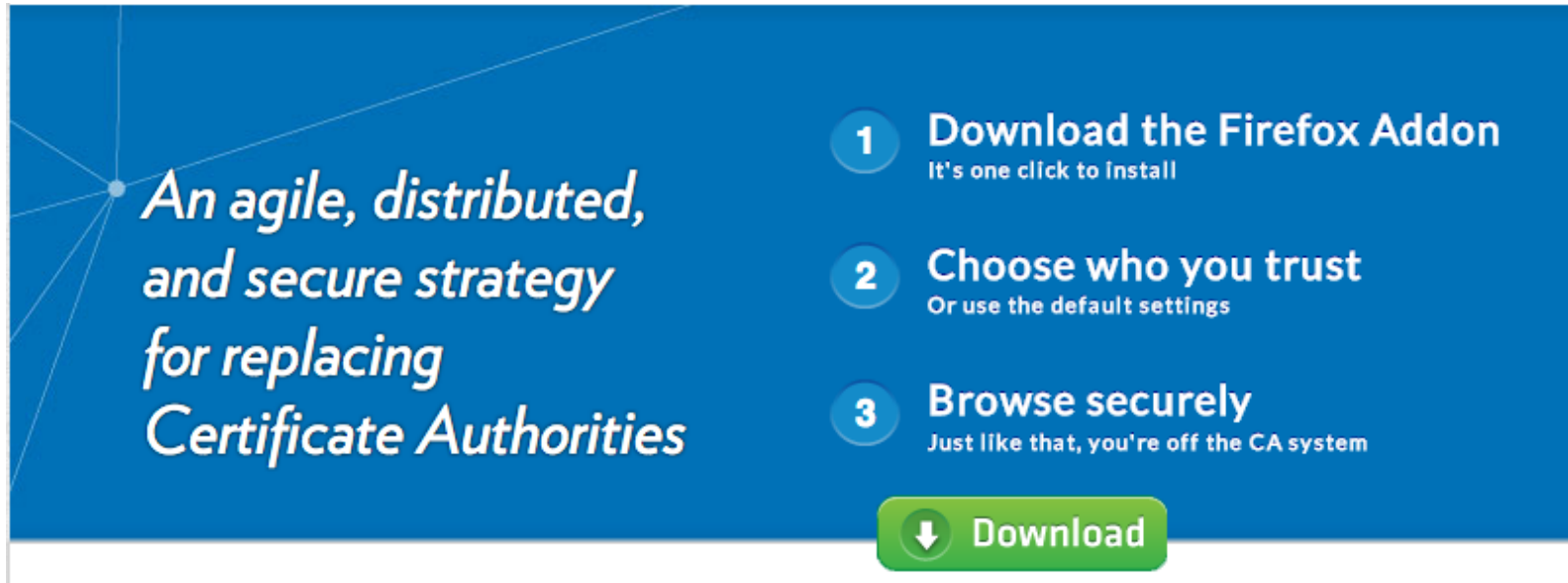
HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

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




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/>



*An agile, distributed,
and secure strategy
for replacing
Certificate Authorities*

- 1 Download the Firefox Addon**
It's one click to install
- 2 Choose who you trust**
Or use the default settings
- 3 Browse securely**
Just like that, you're off the CA system

 **Download**

<http://convergence.io/>

Warning: radical change to how certificates work

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 Java, Flash og PDF?

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



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?

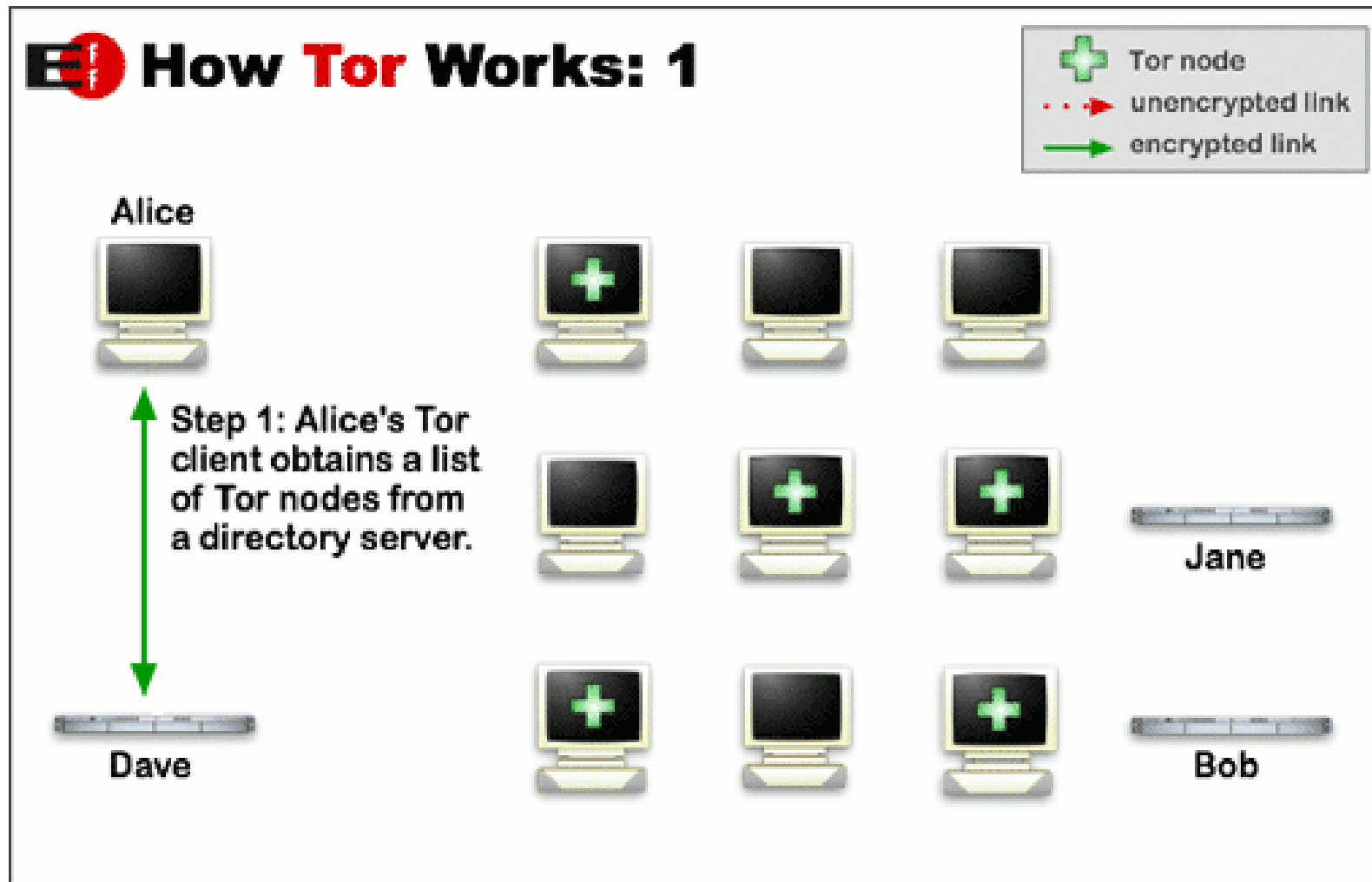


Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

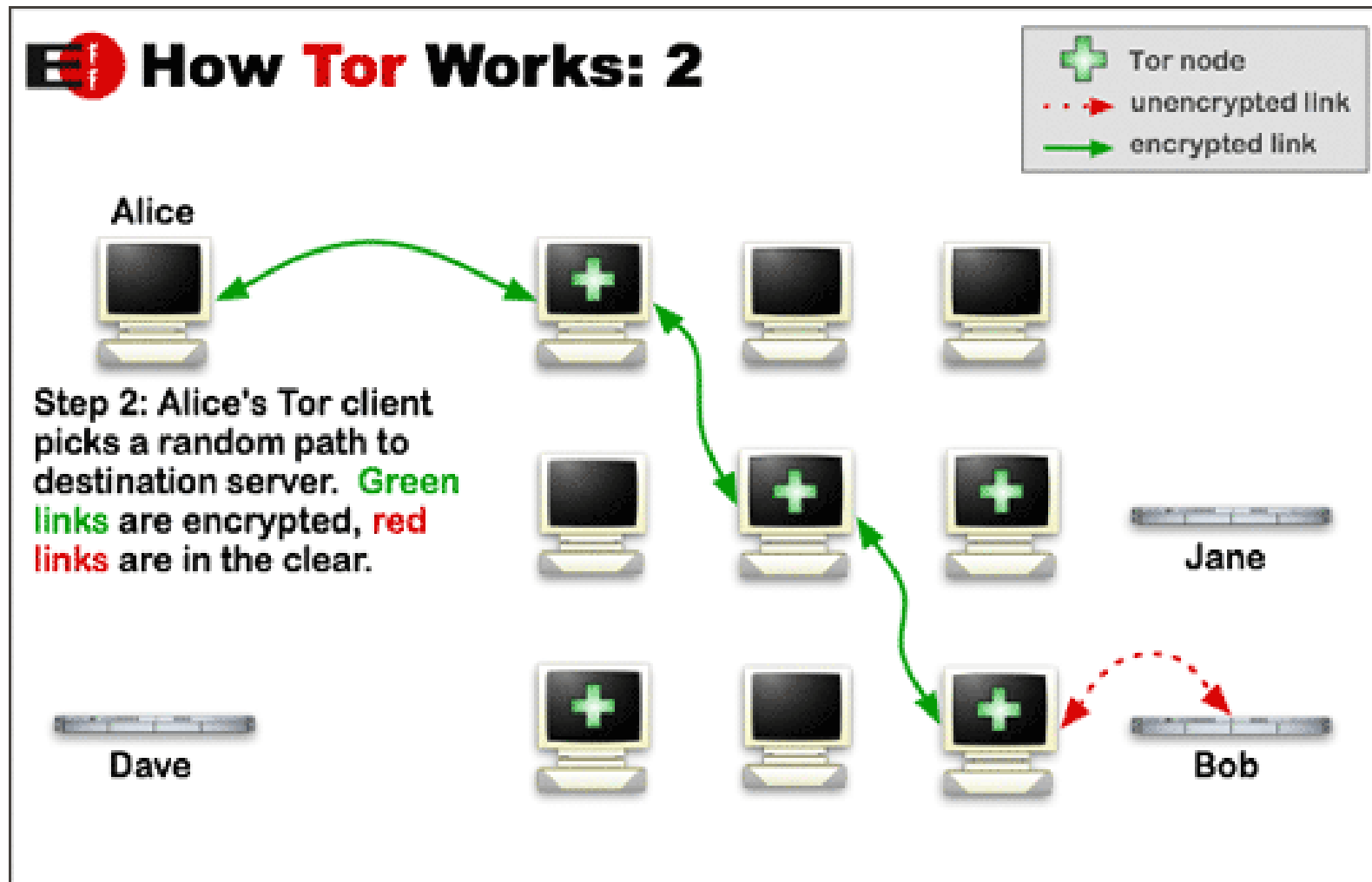
 **Download Tor** 

- ➔ Tor prevents anyone from learning your location or browsing habits.
- ➔ Tor is for web browsers, instant messaging clients, remote logins, and more.
- ➔ Tor is free and open source for Windows, Mac, Linux/Unix, and Android

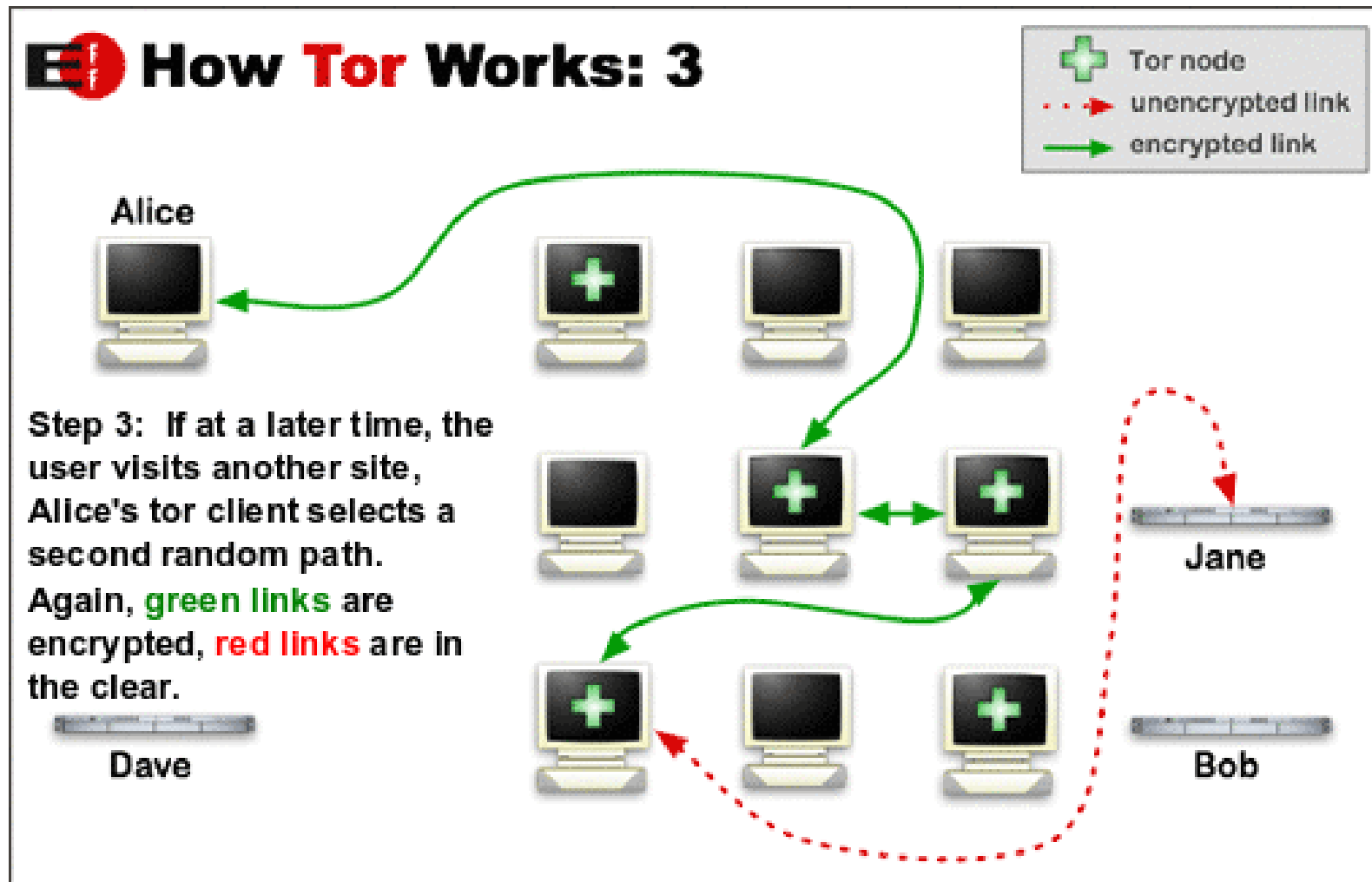
<https://www.torproject.org/>



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



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



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



Lad være med at bruge een computer til alt

Forskellige computere til forskellige formål, webserver vs mailserver

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering, evt. TOR

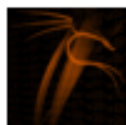
Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- <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



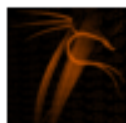
Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me



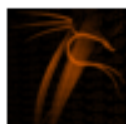
exploitdb [webapps] – BPAffiliate Affiliate Tracking
Authentication Bypass Vulnerability: <http://bit.ly/9LOC3K>

about 5 hours ago via twitterfeed



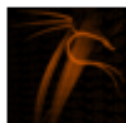
exploitdb [webapps] – BPDIRECTORY Business Directory
Authentication Bypass Vulnerability: <http://bit.ly/c4TeLz>

about 5 hours ago via twitterfeed



exploitdb [webapps] – BPConferenceReporting Web Reporting
Authentication Bypass Vulnerability: <http://bit.ly/cM61AK>

about 5 hours ago via twitterfeed



exploitdb [webapps] – BPRealEstate Real Estate
Authentication Bypass Vulnerability: <http://bit.ly/bYx2aY>

about 5 hours ago via twitterfeed

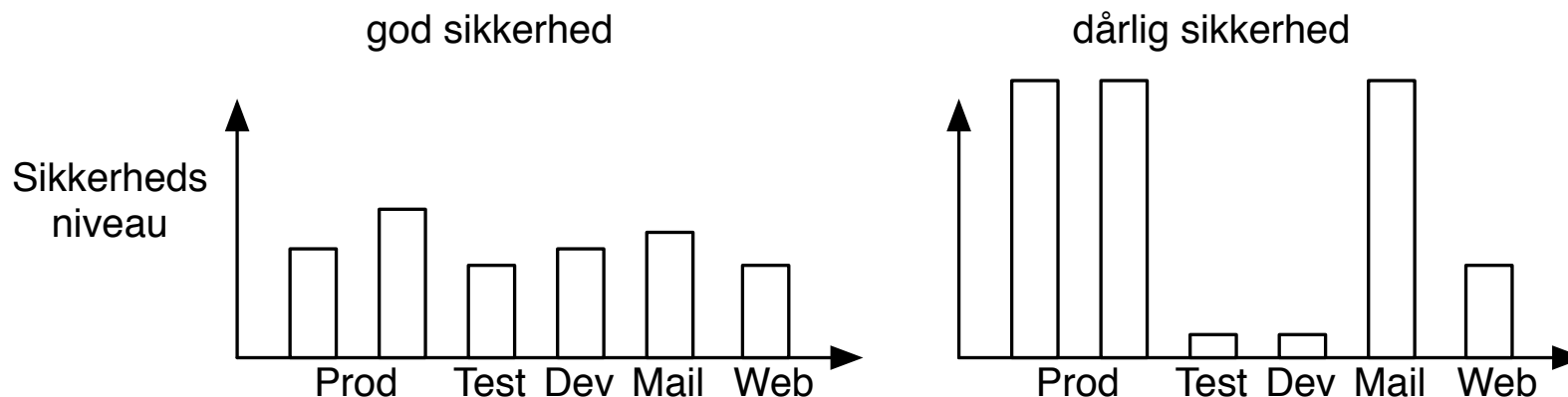


sans_isc [Diary] Mac OS X Server v10.6.5 (10H575) Security
Update: <http://support.apple.com/kb/HT4452>, (Tue, Nov
16th): <http://bit.ly/azBrso>

about 7 hours ago via twitterfeed

Exploits og nye sårbarheder

- 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.



Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vælger ikke med vilje den sværeste vej ind

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>

versionN



IT-NYHEDER

BLOGS

IT-JOB

IT-FIRMAER

WHITEPAPERS

EMNER *Hacking, It-sikkerhed*

 [Se kommentarer \(7\)](#)

Hackerkursus satte Dong på sporet af sårbare servere

En uges kursus i at tænke som en hacker gav flere aha-oplevelser for sikkerhedskonsulent hos Dong Energy. For eksempel fandt han efterfølgende server-software, der kørte med standard-password.

Af Jesper Kildebogaard Mandag, 19. marts 2012 - 6:59

Det kræver kun én lille sprække i forsvarsværkerne, før en hacker kan snige sig ind. Men hvordan opdager man som sikkerhedsansvarlig sprækken før hackeren?

Hos energikoncernen Dong Energy har et af svarene været at lære at tænke som hackerne. Og det gør det muligt at se på systemerne med helt andre øjne, fortæller en af de Dong-folk, der har været på hackerkursus.

»Kurset var et wakeup-call om, hvor nemt det er for hackere, som går systematisk til værks, og som ved, hvad de gør,« siger Keld Hjortskov, der er sikkerhedskonsulent hos Dong.



LIFE IS FOR SHARING.

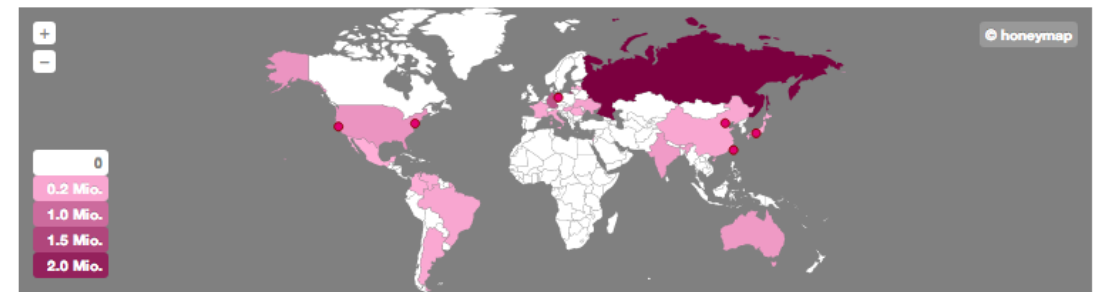
OVERVIEWINFOIMPRINT



Allianz für Cyber-Sicherheit

EnglishGerman

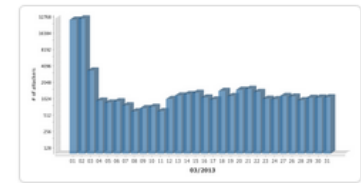
Overview of current cyber attacks (logged by 97 Sensors)



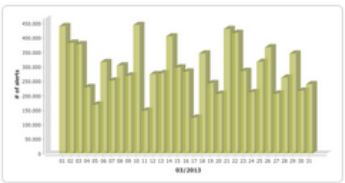
Live-Ticker

Date	Source	Attack on	Parameter
2013-04-09 09:29:38	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	USA	Web site	/administra%20%3Cbr%20/%3E/&sa=U&a
2013-04-09 09:29:40	China	Console/Shell	Kippo.SSH_Connect.Fail
2013-04-09 09:29:20	unbekannt		Kippo.SSH_Connect.Fail

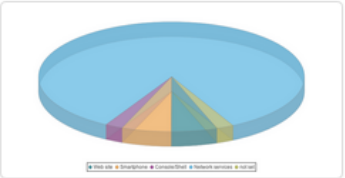
Overall sum of attackers per Day (Last Month)



Overall sum of attacks per Day (Last Month)



Distribution of Attack Targets (Last Month)



Top 15 of Source Countries (Last month)

Source of Attack	Number of Attacks
Russian Federation	2,446,168
Germany	1,308,617
Taiwan, Province of China	536,034
United States	449,853
Australia	378,792
India	358,114
Ukraine	250,213
Hungary	237,607
Brazil	218,265
China	197,152
Italy	194,102
France	184,073
Argentina	182,166
Japan	151,861
Venezuela, Bolivarian Republic of	127,862

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

<http://www.sicherheitstacho.eu/?lang=en>

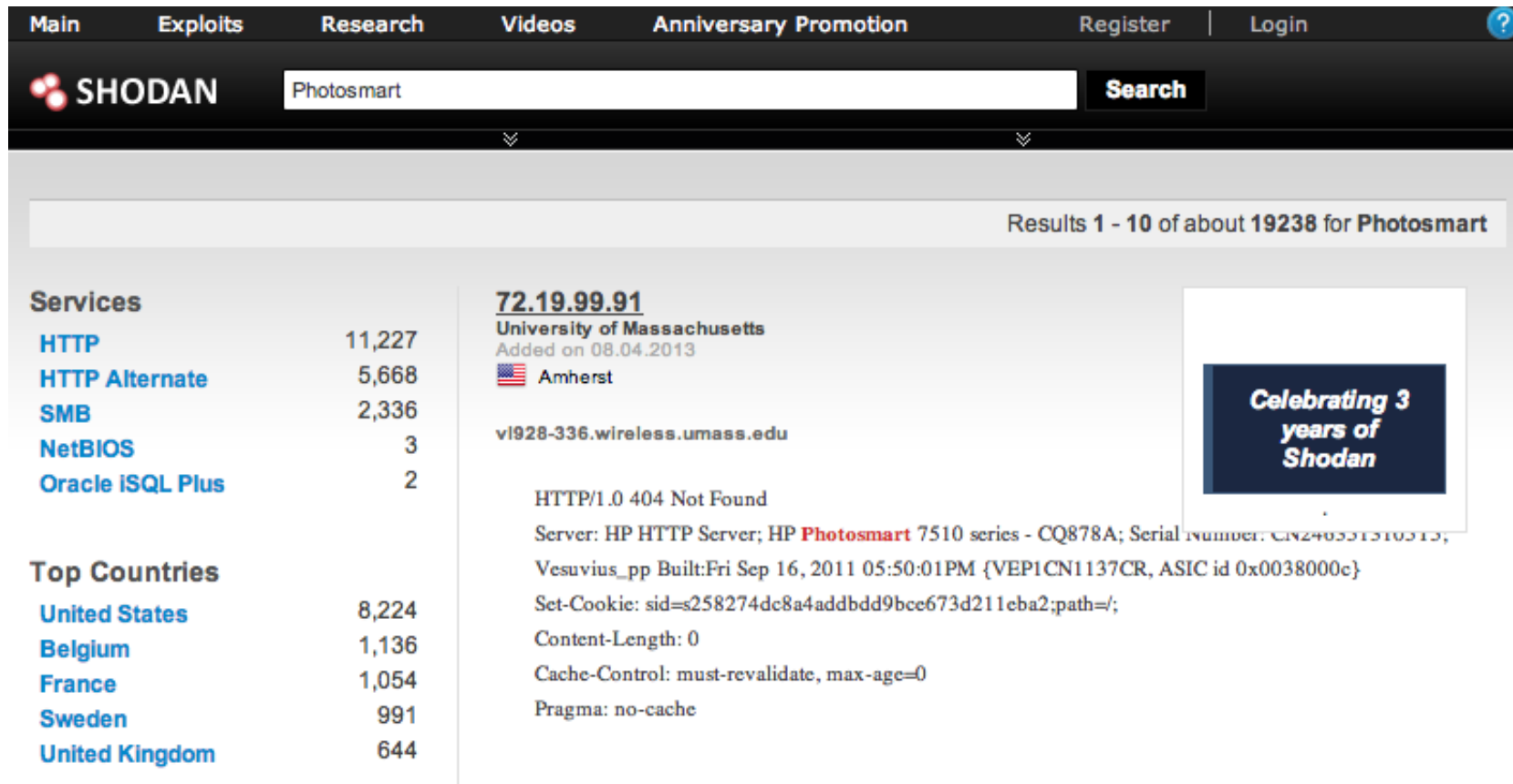
Internet Census 2012 Port scanning /0 using insecure embedded devices

Abstract While playing around with the Nmap Scripting Engine (NSE) we discovered an amazing number of open embedded devices on the Internet. Many of them are based on Linux and allow login to standard BusyBox with empty or default credentials. We used these devices to build a distributed port scanner to scan all IPv4 addresses. These scans include service probes for the most common ports, ICMP ping, reverse DNS and SYN scans. We analyzed some of the data to get an estimation of the IP address usage.

Additionally, with one hundred thousand devices scanning at ten probes per second we would have a distributed port scanner to port scan the entire IPv4 Internet within one hour.

Source: <http://internetcensus2012.bitbucket.org/paper.html>

http://www.theregister.co.uk/2013/03/19/carna_botnet_ipv4_internet_map/



The screenshot shows the Shodan search interface. At the top, there's a navigation bar with links: Main, Exploits, Research, Videos, Anniversary Promotion, Register, and Login. Below this is the Shodan logo and a search bar containing 'Photosmart' with a 'Search' button. The results section shows 'Results 1 - 10 of about 19238 for Photosmart'. On the left, there are two sidebars: 'Services' and 'Top Countries'. The 'Services' sidebar lists HTTP (11,227), HTTP Alternate (5,668), SMB (2,336), NetBIOS (3), and Oracle ISQL Plus (2). The 'Top Countries' sidebar lists United States (8,224), Belgium (1,136), France (1,054), Sweden (991), and United Kingdom (644). The main content area displays the first result for IP 72.19.99.91, identified as the University of Massachusetts Amherst, added on 08.04.2013. It shows the URL vi928-336.wireless.umass.edu and the HTTP response: HTTP/1.0 404 Not Found. The response headers include Server: HP HTTP Server; HP Photosmart 7510 series - CQ878A; Serial number: CN248531310313; Vesuvius_pp Built: Fri Sep 16, 2011 05:50:01PM {VEP1CN1137CR, ASIC id 0x0038000c}; Set-Cookie: sid=s258274dc8a4addbdd9bce673d211eba2;path=/; Content-Length: 0; Cache-Control: must-revalidate, max-age=0; and Pragma: no-cache. A small banner on the right says 'Celebrating 3 years of Shodan'.

Services	Count
HTTP	11,227
HTTP Alternate	5,668
SMB	2,336
NetBIOS	3
Oracle ISQL Plus	2

Top Countries	Count
United States	8,224
Belgium	1,136
France	1,054
Sweden	991
United Kingdom	644

72.19.99.91
University of Massachusetts
Added on 08.04.2013
Amherst
vi928-336.wireless.umass.edu

HTTP/1.0 404 Not Found
Server: HP HTTP Server; HP **Photosmart** 7510 series - CQ878A; Serial number: CN248531310313; Vesuvius_pp Built: Fri Sep 16, 2011 05:50:01PM {VEP1CN1137CR, ASIC id 0x0038000c}; Set-Cookie: sid=s258274dc8a4addbdd9bce673d211eba2;path=/; Content-Length: 0; Cache-Control: must-revalidate, max-age=0; Pragma: no-cache

`http://www.shodanhq.com/search?q=Photosmart`

Title: Cisco's new password hashing scheme easily cracked

Description: In an astonishing decision that has left cryptographic 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>

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)



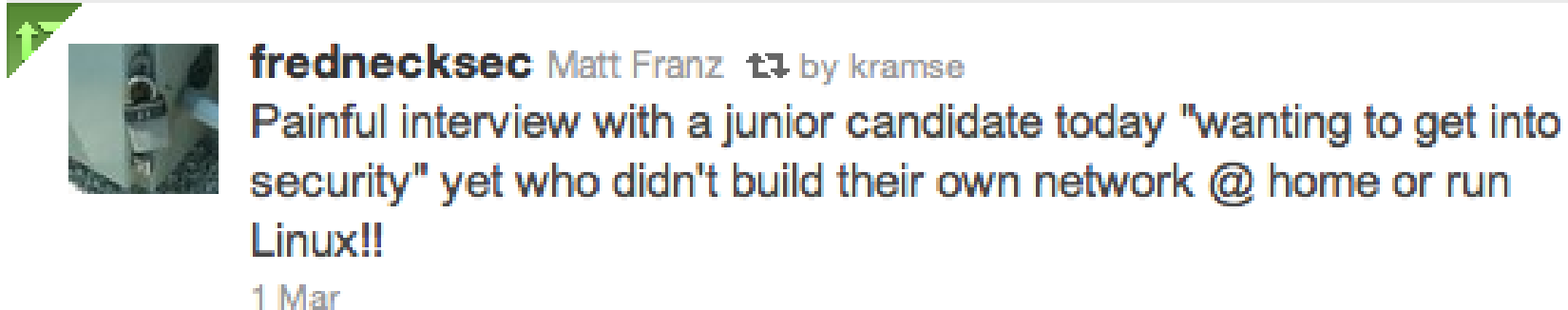
KALI LINUX
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,
REDEFINED.**

A Project By Offensive Security

BackTrack <http://www.backtrack-linux.org>

Kali <http://www.kali.org/>



Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug BackTrack, se evt. youtube videoer om programmerne

Quote fra Jurassic Park <http://www.youtube.com/watch?v=dFU1AQZB9Ng>

- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Aircrack-ng <http://www.aircrack-ng.org/>
- Wireshark netværkssniffer - <http://http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- Skipfish <http://code.google.com/p/skipfish/>

Generelt findes der hackerværktøjer indenfor alle nicheområder!

Listen over de mest anvendte hacker tools <http://sectools.org/>

What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

<http://www.metasploit.com/>

Armitage GUI fast and easy hacking for Metasploit

<http://www.fastandeasyhacking.com/>

Kursus Metasploit Unleashed

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

Bog: Metasploit: The Penetration Tester's Guide, No Starch Press

ISBN-10: 159327288X

hackertools, step by step instruktioner, Kali Linux demo osv.



`securityonion.blogspot.dk`



The Bro Network Security Monitor

Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

While focusing on network security monitoring, Bro provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Bro has successfully bridged the traditional gap between academia and operations since its inception.

<http://www.bro.org/>

The key point that helped me understand was the explanation that Bro is a domain-specific language for networking applications and that Bro-IDS (<http://bro-ids.org/>) is an application written with Bro.

Why I think you should try Bro

<https://isc.sans.edu/diary.html?storyid=15259>

```
global dns_A_reply_count=0;
global dns_AAAA_reply_count=0;
...
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_A_reply_count;
}

event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_AAAA_reply_count;
}
```

source: dns-fire-count.bro from

<https://github.com/LiamRandall/bro-scripts/tree/master/fire-script>



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Billede: Michael Conrad <http://www.hillstreetblues.tv/>

