International Pugwash Workshop

NETWORK & DATA SECURITY

Cyberattacks

– Technical Aspects and Countermeasures –

Prof. Dr. Ulrich Bühler

Hochschule Fulda
University of Applied Sciences

23.10.2015 Berlin

Agenda Cyberattacks and Countermeasures

NETWORK & DATA SECURITY

1 **Digital Society – always connected**
Social Networks, Health Care,
Wearable Techniques, Car Entertainment

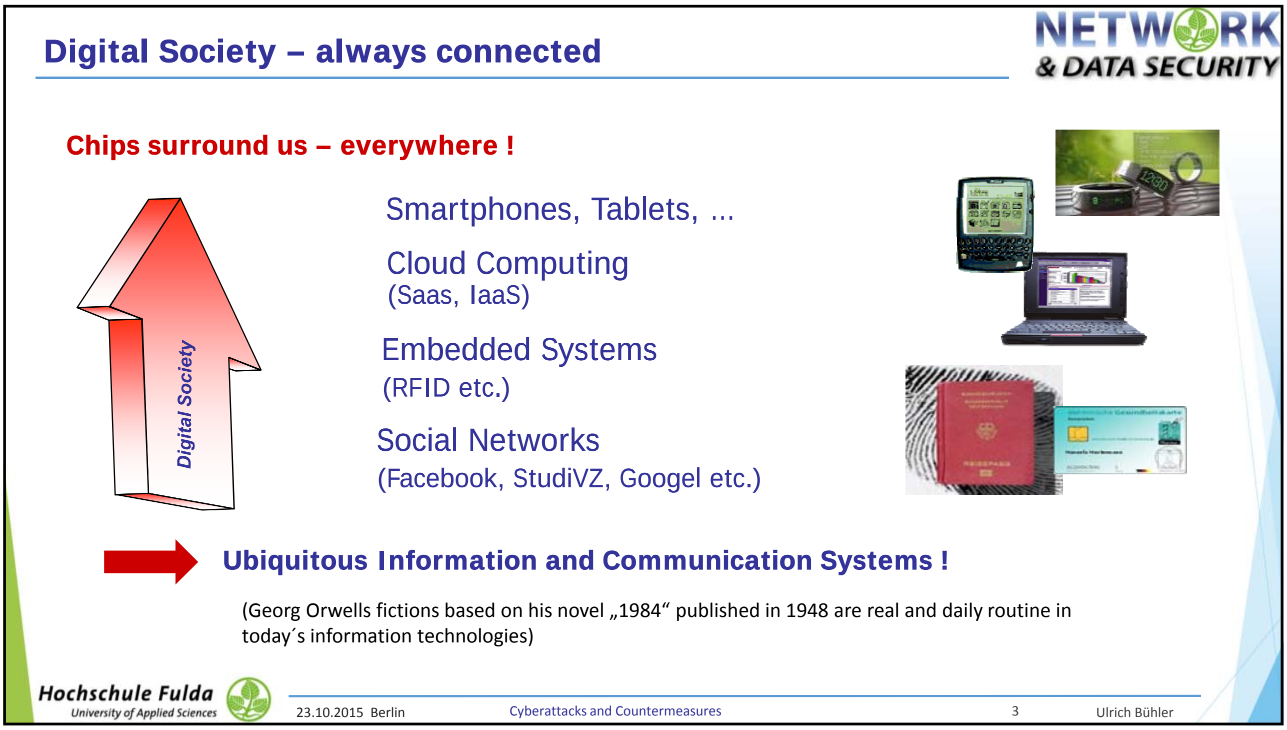
2 **Current Attacks and Implications**
Attack Scenarios, Advanced Persistent Threats,
IT-Espionage

3 **Some Countermeasures**
Encryption, Authentication, Integrity
Network and Data Security

4 **Summary**
Proactive IT-Security, Awareness

Hochschule Fulda
University of Applied Sciences

23.10.2015 Berlin Cyberattacks and Countermeasures 2 Ulrich Bühler



Digital Society – always connected

NETWORK & DATA SECURITY

Chips surround us – everywhere !

Digital Society

Smartphones, Tablets, ...

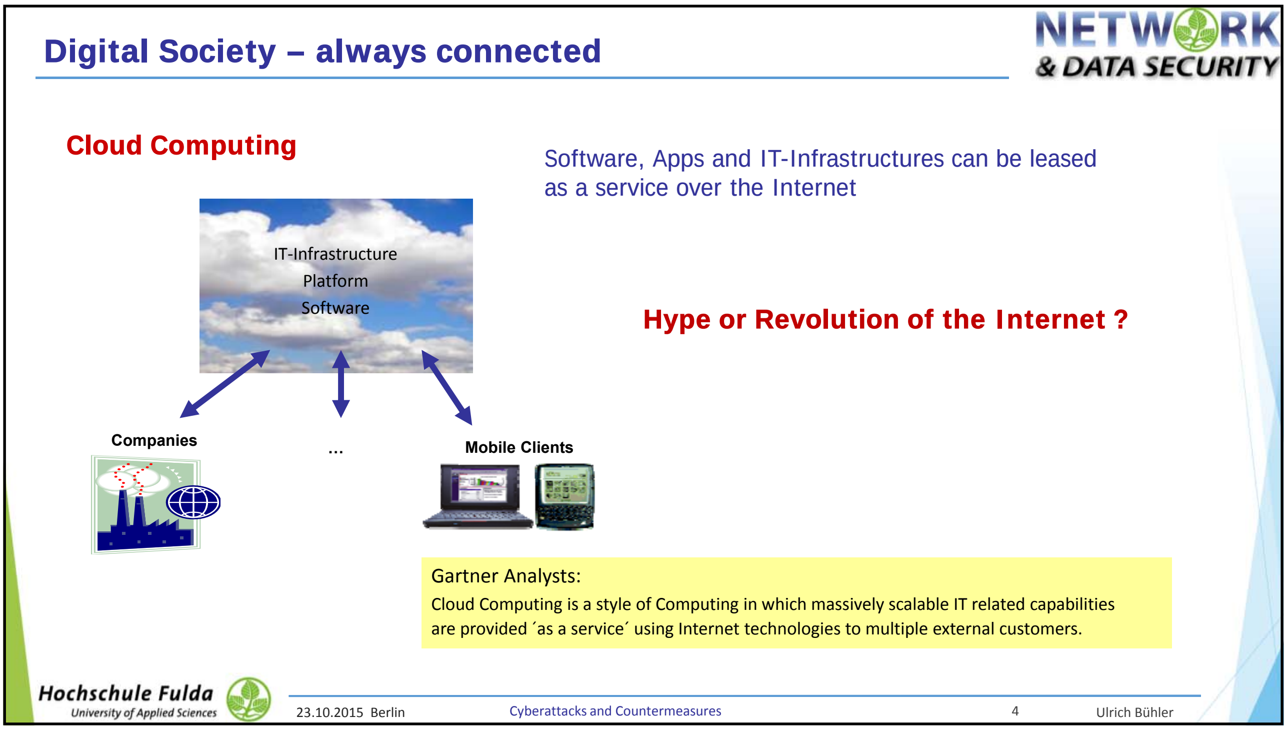
Cloud Computing
(Saas, IaaS)

Embedded Systems
(RFID etc.)

Social Networks
(Facebook, StudiVZ, Googel etc.)

Ubiquitous Information and Communication Systems !

(Georg Orwells fictions based on his novel „1984“ published in 1948 are real and daily routine in today´s information technologies)



Digital Society – always connected

NETWORK & DATA SECURITY

Cloud Computing

IT-Infrastructure
Platform
Software

Companies

...

Mobile Clients

Software, Apps and IT-Infrastructures can be leased as a service over the Internet

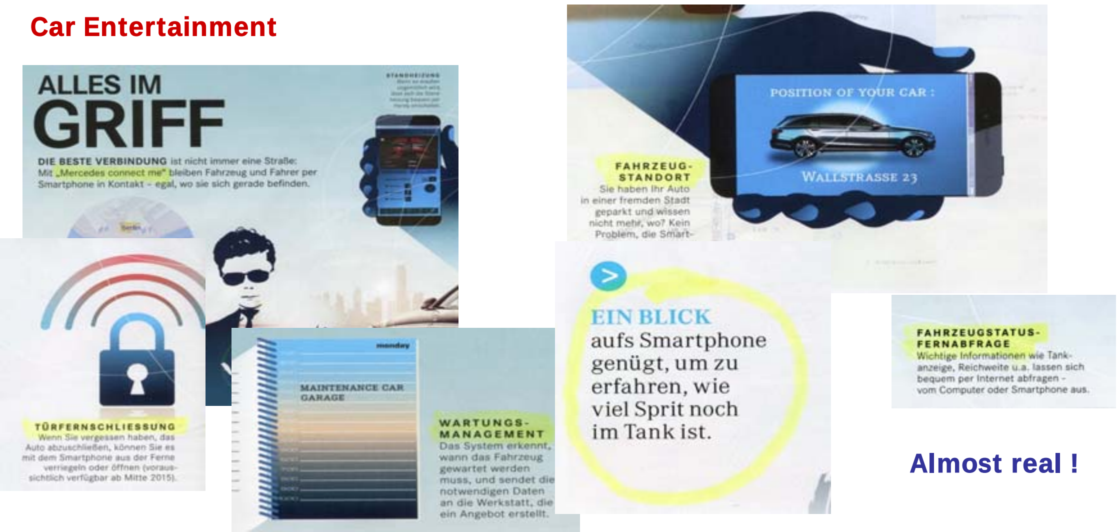
Hype or Revolution of the Internet ?

Gartner Analysts:
Cloud Computing is a style of Computing in which massively scalable IT related capabilities are provided ´as a service´ using Internet technologies to multiple external customers.

Digital Society – always connected

NETWORK & DATA SECURITY

Car Entertainment



ALLES IM GRIFF

DIE BESTE VERBINDUNG ist nicht immer eine Straße: Mit „Mercedes connect me" bleiben Fahrzeug und Fahrer per Smartphone in Kontakt – egal, wo sie sich gerade befinden.

STANDHEIZUNG

TÜRFERNSCHLIESSUNG
Wenn Sie vergessen haben, das Auto abzuschließen, können Sie es mit dem Smartphone aus der Ferne verriegeln oder öffnen (voraussichtlich verfügbar ab Mitte 2015).

WARTUNGS-MANAGEMENT
Das System erkennt, wann das Fahrzeug gewartet werden muss, und sendet die notwendigen Daten an die Werkstatt, die ein Angebot erstellt.

FAHRZEUG-STANDORT
Sie haben Ihr Auto in einer fremden Stadt geparkt und wissen nicht mehr, wo? Kein Problem, die Smart-

EIN BLICK aufs Smartphone genügt, um zu erfahren, wie viel Sprit noch im Tank ist.

FAHRZEUGSTATUS-FERNABFRAGE
Wichtige Informationen wie Tankanzeige, Reichweite u.a. lassen sich bequem per Internet abfragen – vom Computer oder Smartphone aus.

Almost real !

Source: Mercedes-Benz Magazin 3.2014

Digital Society – always connected

NETWORK & DATA SECURITY

Wearable Technologies

The NFC ring can unlock your smartphone or tablet when you slide your hand under the device. It can be used to transfer data, pictures, links, and more to your friends' smartphones. It can start apps with custom parameters, and it can even unlock the door to your house, if you install a compatible lock.

Biggest Market: Health Sector

Digital Society – always connected

NETWORK & DATA SECURITY

Augmented Reality

- Enrichment of real-world environment with digital information over Internet (Outernet)
- Information about the surrounding real world of the mobile user becomes interactive and digitally manipulable

Threats and Risks are ubiquitous in everyday´s life !

Current Attacks and Implications

NETWORK & DATA SECURITY

Threats, Vulnerabilities, Risks, Attacks, Damages

Vulnerabilities arise e.g. from

- **Bugs** in Software: due to unavoidable complexity
- **Backdoors**:

  Software developers implement tools to connect to a computer from a remote location (remote desktop application, remote network maintenance);

  Secret Services install and employ these to gain information
- **Design weaknesses** of network components, enterprise infrastructure systems, software, services, commercial applications, industrial control systems and so on: often not known publicly, not intended by developer

and are the cause of a lot of **threats and cyberattacks**

- Infiltration of malware (e.g. Trojans, Phishing, botnets)
- Activities, which endangers the availability of processes, services and applications (e.g. Stuxnet, Flame)
- Interruption of IT infrastructure as the medium for communication between users, applications, business processes, … (e.g. Spam, Botnets)

Current Attacks and Implications

NETWORK & DATA SECURITY

Malicious Software (Malware) Injection

Malware: all kind of code or programs designed to infiltrate and damage IT systems, to harvest sensitive information, to control machines without users approval; is more and more sophisticated with high complexity

Major Different types

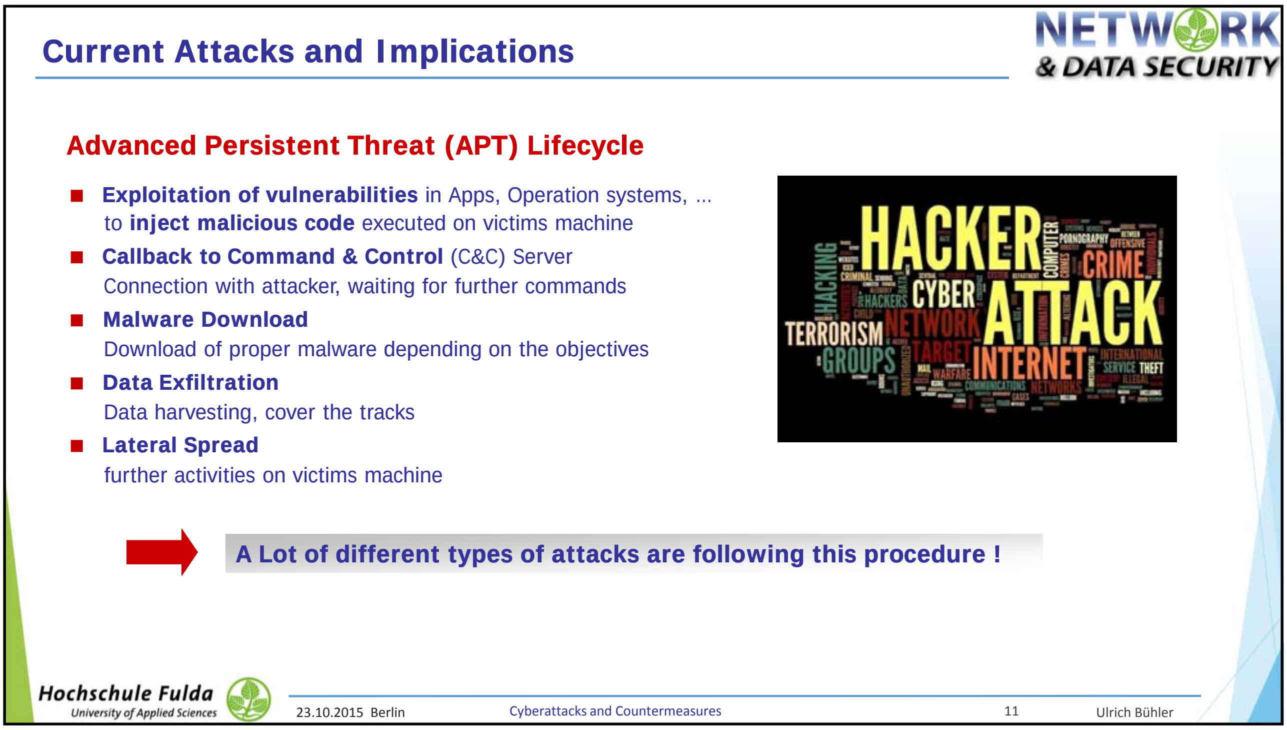
- ***Worms:*** designed to spread without users knowledge (e.g. Slammer, Blaster, Sasser)
- ***Trojan Horses (Trojans):*** combine a visible and a hidden malicious functionality (e.g. Mydoom, Phatbot), with Rootkits
- ***Rootkits:*** a masking technique to protect malware for detection by antimalware tools, so-called stealth techniques; have no malicious capability per se (e.g. Uroburos, Mebroot)
- ***Spyware, Rootkits, Keylogger:*** programs used by miscreants or secret services to steal or gather sensitive information from users, enterprises and governmental authorities or suspicious persons and groups (e.g. Stuxnet, Flame, Regin)

Current Attacks and Implications

NETWORK & DATA SECURITY

Threat landscape and types of attacks has changed dramatically

- **Botnet**: primary means for miscreants to achieve their objectives
  - network of malware-infected hosts (zombies) that are controlled by a miscreant (botmaster)
  - once infected with malware (bot) the botmaster commands the zombies (traffic between the bot and its command and control server, C&C) to attack a victim (installation of Trojans to collect sensitive information and transmits it to the botmaster)
  - Examples: Torbig botnet, Gameover Zeus
- Infection of victims through ´**Drive-by-Download**´
  - Web pages on vulnerable web servers are modified with the inclusion of HTML tags (iframes)
  - tags cause the victims browser to request JavaScript code from a website under control of the attacker (drive-by-download server)
  - the JavaScript code launches exploits against the browser or components (ActiveX controls, plugins)
  - From the drive-by-download server e.g. an executable is downloaded and executed
- Daily thousands of companies are victims of **DDoS-Attacks** by botnets (e.g. Websites are not anymore accessible, e-mail servers are broken down)


NETWORK
& DATA SECURITY
HACKER
CYBER
ATTACK
CRIME
TERRORISM
NETWORK
INTERNET
GROUPS
TARGET
HACKING
COMPUTER
THEFT

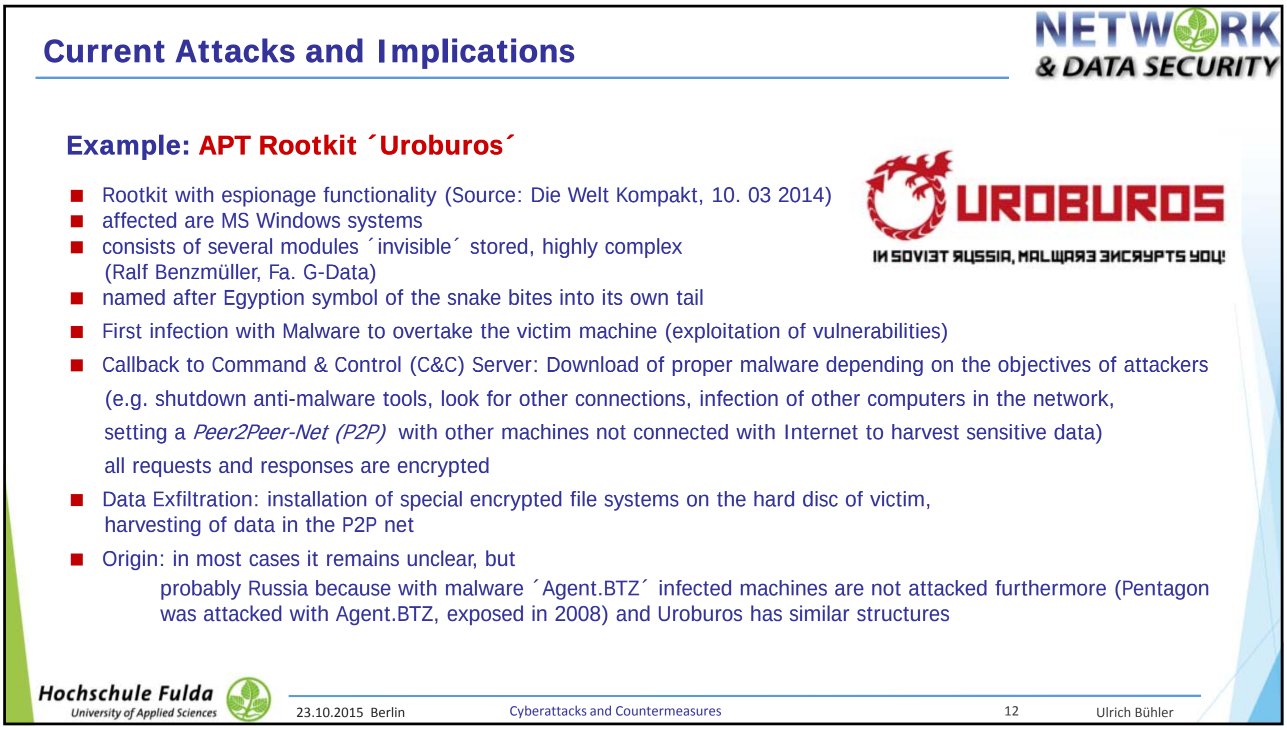
Current Attacks and Implications

Advanced Persistent Threat (APT) Lifecycle

- **Exploitation of vulnerabilities** in Apps, Operation systems, ...
  to **inject malicious code** executed on victims machine
- **Callback to Command & Control** (C&C) Server
  Connection with attacker, waiting for further commands
- **Malware Download**
  Download of proper malware depending on the objectives
- **Data Exfiltration**
  Data harvesting, cover the tracks
- **Lateral Spread**
  further activities on victims machine

➡ **A Lot of different types of attacks are following this procedure !**

Hochschule Fulda University of Applied Sciences 23.10.2015 Berlin Cyberattacks and Countermeasures 11 Ulrich Bühler


NETWORK
& DATA SECURITY
UROBUROS
IИ SOVIƎT ЯUSSIA, MALШAЯƎ ƎИCЯYPTS YOU!

Current Attacks and Implications

Example: APT Rootkit ´Uroburos´

- Rootkit with espionage functionality (Source: Die Welt Kompakt, 10. 03 2014)
- affected are MS Windows systems
- consists of several modules ´invisible´ stored, highly complex
  (Ralf Benzmüller, Fa. G-Data)
- named after Egyption symbol of the snake bites into its own tail
- First infection with Malware to overtake the victim machine (exploitation of vulnerabilities)
- Callback to Command & Control (C&C) Server: Download of proper malware depending on the objectives of attackers
  (e.g. shutdown anti-malware tools, look for other connections, infection of other computers in the network,
  setting a *Peer2Peer-Net (P2P)* with other machines not connected with Internet to harvest sensitive data)
  all requests and responses are encrypted
- Data Exfiltration: installation of special encrypted file systems on the hard disc of victim,
  harvesting of data in the P2P net
- Origin: in most cases it remains unclear, but
  probably Russia because with malware ´Agent.BTZ´ infected machines are not attacked furthermore (Pentagon was attacked with Agent.BTZ, exposed in 2008) and Uroburos has similar structures

Hochschule Fulda University of Applied Sciences 23.10.2015 Berlin Cyberattacks and Countermeasures 12 Ulrich Bühler

Current Attacks and Implications

NETWORK & DATA SECURITY

Example: Ransomware

- Type of trojan horse that blocks user´s computer and encrypt all data on hard disk
- Message on Screen, like

  … due to illegal user activities the computer has been blocked on behalf of regulating authority; after online paying monetary penalty the access will be granted
- In most cases decryption without key is not possible
- Distribution with Botnets and Spam
- In most cases victims are paying penalty

Current Attacks and Implications

NETWORK & DATA SECURITY

Example: Bad USB (Source: heise security 31.07.2014)

- Firmware Manipulation of USB-Storage-Sticks: Communication (data transfer) between PC and Stick is carried out with SCSI protocol, that has no protective mechanisms and so can be reprogrammed with malware
- Malware infect victim system and enables infection of other connected sticks
- impact: e.g. deletion of data and files, modification of settings

Example: Backoff Point-of-Sale Malware (PoS) (Source: US-Cert Alert TA14-212A, 2014)

- Remote Desktop Applications permit connectivity to a computer from a remote location
- Attacker finds out access rights and installs PoS malware to manipulate online paying systems
- Attacker collects customers data (e.g. names, mailing addresses, credit/debit card numbers, phone numbers)
- Misuse of data, e.g. shopping with customers identity, purchasing personal data at great scale in the underground
- *APT functionality*: small malicious code (called stub) in explorer.exe that protects deletion, scans storage, has keylogging functionality and is able to reload further malware from C&C server

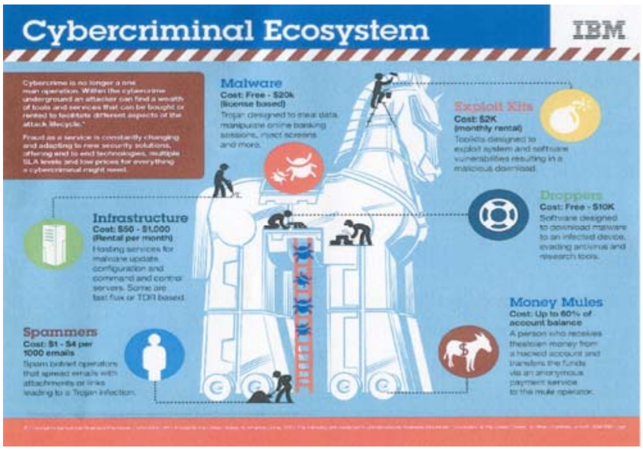
Current Attacks and Implications

NETWORK & DATA SECURITY

Cypercrime underground: Commoditization of Malware Distribution

Pay-Per-Install (PPI) Market:

- Value-chain from creation and distribution of malware to infect victim computers
- Provides a means for miscreants to outsource the global dissemination of their malware
- Consists of three main actors: clients (miscreants), PPI providers (services), affiliates (third parties)
- Typical PPI transactions: the service conducts downloader infections itself or via affiliates on victim computers; installation of client programs onto the target hosts (victims)


Cybercriminal Ecosystem
IBM
Cybercrime is no longer a one man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.
Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.
Malware
Cost: Free - $20k (license based)
Trojan designed to steal data, manipulate online banking sessions, inject screens and more.
Exploit Kits
Cost: $2K (monthly rental)
Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.
Infrastructure
Cost: $50 - $1,000 (Rental per month)
Hosting services for malware update configuration and command and control servers. Some are fast flux or TOR based.
Droppers
Cost: Free - $10K
Software designed to download malware to an infected device, evading antivirus and research tools.
Spammers
Cost: $1 - $4 per 1000 emails
Spam botnet operators that spread emails with attachments or links leading to a Trojan infection.
Money Mules
Cost: Up to 60% of account balance
A person who receives the stolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.

Perfect Infrastructure for Cybercrime: PPI marketplaces

Current Attacks and Implications

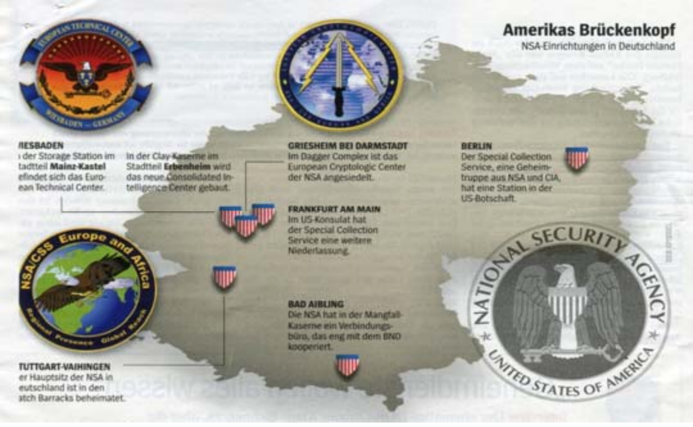
NETWORK & DATA SECURITY

NSA Locations in Germany

- Task of the National Security Agency: *Interception and decoding of all kinds of foreign communication, which might be of interest for US security*
- Tools disclose all interrelation in connection with data

Die Analyse erfasst strukturierte und unstrukturierte Informationen

Statistik-Tools decken in den Daten die Zusammenhänge auf


Amerikas Brückenkopf
NSA-Einrichtungen in Deutschland
European Technical Center Wiesbaden – Germany
NSA/CSS Europe and Africa
Regional Presence Global Reach
National Security Agency United States of America
IESBADEN
der Storage Station im tadtteil Mainz-Kastel efindet sich das European Technical Center.
In der Clay-Kaserne im Stadtteil Erbenheim wird das neue Consolidated Intelligence Center gebaut.
GRIESHEIM BEI DARMSTADT
Im Dagger Complex ist das European Cryptologic Center der NSA angesiedelt.
BERLIN
Der Special Collection Service, eine Geheimtruppe aus NSA und CIA, hat eine Station in der US-Botschaft.
FRANKFURT AM MAIN
Im US-Konsulat hat der Special Collection Service eine weitere Niederlassung.
BAD AIBLING
Die NSA hat in der Mangfall-Kaserne ein Verbindungsbüro, das eng mit dem BND kooperiert.
TUTTGART-VAIHINGEN
er Hauptsitz der NSA in eutschland ist in den atch Barracks beheimatet.

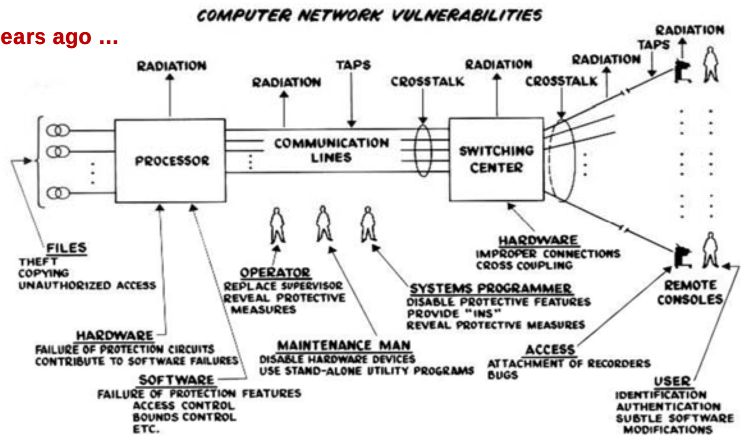
Source: Der Spiegel 25/2014

In principle: from abstract syntax to semantic

Metadata – Information – Intelligence

Current Attacks and Implications

It began many years ago …



Ware, W.: *Security Controls for Computer Systems*: Report of Defense Science Board Task Force on Computer Security – RAND Report R-609-1. Santa Monica 1967

Current Attacks and Implications

NSA Attacks (Edward Snowden´s disclosures)

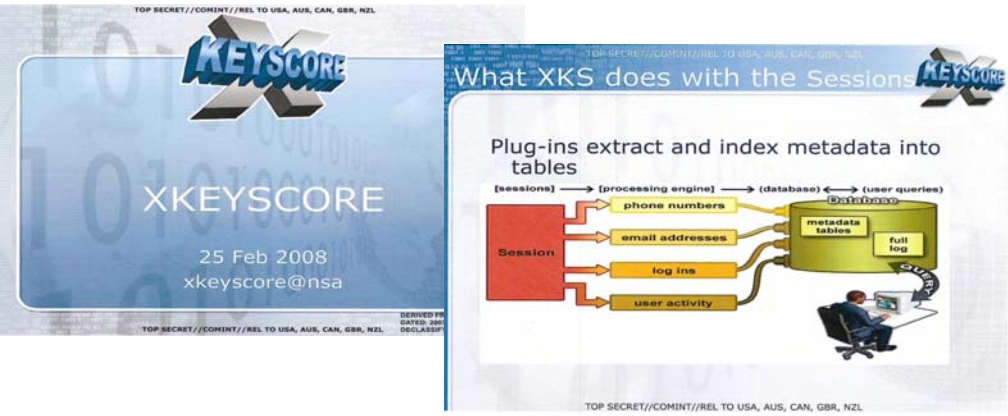
- Tapped facilities: *Facebook*, *Google, Yahoo*, also *Microsoft* and *Apple* !!!
  - Everybody leaves tracks in Web !
  - Preferences, frequently used websites, movement, …
- Eavesdrop of E-Mail- and Mobile communication
  - Tapped infrastructure notes, internet service provider
  - Gmail (Google Mail), …
  - Record communication via Whatsapp, Skype, Googletalk
- Analysis of photos (*Flickr* etc.) and videos (*Youtube* etc.)
  - Face recognition
  - Movement profiles (GPS data)
- Attacks on encrypted communication
  - ´Cracking´ weak Encryption algorithms
  - ´Place´ backdoors into tools of widespread encryption algorithms
  - Data harvesting bevor encryption
  - Chip ´Sabotage´
- Collaboration with other secret services (e.g. Data exchange to avoid legal conflicts)

"HE TOLD ME IT WAS ALL PERFECTLY LEGAL!"

Current Attacks and Implications

NETWORK & DATA SECURITY

Example: NSA Tool XKeyscore



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

XKEYSCORE

25 Feb 2008

xkeyscore@nsa

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

DERIVED FR
DATED: 200
DECLASSIF

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

What XKS does with the Sessions

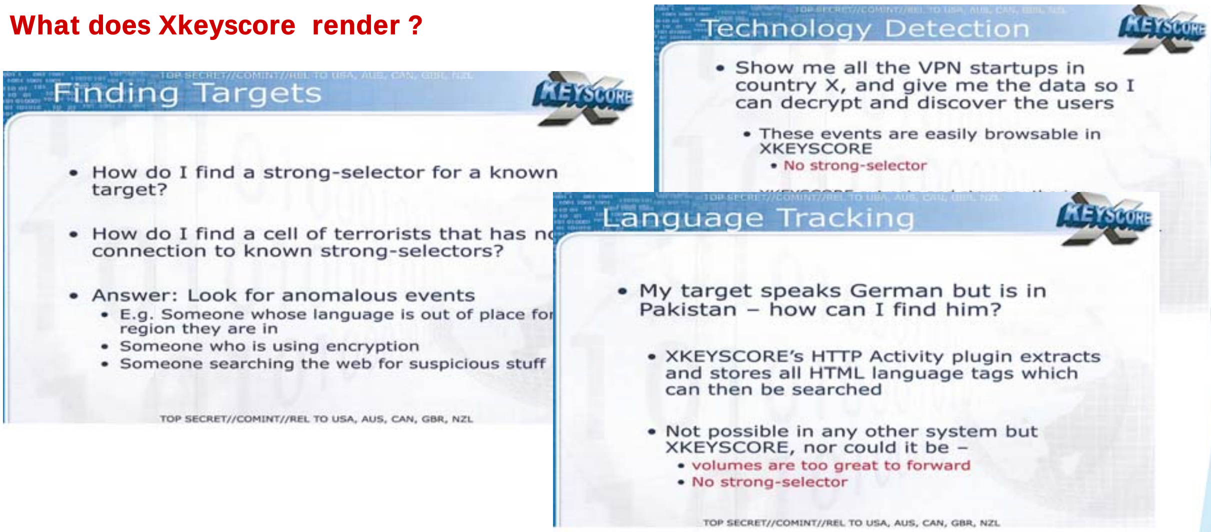
Plug-ins extract and index metadata into tables

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Current Attacks and Implications

NETWORK & DATA SECURITY

What does Xkeyscore render ?



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Finding Targets

- How do I find a strong-selector for a known target?
- How do I find a cell of terrorists that has no connection to known strong-selectors?
- Answer: Look for anomalous events
  - E.g. Someone whose language is out of place for region they are in
  - Someone who is using encryption
  - Someone searching the web for suspicious stuff

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Technology Detection

- Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users
  - These events are easily browsable in XKEYSCORE
    - No strong-selector

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Language Tracking

- My target speaks German but is in Pakistan – how can I find him?
  - XKEYSCORE's HTTP Activity plugin extracts and stores all HTML language tags which can then be searched
  - Not possible in any other system but XKEYSCORE, nor could it be –
    - volumes are too great to forward
    - No strong-selector

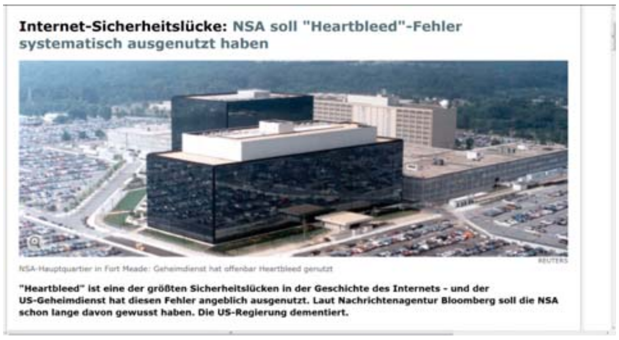
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Current Attacks and Implications

NETWORK & DATA SECURITY

Open Source – not secure too ?

- **Open SSL Heartbleed Bug** (CVE-2014-0160): Vulnerability into *TLS/DTLS-Heartbeat-Extension*
  - TLS-Heartbeat function enables the maintenance of connectivity between server and client
  - The bug leads to the leak of memory content from server to the client and vice versa
  - Reason: security protocol doesn´t verify payload size and content
  - More than 16 KByte server storage content will be sent (e.g. secret keys used to identify the service providers and to encrypt the traffic, user passwords)



Internet-Sicherheitslücke: NSA soll "Heartbleed"-Fehler systematisch ausgenutzt haben

NSA-Hauptquartier in Fort Meade: Geheimdienst hat offenbar Heartbleed genutzt

REUTERS

"Heartbleed" ist eine der größten Sicherheitslücken in der Geschichte des Internets - und der US-Geheimdienst hat diesen Fehler angeblich ausgenutzt. Laut Nachrichtenagentur Bloomberg soll die NSA schon lange davon gewusst haben. Die US-Regierung dementiert.

  - It is no design flaw, it is a programming mistake in popular OpenSSL library

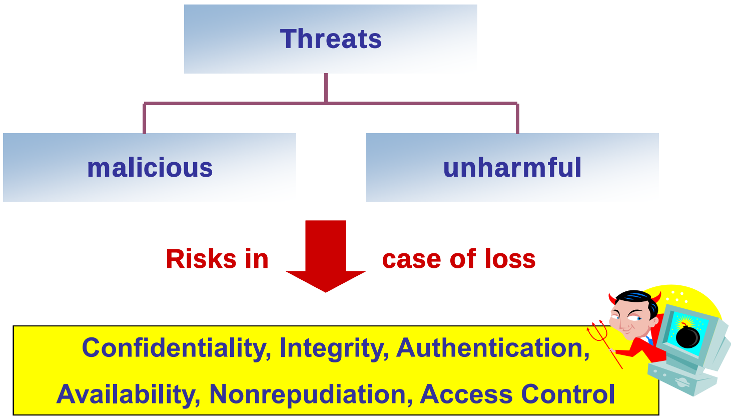
Hochschule Fulda
University of Applied Sciences

23.10.2015 Berlin Cyberattacks and Countermeasures 21 Ulrich Bühler

Some Countermeasures

NETWORK & DATA SECURITY

Security Objectives



Threats

malicious

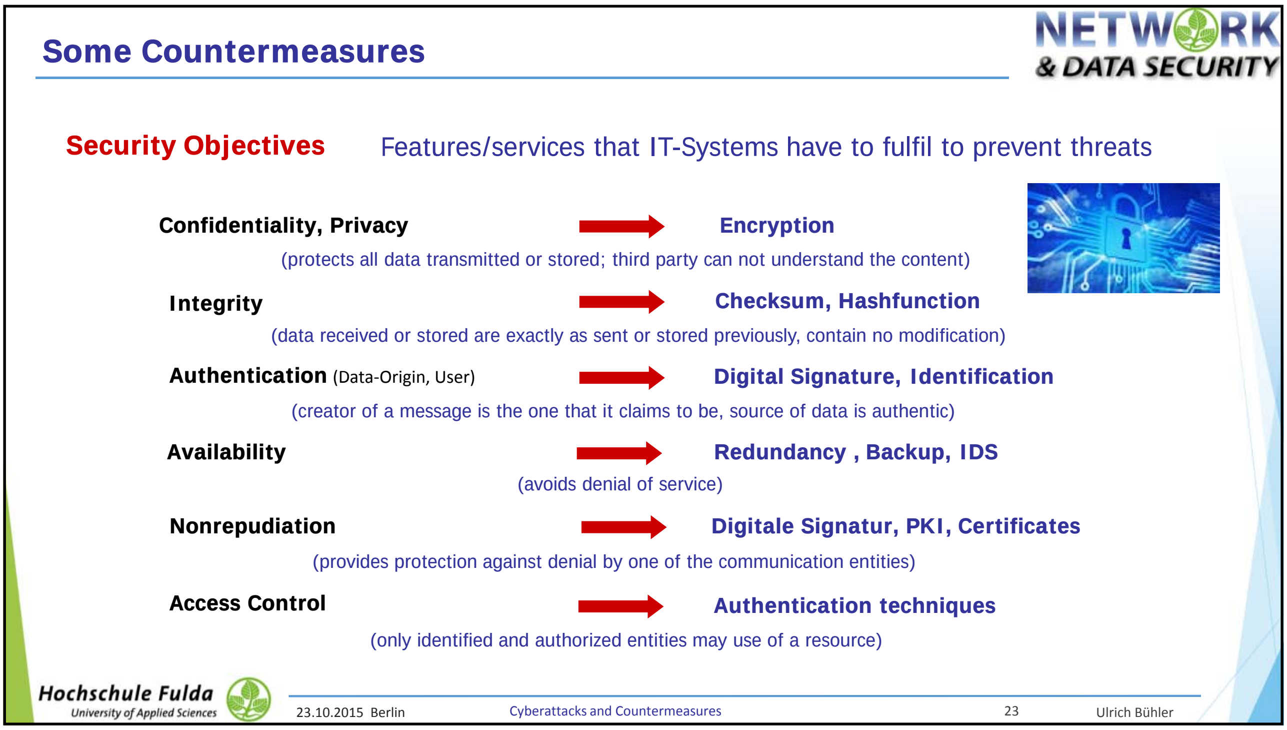
unharmful

Risks in case of loss

Confidentiality, Integrity, Authentication, Availability, Nonrepudiation, Access Control

Hochschule Fulda
University of Applied Sciences

23.10.2015 Berlin Cyberattacks and Countermeasures 22 Ulrich Bühler



Some Countermeasures

NETWORK & DATA SECURITY

Security Objectives Features/services that IT-Systems have to fulfil to prevent threats

Confidentiality, Privacy → **Encryption**

(protects all data transmitted or stored; third party can not understand the content)

Integrity → **Checksum, Hashfunction**

(data received or stored are exactly as sent or stored previously, contain no modification)

Authentication (Data-Origin, User) → **Digital Signature, Identification**

(creator of a message is the one that it claims to be, source of data is authentic)

Availability → **Redundancy , Backup, IDS**

(avoids denial of service)

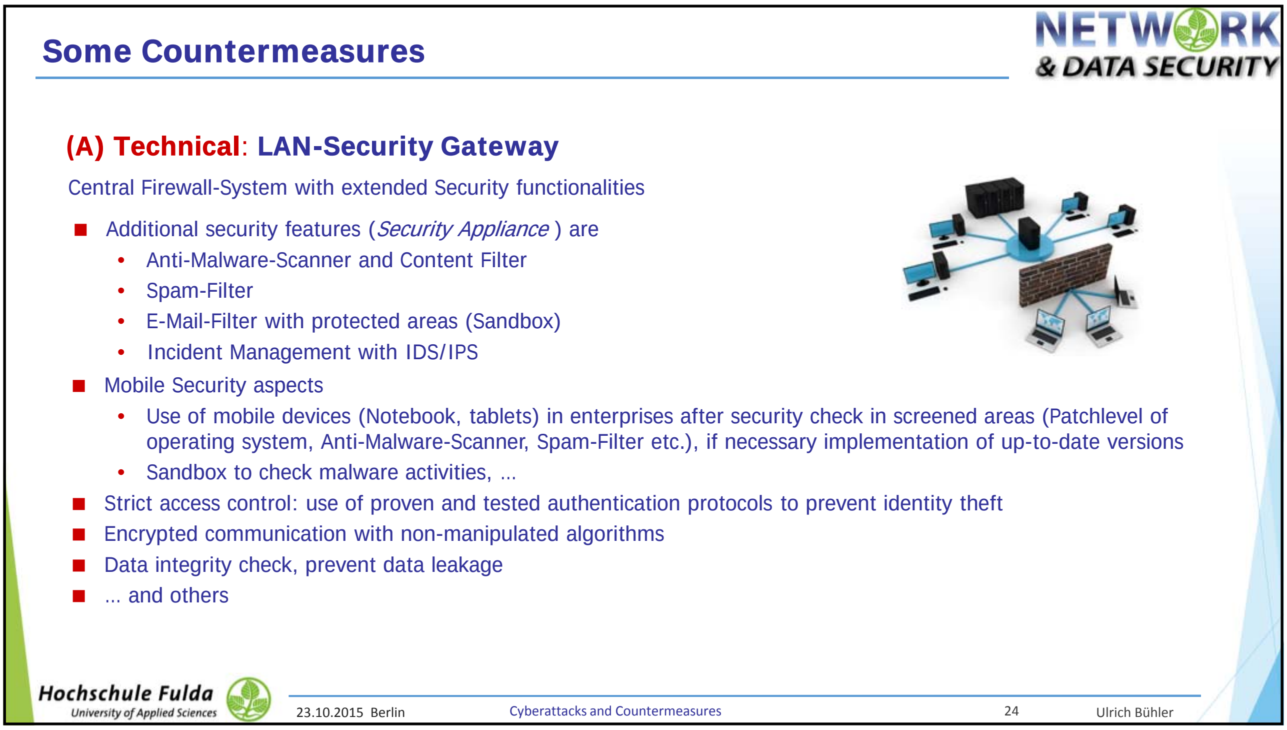
Nonrepudiation → **Digitale Signatur, PKI, Certificates**

(provides protection against denial by one of the communication entities)

Access Control → **Authentication techniques**

(only identified and authorized entities may use of a resource)

Hochschule Fulda
University of Applied Sciences



Some Countermeasures

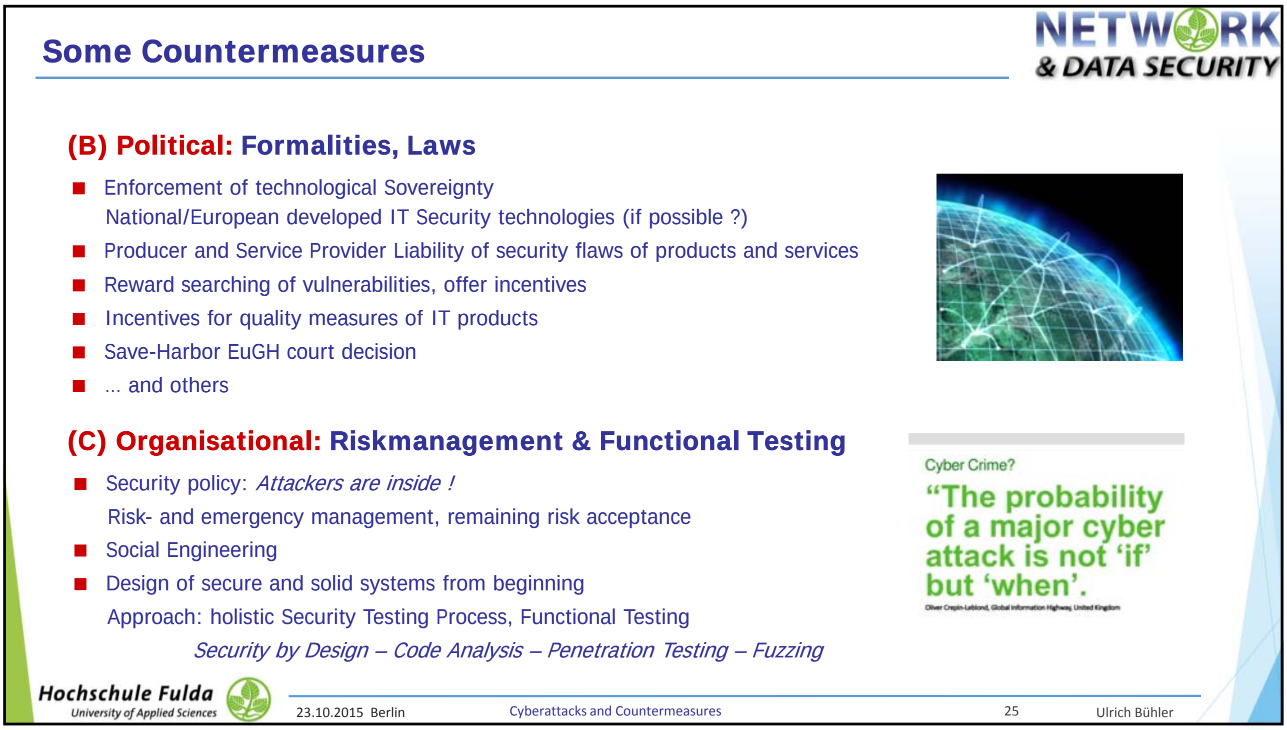
NETWORK & DATA SECURITY

(A) Technical: LAN-Security Gateway

Central Firewall-System with extended Security functionalities

- Additional security features (*Security Appliance*) are
  - Anti-Malware-Scanner and Content Filter
  - Spam-Filter
  - E-Mail-Filter with protected areas (Sandbox)
  - Incident Management with IDS/IPS
- Mobile Security aspects
  - Use of mobile devices (Notebook, tablets) in enterprises after security check in screened areas (Patchlevel of operating system, Anti-Malware-Scanner, Spam-Filter etc.), if necessary implementation of up-to-date versions
  - Sandbox to check malware activities, ...
- Strict access control: use of proven and tested authentication protocols to prevent identity theft
- Encrypted communication with non-manipulated algorithms
- Data integrity check, prevent data leakage
- ... and others

Hochschule Fulda
University of Applied Sciences



Some Countermeasures

NETWORK & DATA SECURITY

(B) Political: Formalities, Laws

- Enforcement of technological Sovereignty
  National/European developed IT Security technologies (if possible ?)
- Producer and Service Provider Liability of security flaws of products and services
- Reward searching of vulnerabilities, offer incentives
- Incentives for quality measures of IT products
- Save-Harbor EuGH court decision
- … and others

Cyber Crime?

“The probability of a major cyber attack is not ‘if’ but ‘when’.

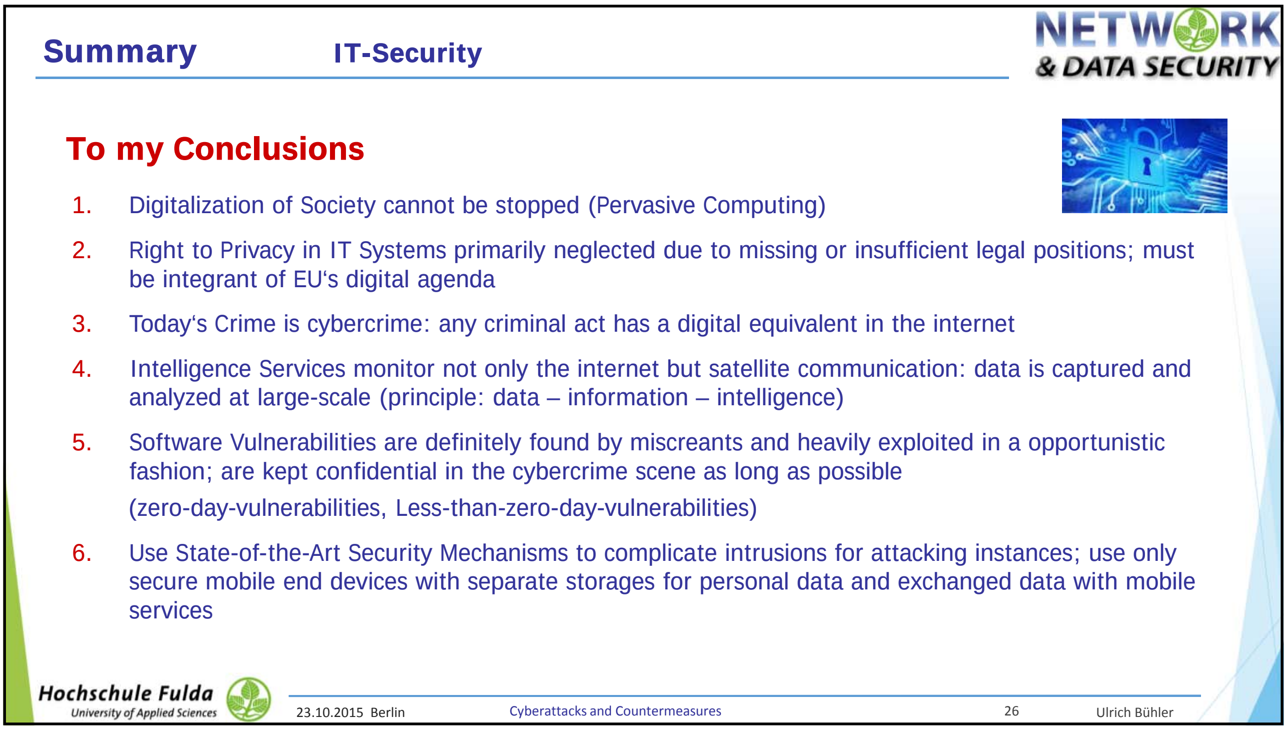
Oliver Crepin-Leblond, Global Information Highway, United Kingdom

(C) Organisational: Riskmanagement & Functional Testing

- Security policy: *Attackers are inside !*
  Risk- and emergency management, remaining risk acceptance
- Social Engineering
- Design of secure and solid systems from beginning
  Approach: holistic Security Testing Process, Functional Testing
  Security by Design – Code Analysis – Penetration Testing – Fuzzing

Hochschule Fulda
University of Applied Sciences

23.10.2015 Berlin Cyberattacks and Countermeasures 25 Ulrich Bühler



Summary IT-Security

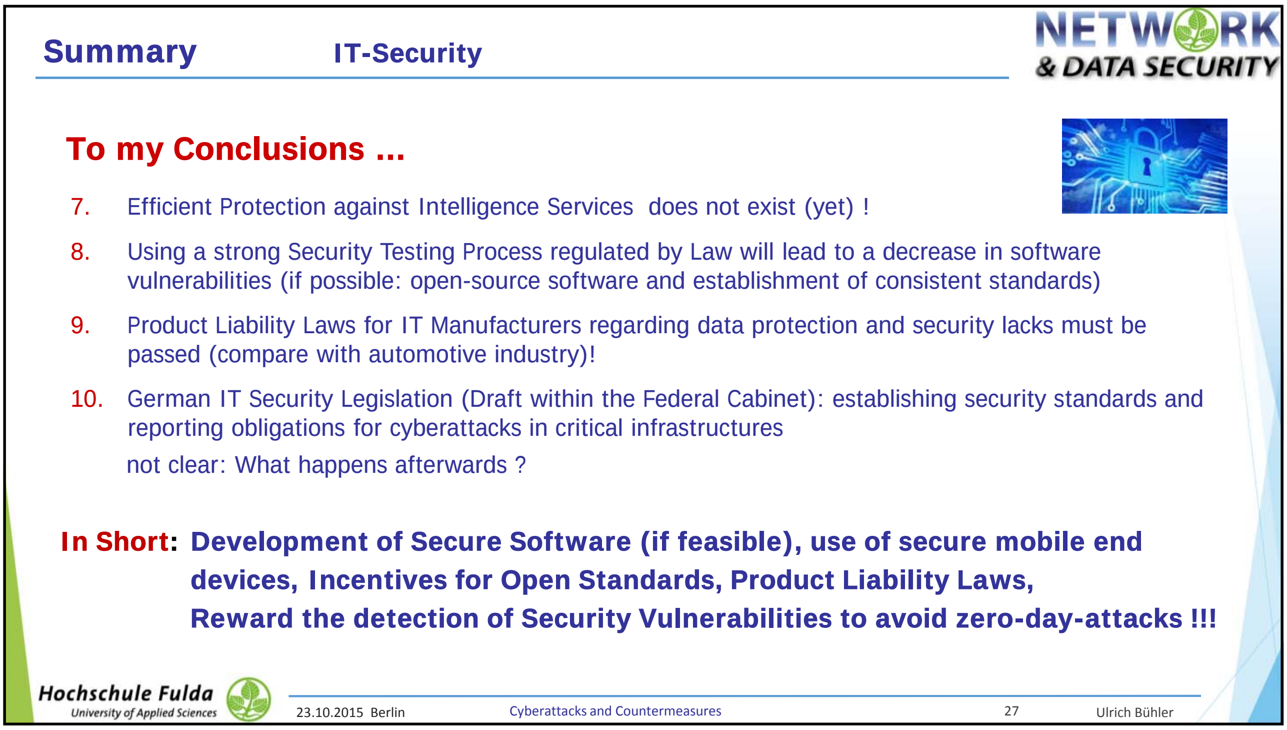
NETWORK & DATA SECURITY

To my Conclusions

1. Digitalization of Society cannot be stopped (Pervasive Computing)
2. Right to Privacy in IT Systems primarily neglected due to missing or insufficient legal positions; must be integrant of EU‘s digital agenda
3. Today‘s Crime is cybercrime: any criminal act has a digital equivalent in the internet
4. Intelligence Services monitor not only the internet but satellite communication: data is captured and analyzed at large-scale (principle: data – information – intelligence)
5. Software Vulnerabilities are definitely found by miscreants and heavily exploited in a opportunistic fashion; are kept confidential in the cybercrime scene as long as possible
   (zero-day-vulnerabilities, Less-than-zero-day-vulnerabilities)
6. Use State-of-the-Art Security Mechanisms to complicate intrusions for attacking instances; use only secure mobile end devices with separate storages for personal data and exchanged data with mobile services

Hochschule Fulda
University of Applied Sciences

23.10.2015 Berlin Cyberattacks and Countermeasures 26 Ulrich Bühler



Summary IT-Security

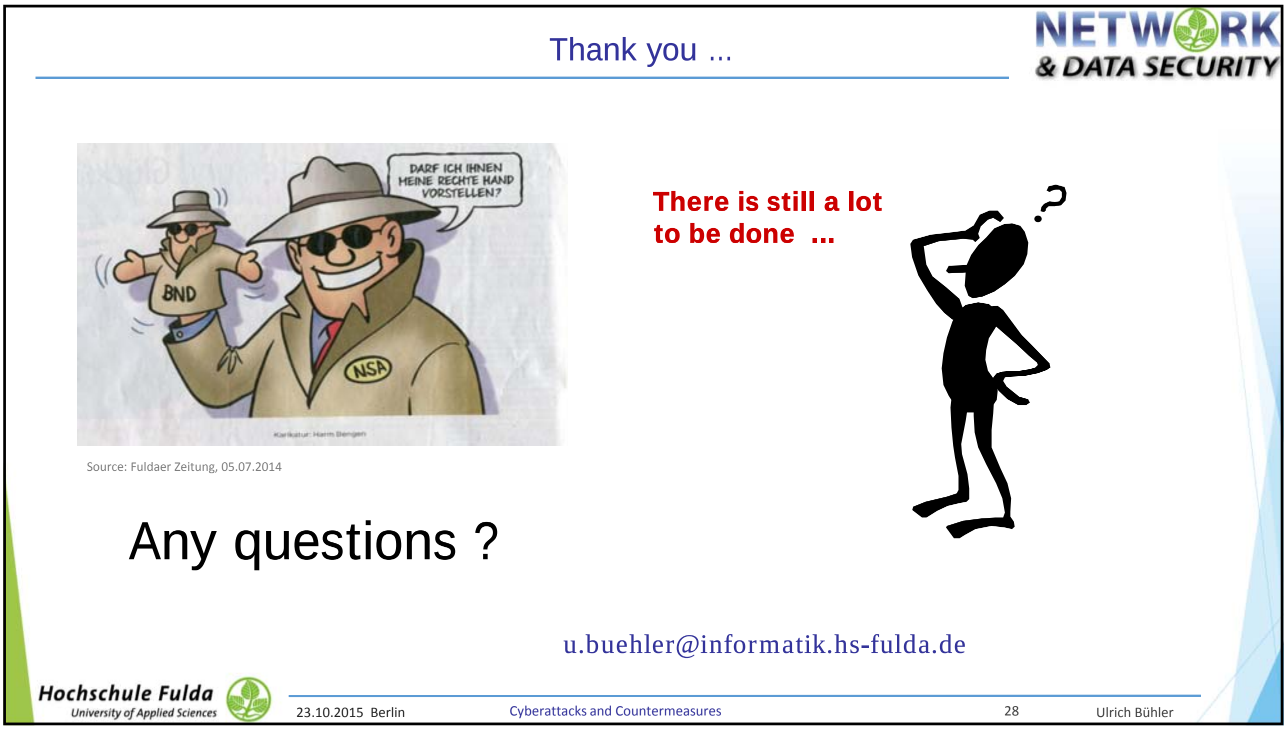
NETWORK & DATA SECURITY

To my Conclusions ...

7. Efficient Protection against Intelligence Services does not exist (yet) !
8. Using a strong Security Testing Process regulated by Law will lead to a decrease in software vulnerabilities (if possible: open-source software and establishment of consistent standards)
9. Product Liability Laws for IT Manufacturers regarding data protection and security lacks must be passed (compare with automotive industry)!
10. German IT Security Legislation (Draft within the Federal Cabinet): establishing security standards and reporting obligations for cyberattacks in critical infrastructures

    not clear: What happens afterwards ?

In Short: Development of Secure Software (if feasible), use of secure mobile end devices, Incentives for Open Standards, Product Liability Laws, Reward the detection of Security Vulnerabilities to avoid zero-day-attacks !!!



Thank you ...

NETWORK & DATA SECURITY

DARF ICH IHNEN MEINE RECHTE HAND VORSTELLEN?
BND
NSA
Karikatur: Harm Bengen

Source: Fuldaer Zeitung, 05.07.2014

There is still a lot to be done ...

Any questions ?

u.buehler@informatik.hs-fulda.de