sicherheitskultur.at

THE SORRY STATE OF INFORMATION SECURITY

Philipp Schaumann

http://sicherheitskultur.at/

philippschaumann@hotmail.com

Disclaimer:
- The following positions are purely personal
- The details do NOT reflect in any way the products or solutions from employer

sicherheitskultur.at

Agenda

The State of Information Security

What could be done?

What should be done?

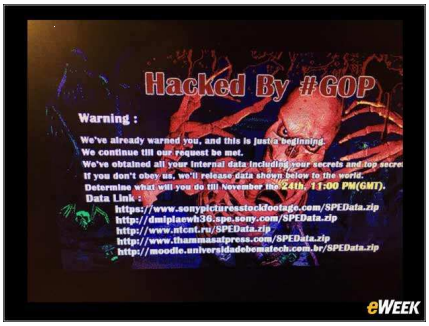
It seems to be a Never-Ending Story ☹

Lot‘s of Trouble and no End in Sight

2014 – Year of Mega-Vulnerabilities and Leaks

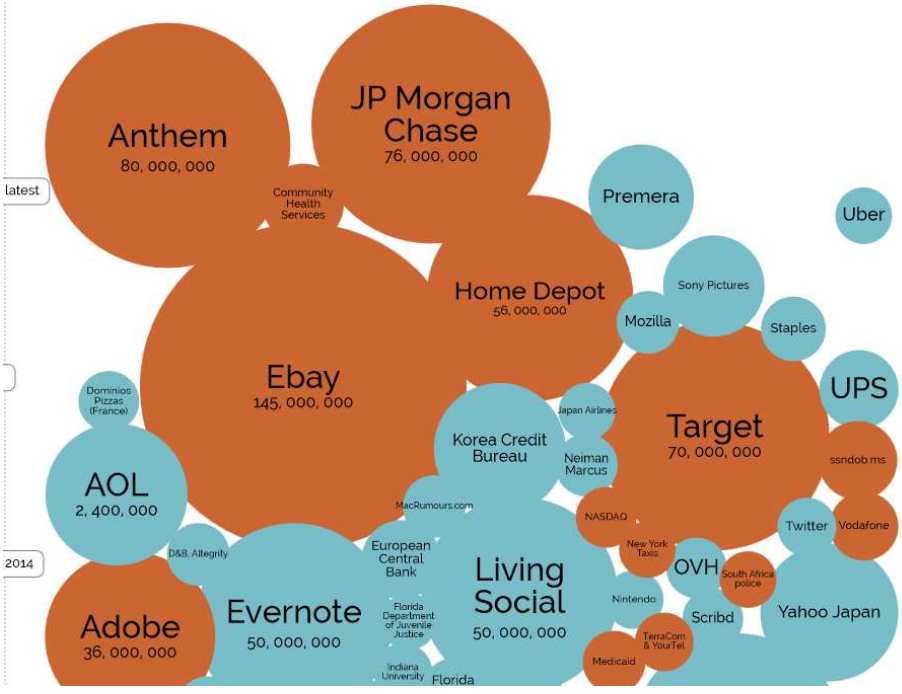
Heartbleed
(SSL-Vulnerability)

Poodle
(man-in-the-middle downgrade exploit)



Sony

2014, 2015 Data Leaks

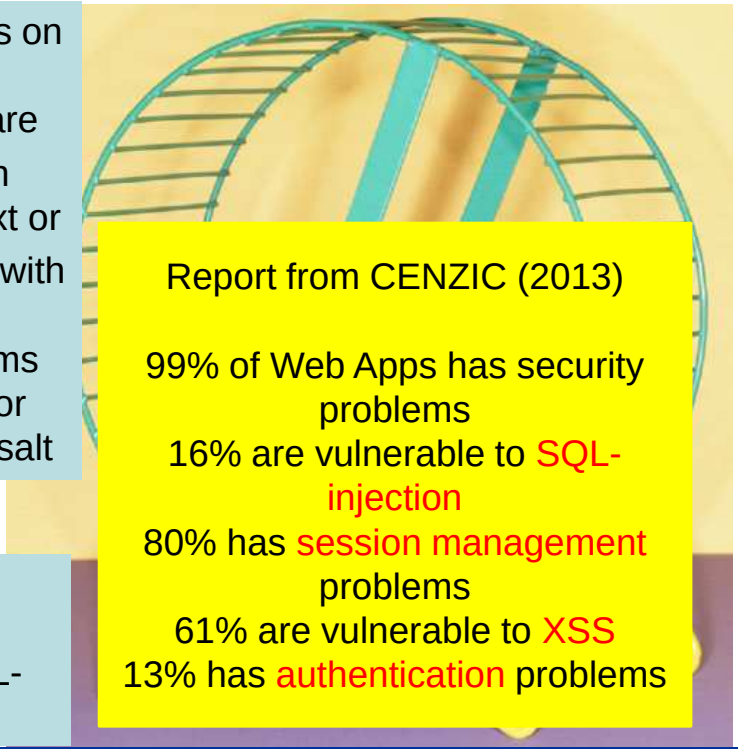


http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

We know how to implement Secure Systems, but . . .

Passwords on corporate websites are

- stored in clear text or
- hashed with broken algorithms (MD-5) or without salt



Report from CENZIC (2013)

99% of Web Apps has security problems
16% are vulnerable to SQL-injection
80% has session management problems
61% are vulnerable to XSS
13% has authentication problems

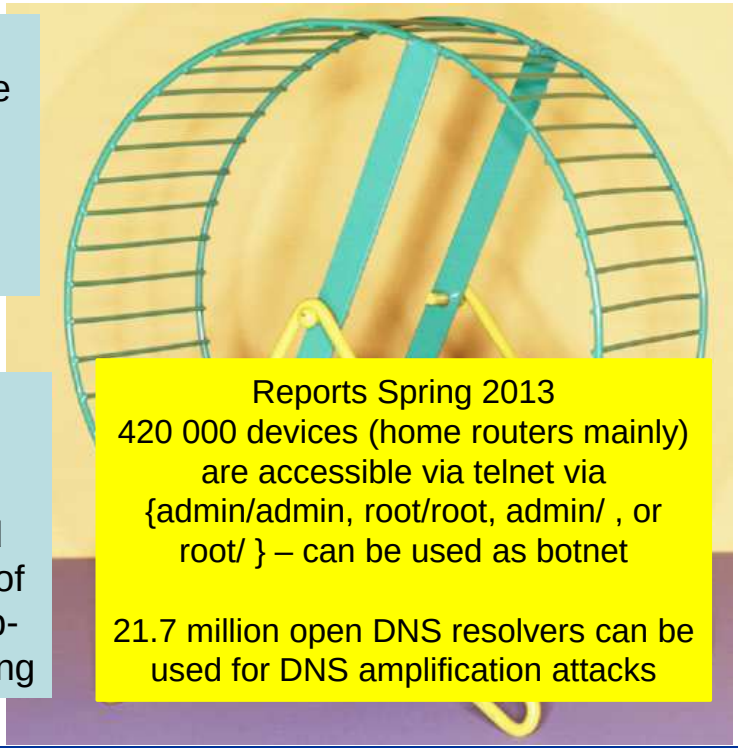
Sensitive data is still sent via HTTP

Smartphone apps with HTTPS still allow man-in-the-middle attacks (40%)

Plenty of Websites allow SQL-injection

We are preaching to IT-Departments, but . . .

Web servers are using insecure software versions



Reports Spring 2013
420 000 devices (home routers mainly) are accessible via telnet via {admin/admin, root/root, admin/ , or root/ } – can be used as botnet

21.7 million open DNS resolvers can be used for DNS amplification attacks

Programming languages still allow

- buffer-overflow,
- type-mismatch,
- data executed as code, . . .

Web developers don't understand the basics of secure web-programming

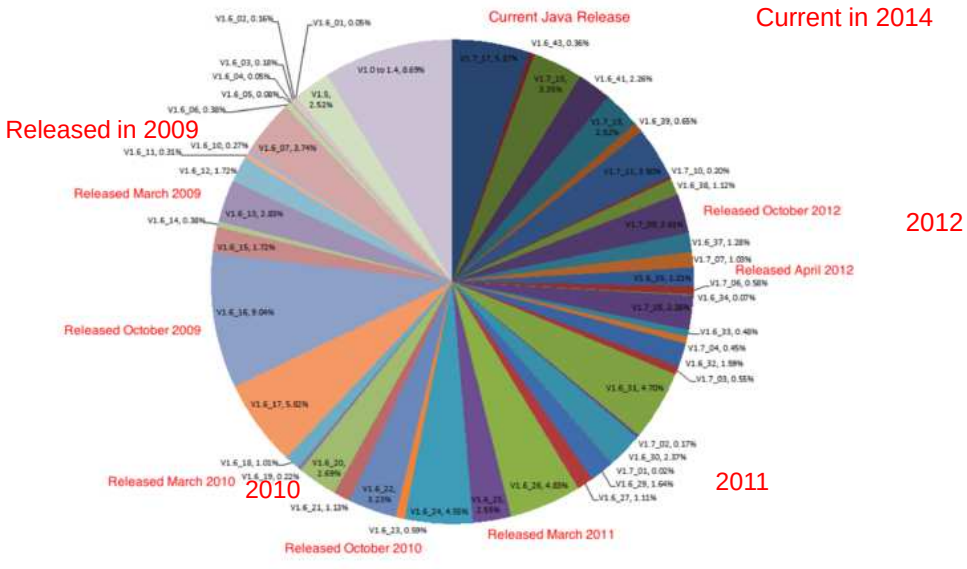
The internet does not seem to be defendable

The Quick Solution. . .

Let‘s put more effort on Security Awareness!

Let‘s educate end-users, developers, managers, CEOs, …..

Browsers with Java vulnerabilities – 2014 state



http://sicherheitskultur.at/

93% percent of the browser are vulnerable to Java Exploits

3 Billion Devices Run Java

Software needs to be patched, but . . .

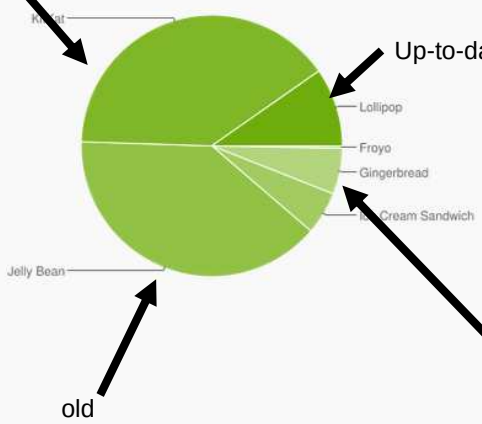
Nearly half of all Android devices are still vulnerable to two serious browser exploits

Lucian Constantin Oct 8, 2014 8:48 AM

Somewhat outdated

Version	Codename	API	Distribution
2.2	Froyo	8	0.3%
2.3.3 - 2.3.7	Gingerbread	10	5.7%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	5.3%
4.1.x	Jelly Bean	16	15.6%
4.2.x		17	18.1%
4.3		18	5.5%
4.4	KitKat	19	39.8%
5.0	Lollipop	21	9.0%
5.1		22	0.7%

Data collected during a 7-day period ending on May 4, 2015.
Any versions with less than 0.1% distribution are not shown.



Up-to-date

Very old

old

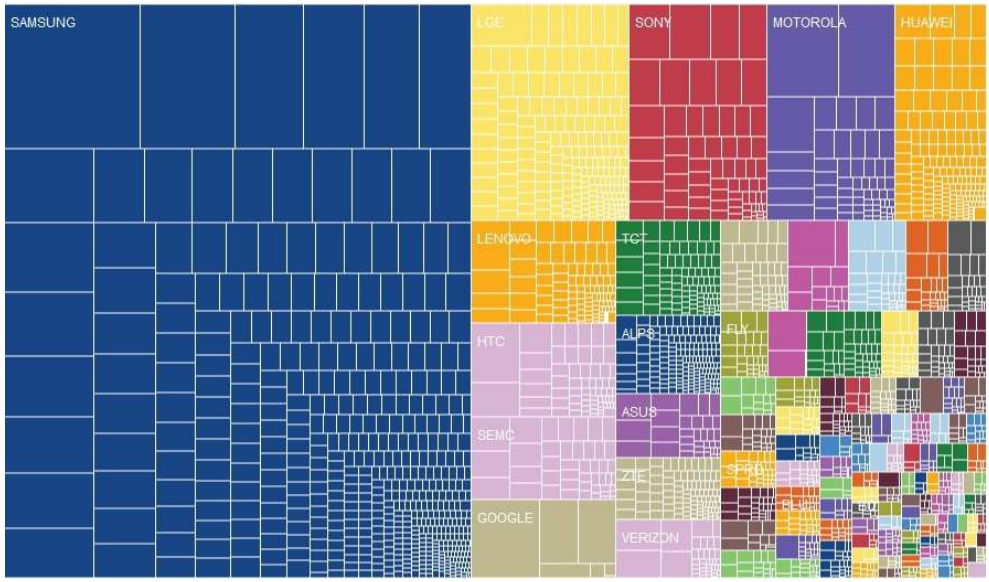
End-users fail to keep their **software up-to-date**

Often, they can't !

https://developer.android.com/about/dashboards/index.html

http://www.pcworld.com/article/2823012/almost-half-of-android-devices-still-have-a-vulnerable-browser-installed.html

With 19 000 Android Variants in 2014 Patch Management becomes fun ;-)



Smartphones

Strength

- The concept of Sandboxes promises to isolate the processes of the apps – a very important security feature Result is higher security than MS Windows und MacOS
- Trend towards hardware-based memory encryption

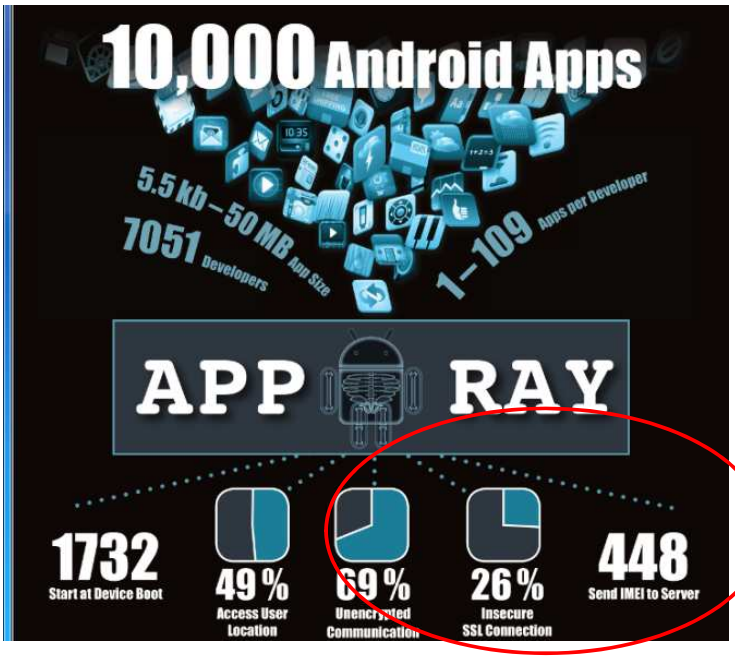
Fraunhofer March 2011:
http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt54/forum-mobileit-heider.pdf

My Claim:
Smartphones, conceptually are more secure than current Computer

And along comes cloud and fun with games

- All Smartphones are cloud-based
- The number of secure Cloud-Solutions is close to Zero
- „User Experience“ always beats Security

App-Developer are as lousy as Web-Developer



Apple iOS:

22% not encrypted

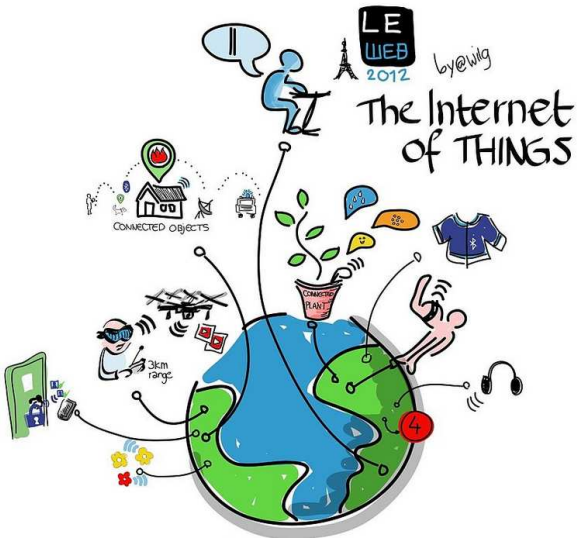
14% use TLS/SSL, but incorrectly

http://www.heise.de/newsticker/meldung/SSL-Verschluesselung-auch-in-iOS-Apps-problematisch-2138829.html

Android:

see left side

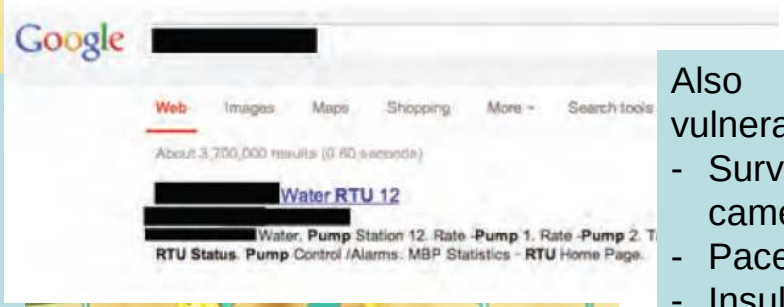
First, only computers were at risks, now . . .



First, only computers were at risks, now . . .

sicherheitskultur.at

Vulnerabilities in ICS and SCADA systems put the safety of water and electricity supply at risk



Vulnerable SCADA systems can be found on the Internet via Google or Nessus or many

Also vulnerable:
- Surveyance cameras
- Pace maker
- Insulin pumps
- Cars
- . . . .

Resilence

A System is resilient if there are diversity and redundancy.

Each form of centralization makes a system vulnerable.

Myriam Dunn Cavelty – ETH Zürich

Growing Monopolies (1)

- In the 60s and 70s there were 8 – 10 big system houses, today we have
  - Microsoft
  - Apple
  - Google
  - Linux (See →Heartbleed)
- 2 Smartphone operating systems
- Gemalto for 50% of all SIM-cards

Growing Monopolies (2)

- 5 – 6 big (US-)Cloud Infrastructures
- Facebook + 5 other Social Networks
- Amazon, Alibaba, eBay share most of the trading market
- Google dominates the search engines

Bring your Own Device

- **Customers** expect to do their internetbanking on the underground using the smartphone
- **Staff m** en brand of mobile, cts

Company IT replaced by Shadow IT

Kübler-Ross Modell - Five Stages of Grief
http://en.wikipedia.org/wiki/K%C3%BCbler-Ross_model

The Problem should have been solved long ago

5 Decades Ago

Programming Languages that

- Support strong typing
- can automatically diagnose many programming bugs
- Can prevent buffer overflows

The Problem should have been solved long ago

3 Decades Ago

we can transmit and store data securely based on **cryptography**

we know how to securely separate data and code

The Problem should have been solved long ago

2 Decades Ago

we have threat assessment methodologies that have been proven to improve the security of an IT-system

http://sicherheitskultur.at/

States have created a „Hacker-Market“

Many law enforcement organisations and secret services (not only the NSA) have created
a big and very lucrative and (nearly) legal market for Vulnerabilities/ Zero Days and Botnets

Breaches maybe cheaper than implementing security

- **Target:** 40 Mio credit cards, 70 Mio customer data
  $225 Mio cost of breach- minus $162 Mio insurance – minus tax deductions = $105 Mio = 0.1% of sales

- **Sony Pictures:** $35 Mio for investigation and remediation – for a movie that cost $44 Mio to make and that made $46 Mio in sales over Xmas

- **Home Depot:** 56 Mio credit cards + 53 Mio Email-addresses
  Net cost after security reimbursement: $28 Mio = 0.01% of sales

http://www.techrepublic.com/article/data-breaches-may-cost-less-than-the-security-to-prevent-them/

Wrong Incentives (1)

Vendors are “penalized” by the market

- If the prioritize security over time-to-market
- prioritize security over “features”
- prioritize security over convenience

Wrong Incentives (2)

Vendors run little risk because

- No Liability for “Bugs”
- Users can’t judge the Security State anyhow

Why can‘t software be as secure as a powerdrill is safe?

Powerdrills

- Have a requirement for VDE-tests tested for electrical safety (at least in so many countries, that the test makes sense) - 100,000 product tests a year for 5,000 customers around the world
- Are tested against a common safety standard
- Come with a VDE-Sticker that informs customers whether this device has been tested or not (transparent market)
- Come with a liability for product replacement if the products fails to perform it‘s intended functionality
- Come with a liability concerning damages caused by the malfunctioning machine

sicherheitskultur.at

Powerdrills

At a minimum we need a law like the requirements to have seat-belts in our cars!

What do we get instead of some minimum security requirements?

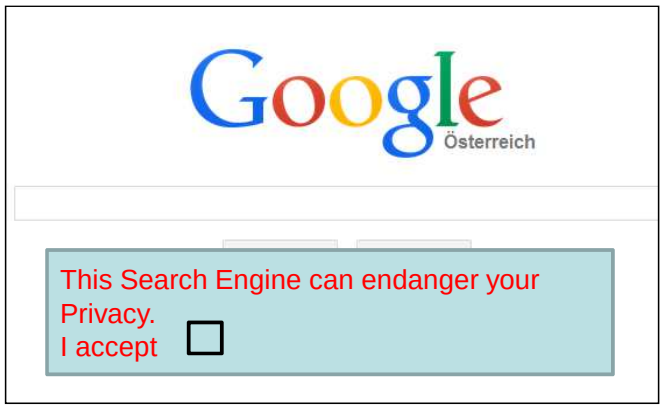
- Increasing surveyance requirements like data retention
- Lots of choices for hardware boxes to solve our problems – to cover up the holes that the programmers have left in our softwares, (some with additional security flaws)

How about this for IT?

Some examples

This App includes:

- Unsecure transfer of passwords
- Unauthorized usage of your contacts and GPS positions



Thanks