Interreg
EUROPEAN UNION
Austria-Czech Republic
European Regional Development Fund

INFORMATICS

IT security

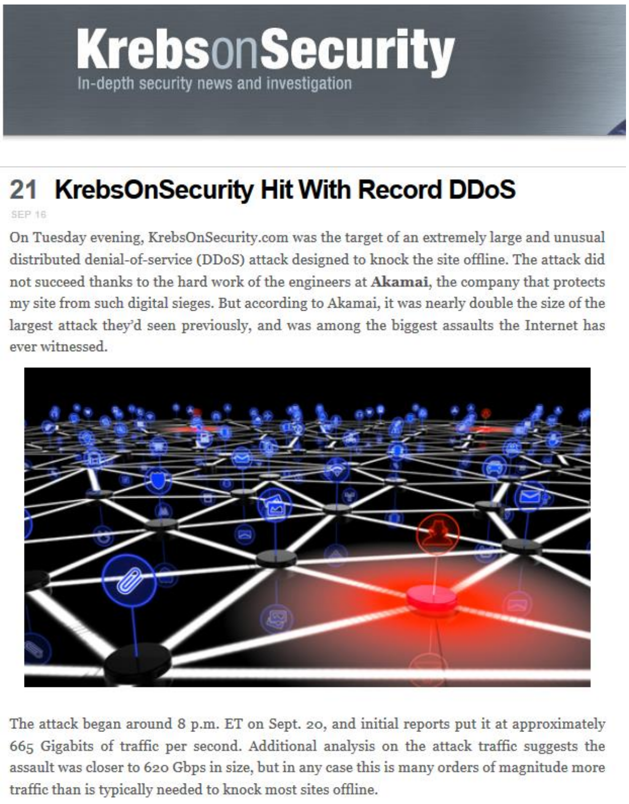
UNIVERSITY
OF APPLIED SCIENCES
UPPER AUSTRIA

VŠTE

EUROPEAN UNION

Contents

1. MOTIVATION



KrebsonSecurity

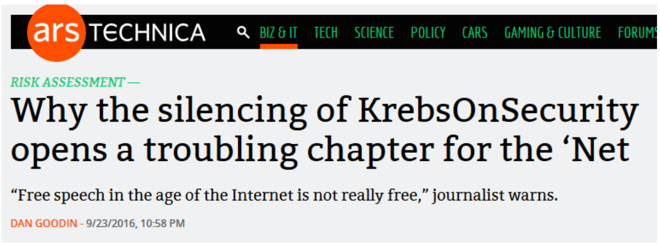
In-depth security news and investigation

21 SEP 16

KrebsOnSecurity Hit With Record DDoS

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

The attack began around 8 p.m. ET on Sept. 20, and initial reports put it at approximately 665 Gigabits of traffic per second. Additional analysis on the attack traffic suggests the assault was closer to 620 Gbps in size, but in any case this is many orders of magnitude more traffic than is typically needed to knock most sites offline.



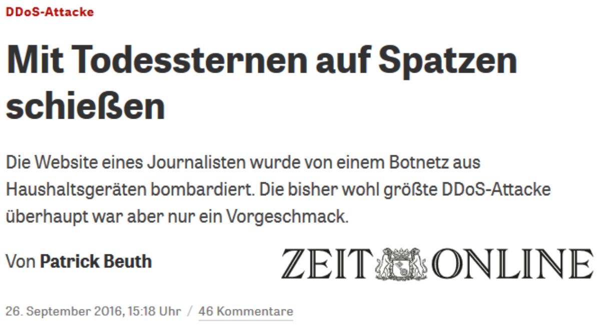
ars TECHNICA

RISK ASSESSMENT —

Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net

"Free speech in the age of the Internet is not really free," journalist warns.

DAN GOODIN - 9/23/2016, 10:58 PM



DDoS-Attacke

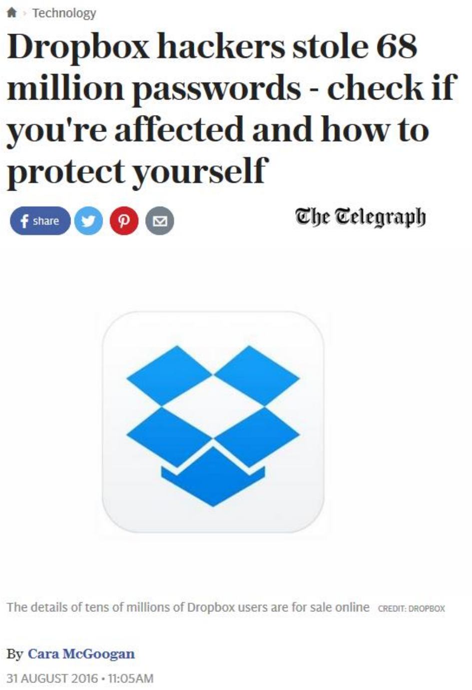
Mit Todessternen auf Spatzen schießen

Die Website eines Journalisten wurde von einem Botnetz aus Haushaltsgeräten bombardiert. Die bisher wohl größte DDoS-Attacke überhaupt war aber nur ein Vorgeschmack.

Von **Patrick Beuth**

ZEIT ONLINE

26. September 2016, 15:18 Uhr / 46 Kommentare



Technology

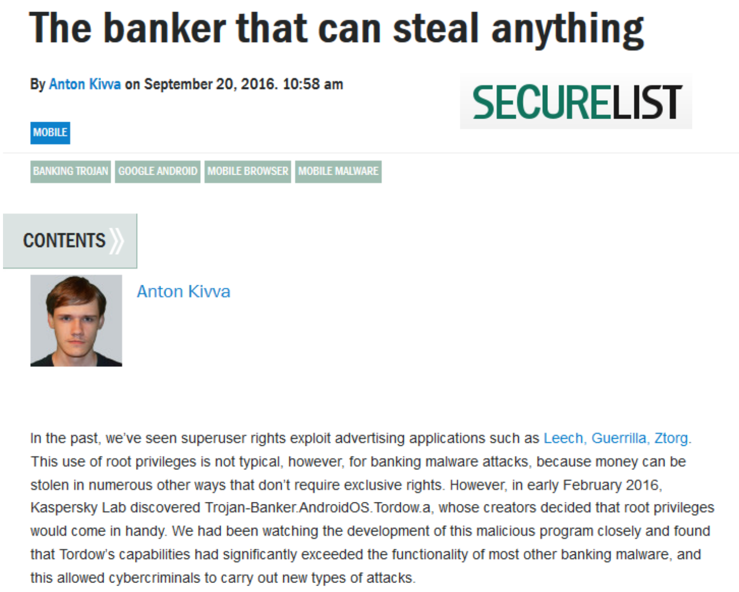
Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself

The Telegraph

The details of tens of millions of Dropbox users are for sale online CREDIT: DROPBOX

By Cara McGoogan

31 AUGUST 2016 • 11:05AM



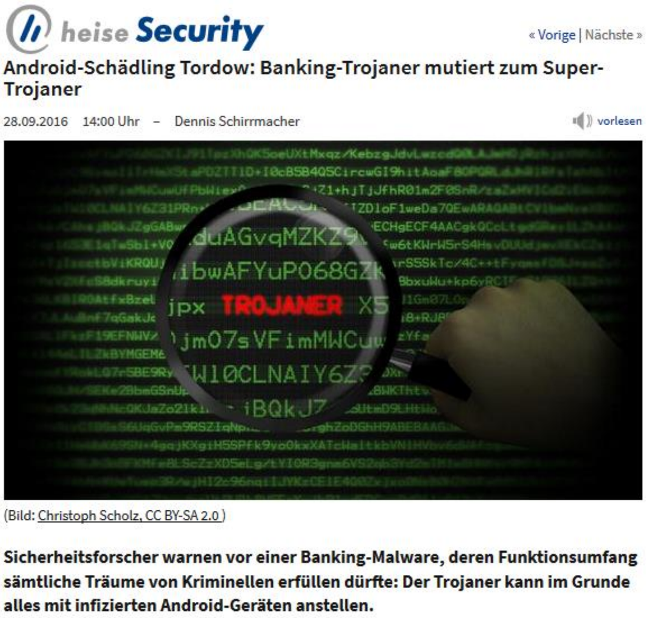
The banker that can steal anything

By Anton Kivva on September 20, 2016. 10:58 am

SECURELIST

Anton Kivva

In the past, we've seen superuser rights exploit advertising applications such as Leech, Guerrilla, Ztorg. This use of root privileges is not typical, however, for banking malware attacks, because money can be stolen in numerous other ways that don't require exclusive rights. However, in early February 2016, Kaspersky Lab discovered Trojan-Banker.AndroidOS.Tordow.a, whose creators decided that root privileges would come in handy. We had been watching the development of this malicious program closely and found that Tordow's capabilities had significantly exceeded the functionality of most other banking malware, and this allowed cybercriminals to carry out new types of attacks.

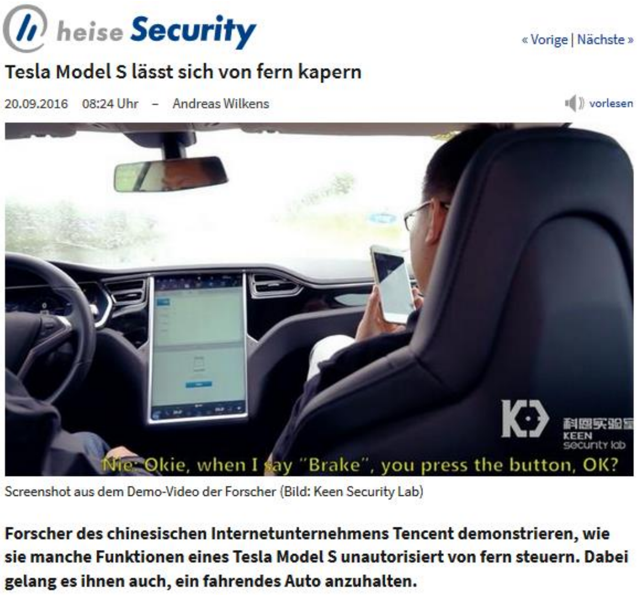


Android-Schädling Tordow: Banking-Trojaner mutiert zum Super-Trojaner

28.09.2016 14:00 Uhr – Dennis Schirrmacher

(Bild: Christoph Scholz, CC BY-SA 2.0)

Sicherheitsforscher warnen vor einer Banking-Malware, deren Funktionsumfang sämtliche Träume von Kriminellen erfüllen dürfte: Der Trojaner kann im Grunde alles mit infizierten Android-Geräten anstellen.

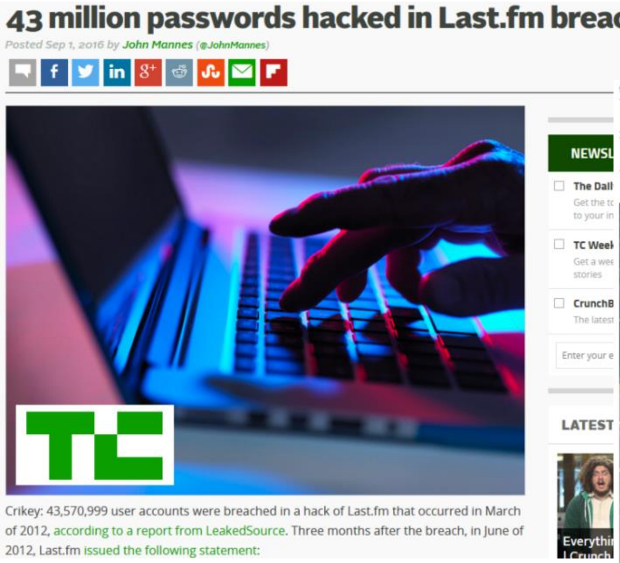


Tesla Model S lässt sich von fern kapern

20.09.2016 08:24 Uhr – Andreas Wilkens

Screenshot aus dem Demo-Video der Forscher (Bild: Keen Security Lab)

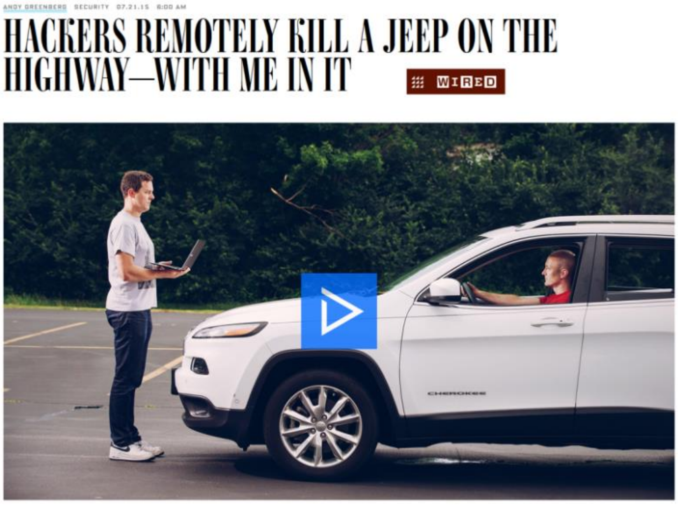
Forscher des chinesischen Internetunternehmens Tencent demonstrieren, wie sie manche Funktionen eines Tesla Model S unautorisiert von fern steuern. Dabei gelang es ihnen auch, ein fahrendes Auto anzuhalten.



43 million passwords hacked in Last.fm breach

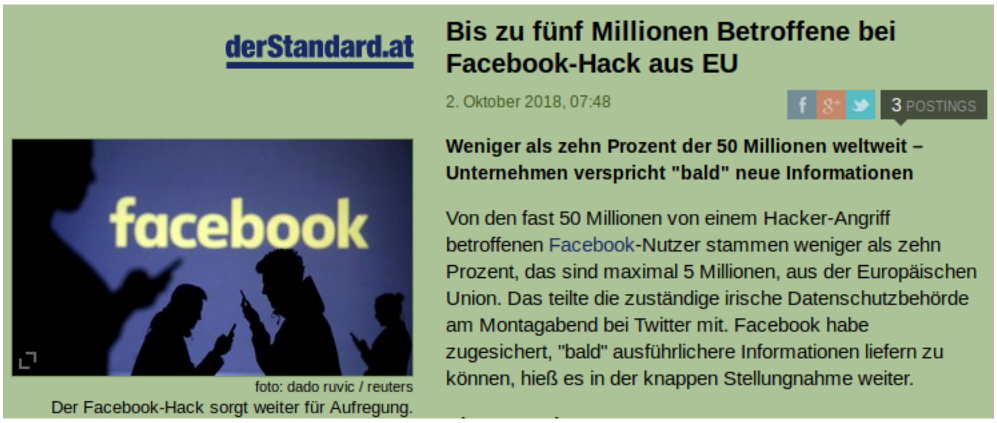
Posted Sep 1, 2016 by John Mannes (@JohnMannes)

Crikey: 43,570,999 user accounts were breached in a hack of Last.fm that occurred in March of 2012, according to a report from LeakedSource. Three months after the breach, in June of 2012, Last.fm issued the following statement:



ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



Bis zu fünf Millionen Betroffene bei Facebook-Hack aus EU

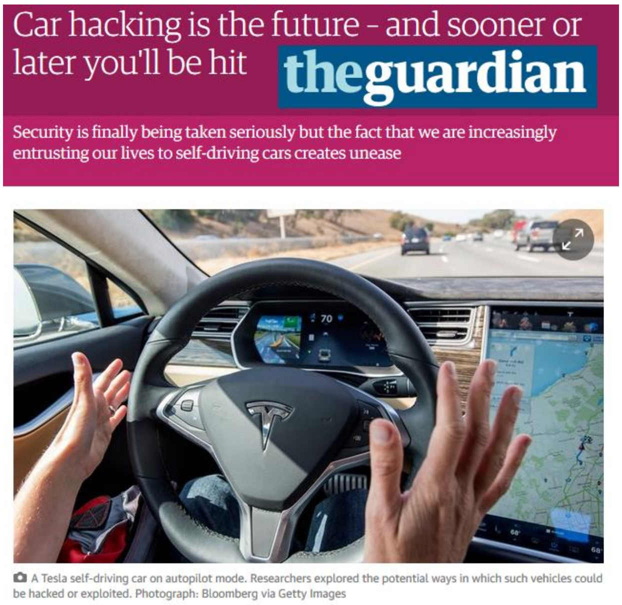
2. Oktober 2018, 07:48

foto: dado ruvic / reuters

Der Facebook-Hack sorgt weiter für Aufregung.

Weniger als zehn Prozent der 50 Millionen weltweit – Unternehmen verspricht "bald" neue Informationen

Von den fast 50 Millionen von einem Hacker-Angriff betroffenen Facebook-Nutzer stammen weniger als zehn Prozent, das sind maximal 5 Millionen, aus der Europäischen Union. Das teilte die zuständige irische Datenschutzbehörde am Montagabend bei Twitter mit. Facebook habe zugesichert, "bald" ausführlichere Informationen liefern zu können, hieß es in der knappen Stellungnahme weiter.

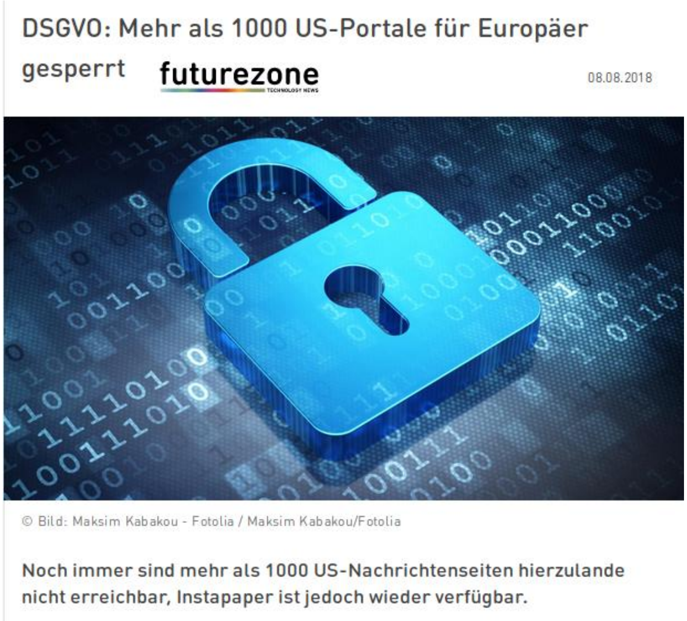


Car hacking is the future – and sooner or later you'll be hit

theguardian

Security is finally being taken seriously but the fact that we are increasingly entrusting our lives to self-driving cars creates unease

A Tesla self-driving car on autopilot mode. Researchers explored the potential ways in which such vehicles could be hacked or exploited. Photograph: Bloomberg via Getty Images



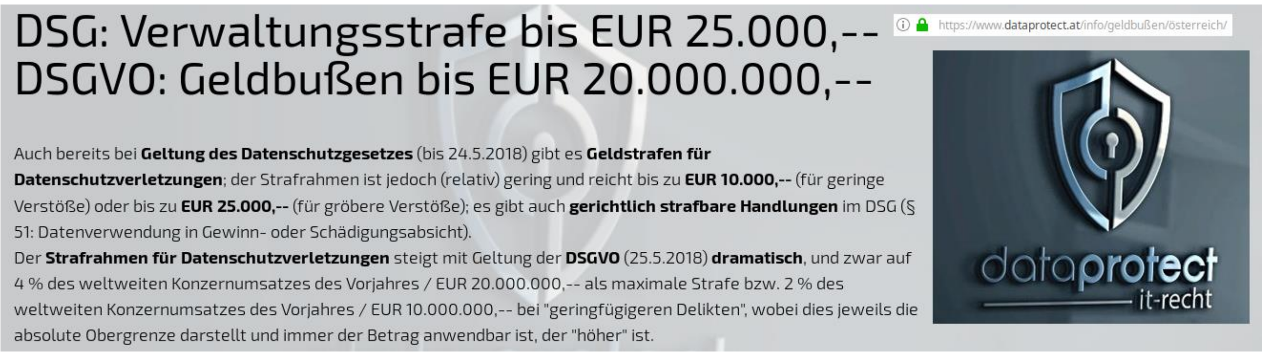
DSGVO: Mehr als 1000 US-Portale für Europäer gesperrt

futurezone

08.08.2018

© Bild: Maksim Kabakou - Fotolia / Maksim Kabakou/Fotolia

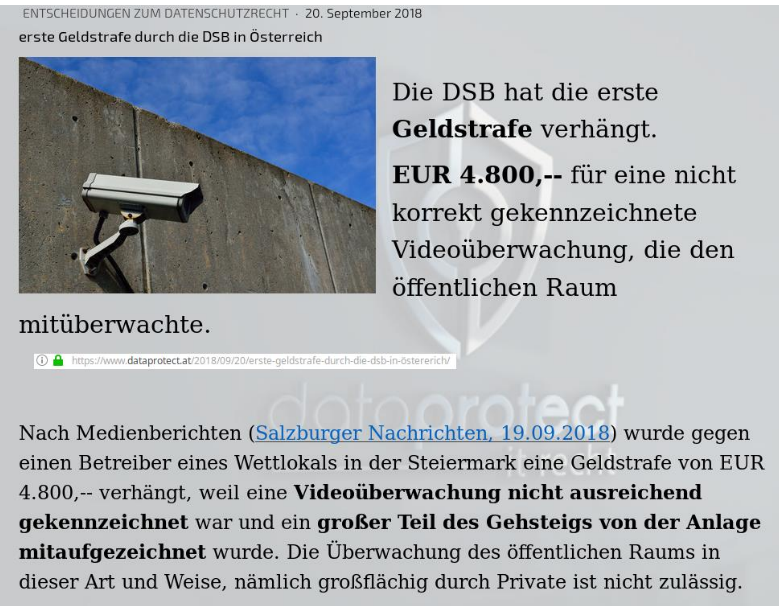
Noch immer sind mehr als 1000 US-Nachrichtenseiten hierzulande nicht erreichbar, Instapaper ist jedoch wieder verfügbar.



DSG: Verwaltungsstrafe bis EUR 25.000,--
DSGVO: Geldbußen bis EUR 20.000.000,--

https://www.dataprotect.at/info/geldbußen/österreich/

Auch bereits bei **Geltung des Datenschutzgesetzes** (bis 24.5.2018) gibt es **Geldstrafen für Datenschutzverletzungen**; der Strafrahmen ist jedoch (relativ) gering und reicht bis zu **EUR 10.000,--** (für geringe Verstöße) oder bis zu **EUR 25.000,--** (für gröbere Verstöße); es gibt auch **gerichtlich strafbare Handlungen** im DSG (§ 51: Datenverwendung in Gewinn- oder Schädigungsabsicht).
Der **Strafrahmen für Datenschutzverletzungen** steigt mit Geltung der **DSGVO** (25.5.2018) **dramatisch**, und zwar auf 4 % des weltweiten Konzernumsatzes des Vorjahres / EUR 20.000.000,-- als maximale Strafe bzw. 2 % des weltweiten Konzernumsatzes des Vorjahres / EUR 10.000.000,-- bei "geringfügigeren Delikten", wobei dies jeweils die absolute Obergrenze darstellt und immer der Betrag anwendbar ist, der "höher" ist.



ENTSCHEIDUNGEN ZUM DATENSCHUTZRECHT · 20. September 2018

erste Geldstrafe durch die DSB in Österreich

Die DSB hat die erste **Geldstrafe** verhängt.

EUR 4.800,-- für eine nicht korrekt gekennzeichnete Videoüberwachung, die den öffentlichen Raum mitüberwachte.

https://www.dataprotect.at/2018/09/20/erste-geldstrafe-durch-die-dsb-in-österreich/

Nach Medienberichten (Salzburger Nachrichten, 19.09.2018) wurde gegen einen Betreiber eines Wettlokals in der Steiermark eine Geldstrafe von EUR 4.800,-- verhängt, weil eine **Videoüberwachung nicht ausreichend gekennzeichnet** war und ein **großer Teil des Gehsteigs von der Anlage mitaufgezeichnet** wurde. Die Überwachung des öffentlichen Raums in dieser Art und Weise, nämlich großflächig durch Private ist nicht zulässig.

- Strong dependence of modern society on ICT (especially critical infrastructures).

- ICT is becoming the Critical Information Infrastructure (CII)

- The following trends make the protection of ICT a central issue (according to Eckert2008, among others):
    - Globalization
    - Mobility (Smartphone, Information at your fingertips)
    - Networking
    - Ubiquitous/Pervasive Computing, Internet of Things (IoT)
    - Industry x.0
    - Smart Home/Grid/Car/*
    - Cyber War/Warfare/Espionage/*

- Conclusion: Protection of ICT is of central importance for society!

2. PROTECTION OBJECTIVES OF INFORMATION SECURITY

Information security (or IT security) has the task of ensuring the following protection goals (basic values) [Stallings2006]:

1. Confidentiality
2. Integrity C-I-A
3. Availability
4. Authenticity
5. Accountability or non-repudiation

2.1. Confidentiality

- The protection of data from unauthorized disclosure. [Stallings2006]
- **Traffic Flow Confidentiality** = Protection from traffic data analysis
- Confidentiality in daily life
  - Confidentiality of Letters & Telecommunications Confidentiality
  - Official secrecy
  - Confession secret
  - Duty of confidentiality of attorneys/notaries/doctors
  - Non-disclosure agreements/NDAs
- Accessible by encryption (Encryption)
  - Symmetric encryption
    - a common shared key (same key for encrypting and decrypting) => key distribution problem; stream/block ciphers, substitution & transposition
  - Asymmetric encryption

        - public and private key (public key for encrypting and private key for decrypting) => key distribution problem solved, algorithmically more complex and therefore slower

    - Practice hybrid: Exchange of a generated session key via asymmetric crypto and then symmetric encryption

2.2. Integrity

- The assurance that data received are exactly as sent by an authorized entity (i.e. contain no modification, insertion, deletion, or replay). [Stallings2006]

- Changes (e.g. due to transmission errors or active attacks) **cannot** be **prevented** but can be **detected**!

- Authenticity and integrity are often seen as a unity. The one is useless without the other.

- Accessible through the use of (**cryptographic**) **checksums**, e.g.
    - CRC (Cyclic Redundancy Check) only for transmission errors
    - (Keyed-Hash) Message Authentication Code (MAC, HMAC)
    - Digital signatures

A **cryptological hash function** or **cryptographic hash function** is a special form of hash function which is collision resistant or a one-way function (or both).

A hash function is a function that maps a string of any length to a string of fixed length. Mathematically this function is not injective and not necessarily surjective.

2.3. Availability

- Availability is the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. [Stallings2006]

- What types of performance?
    - Usable or applicable
    - Sufficient capacity
    - Clear progress and/or clearly defined waiting times
    - Completion within acceptable timeframe
    - ...

- Approaches to the implementation/guarantee of availability
    - Technical: fault tolerance and redundancy through e.g. RAID, clustering, ..., mirrored data centers, uninterruptible power supply (UPS), ...
    - Organizational: Service Level Agreements (SLAs), Availability Classes

- Availability classes
    - 2-6: 99% (failure of ~ 90 hours per year)
    - 99.9%, ... to 99.9999% (= failure of ~ 30 seconds per year!)

2.4. Authenticity

- Authenticity
    - **Entity authenticity** = I know who I'm communicating with
    - **Data origin authenticity** = I know who the data comes from

- Authentication and authentication

- The assurance that the communicating entity is the one that it claims to be. [Stallings2006]

- Authentication features = feature with which a participant can be authenticated
    - Based on knowledge (PIN, password)
    - Based on ownership (key, card)
    - Based on property (biometric characteristics such as fingerprint, iris, voice, signature, retina, ...)
        - Retina = Back of the eye (infrared scan)
        - Iris Scan (using normal optical camera)

- Access Control (Access Control)
    - Authenticity is a prerequisite for access control!

2.5. Access Control

- The prevention of unauthorized use of resources. [Stallings2006]

- The **authenticity** of the accessing entity **must be ensured**.

- The following is checked
    - Who can have access to a resource,
    - the conditions under which the access may take place, and
    - what rights the accessing entity may have.

- Principle of necessary knowledge (**Need-to-know principle**)

- Basic models
    - Discretionary Access Control (DAC)
        - Definition of rights exclusively on the basis of user identity
    - Mandatory Access Control (MAC)
        - Not only user identity but additional rules and features
    - Role Based Access Control (RBAC)
        - Role-based assignment of rights, i.e. not on the basis of user identity but on the basis of user role (group membership)

2.6. Accountability or non-repudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. [Stallings2006]

- **Non-repudiation of emission** = Sender cannot deny sending the message.

- **non-repudiation of receipt** = recipient cannot deny receipt of the message

- Accessible through the use of digital signatures (not through [H]MACs!).

3. INFORMATION VS. IT SECURITY

- Information Security (InfoSec) deals with **data in any form** (electronic, written, verbal).
- IT Security (IT-Sec) focuses exclusively on **electronic data processing**.
- Definition of IT security (transferable to InfoSec, according to [BSI1992]):

> IT security is the state of an IT system in which the **risks** that are present when using this IT system due to **threats** are limited to a **tolerable (acceptable) level** by **appropriate measures**.

- Highly important (!!) consequence: There is no absolute safety!

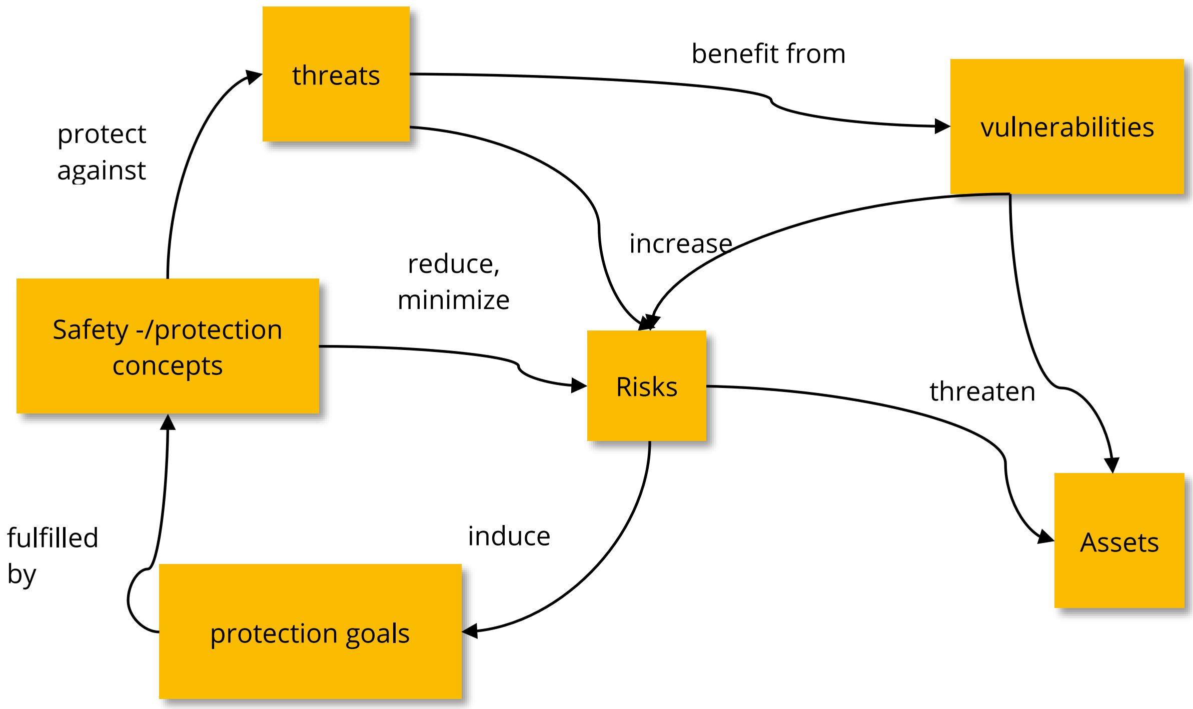
4. WEAKNESS, THREAT AND RISK

- A **weakness/vulnerability** is a weakness of the system or a point at which the system may be vulnerable (through an **exploit**).

- **Threats** result from possible attacks that exploit one or more vulnerabilities in a system to compromise one or more protection goals.

- The **risk R** of a threat is the **probability E** of the occurrence of a loss event and the **amount of the potential loss S** that can result from it: R = E · S

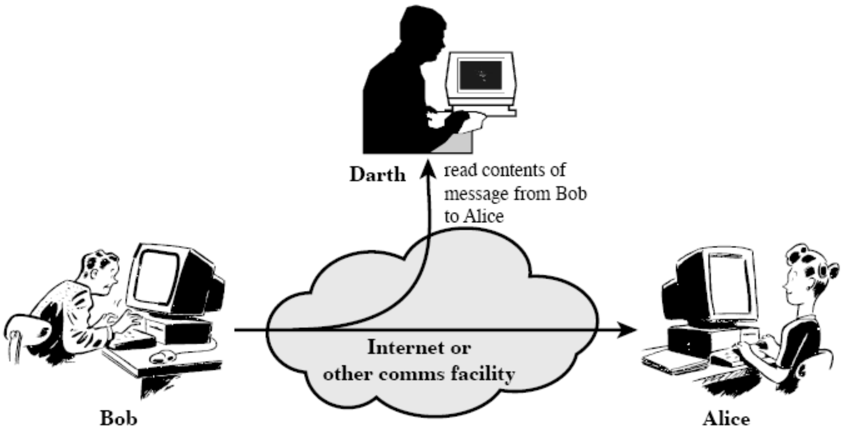
4.1. Interrelations



5. ATTACK CATEGORIES, LEVELS & CAUSES

Passive Attacks - Eavesdropping

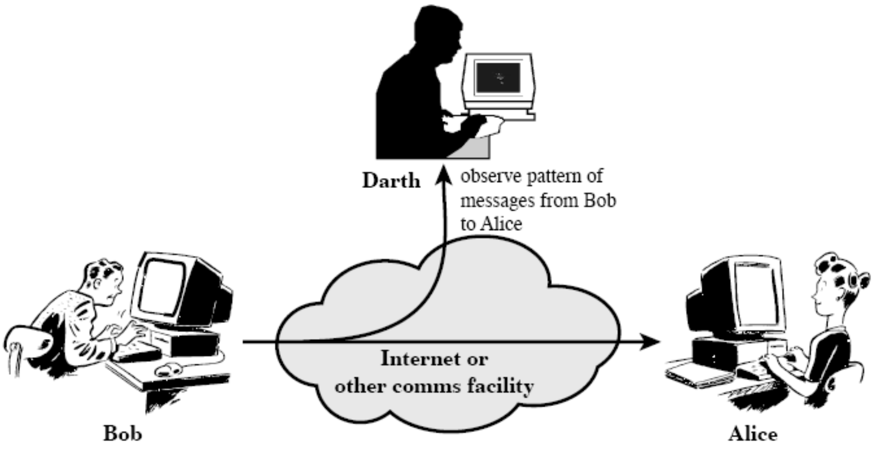
- Attacker intercepts the communication channel but does not actively intervene in the communication.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents

Passive Attacks – Traffic Analysis

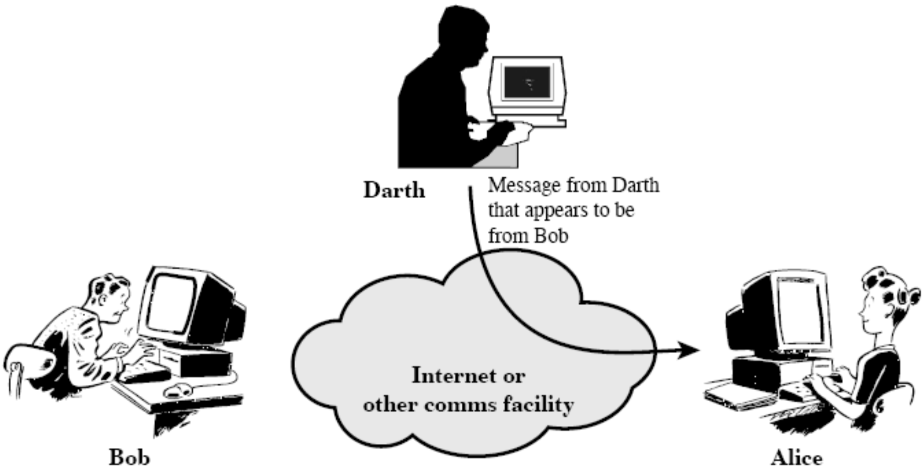
- With an encrypted data channel, a passive attacker may be able to perform a traffic analysis (who communicates with whom and when?).


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

Active Attacks – Masquerade

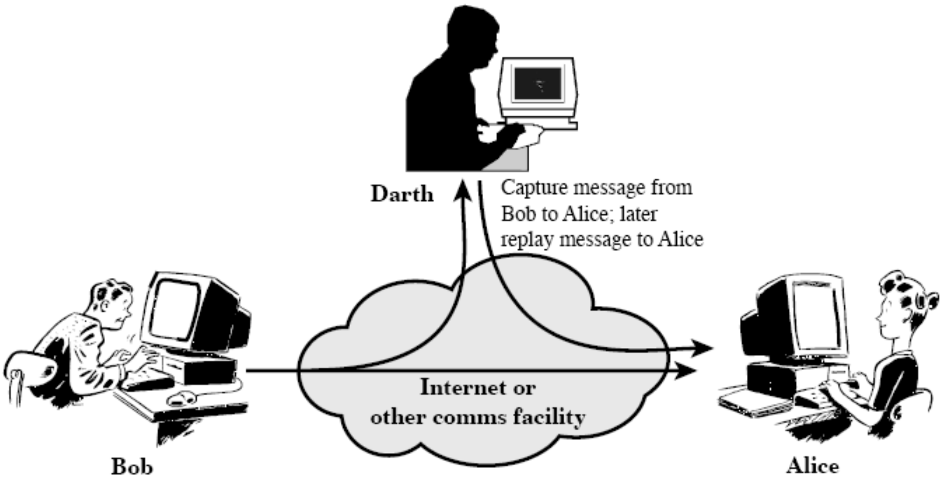
- Masquerade: Attacker impersonates someone else


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Active Attacks – Insertion & Replay

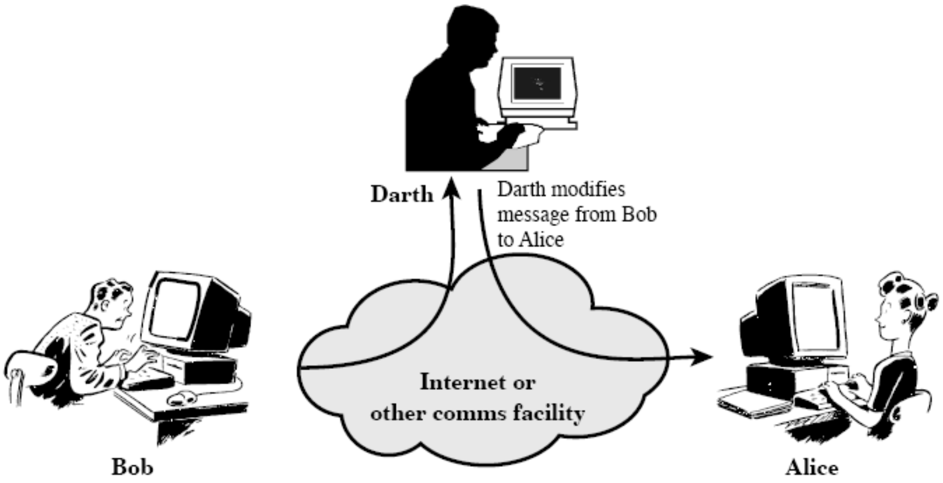
- Insertion: Attacker adds messages (parts) to a communication.
- Replay: Attacker sends recorded data again at a later time.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Active Attacks – Modification

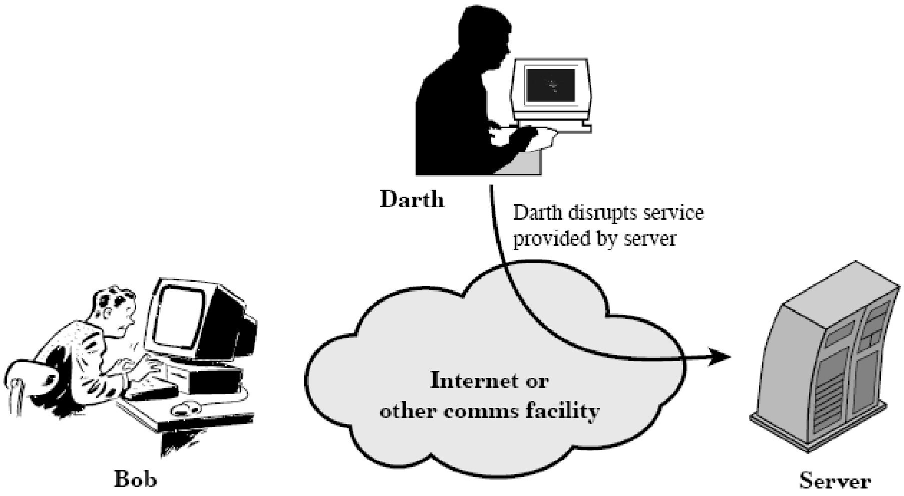
- An attacker changes a communication by delaying, changing or deleting messages.


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Active Attacks – Denial of Service

- Attacker disrupts the availability of communication facilities


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

5.1. Current attack levels (excerpt)

- Network
  - Botnets
  - (Distributed) Denial of Service, Reflection, Amplification
  - Spam (Unsolicited Commercial/Bulk E-Mail, Social Media Spam)
  - Man-in-the-middle attacks (e.g. for reading/modifying communication)

- Applications (especially web applications, see OWASP Top 10), e.g.
  - Injektion (z. B. SQL Injection, Command Injection)
  - Standortübergreifendes Scripting (XSS)
  - Betriebsübergreifende Antragsfälschung (CSRF)
  - Verunstaltungen
  - Pufferüberläufe

- User
  - Social Engineering
  - (Spear) Phishing
  - Scareware, Ransomware
  - Spam

5.2. Causes

- Missing/Deficient identity verification
  - e.g. weak authentication procedures, unilateral authentication, ...

- Missing/Deficient Input Validation
  - e.g. user entries in web applications are not checked on the server side

- Psychological deficiencies and obstacles
  - e.g. Social Engineering

- Factors cost and time in product development
  - e.g. short release cycles, missing tests, security not integrated into development processes

- Organisational deficiencies
  - e.g. missing security management, missing user awareness, ...

6.ATTACKER TYPES & THEIR MOTIVATION

- Amateurs (Script Kiddies)
    - Responsible for most (automated) attacks
    - Few in-depth knowledge Application of ready-made attack tools
    - Motives: Prestige, personal revenge, boredom

- Crackers vs. Hackers (Blackhats vs. Whitehats)
    - Crackers are malicious hackers (terminology unclear)
    - Deep technical understanding (students, computer scientists)
    - Motives: Prestige, intellectual challenge

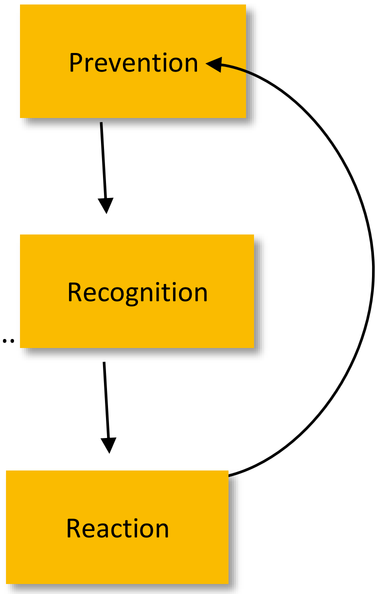
- Criminals (Cybercrime)
    - Classic criminals who change profession only for reasons of profit
    - Spamming, online extortion, bulletproof hosting/services, botnets (rental), …
    - Well organised networks with links to organised crime (e.g. Russian Business Network, Silk Road, …)
    - Motives: Profits

- Terrorists (cyber-terrorism)
    - IT as attack target Damage/destroy target infrastructure
    - Propaganda purposes
    - Communication and organization

- Countries and their military/ intelligence apparatuses (cyber war(fare), cyber espionage)
    - Switching off the IT infrastructure as a target of military attacks
    - Economic, political and military espionage (China, USA)
    - The Internet as a weapon
    - Examples: Stuxnet, Flame, Regin, NSA surveillance scandal

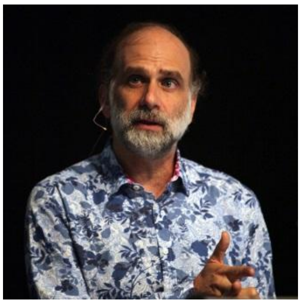
7. CLASSIFICATION OF SECURITY MEASURES

- Preventive measures (a priori)
  - e.g. authentication, access control, deployment of encryption, firewalls, hardening of systems, Security concept, security policy, creating awareness, ...
- Recognition measures
  - Dynamic at runtime
  - z. B. Firewalls, intrusion detection systems, log-analysis, ...
- Damage limitation measures (a posteriori)
  - e.g. tightening of controls, improvement of Security measures, Internet connection caps, ...



8. CONTINUOUS HOLISM IN INFORMATION SECURITY

Security is not a product; it‘s process!



Bruce Schneier
Photograph by Rama, Cc-by-sa-2.0-fr, from Wikimedia Commons

- Holistic approach is a critical success factor for IT/information security
  - e.g. firewall to filter traffic, but users can connect WLAN access points to the network
  - e.g. accesses to the systems are protected with passwords attached to the black board
  - e.g. users write down their Windows passwords on post-it's on their monitors

- IT/information security requires a combination of technical and organisational measures!

- IT/information security in the company must be supported by the management!

- IT/information security must be continuously lived and improved (examples?)!

8.1. Safety Standards

- Security management/security process, e.g.
  - ISO 27000 family
  - BSI basic protection standards 100-1, 100-2, 100-3 and 100-4

- System security (certification of products), e.g.
  - TCSEC (Trusted Computer System Evaluation Criteria)
  - ITSEC (Information Technology Security Evaluation Criteria)
  - Common Criteria for Information Technology Security Evaluations (ISO 15408)

- Action catalogs (technical/organizational), e.g.
    - BSI basic protection catalogues

- Other relevant standards ([IT] governance, compliance), e.g.
    - COBIT (Control Objectives for Information and Related Technology)
    - ITIL (IT Infrastructure Library)

8.2. Legal norms / laws

- Austrian Strategy for Cyber Security (ÖSCS)
    - Future: Austrian Cyber Security Act

- EU Directive on measures to ensure a high level of common network and information security (NIS Directive)
    - Incorporation into the Austrian Cyber Security Act

- EU Basic Data Protection Regulation

9. LITERATURE

[Eckert2008] Eckert, C., Vorlesungsskript zur VO IT-Sicherheit, TU Darmstadt, SS 2008

[Stallings2006] Stallings, W., Cryptography and Network Security, 4th edition, Prentice Hall, 2006

[BSI1992] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0, März 1992,

[BSI2005] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch, Stand 2005