MuSe
Munich IT Security Research Group

Reality Check: Practical Limitations of Technical Privacy Protection

Hans-Joachim Hof

MuSe - **Mu**nich IT **Se**curity Research Group
Munich University of Applied Sciences

hof@hm.edu
http://muse.bayern

Prof. Dr.-Ing. Hans-Joachim Hof

University of Karlsruhe, Germany

Karlsruhe Institute of Technology (KIT)

- CS student, PhD student, lecturer

SAP Markets, Palo Alto, USA

- Software Developer

Siemens AG, Corporate Technology

- Research Center „IT Security“

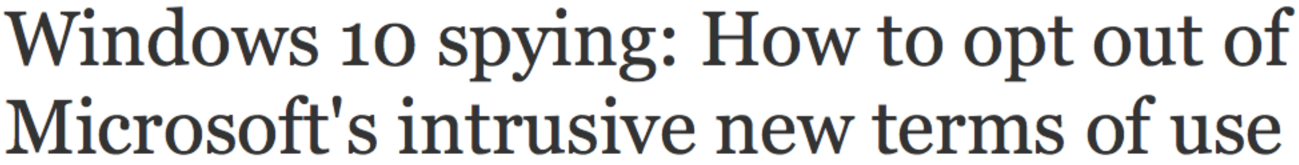
Munich University of Applied Sciences

- Full Professor
- Leader Munich IT Security Research Group
  - Network Security
  - Software Security

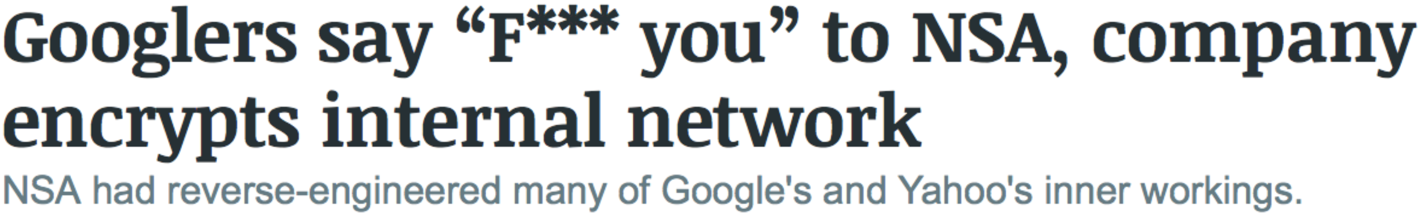
German Chapter of the ACM

- Vice Chair

Introduction

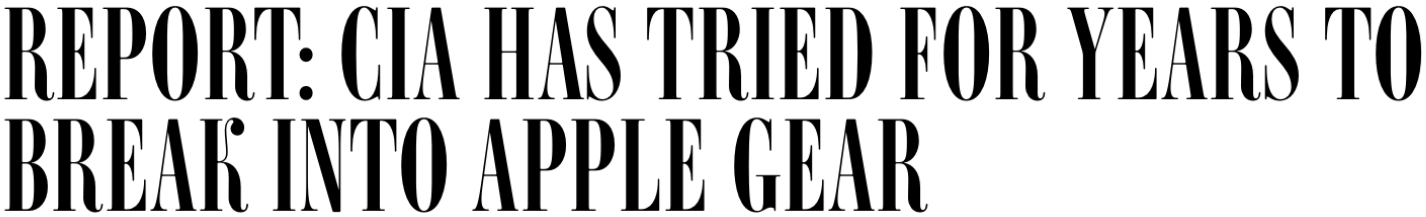


Windows 10 spying: How to opt out of Microsoft's intrusive new terms of use

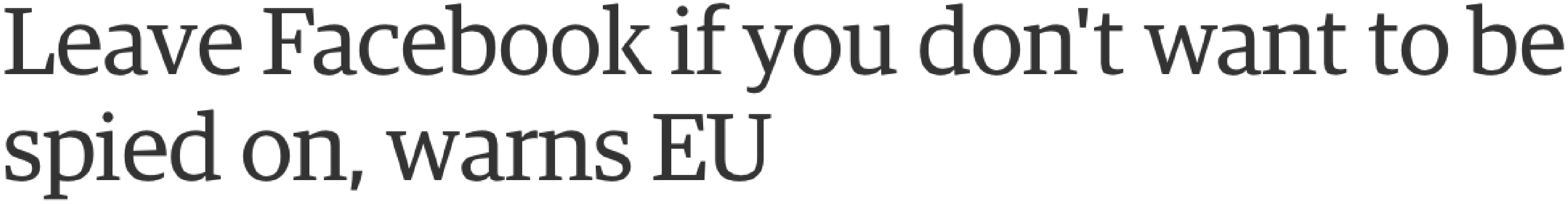


Googlers say “F*** you” to NSA, company encrypts internal network

NSA had reverse-engineered many of Google's and Yahoo's inner workings.



REPORT: CIA HAS TRIED FOR YEARS TO BREAK INTO APPLE GEAR



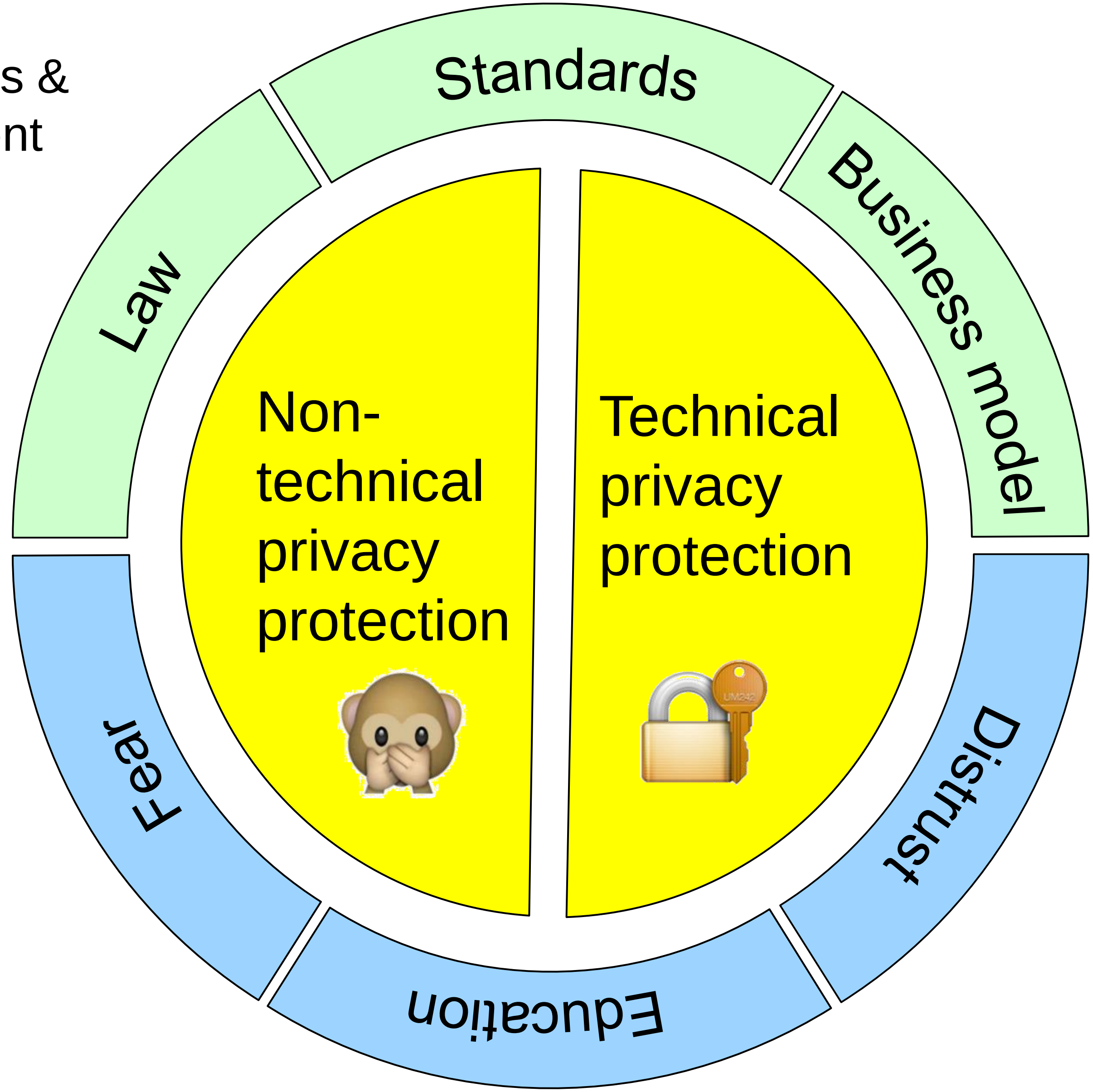
Leave Facebook if you don't want to be spied on, warns EU

Lax Privacy Today

- Businesses value personal data
- Businesses have strong lobby
- Governments tend to paranoia
- Study:
  - Users see growing need for privacy
  - However: they do not act privacy aware (e.g. more social network activities)

Drivers of Privacy Protection

Businesses & Government



Standards

Law

Business model

Non-technical privacy protection

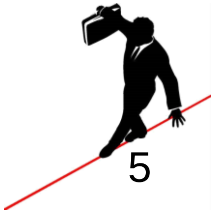
Technical privacy protection

Fear

Education

Distrust

Users



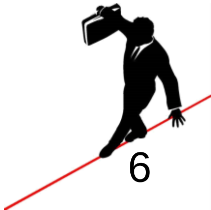
Privacy Protection

- Non-Technical
  - Data avoidance, data minimization, anonymization, special roles in companies (privacy officers)...
  - Often accompanied by technical privacy protection

- Technical
  - Uses IT security means
  - Encryption, authentication, …

- Technical privacy protection often presented as silver bullet, especially on user side

  ➔ True???

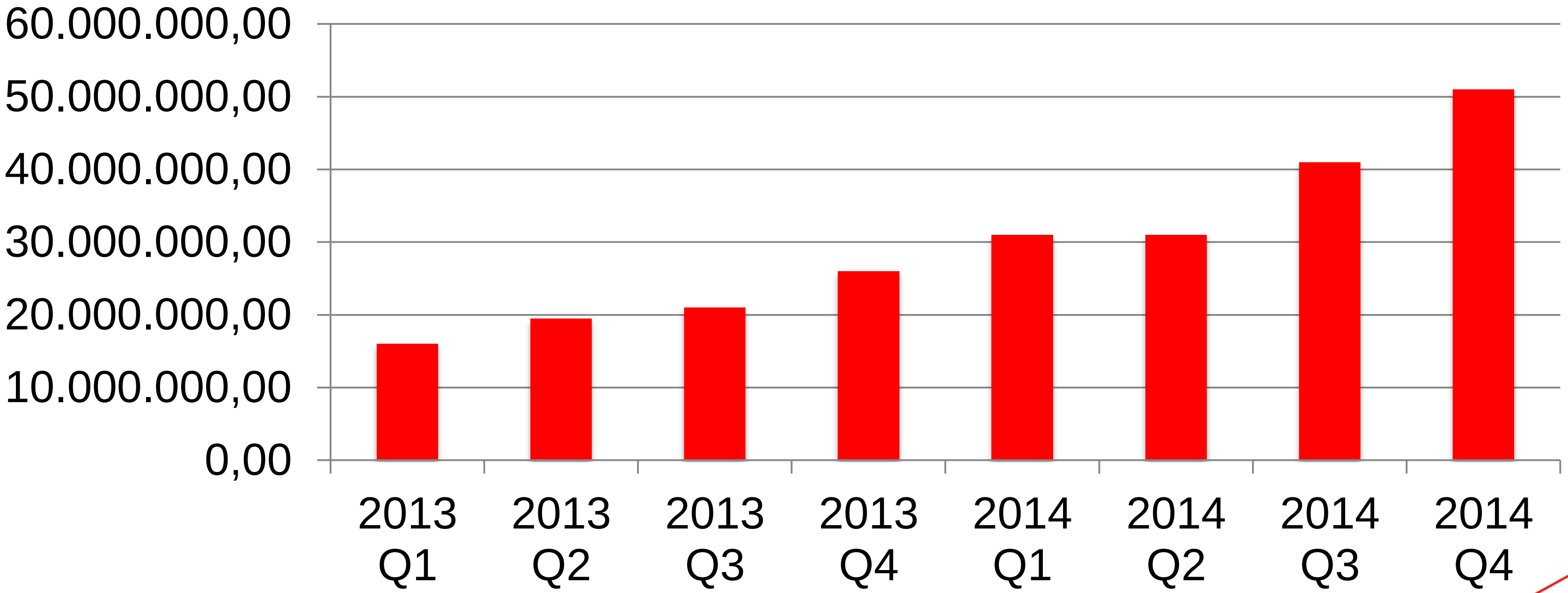


Effectiveness of IT Security Means

- Many sources on IT security incidents
- Focus on special aspects of IT security
- Surprisingly hard to compare figures (timescale, metrics, approach,...)
- Available sources of information:
  - Academia (e.g. Georgia Tech)
  - Governments (e.g. BSI, UK-Cert)
  - Security suppliers (e.g. Symantec, Kaspersky, McAfee)
  - Activists (e.g. Hackmageddon)
  - Personal communication (e.g. ACM IT Security Live)
  - Personal observation (e.g. B.Hive Honeypot)
  - Whistleblowers (e.g. Snowden)
- Be careful: all sources have a bias

Attack Numbers in 2014 (Latest Numbers)

- Malware (viruses, worms, ...) can be used to bypass security
- New malware pieces in 2014 (million)
  - 317 (Symantec)
  - 155 (McAfee)
  - 80 (BSI - only Windows)
- McAfee: Number of new malware per quarter is increasing:



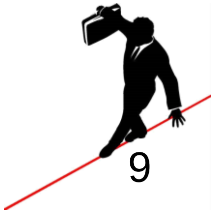
New Attack Quality in 2014

- McAfee: serious attacks on cryptography (esp. SSL/TLS) in last year
  - E.g. Heartbleed attack allows to wiretap encrypted communication with servers with little effort

- BSI: detected attacks by intelligence agencies on German infrastructure in business, research, and public administration

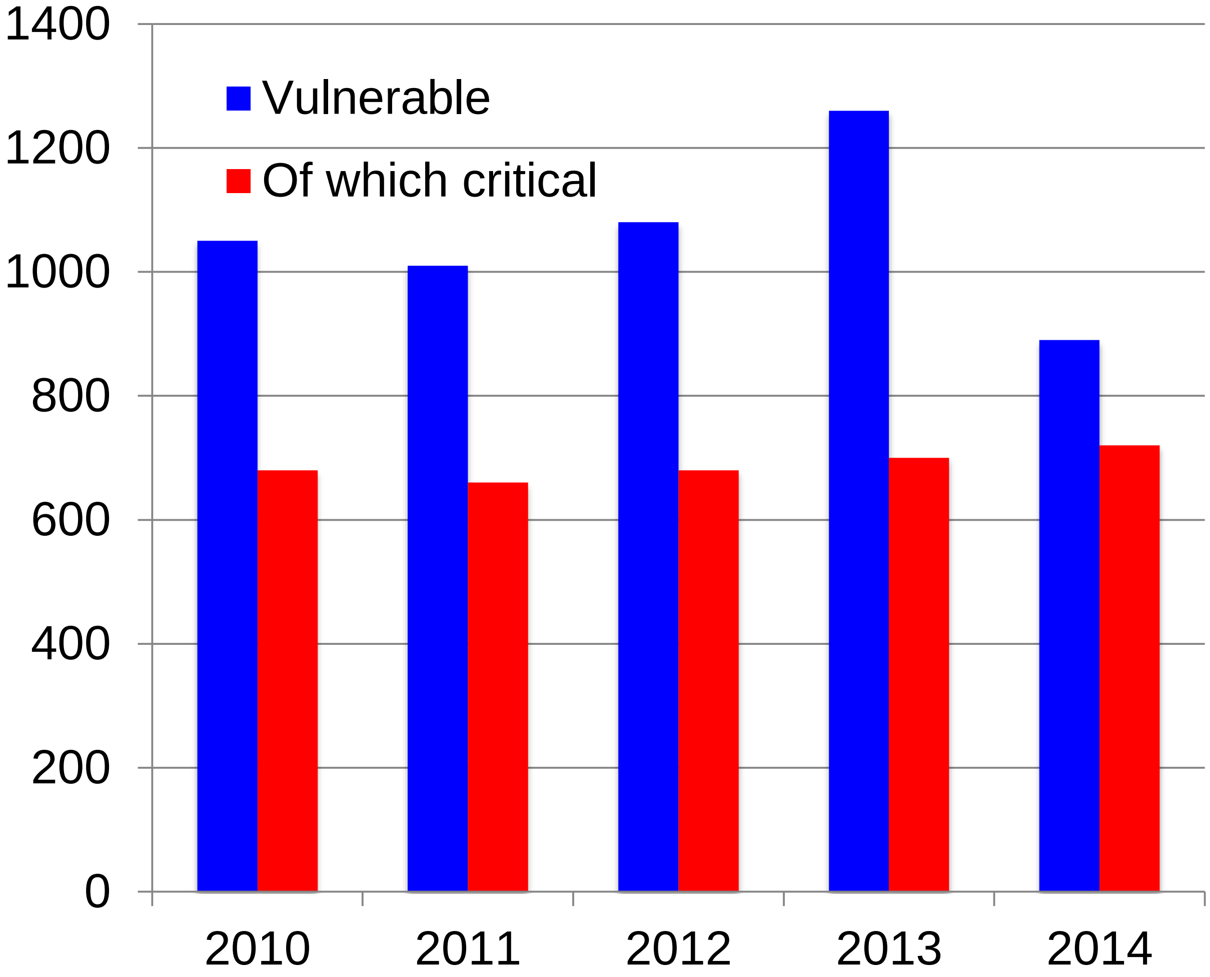
- BSI: 2014: > 1 million infections a month in Germany

- EU Study: 47% of users discovered malware



Attack targets

- BSI: Number of critical vulnerabilities in standard IT product remains high, for 13 products:



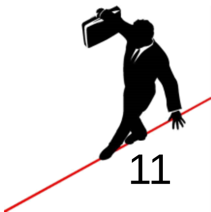
Defense

- Symantec: average time to patch top 5 zero-days:
  - 2013: 4 days
  - 2014: 59 days

- Symantec: total days of exposure for top 5 zero-days:
  - 2013: 19 days
  - 2014: 295 days

- McAfee: most vulerable high-traffic websites were quickly patched, many low-traffic sites and IP-enabled devices remain vulnerable (Heartbleed)

- Heartbleed study: 43 % of admins tried to fix vulnerability, only 14% succeeded

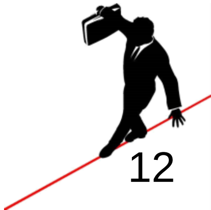


Defense

- ENISA: Over 50% of malware undetected by antivirus products

- McAfee: Multiple Android applications fail to properly validate SSL certificates (allows wiretapping)
  - 18 apps from Top 25 downloaded mobile apps still vulnerable months after notification (!!!)
  - Leak account data of third party services (social networks, cloud, ...)

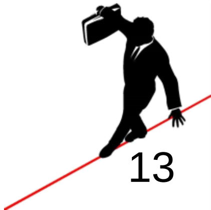
- Kaspersky: Analysis of home appliances, found a large number of vulnerabilities



To sum it up

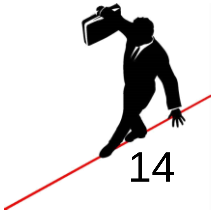
- Huge increase in number of attacks
- Software quality (security) does not improve
- Software developers have problems in providing patches in a reasonable time or do not provide patches at all
- Service providers have problems proving secure services or do not care about security
- Common defense means becoming more and more useless

Effectiveness of security means not given



Areas for Improvement

- Software and service quality
- Trustworthiness of software
- Diversity for critical software components
- Use of standard IT in new domains
- Security and privacy education



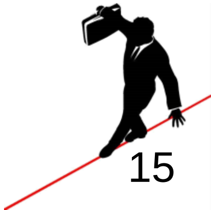
Action Item: Software and Service Quality

- Software quality must be improved
  - Should target for zero vulnerabilities
  - Should target for attack resilient systems
  - Should over-engineer security
    ➔ current risk-based approach may be wrong

- Usability of security means must be improved
  - Build usable software
  - Security by default
  - Automate: auto-update, …

- Incident management must be improved
  - Software Developers: target for a very short time and good quality
  - Admins: detect problems fast, take countermeasures fast

- To improve situation, external pressure may be necessary (e.g. software liability law)



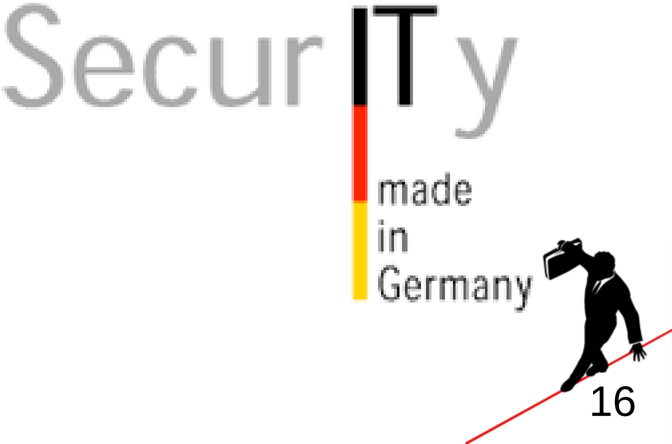
Action Item: Trustworthiness of Software

- Developers and users have problems judging on the trustworthiness of software
  - Many third party components (and many version changes)
  - Hard to verify OS and hardware

- Governments suspected to force developers to insert backdoors/vulnerabilities for surveillance (e.g. USA)

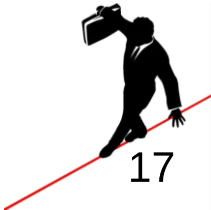
- German or European hardware platform and OS is desirable

- First steps: IT security made in Germany (However: limited approach)



Action Item: Diversity for Critical Software Components

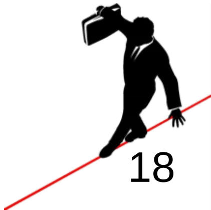
- Too little diversity in critical (=widely used) components (e.g. OpenSSL library)
- Obviously: many eyes looking on these components did not succeed in avoiding vulnerabilities
- Forking existing Open Source projects could not be the solution



Action Item: Use of Standard IT in new Domains

- Computer Science, standard IT, and connection to the Internet coming to new domains
  - Connected Car
  - Internet of Things
  - Industry 4.0
  - Smart Homes
  - Smart TVs
  - ...

- Infects domains with new security problems
  - Often out of expertise of developers of these domains
  - Observations:
    - Domain experts often naive in considering risks
    - Computer scientists often ignorant to domain specific problems

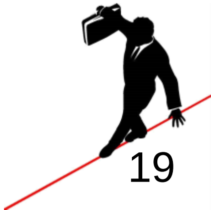


Action Item: Security and Privacy Education

- Education of software developers helps to avoid vulnerabilities
  - Example: OWASP
  - Decline of SQL Injection and CSRF

- Security and privacy courses should be mandatory in CS education

- Teach
  - respect for security problems (baseline: know when to ask a security expert)
  - understanding of security problems, not recipes for security solutions
  - limitations of security means (e.g. certification)
  - importance of privacy



Thank you for your Attention