

Welcome to

Introduktion til IT-sikkerhed idag

December 2014

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

Slides are available as PDF, kramshoej@Github

Goals of today

Update on trends in information security and internet security

Offer input to what things to look into

I will try to limit myself to things from 2014

Hodge-podge of security related things - inspiration

Please give feedback and join me in discussions, dialogue 😊




KI 09:30-11:00

Less presentation, more talk

Less me talking (only) and more 2.0 social media interaction

par·a·noi·a

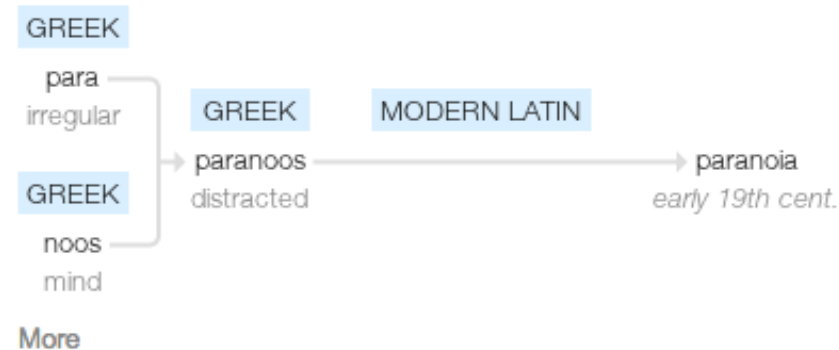
/ˌparəˈnoɪə/ 

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



Source: google paranoia definition

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
- Hackers break in and steal information
- 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!

What is data?



Personal data you dont want to loose:

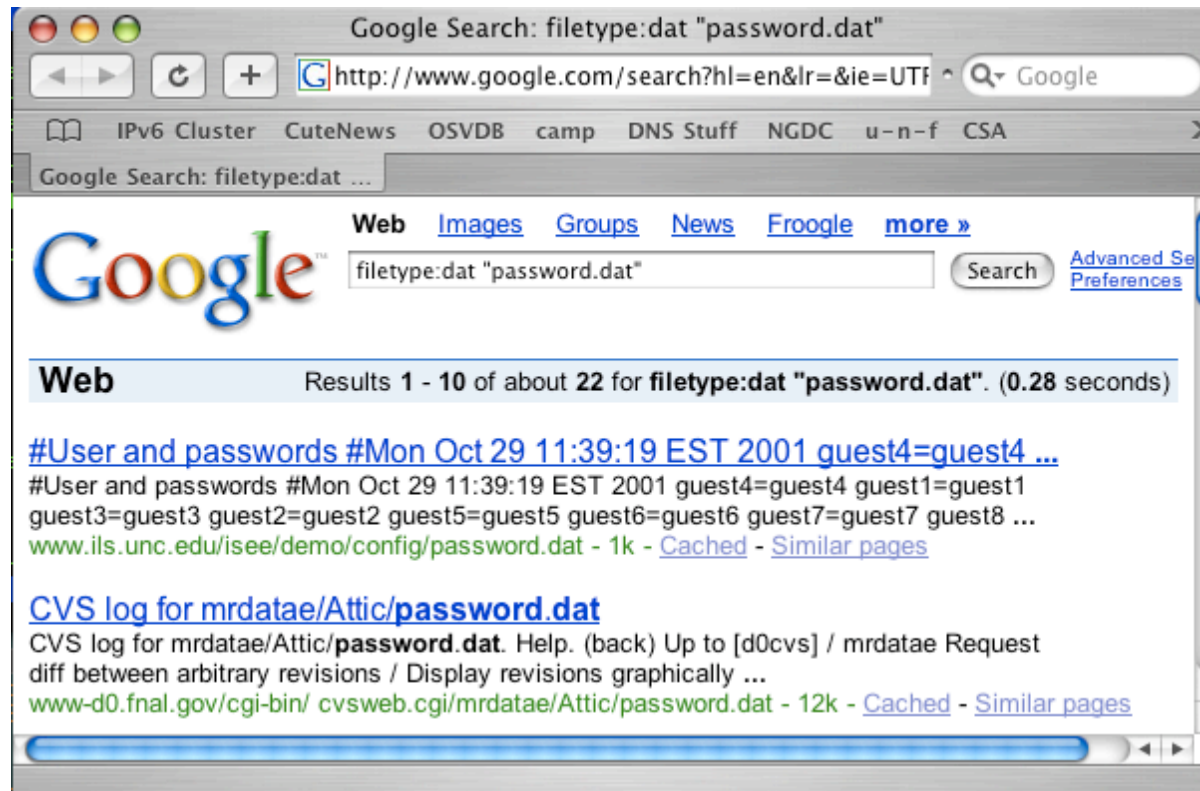
- Wedding pictures
- Pictures of your children
- Sextapes
- Personal finances

Source: picture of my son less than 24 hours old - precious!




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?




Google as a hacker tools?

Concept named googledorks when google indexes information not supposed to be public <http://www.hackersforcharity.org/ghdb/>



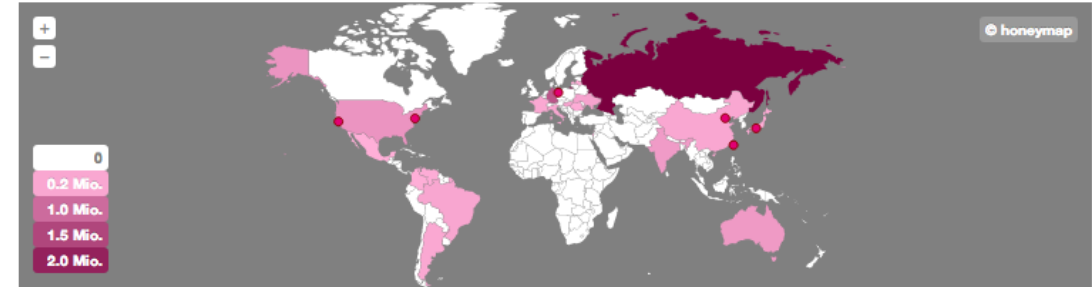
LIFE IS FOR SHARING.

OVERVIEWINFOIMPRINT



EnglishGerman

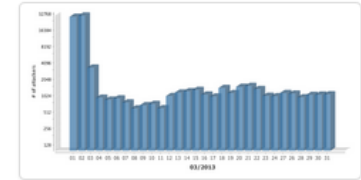
Overview of current cyber attacks (logged by 97 Sensors)



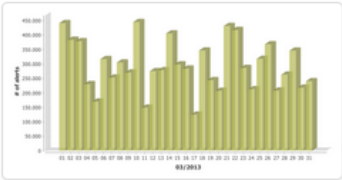
Live-Ticker

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

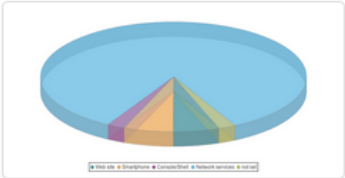
Overall sum of attackers per Day (Last Month)



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>

nearly 40GB of data hacked and leaked from Sony Pictures Entertainment's (SPE) internal computer systems.

Passwords - complete infrastructure and all passwords must be reset

Payroll information, financial information about products and earnings

Information about planned products and strategy is out

Bad passwords allow access to critical assets

Leaked unreleased titles Annie, Mr. Turner, Still Alice, and To Write Love On Her Arms, as well as World War II drama Fury.

Source:

<http://techcrunch.com/2014/11/30/five-sony-pictures-movie-screener/>

<http://mashable.com/2014/12/04/sony-hack-data-details/>

Movie:



Just search for: kryptonite lock bic pen

<https://www.youtube.com/watch?v=LahDQ2ZQ3e0>

The Heartbleed Bug

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

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



Source: <http://heartbleed.com/>

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

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

Malware is advanced and sophisticated

Modular frameworks

Use strong cryptography to hide

Use 0-day exploits - unknown to others

Use rootkits to stay under radar and avoid anti-virus

Mutate and change to avoid detection

In general less noisy



**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 act like software houses

”Buy this version with updates and support”

Rent a bot net with 100.000 computers

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 kan brugere

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*

TwoFactor authentication: Example Duosecurity



Push Notification

Quickly view login or transaction details and tap "Approve" on your iOS or Android device.

Learn more at duosecurity.com/duo-push



Smartphone Passcodes

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



Text Message

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

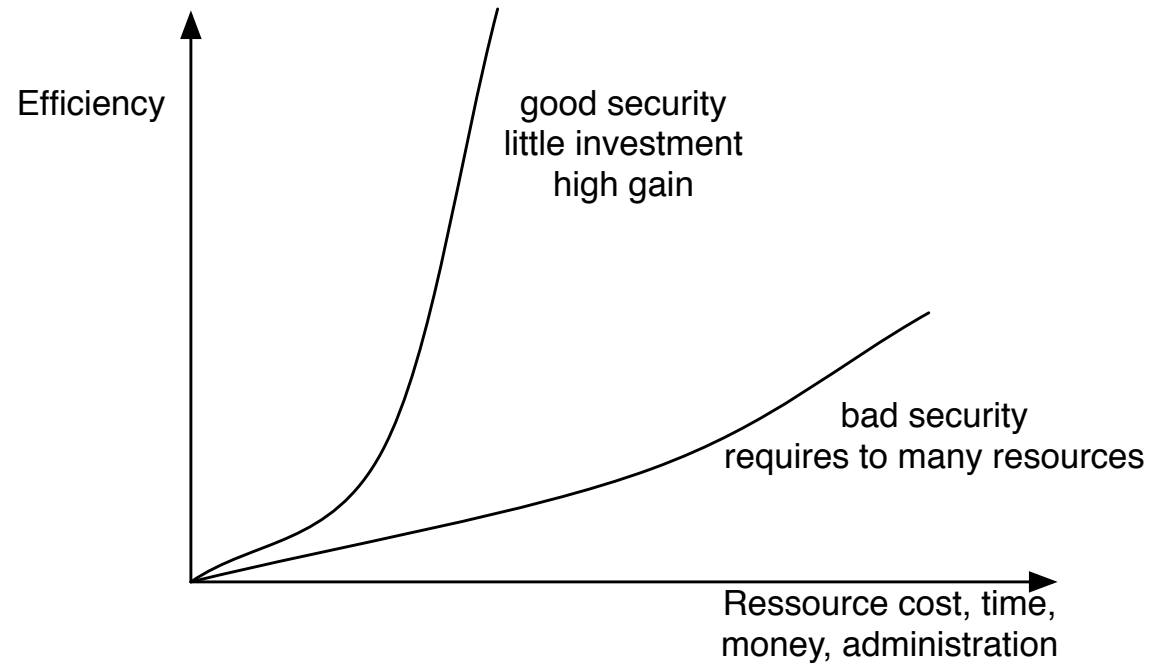


Phone Call

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

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

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



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

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: **IMAPS**, **POP3S**, **HTTPS** 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

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

Many people can easily be distracted around crowds

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

... making theft likely/easy

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

Industrial espionage, economic espionage or corporate espionage is real

Security breaches happens any day of the week

Kom igang!

- Write a backup to DVD - most laptops today can do that
- Save stuff in the cloud, examples Dropbox, Google Drive
- Save data to external harddrive, cheap today

Sad story Mat Honan epic hacking :-)

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

Recommendations

- Lock your devices, phones, tables and computers
- Update software and apps
- Do NOT use the same password everywhere
- Watch out when using open wifi-networks
- Multiple browsers: one for Facebook, and separate for home banking apps?
- Multiple laptops? One for private data, one for work?
- Think of the data you produce, why do people take naked pictures and SnapChat them?
- Use pseudonyms and aliases, do not use your real name everywhere
- Enable encryption: IMAPS, POP3S, HTTPS





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



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`



Orbot:
Proxy With Tor



Orweb:
Private Web Browser



ChatSecure:
Private and Secure Messaging



ObscuraCam:
The Privacy Camera



Ostel:
Encrypted Phone Calls



CSipSimple:
Encrypted Voice Over IP (VOIP)



K-9 and APG:
Encrypted E-mail



KeySync:
Syncing Trusted Identities

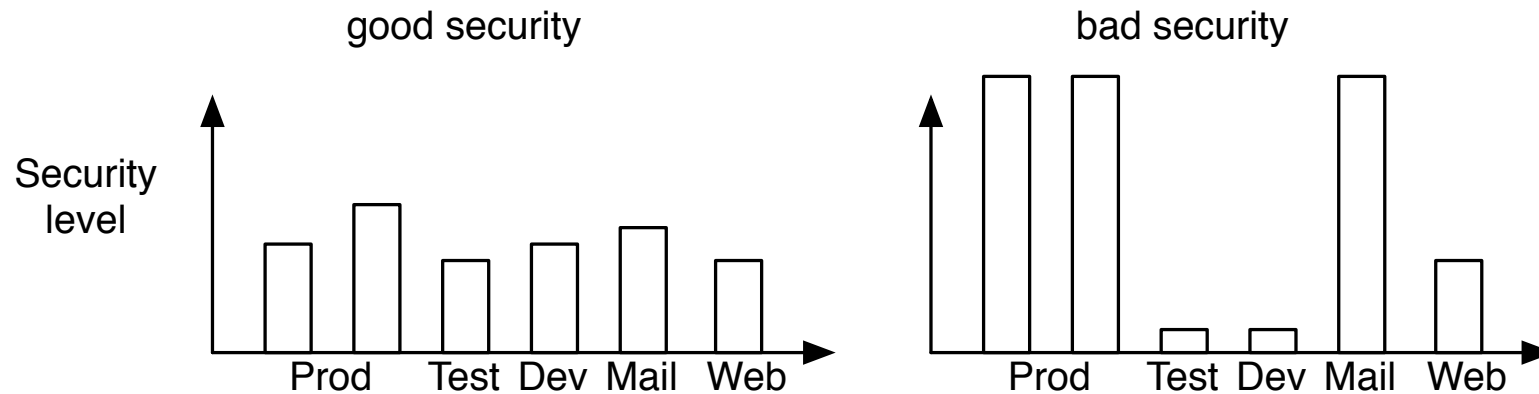


TextSecure:
Short Messaging Service (SMS)



Pixelknot:
Hidden Messages

Dont forget your mobile platforms <https://guardianproject.info/>



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



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

Walk through your infrastructure
get a detailed view of data, flows, protocols, bandwidth, ports and services

Make sure your organization is also in control, know your vendors

Create a list of critical phone numbers and contacts, enter it in your phone

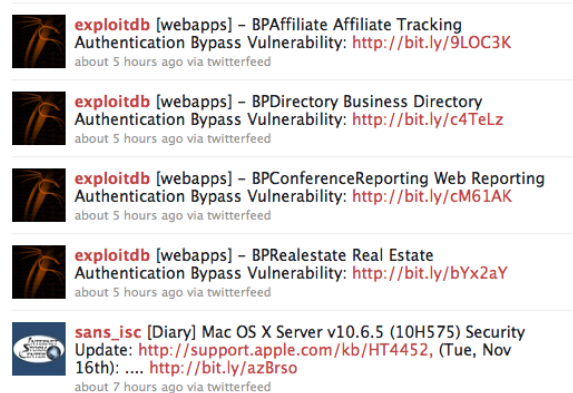
Get control of BYOD Bring Your Own Devices



Tips, Tools and How-tos For Safer Online Communications

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

Source: <https://ssd.eff.org/>



Twitter has replaced RSS for me

Email lists are still a good source of data

Favourite Security Diary from Internet Storm Center

<http://isc.sans.edu/index.html>

<https://isc.sans.edu/diaryarchive.html?year=2013&month=4>

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

You are always welcome to send me questions later via email