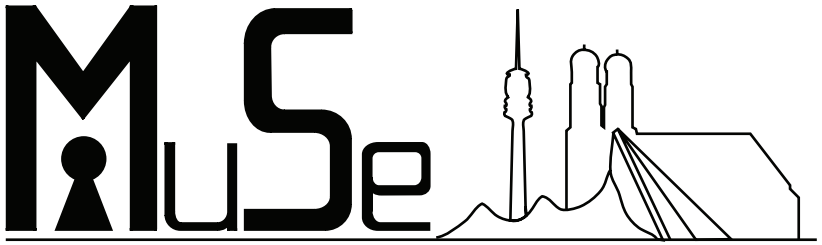


IT Security – Quo Vadis?

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

Munich IT Security Research Group

University of Karlsruhe, Germany
Karlsruhe Institute of Technology (KIT)
- CS student, PhD student

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

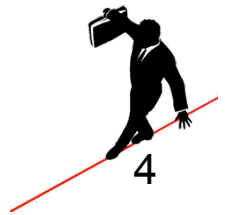
- Quo vadis ((ˈkwəʊ ˈvɑːdɪs)
  - Latin: from the Vulgate version of John 16:5
  - Literal: „Where are you going?”
  - In a broader sense: ”what is going to happen next?”

- Outline
  - Current Situation:
    - Facts and Figures
    - IT Security in the News
  - Problem Areas
  - Action Items

Facts and Figures

Munich IT Security Research Group

- 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) => SECURWARE 6
- Be careful: all sources have a bias

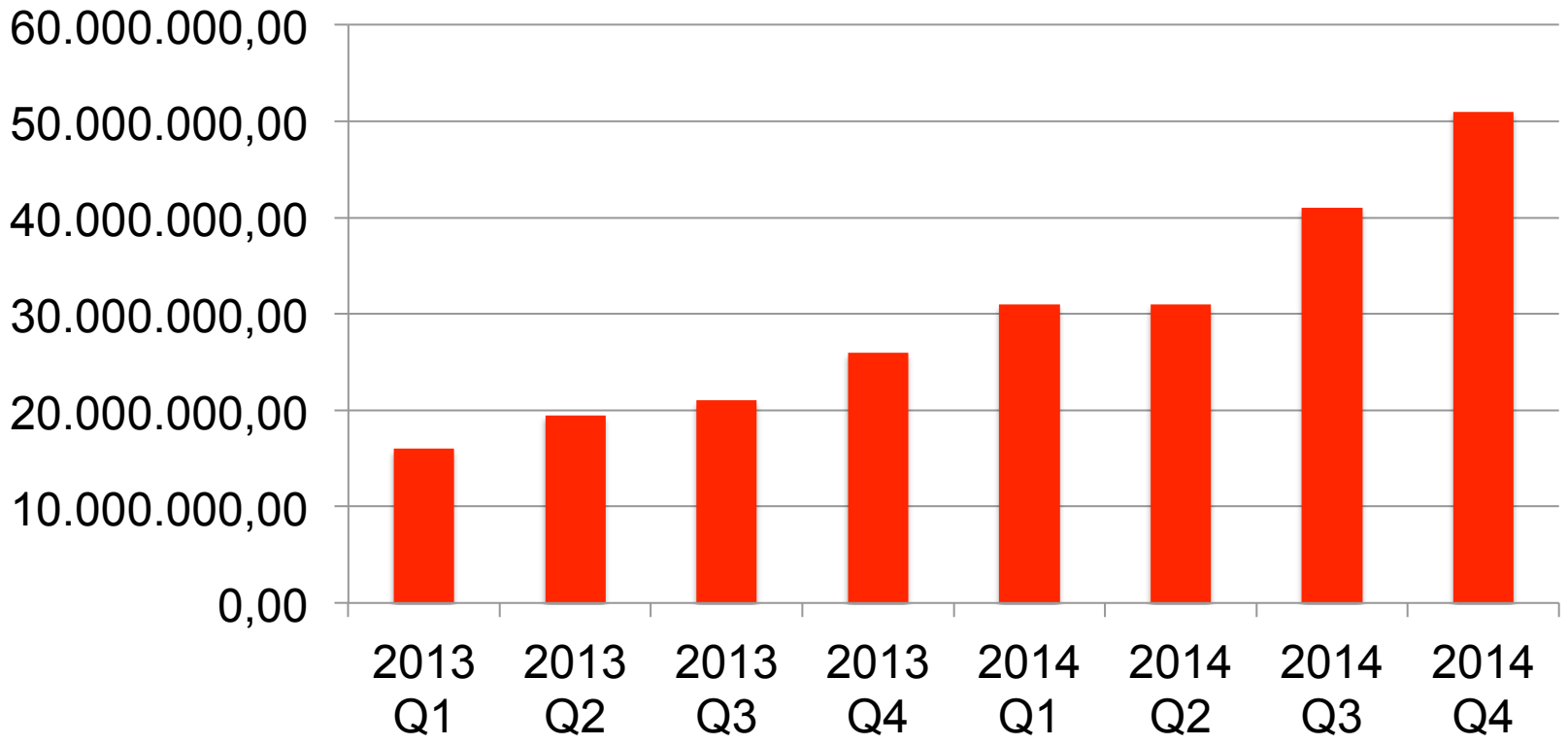


Attack numbers

Munich IT Security Research Group

- New malware pieces in 2014 (million)
  - 317 (Symantec)
  - 155 (McAfee)
  - 80 (BSI - only Windows)

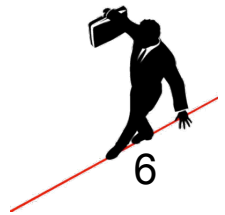
- McAfee: Number of new malware per quater is increasing:



Attack numbers

Munich IT Security Research Group

- BSI: 2014: > 1 million infections a month in Germany
- EU Study: 47% of users discovered malware
- CERT-UK : Malware biggest threat
- CERT-UK: Malware costs the UK economy billions every year



Attack quality

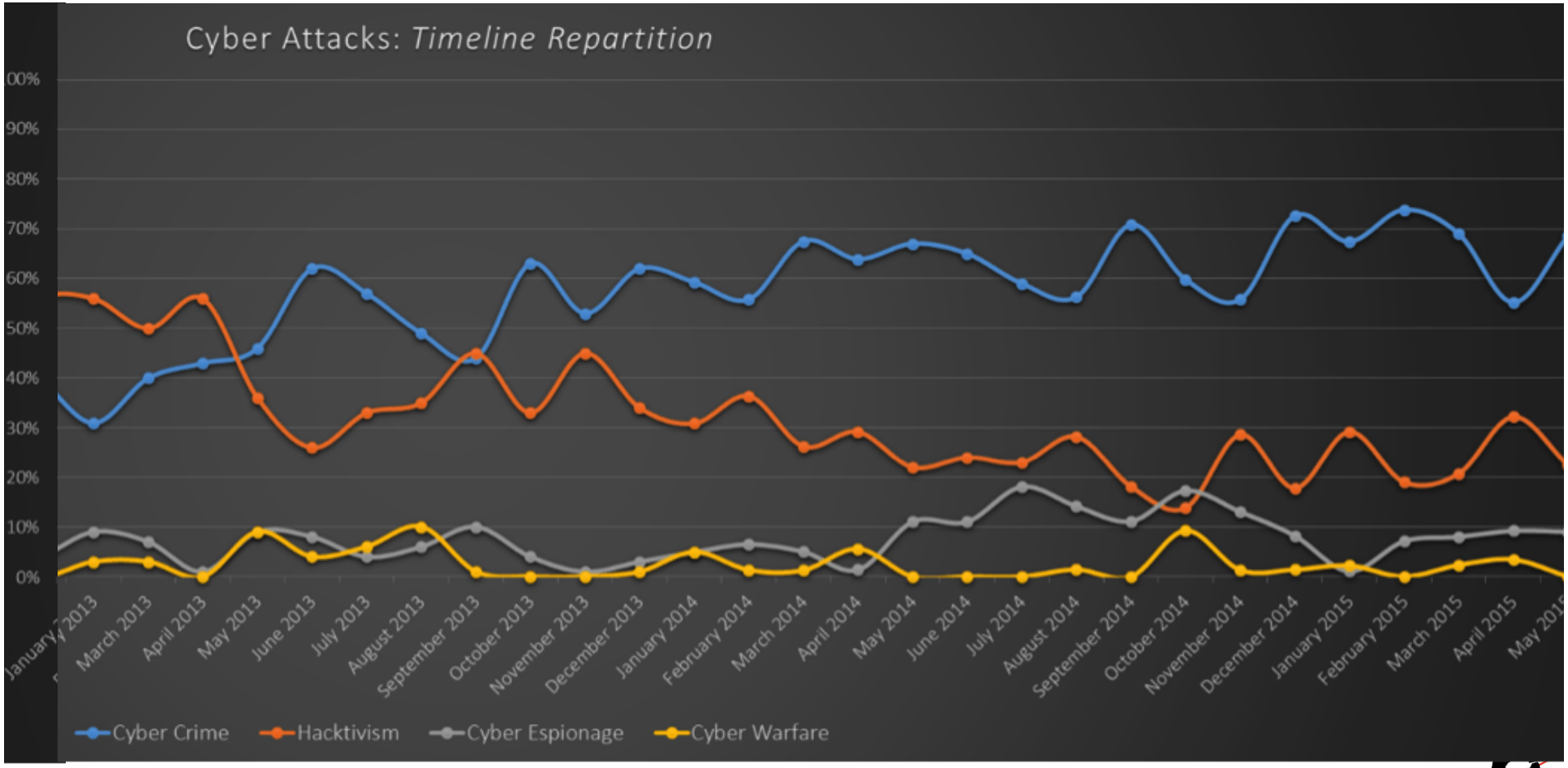
Munich IT Security Research Group

- McAfee: serious attacks on cryptography (esp. SSL/TLS) in last year
- BSI: Frequently attacks initially focus on less technologically aware target individuals within companies
- BSI: Germany is subject to continuous cyber attacks with the objective of obtaining information and gaining financial advantages.
- BSI: detected attacks by intelligence agencies on German infrastructure in business, research, and public administration

Attack quality

Munich IT Security Research Group

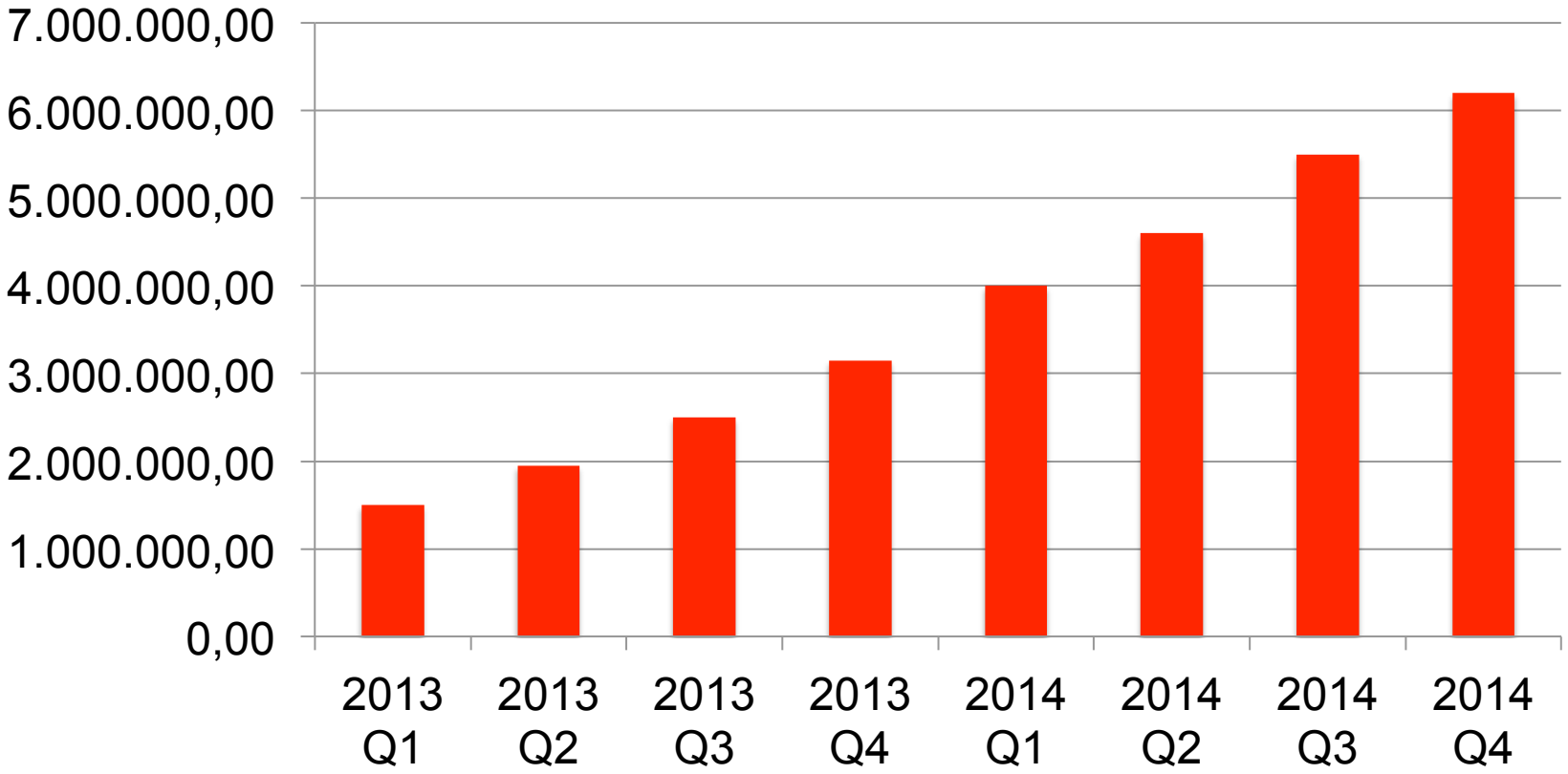
- Classification of attacks (distribution of motivation behind attacks listed on Hackmageddon)



Attack targets

Munich IT Security Research Group

- McAfee: Total number of malware increasing for mobile devices (especially Android)

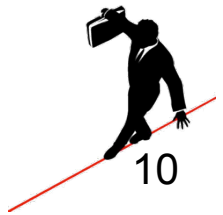


- Kaspersky: 295.539 mobile malware samples in 2014 (more than 2003-2013 in total)

Attack targets

Munich IT Security Research Group

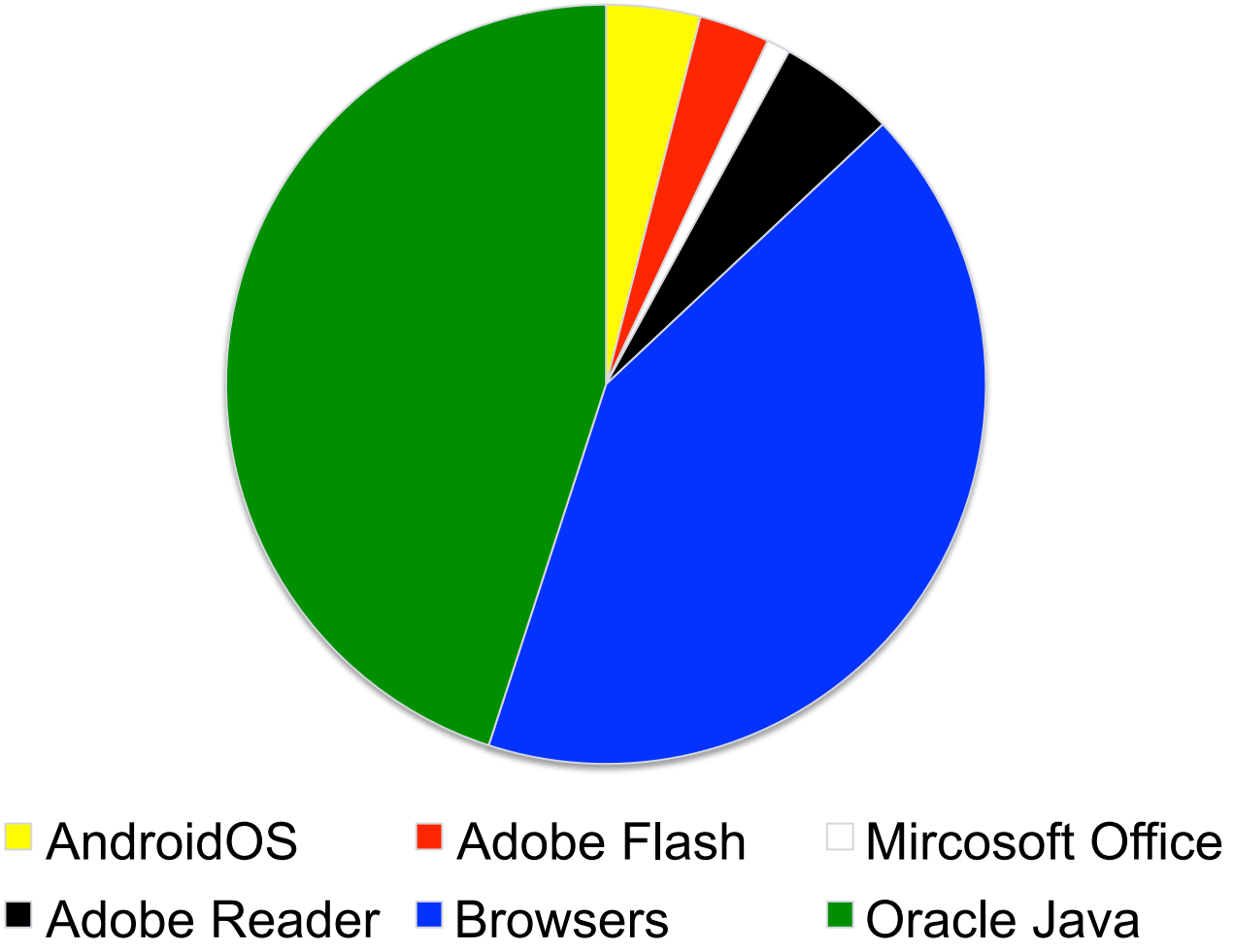
- Kaspersky: 19% of Android users encountered a mobile threat at least once during the year (e.g. March 2014: 644.000 attacks)
- BSI: Production and process automation systems are increasingly susceptible to cyber attack
- BSI: Advanced Persistent Threats (APT) focus chiefly on the defense industry, high-tech sectors [...], research institutes and public administration.



Attack targets

Munich IT Security Research Group

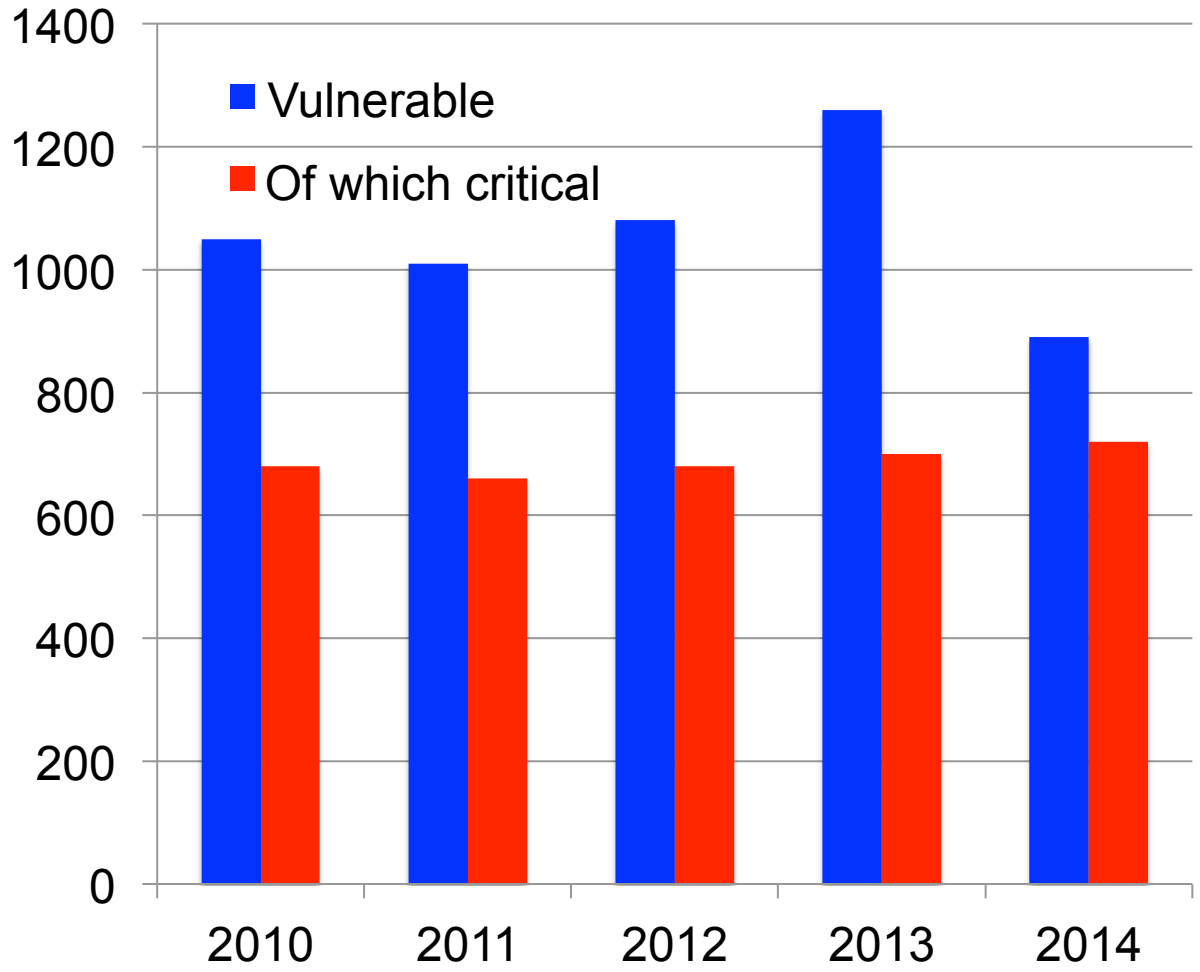
- ENISA: around 90 percent of web exploits are Java related
- Kaspersky: Target Applications:



Attack targets

Munich IT Security Research Group

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



Defense

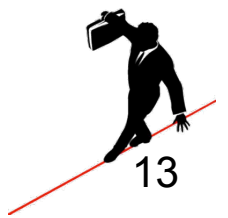
Munich IT Security Research Group

- 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: number of vulnerable host found in scan area:
  - Day 0 : 600.000
  - Day 0 + 30 : 300.000
  - Day 0 + 60 : 300.000 (!!!)
  - 43 % of admins tried to fix vulnerability, only 14% succeeded



Defense

Munich IT Security Research Group

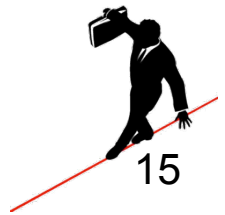
- ENISA: Over 50% of malware undetected by antivirus products
- ENISA: Conficker worm (6 years old) still most commonly detected malware
- ENISA: 70% of web sites use unsupported Java versions
- CERT-UK: 800.000 vulnerable network services observed in the UK
- McAfee: Multiple Android applications fail to properly validate SSL certificates
  - 18 apps from Top 25 downloaded mobile apps still vulnerable months after notification (!!!)
  - Leak account data of third party services (social networks, cloud, ...)

Defense

Munich IT Security Research Group

- Kaspersky: Analysis of home appliances
  - 14 vulnerabilities in NAS
  - 1 vulnerability in Smart TV
  - Several potentially hidden remote control functions in the router

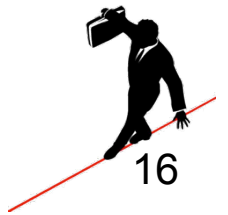
- ENISA/OWASP: Reduction of web application attack surfaces SQL Injection, Clickjacking and Cross Site Request Forgery (CSRF)



Trends: ENISA

Munich IT Security Research Group

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑



Trends: BSI

Munich IT Security Research Group

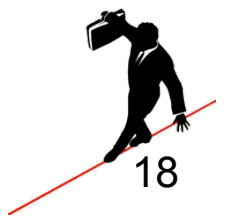
Threats	2013	2014	Forecast
Vulnerabilities	↑	→	→
Spam	↓	↑	→
Malware	↑	↑	↑
Drive-by exploits and exploit kits	↑	→	→
Botnets	→	→	→
Social engineering	→	↑	→
Identity theft	↑	↑	↑
Denial of Service (Dos; DDos)	→	→	→
Advanced Persistent Threats (APT)	↑	→	↑

↑ Increasing → Unchanged ↓ Decreasing

Summary Facts and Figures

Munich IT Security Research Group

- 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
- Cyber Crime is on the rise
- Attackers move quickly to new areas (at the moment: mobile devices, Smart Homes, ...)
- Common defense means becoming useless



IT Security in the news (September 2014)

Munich IT Security Research Group

BBC | Sign in | News | Sport | Weather | Shop | Earth | Trave

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

Technology

Shellshock: 'Deadly serious' new vulnerability found

By Dave Lee
Technology reporter, BBC News

25 September 2014 | Technology

IT Security in the news (October 2014)

Munich IT Security Research Group

KIM ZETTER SECURITY 10.14.14 9:01 PM

THERE IS A NEW SECURITY VULNERABILITY NAMED POODLE, AND IT IS NOT CUTE

IT Security in the news (March 2015)

Munich IT Security Research Group

IT Security in the news (May 2015)

Munich IT Security Research Group

REUTERS EDITION: U.S. SIGN IN | REGISTER Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

Industries | Fri May 15, 2015 11:03am EDT

Related: TECHNOLOGY

Unknown hackers attack German parliament's data network

BERLIN

IT Security in the news (June 2015)

Munich IT Security Research Group

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS **SECURITY** INFRASTRUCTURE BUSINESS HARDWARE SCIE

Dumb MongoDB admins spew 600 TERABYTES of unauthenticated data

Flaw identified three years ago comes back to bite NoSQL crowd

IT Security in the news (July 2015)

Munich IT Security Research Group

WIRED Hacking Team Breach Shows a Global Spying Firm Run Amok SUBSCRIBE

SHARE

SHARE

TWEET

ANDY GREENBERG SECURITY 07.06.15 10:26 AM

HACKING TEAM BREACH SHOWS A GLOBAL SPYING FIRM RUN AMOK

free become a member sign in search jobs more International beta

theguardian

home › tech UK world politics sport football opinion culture business all

Hacking

Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim

IT Security (?) in the news (July 2015)

Munich IT Security Research Group

abc NEWS U.S. World Politics Entertainment ...

GOSTREAM: REBUILDING NEW ORLEANS WITH HABITAT FOR HUMANITY

New York Stock Exchange Blames Shutdown on 'Configuration Issue' as Dow Falls

Jul 8, 2015, 4:48 PM ET

By SUSANNA KIM

News › Technology & Science › Cybersecurity

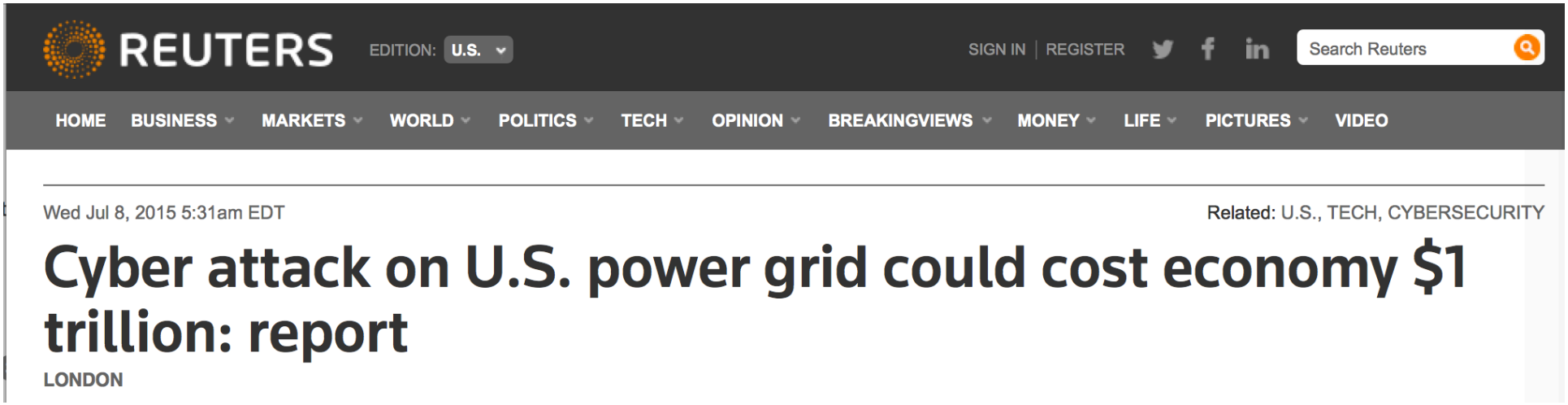
Did hackers gain access to terrifying anti-aircraft missiles?

11:49, 8 JULY 2015 | BY OLIVIA SOLON

★ Recommended In News

IT Security in the news (July 2015)

Munich IT Security Research Group



REUTERS EDITION: U.S. SIGN IN | REGISTER Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

Wed Jul 8, 2015 5:31am EDT

Related: U.S., TECH, CYBERSECURITY

Cyber attack on U.S. power grid could cost economy $1 trillion: report

LONDON

IT Security in the news (July 2015)

Munich IT Security Research Group

WIRED Hackers Can Disable a Sniper Rifle—Or Change Its Target SUBSCRIBE

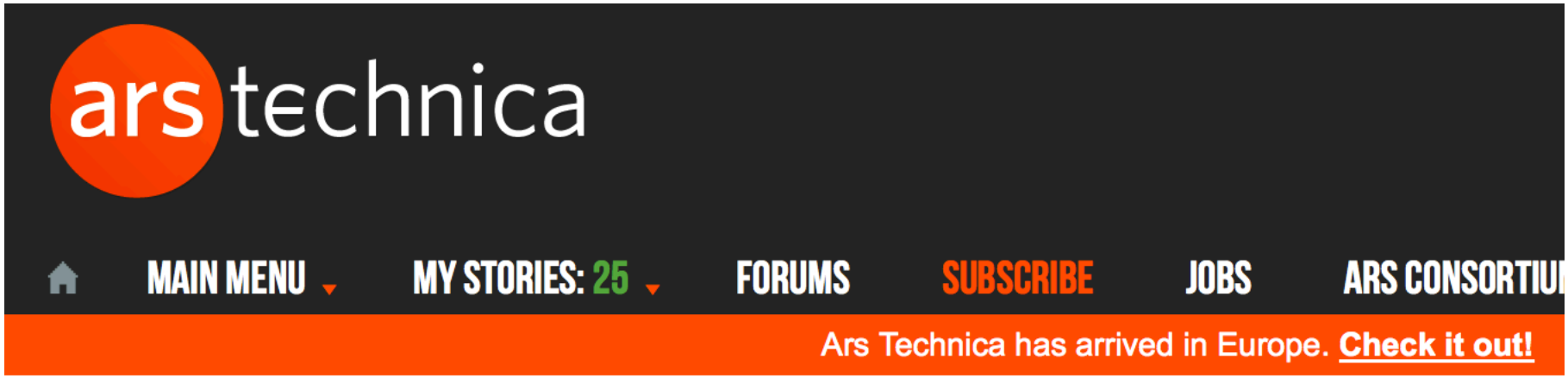
BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE | SECURITY

ANDY GREENBERG SECURITY 07.29.15 7:00 AM

HACKERS CAN DISABLE A SNIPER RIFLE—OR CHANGE ITS TARGET

IT Security in the news (August 2015)

Munich IT Security Research Group



RISK ASSESSMENT / SECURITY & HACKTIVISM

Parrot drones easily taken down or hijacked, researchers demonstrate

Open telnet port, open Wi-Fi, root access, open season.

IT Security in the news (August 2015)

Munich IT Security Research Group

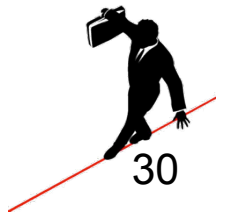
WIRED Hackers Can Seize Control of Electric Skateboards and Toss Riders SUBSCRIBE

HACKERS CAN SEIZE CONTROL OF ELECTRIC SKATEBOARDS AND TOSS RIDERS

Summary: IT Security in the News

Munich IT Security Research Group

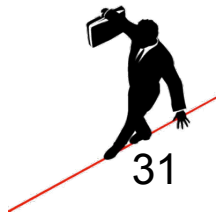
- High-value targets hacked
- Everything gets hacked (Internet of Hacked Things)
- Non-excusable security vulnerabilities (not checking default configuration…)
- Components used by many products are dangerous
- Even many eyes (Open Source) cannot prevent vulnerabilities
- Establishment of trust by certificates has limitations



Problem Areas to Focus on in the Future

Munich IT Security Research Group

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

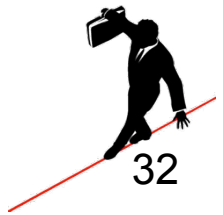


Action Item: Software and Service Quality

Munich IT Security Research Group

- Have software developer given up?
  - Still many vulnerabilities in software
  - Incident handling worse than ever
  - It seems as if there is a “don’t care” attitude

- Have service provider given up?
  - Many vulnerable services
  - Services not kept up to date concerning security
  - It seems as if there is a “don’t care” attitude

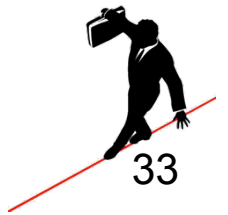


Action Item: Software and Service Quality

Munich IT Security Research Group

- 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
  - Do not value time to market over security (no “banana software”)
  - Secure Scrum@SECURWARE 1

- Make using product in a secure way easy
  - Security by default: Default installation/configuration should be secure
  - Many unprofessional administrators: Offer auto-update, take care auto-update does not screw the system
  - Design usable security



Action Item: Software and Service Quality

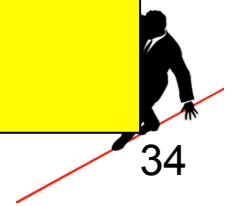
Munich IT Security Research Group

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

- Open Source software may be dangerous
  - Current attacks target open source components
  - Heartbleed: trivial programming error that should not have slipped professional quality management
  - Perhaps the “many eyes see all” paradigm of open source security is wrong (see Shellshock)

Quo vadis?

- Situation will not improve much in the future
- External pressure necessary (software liability law, privacy law, regulation of app stores)
- Other domains do not accept crappy products (learn from safety)



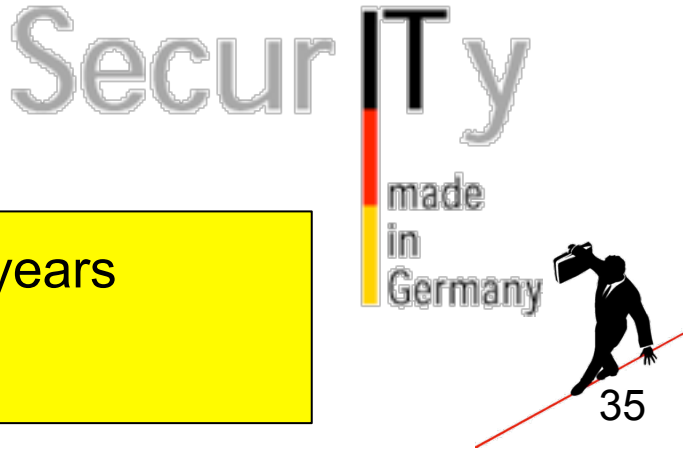
Action Item: Trustworthiness of Software

Munich IT Security Research Group

- 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)
- Backdoors can also be used by attackers
- European hardware platform and OS is necessary
- First steps: IT security made in Germany (However: limited approach)

Quo vadis?

We will still be dependent on US software in 10 years (problem!!!)



Action Item: Diversity for Critical Software Components

Munich IT Security Research Group

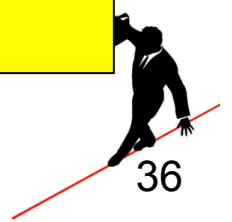
- Too little diversity in critical (=widely used) componentes
  - OpenSSL
  - Browsers
  - Web-Servers
  - Java
  - ...

- Obviously: many eyes looking on these components did not succeed in avoiding vulnerabilities

- Forking existing Open Source projects could not be the solution

Quo vadis?

There may be more alternatives, but it is very likely that they share code and that there still will be a preferred component that is ubiquitously used

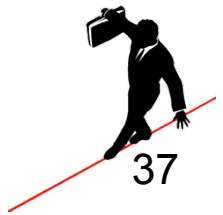


Action Item: Use of Standard IT in new Domains

Munich IT Security Research Group

- Computer Science, standard IT, and connection to the Internet coming to new domains
  - Connected Car => SECURWARE 8
  - 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: Use of Standard IT in new Domains

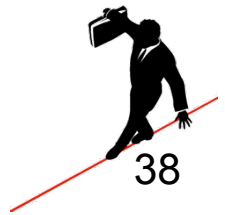
Munich IT Security Research Group

- „Those industry guys are so stupid, Industry 4.0 will be a total security failure, these people don‘t even have a Chief Security Officer in their company“

- Both sides should learn from each other
  - Safety understand in depth in industry, many high quality processes, IT security could learn from safety engineering

Quo vadis?

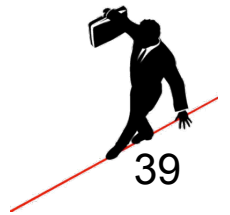
After a period of spectacular hacks, IT security will be on a high level in new domains. IT security itself will benefit from contact with new domains



Action Item: Security Education

Munich IT Security Research Group

- Education of software developers helps to avoid vulnerabilities
  - Example: OWASP
  - Decline of SQL Injection and CSRF
- IT security courses should be mandatory in CS education
- Teach people respect for IT security problems: People should know when to ask a security expert
- Teach understanding of security problems, not recipes for security solutions
- Teach a system view (necessary for IT security)
- Teach limitations of security means
  - E.g. certification



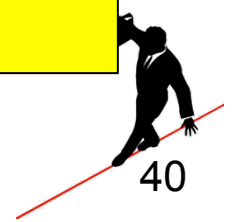
Action Item: Security Education

Munich IT Security Research Group

- Typical Bachelor student:
  - Read first (maybe second sentence) of exercise
  - Google, click first result (maybe also second)
  - Do whatever is written on this page, regardless of whether it is a solution for the problem at hand or not
- Boundary conditions never considered
- Side effects never considered
- Computer Science education must really change!

Quo vadis?

Interest in IT security education will increase in the near future (job options...). Big changes in computer science education will take decades.



Action Item: Traceability of Attacks

Munich IT Security Research Group

- Today: hacking teams affiliated with states
  - E.g. „Team Red“, military unit 61398 (APT1)
  - Espionage, sabotage
- IT forensic is a hard problem, identities can be spoofed
- Knowledge of origins of an attack is necessary for responsible reaction on a state level (diplomatic, weapons, ...)
- States thinking about non-cyber responses on cyber attacks (Tallinn Manual 2.0 to be published 2016)
- Traceability may be a good means to avoid cyber attacks by intelligence agencies or military cyber units

Quo vadis?

There will be a kind of attack radar to trace the origin of attacks in the future

Thank you for your attention

Munich IT Security Research Group

Contact details:

Prof. Dr.-Ing. Hans-Joachim Hof
MuSe – Munich IT Security Research Group
Department of Computer Science and Mathematics
Munich University of Applied Sciences
Lothstrasse 64
80335 Munich
Germany

hof@hm.edu
http://muse.bayern
(register for my newsletter)