Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

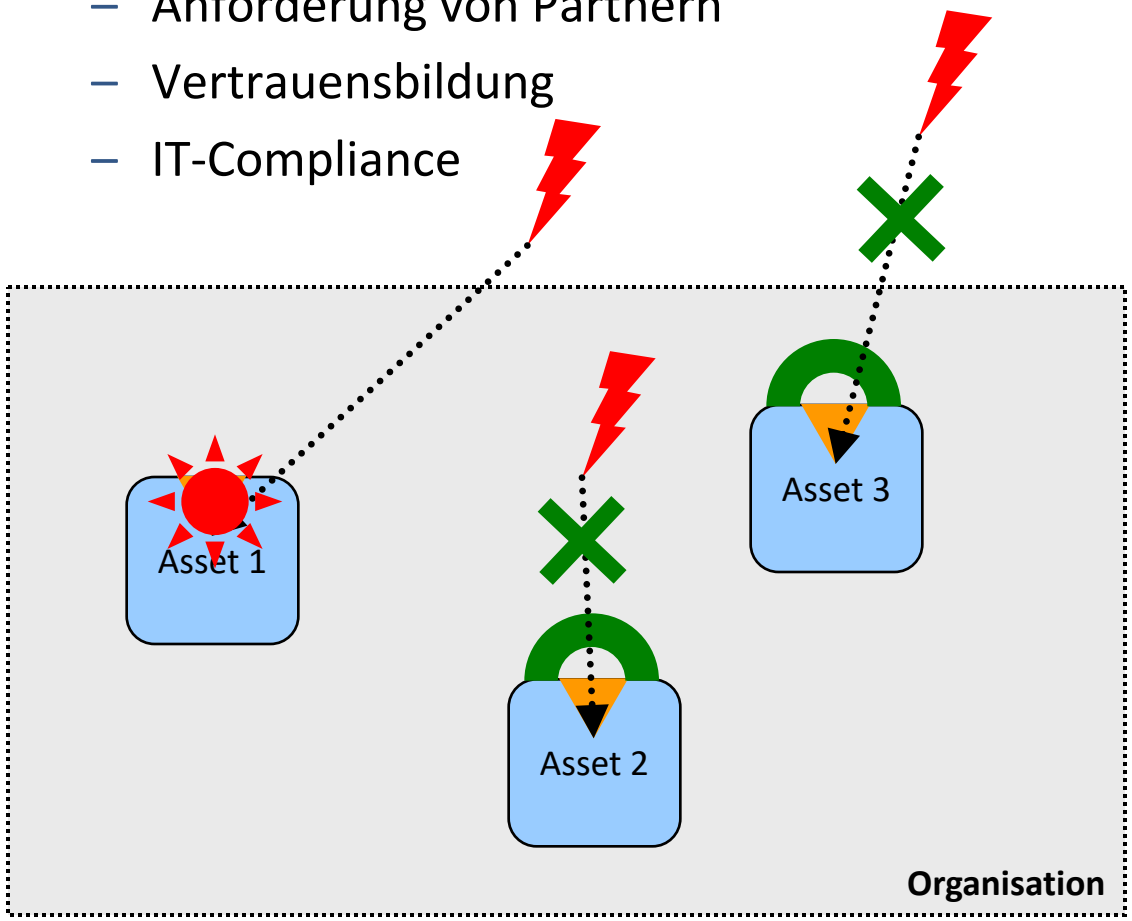
Handelskammer Hamburg, 18. März 2019

Anforderungen an die Datensicherheit im Internet der Dinge

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Von der Bedrohung zum Sicherheitsvorfall

- Warum IT-Sicherheitsmanagement?
  - Schutz von Unternehmenswerten (Assets)
  - Anforderung von Partnern
  - Vertrauensbildung
  - IT-Compliance



Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

vgl. Nowey, 2011

Von der Bedrohung zum Sicherheitsvorfall

- Präventive Maßnahmen
  - Einsatz kryptographischer Verfahren
    - obligatorische Datenverschlüsselung
    - gegenseitige starke Authentifizierung
  - Perimeterschutz mit Firewalls
  - Aufteilung Test- und Produktivumgebung
- Detektive Maßnahmen
  - Einsatz von Intrusion Detektion Systemen
  - Malware-Schutz
- Reaktive Maßnahmen
  - Systemtrennung
  - Fail-Safe-Prozeduren
  - Protokollierung

Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

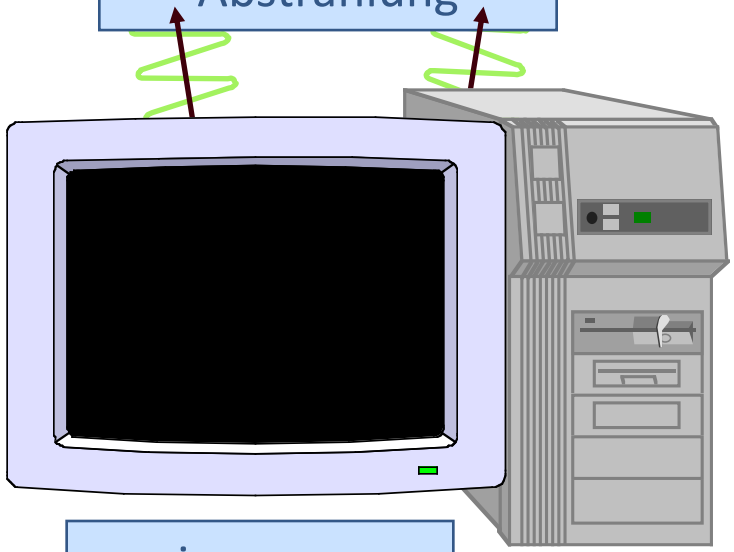
Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

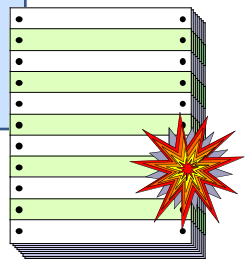
Angriffspunkte

Rechner

von außen:
Abstrahlung

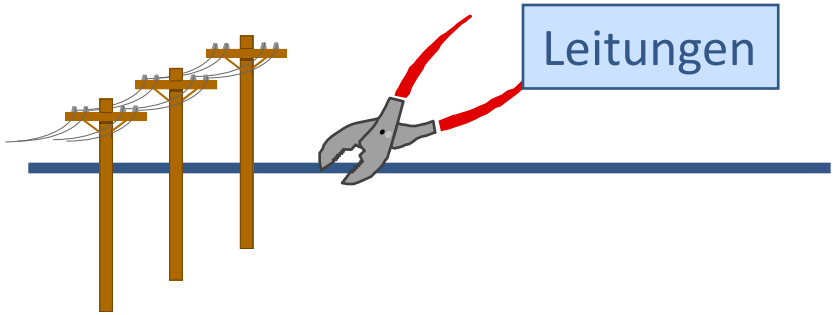


von innen:
Malware

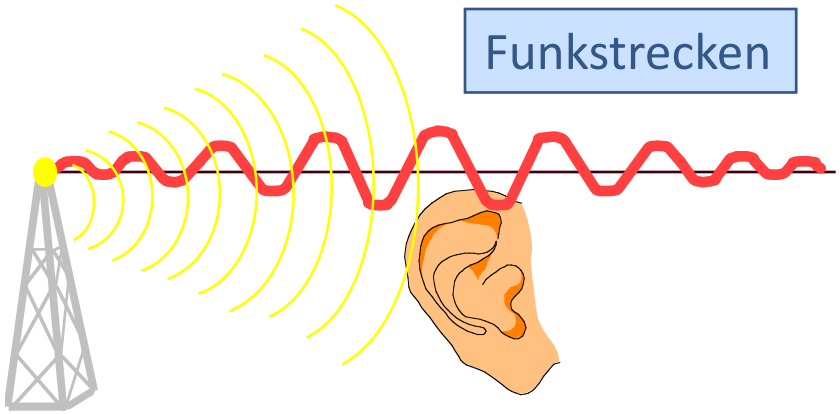


Übertragungswege

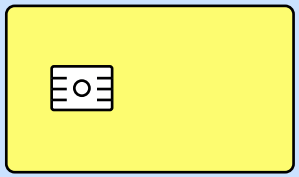
Leitungen



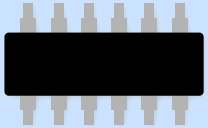
Funkstrecken



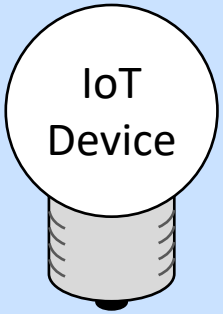
Angriffspunkte



Chipkarte

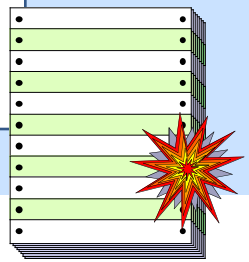


Tamper Proof Module
TPM



Glühlampe
Temperatursensor
Internet-Steckdose
Heizungssteuerung

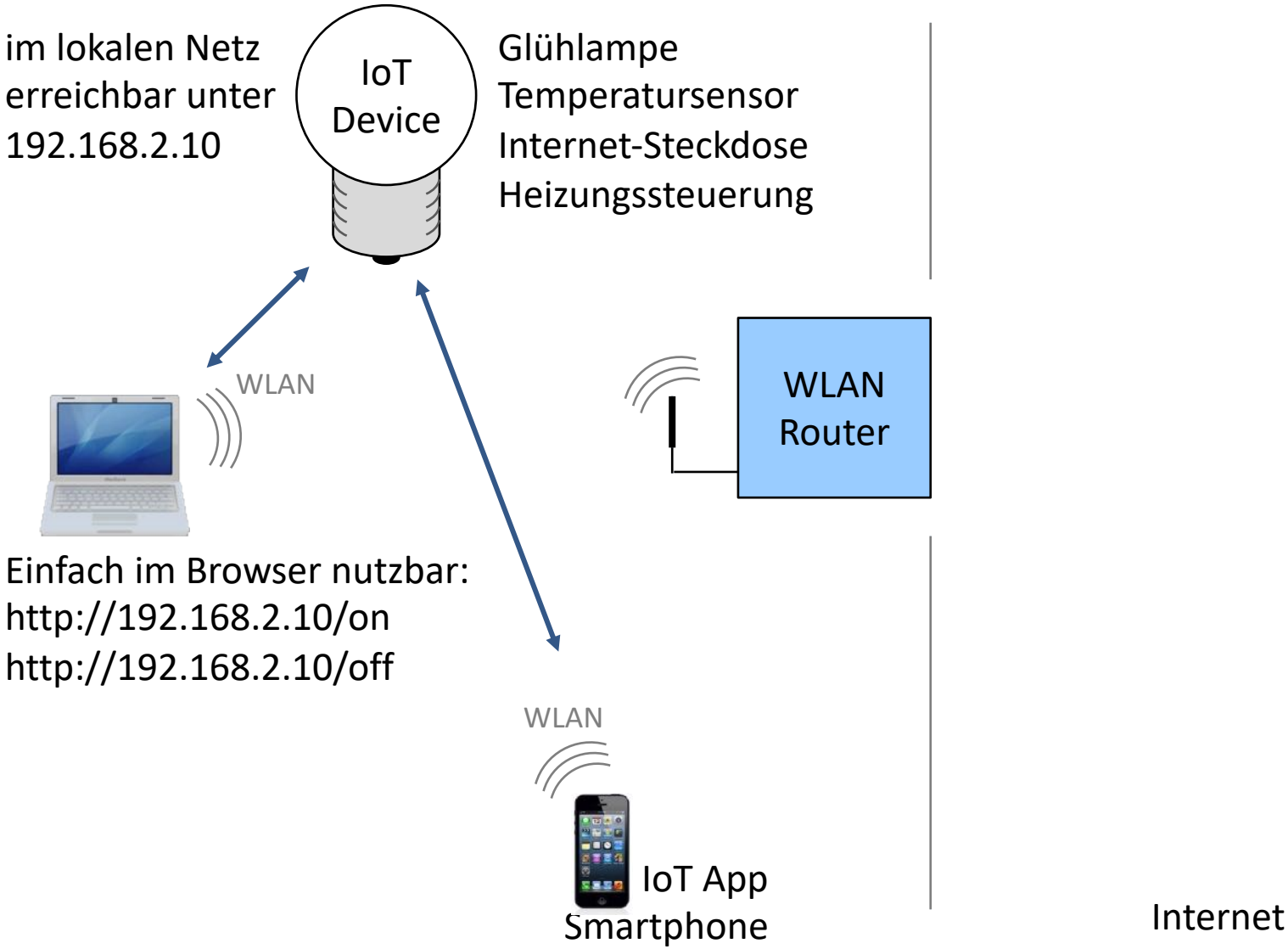
von innen:
Malware



Angreifer kann alle drei Schutzziele verletzen:

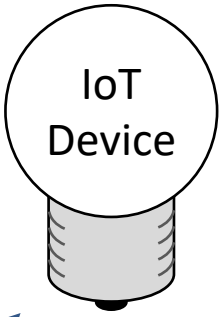
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Internet of Things – im lokalen Netz



Internet of Things – im lokalen Netz angreifbar

im lokalen Netz
erreichbar unter
192.168.2.10

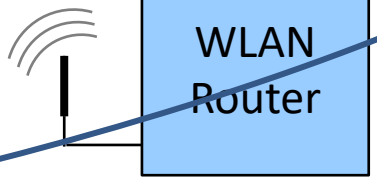


Glühlampe
Temperatursensor
Internet-Steckdose
Heizungssteuerung

Angreifer

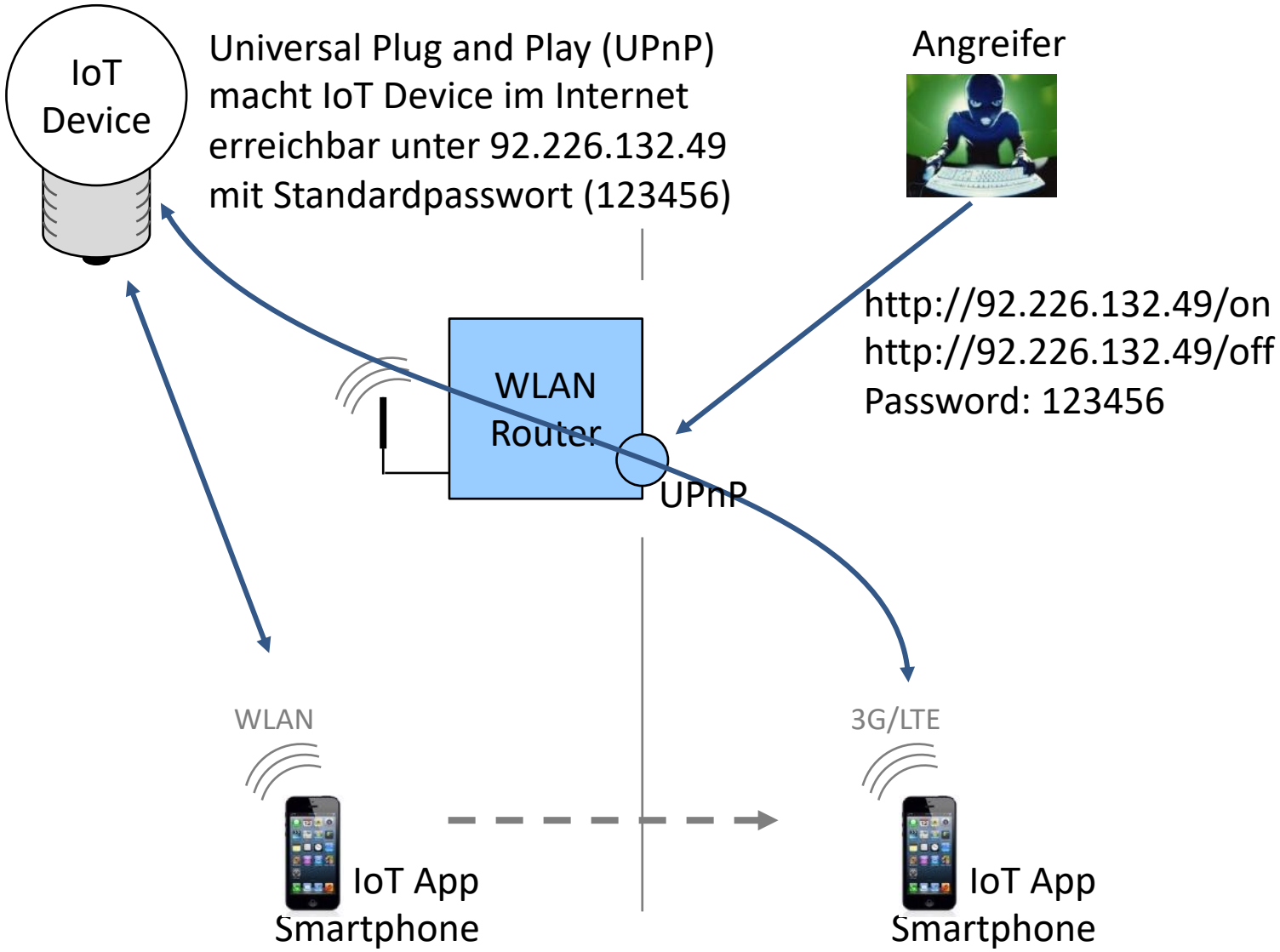
Command and
Control Center

WLAN

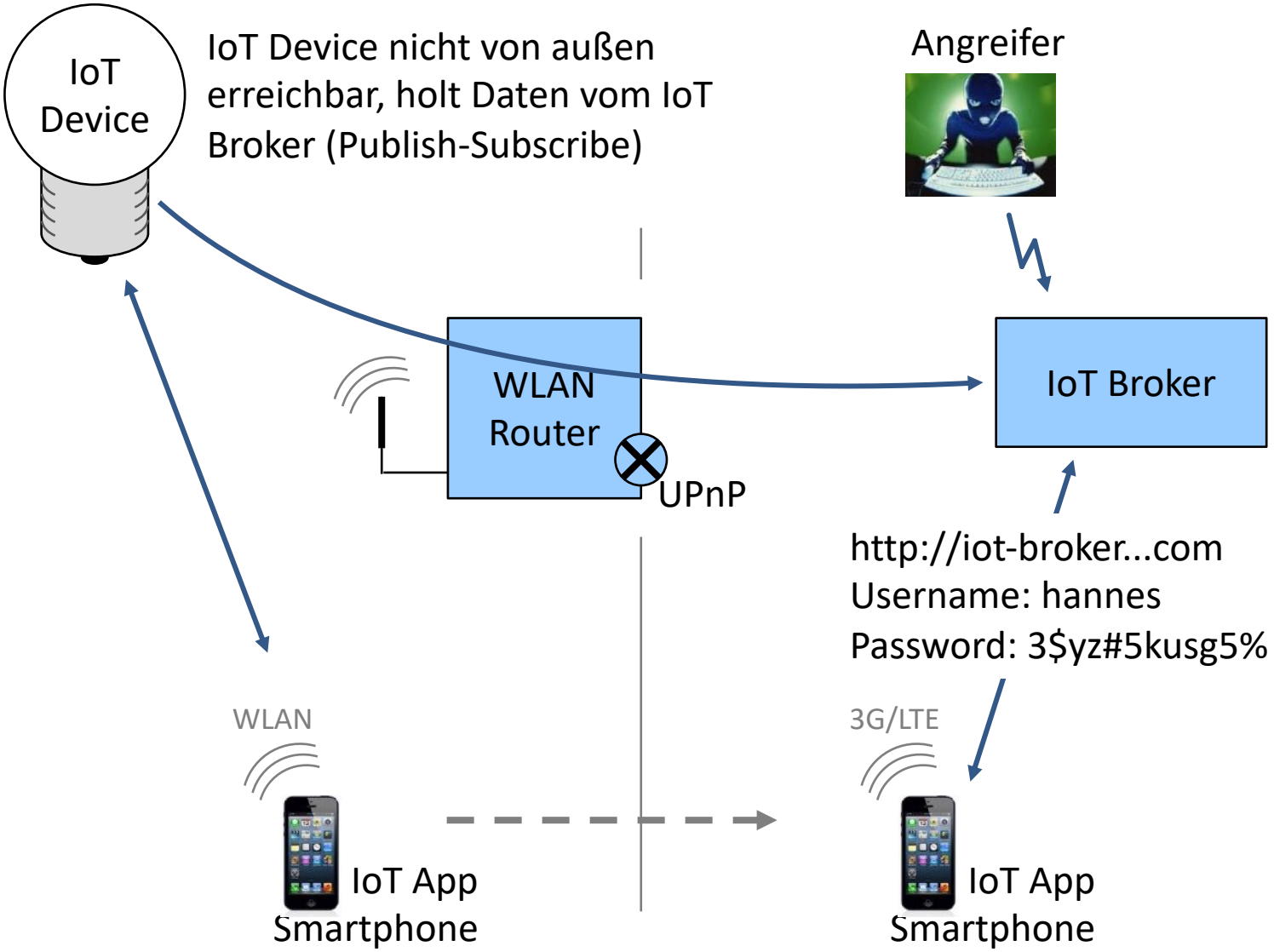


Malware auf PC kann
Daten sammeln,
Steuerfunktionen
auslösen, …

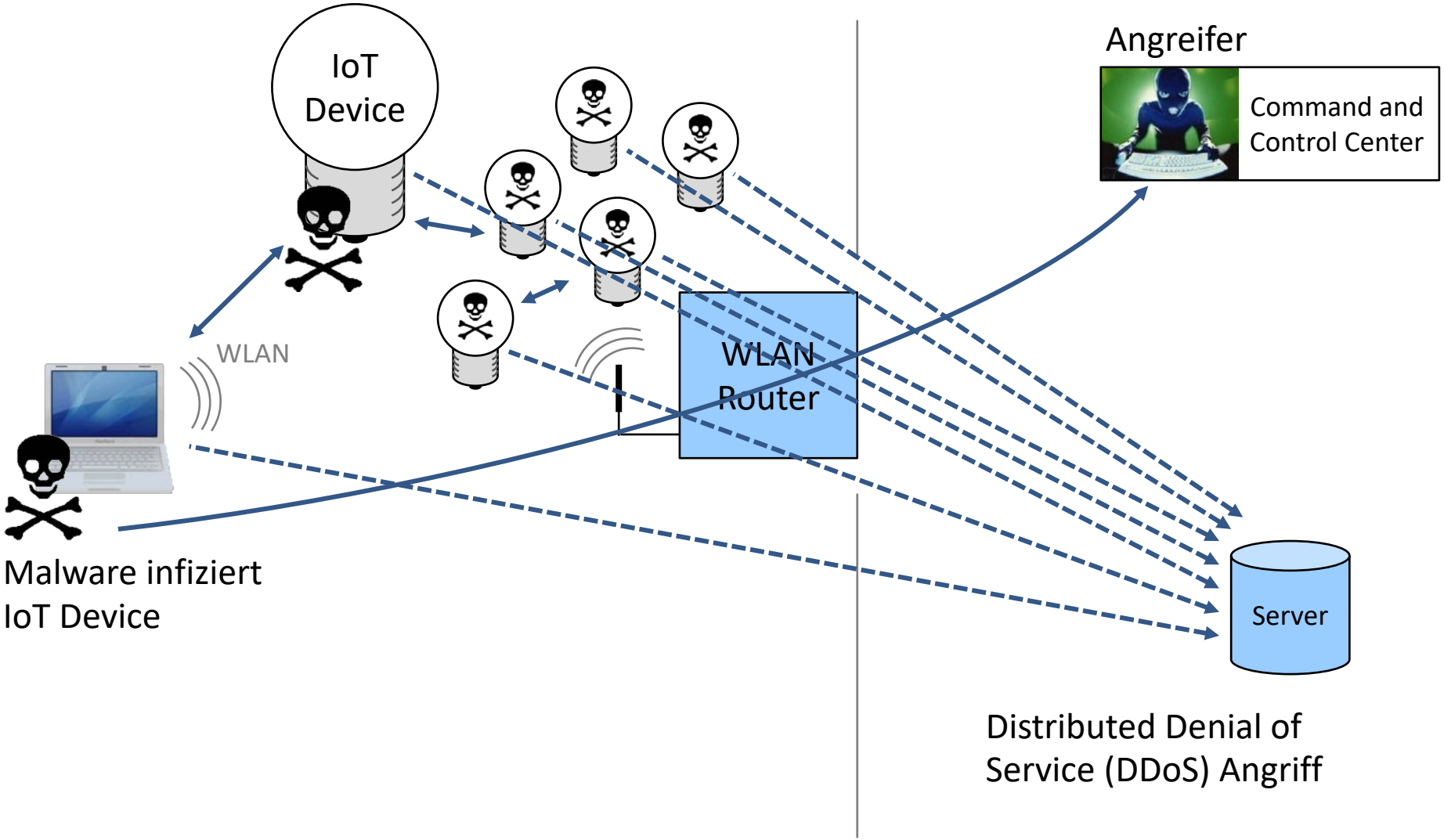
Internet of Things – Angriff über Universal Plug and Play (UPnP)



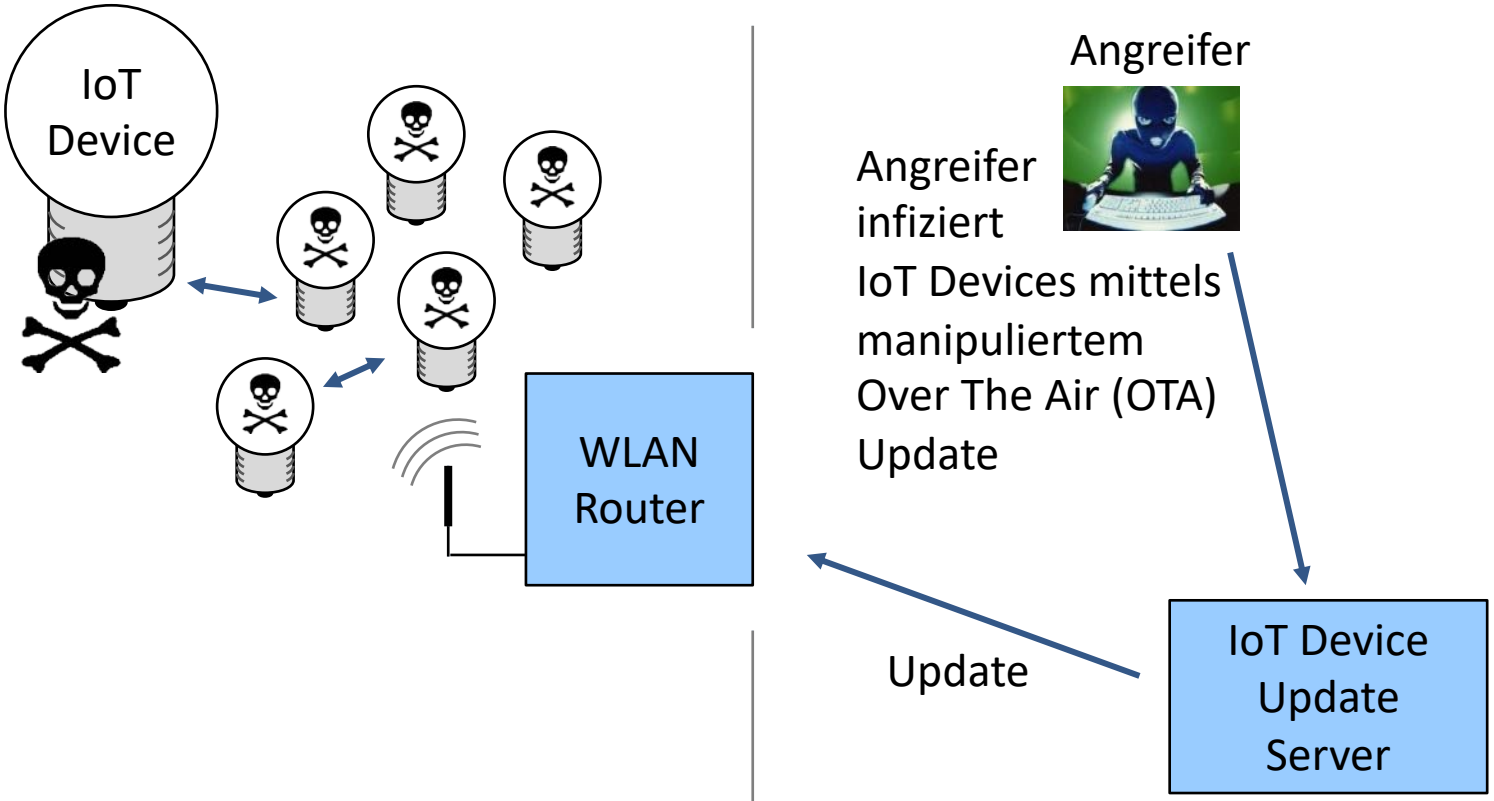
Internet of Things – Sichere Kommunikation über IoT Broker



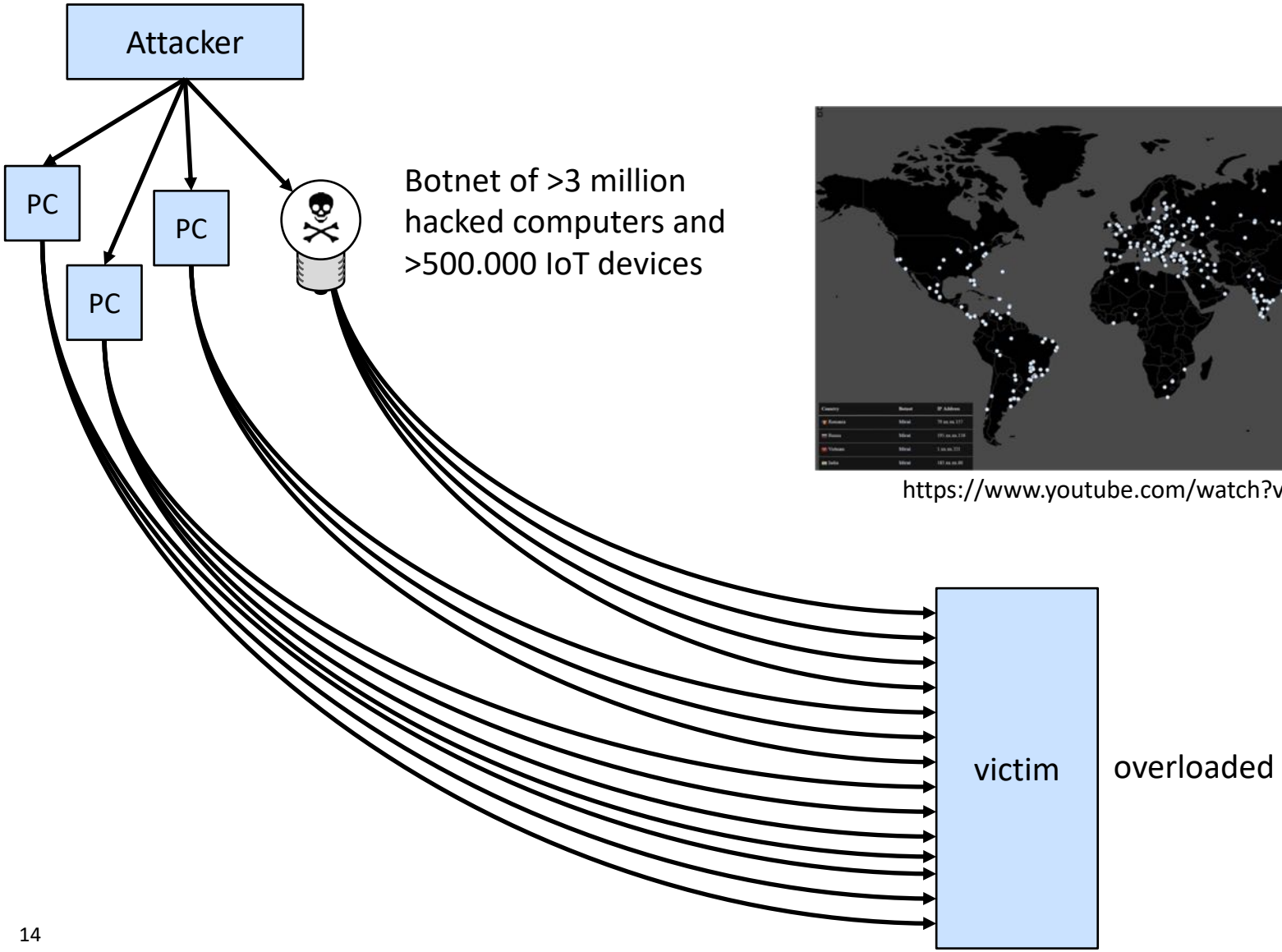
Internet of Things – IoT Devices als Teil eines Botnetzes



Internet of Things – Over The Air (OTA) Update



Mirai Botnet (2016)



Botnet of >3 million hacked computers and >500.000 IoT devices

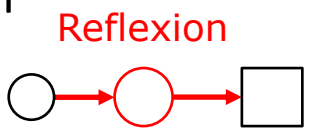
https://www.youtube.com/watch?v=cQkQpbkhzIo

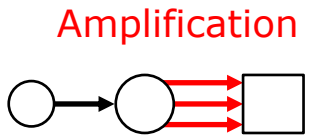
Distributed Denial-of-Service Angriffe im Internet

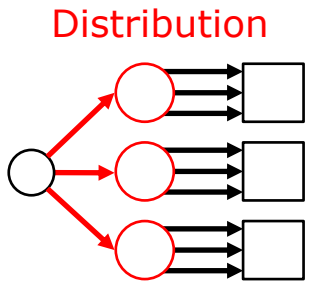
- Charakterisierung
  - Ziel wird von mehreren Quellen gleichzeitig angegriffen

- Typische Angriffsmuster
  - Reflexion, Spoofing
  - Amplification
  - Distribution (Botnets)

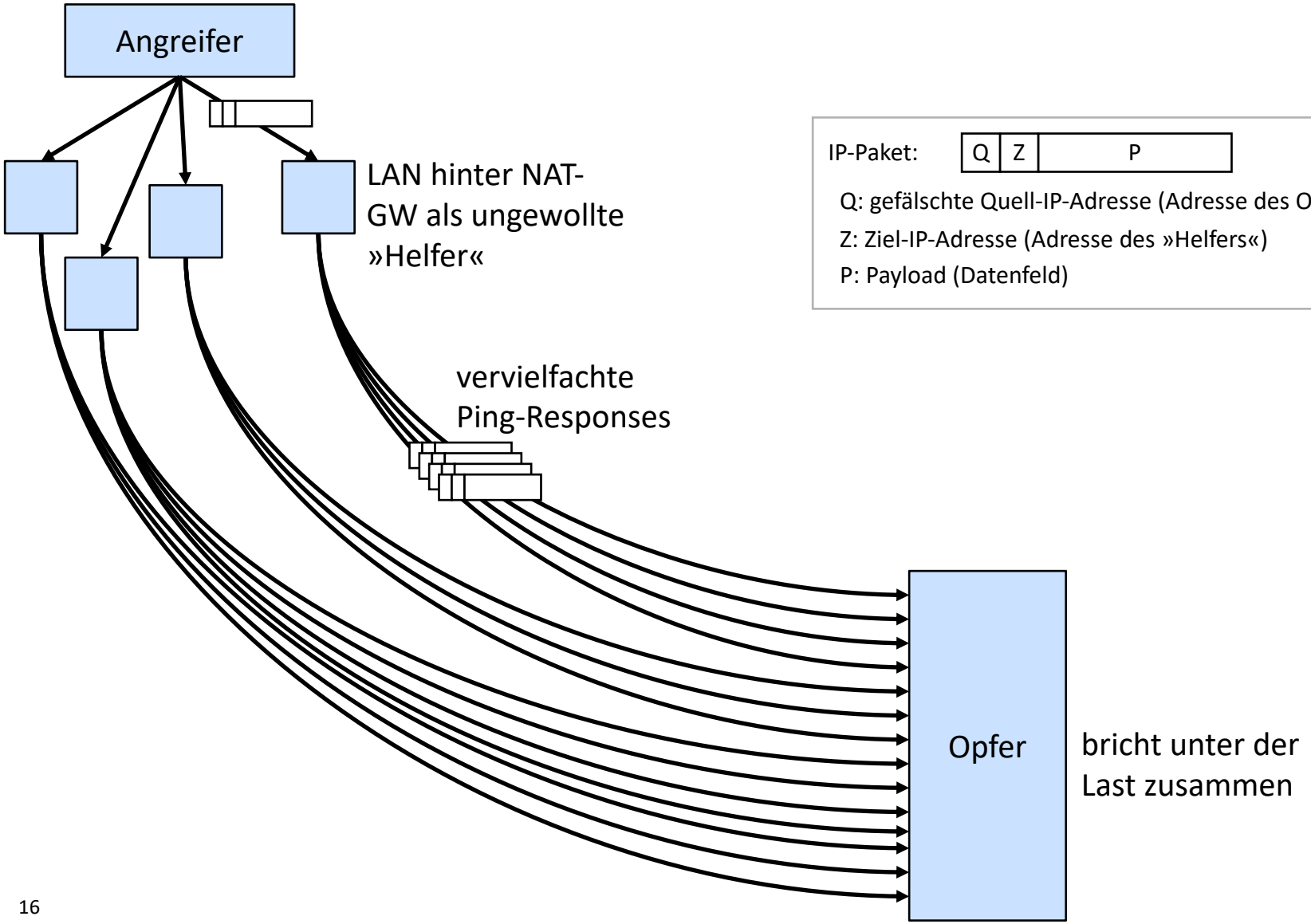
- Beispiele
  - Smurf IP Denial-of-Service Attack von 1998
  - Mirai-Botnet (2016)
  - Memcached-Angriff von 2017



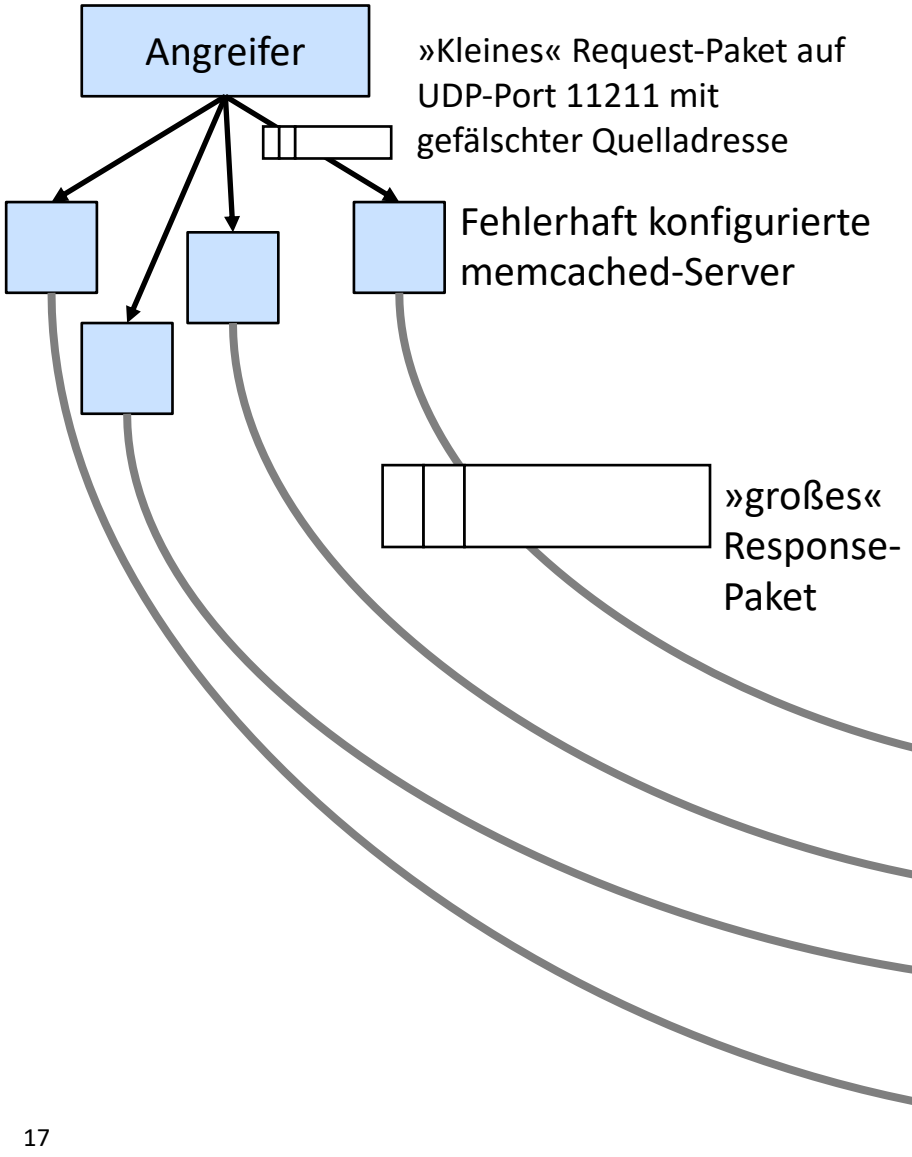




Smurf IP Denial-of-Service Attack (1998)



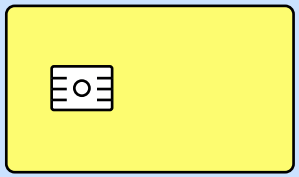
Memcached-Angriff (2017)



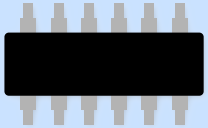
Herkunft der fehlerhaft konfigurierten Memcached-Server

https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/

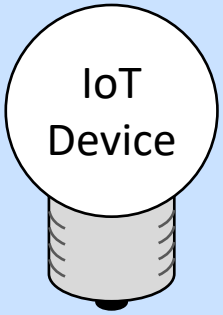
Angriffe auf die physische Sicherheit



Chipkarte

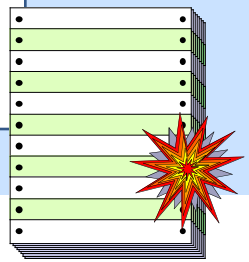


Tamper Proof Module
TPM



Glühlampe
Temperatursensor
Internet-Steckdose
Heizungssteuerung

von innen:
Malware



Physische Sicherheit

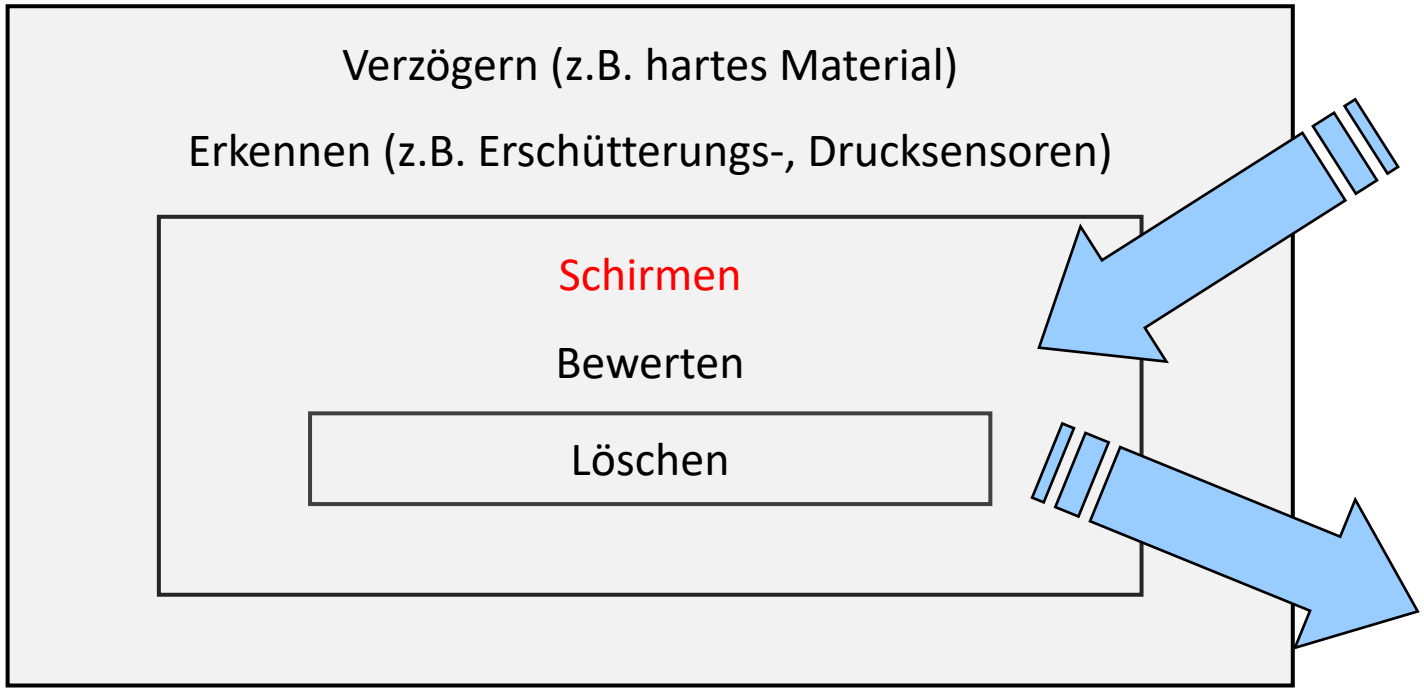
- Alle technischen Schutzmaßnahmen benötigen eine physische »Verankerung« in Form eines Systemteils, auf den der Angreifer keinen physischen Zugriff hat.
- Physische Sicherheit zu erhalten, gelingt bestenfalls auf Zeit.

Probleme

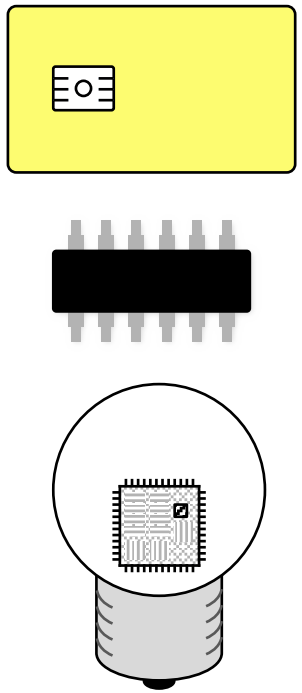
- Schirmung schwierig
- Angriffserkennung schwierig
- kein Löschen vorgesehen, selbst bei Stromversorgung

Physische Sicherheit: Grundfunktionen

- Schutz gegen beobachtende Angriffe:
  - Schirmung (elektromagnetische Abstrahlung, Energieverbrauch – unabhängig von den zu schützenden Geheimnissen)
- Schutz gegen verändernde Angriffe:
  - Erkennen, Bewerten, Verzögern und ggf. Löschen der geheimen Informationen.

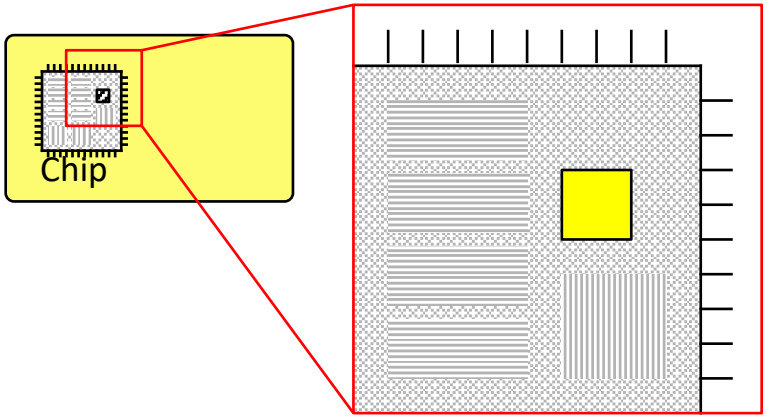


Beispiele für Angriffe

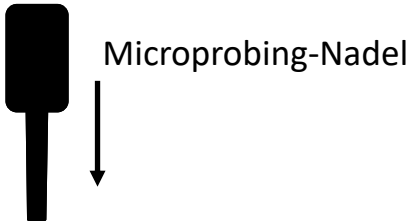


- Zerstörend
  - Abschleifen und Anätzen der Schutzschichten
  - Reverse Engineering: Untersuchung der Strukturen unter Elektronenmikroskop, wenn Funktion unbekannt
  - Microprobing-Nadel
  - Fault Injection: gezielte Manipulation von Bits durch Beschuss mit elektromagnetischer Strahlung
- Zerstörungsfrei meist sog. sidechannel attacks
  - Messung des Energieverbrauchs: power analysis
  - Messung der benötigten Rechenzeit: timing attacks

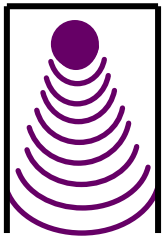
Zerstörende Angriffe und Schutz davor



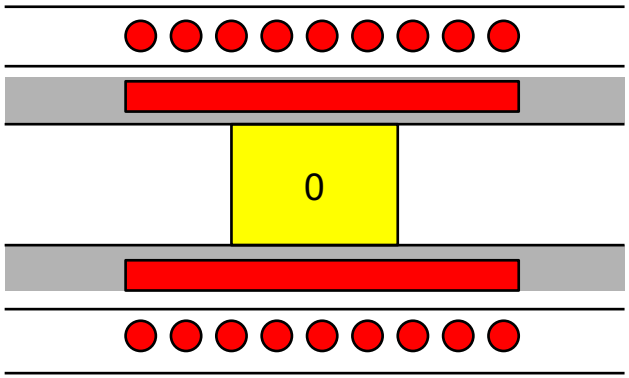
Ansicht von oben



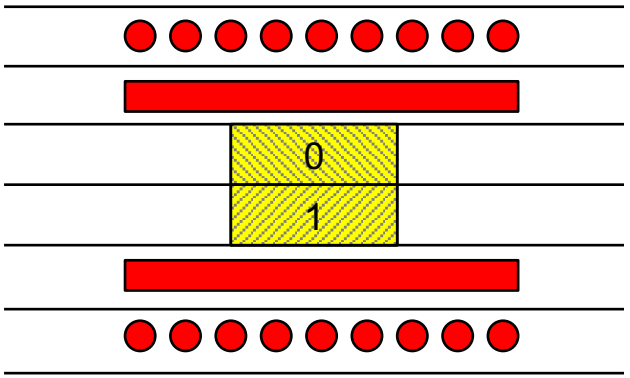
Microprobing-Nadel



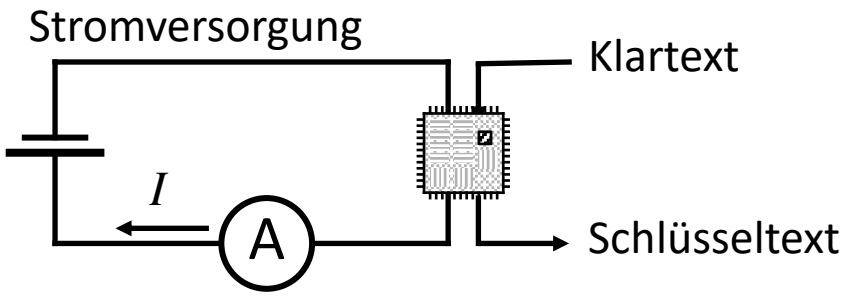
Fault Injection



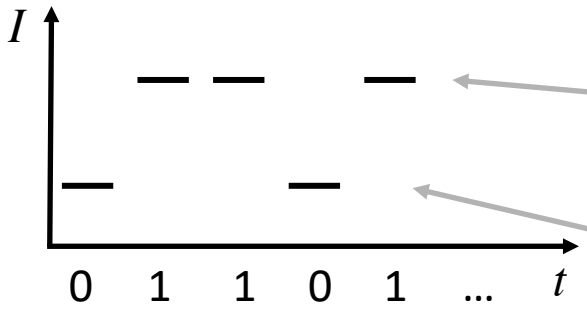
Ansicht von der Seite



Timing Attack / Power Analysis (Skizze)



Angriffsziel: Key ermitteln



1 = hoher Stromverbrauch
0 = niedriger Stromverbrauch

Schlüsselbits sind direkt auslesbar.

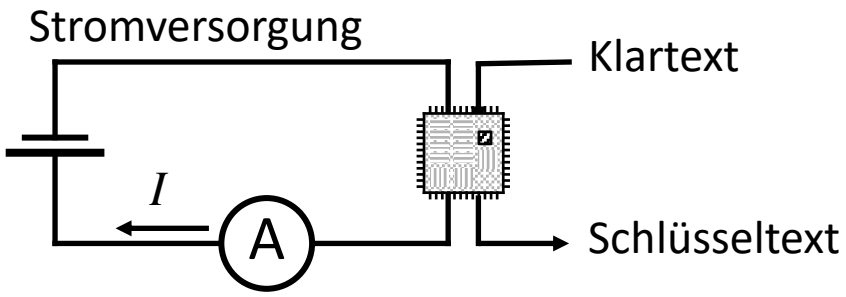
Schlüssel ist dem Angreifer unbekannt:

```
key = array of bit
    = ( 0, 1, 1, 0, 1, ...)
```

Quellcode ist dem Angreifer bekannt:

```
encrypt (Klartext, key) {
    ...
    for i = 1 to length(key){
        ...
        if (key[i] == 1){
            <code1>
            // ΔI ≈ I1
            // Δt ≈ t1
        } else {
            <code2>
            // ΔI ≈ I2
            // Δt ≈ t2
        }
    }
}
```

Timing Attack / Power Analysis (Skizze)



Angriffsziel: Key ermitteln

Auswege:

- interner Energiepuffer
- Verzweigungen vermeiden
- <code2> durch Dummy-Befehle der exakt gleichen Zykluszeit wie <code1> ersetzen

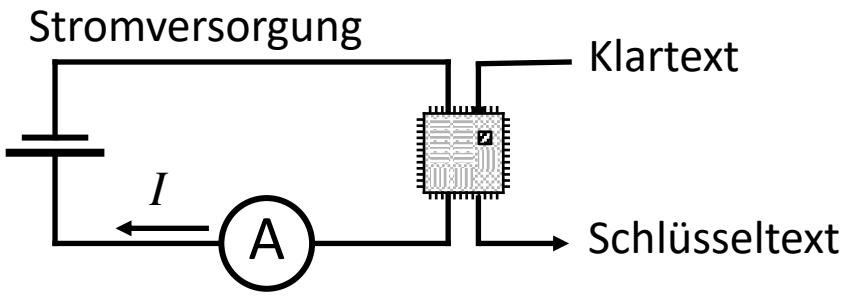
Schlüssel ist dem Angreifer unbekannt:

```
key = array of bit
    = ( 0, 1, 1, 0, 1, ...)
```

Quellcode ist dem Angreifer bekannt:

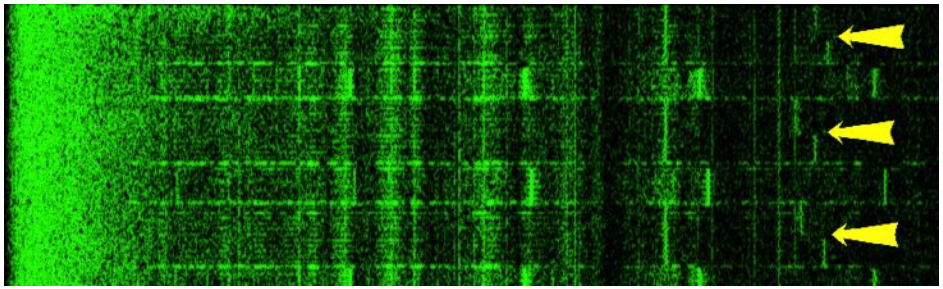
```
encrypt (Klartext, key) {
    ...
    for i = 1 to length(key){
        ...
        if (key[i] == 1){
            <code1>
            // ΔI ≈ I1
            // Δt ≈ t1
        } else {
            <code2>
            // ΔI ≈ I2
            // Δt ≈ t2
        }
    }
}
```

Timing Attack / Power Analysis (Skizze)



Angriffsziel: Key ermitteln

Symbolische Darstellung für Abstrahlung:



Source: https://www.tau.ac.il/~tromer/acoustic/

Schlüssel ist dem Angreifer unbekannt:

```
key = array of bit
    = ( 0, 1, 1, 0, 1, ...)
```

Quellcode ist dem Angreifer bekannt:

```
encrypt (Klartext, key) {
    ...
    for i = 1 to length(key){
        ...
        if (key[i] == 1){
            <code1>
            // ΔI ≈ I1
            // Δt ≈ t1
        } else {
            <code2>
            // ΔI ≈ I2
            // Δt ≈ t2
        }
    }
}
```

Physische Sicherheit zu erhalten, gelingt bestenfalls auf Zeit.

Beispiel EC-Terminals:

- unzureichende Überprüfung des Schutzes des Hardware-Security-Moduls (HSM)
- Angreifer konnten erfolgreich Mesh-Gewebe entfernen

golem.de

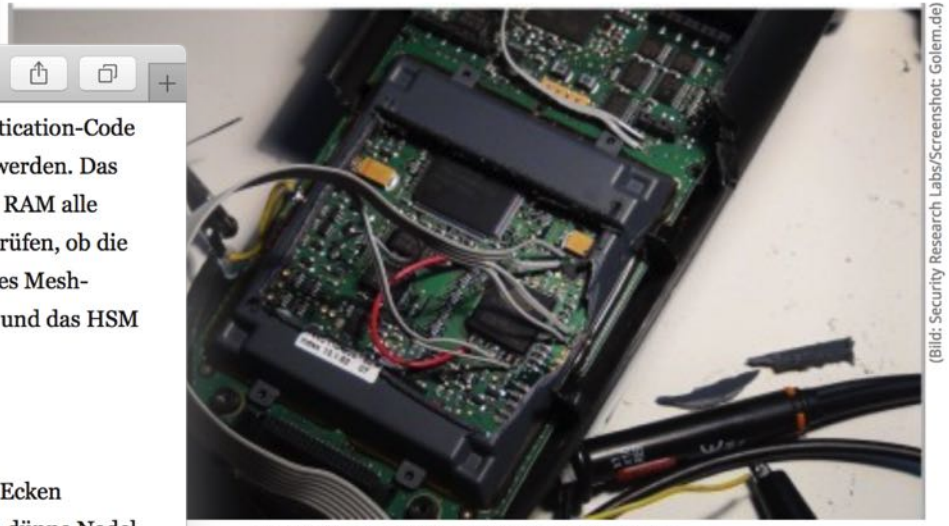
EC-TERMINALS

Hacker knacken Hardware-Security-Modul

32C3

Nicht nur die Protokolle zur Abwicklung des EC-Zahlungsverkehrs sind schwach, auch die verwendete Hardware ist offenbar nicht besonders gut gegen Angriffe abgesichert. Auf dem 32C3 stellten Berliner Hacker jetzt vor, wie sich das Hardware-Security-Modul eines EC-Terminals hacken lässt.

28. Dezember 2015, 10:40 Uhr, Hauke Gierow



(Bild: Security Research Labs/Screenshot: Golem.de)

Das HSM von EC-Terminals ist angreifbar - mit einigen Tricks.

golem.de AA

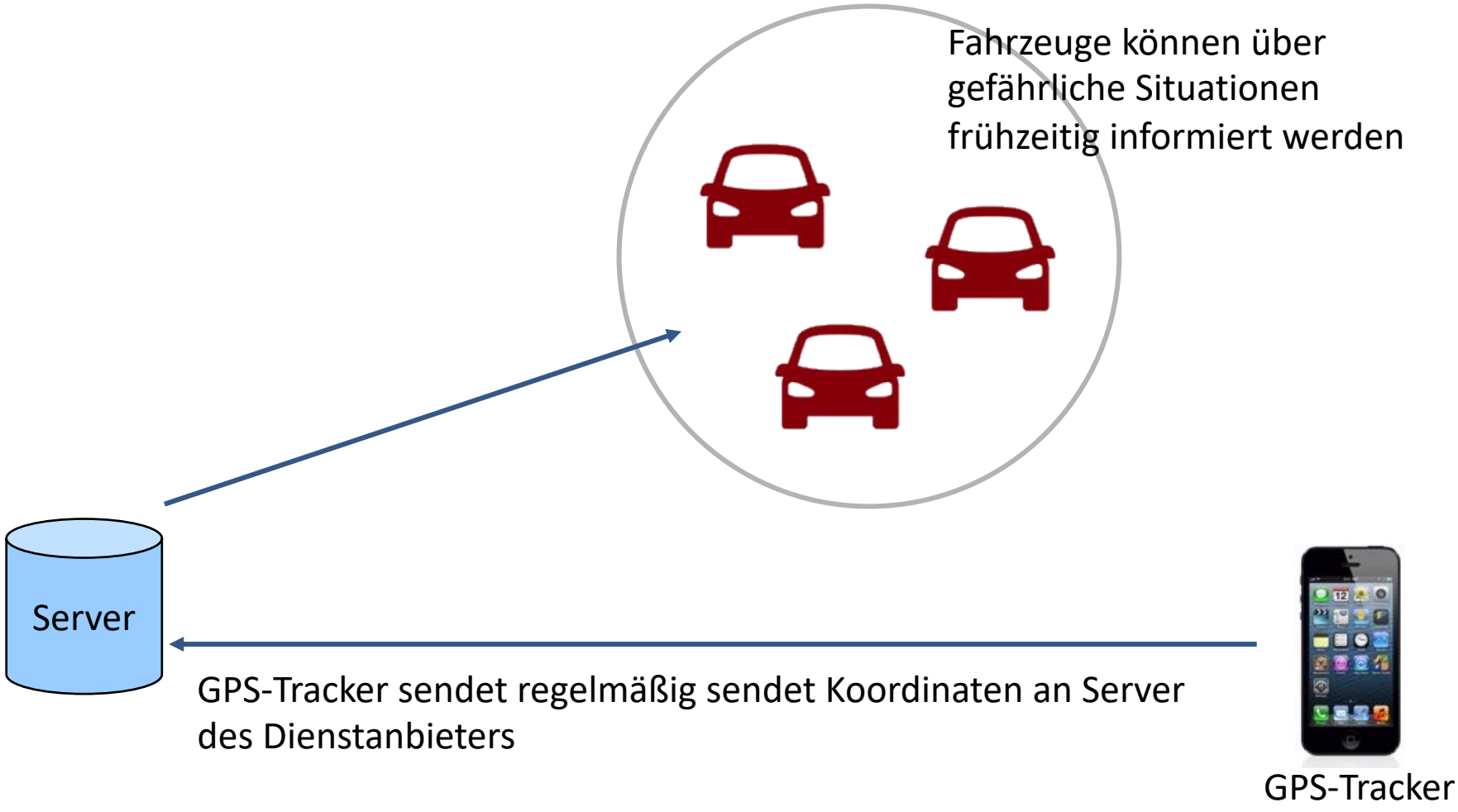
Das HSM beherbergt unter anderem den kryptographischen Message-Authentication-Code (MAC), mit dem sicherheitsrelevante Informationen wie die PIN abgesichert werden. Das HSM befindet sich unter einer Abdeckung - wird diese entfernt, "vergisst" der RAM alle Informationen, weil automatisch die Stromversorgung gekappt wird. Um zu prüfen, ob die Abdeckung intakt ist, ist an der Unterseite der Abdeckung ein dünnes, leitendes Mesh-Gewebe angebracht. Bei Beschädigungen wäre der Stromfluss unterbrochen - und das HSM stromlos.

Mesh-Status wird nur an den Ecken überprüft

Doch wie die Hacker herausfanden, wird der Status des Mesh nur an den vier Ecken überprüft, nicht aber an den langen Kanten. Daher war es ihnen möglich, eine dünne Nadel unter die Abdeckung zu führen und dort den Prüfmechanismus für das Mesh außer Kraft zu setzen. Danach konnten sie die Abdeckung problemlos aufschneiden und den RAM des HSM auslesen. Dazu nutzten sie einen speziell angepassten Arduino.

https://www.golem.de/news/ec-terminals-hacker-knacken-hardware-security-modul-1512-118210.html

Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT



Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT

Eltern

Eltern können auf Standort zugreifen

https://example.com/device/<Device-Id>/locate/
HTTP Basic Auth: ios_usr:73gqjjrf85uv

Beispiel einer Device-Id:
786572032150562

Server

https://example.com/device/<Device-Id>/update/<GPS-Pos>
HTTP Basic Auth: ios_usr:73gqjjrf85uv

GPS-Tracker sendet regelmäßig sendet Koordinaten an Server des Dienstanbieters, gleiches Passwort für alle Tracker, fest in App eingebaut

GPS-Tracker

Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT

Angreifer

Angreifer kann Device-Ids durchprobieren und auf fremde GPS-Koordinaten zugreifen

https://example.com/device/<Device-Id>/locate/
HTTP Basic Auth: ios_usr:73gqjjrf85uv

Beispiel einer Device-Id:
786572032150562

Server

https://example.com/device/<Device-Id>/update/<GPS-Pos>
HTTP Basic Auth: ios_usr:73gqjjrf85uv

GPS-Tracker sendet regelmäßig sendet Koordinaten an Server des Dienstanbieters, gleiches Passwort für alle Tracker, fest in App eingebaut

GPS-Tracker

Unzureichende Schutzmaßnahmen gefährden Vertrauen in IT

Angreifer

Angreifer kann Device-Id im Request weglassen und Server liefert alle Device-Ids inkl. aller Standorte der Nutzer

https://example.com/devices/
HTTP Basic Auth: ios_usr:73gqjjrf85uv

"id":"786572032150562",
"phone":"004915156833300",
"name":"Mikes Tasche",
"lastUpdate":1515137867000,
"lastPosition":351528783,

"id":"786542032376175",
"phone":"004915154563702",
"name":"Sonja unterwegs",
"lastUpdate":1515137629000,
"lastPosition":351918722,
...

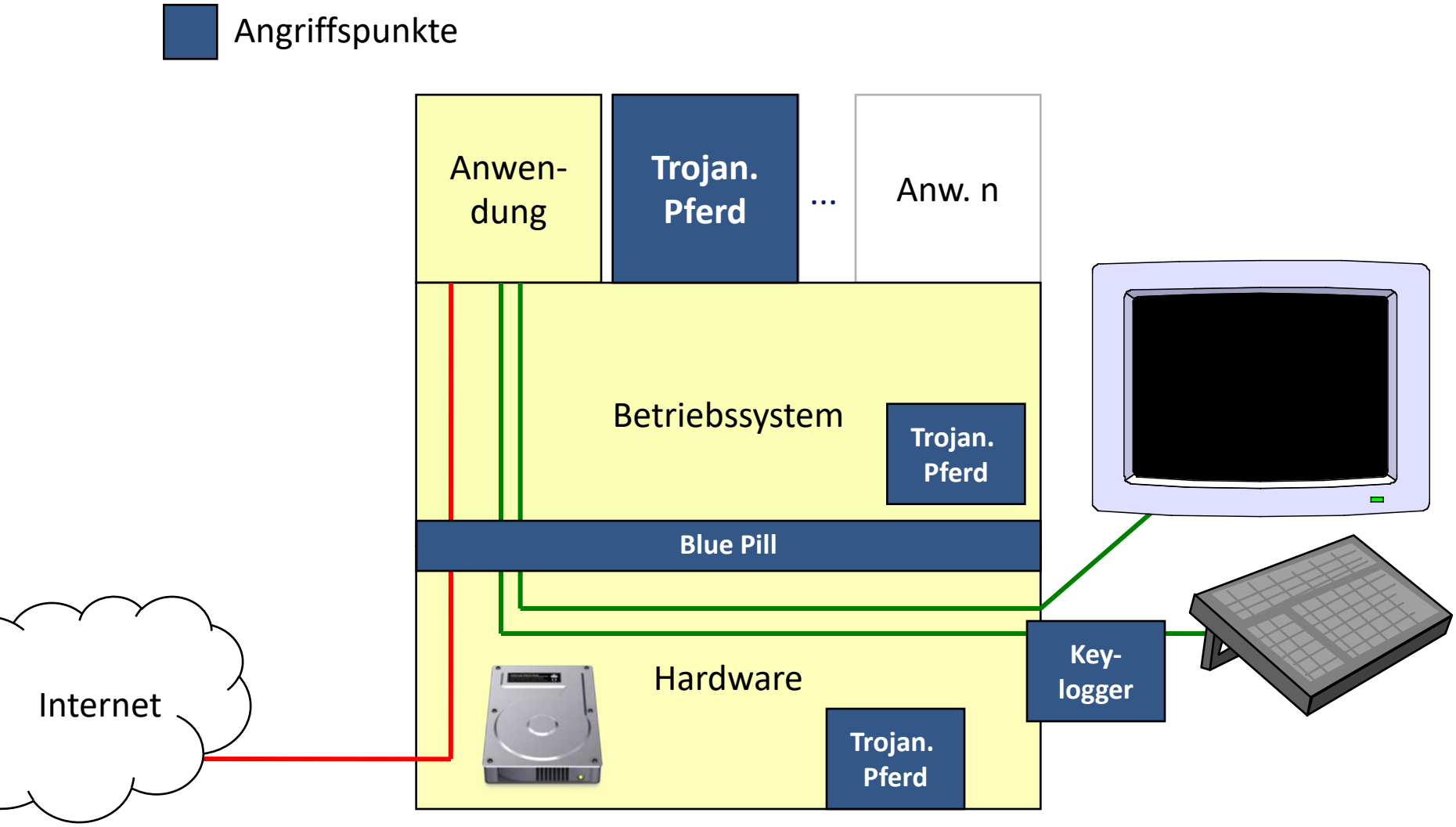
Server

https://example.com/device/<Device-Id>/update/<GPS-Pos>
HTTP Basic Auth: ios_usr:73gqjjrf85uv

GPS-Tracker sendet regelmäßig sendet Koordinaten an Server des Dienstanbieters, gleiches Passwort für alle Tracker, fest in App eingebaut

GPS-Tracker

Angriffspunkte für Malware



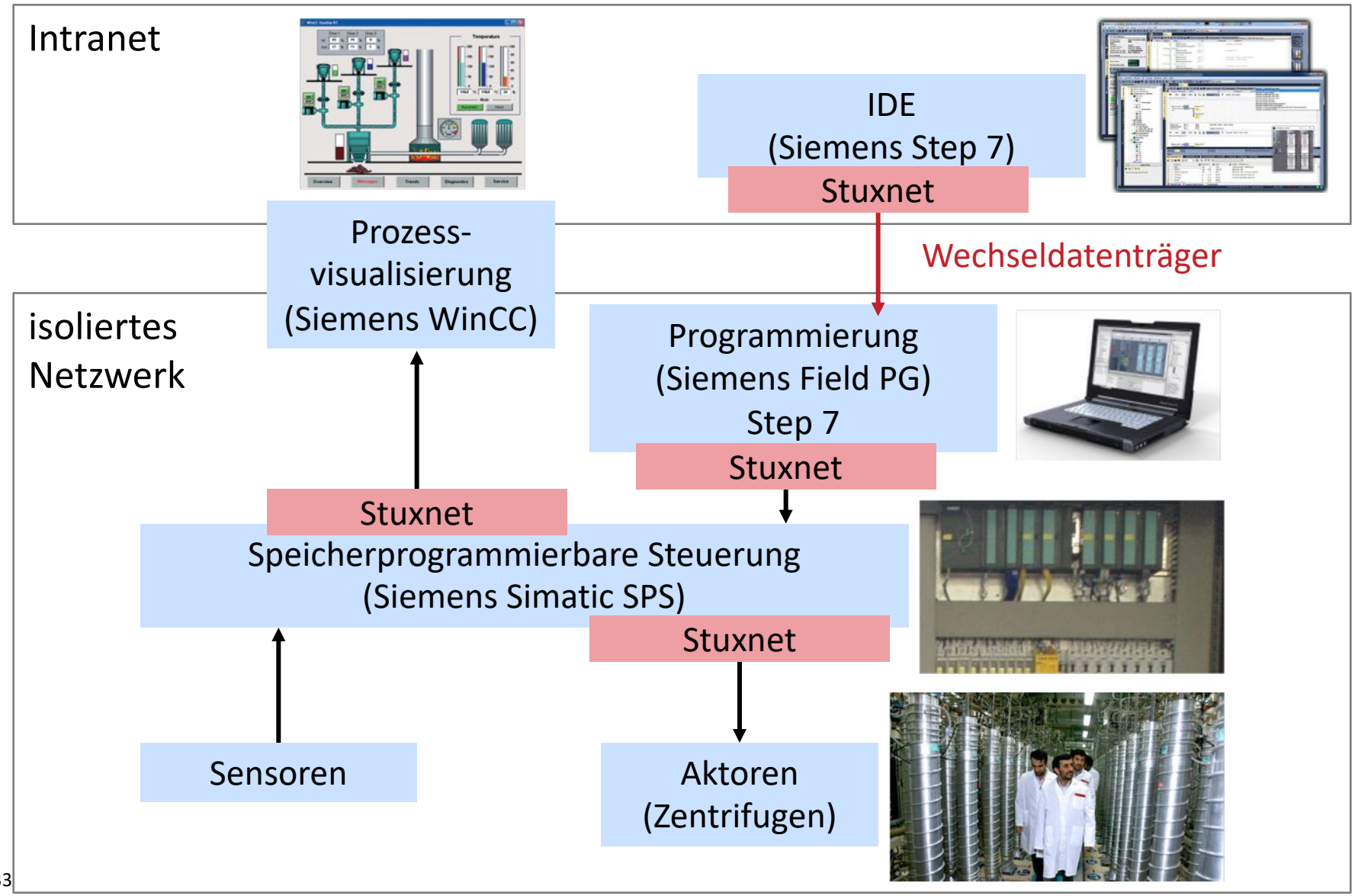
Stuxnet

- Internetwurm, der mit dem Ziel entwickelt wurde, die innerbetrieblichen Abläufe eines speziellen Typs von Industrieanlagen empfindlich zu stören.

  - Entdeckung im Juli 2010
  - Ziel: Unbemerkte Änderung von Programmteilen in speicherprogrammierbaren Steuerungen (SPS)
  - Verwendet vier Zeroday-Exploits zur Verbreitung und Rechteausweitung
  - Insiderwissen für Entwicklung erforderlich
  - Selbstzerstörung (nur Windows-Komponente) nach 35 Tagen

Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet - Szenario (Industrieanlage)



inf.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

DEPARTMENT OF INFORMATICS
SECURITY AND PRIVACY

HOME COURSES THESES RESEARCH PEOPLE SERVICE

UHH → MIN-Fakultät → Fachbereich Informatik → Einrichtungen → Arbeitsbereiche → Security and Privacy → **Home**

WORKING GROUP ON «SECURITY AND PRIVACY»

Security and Privacy

Information systems become more and more important in critical infrastructures, while the Internet has evolved to a critical infrastructure itself. The secure operation of these infrastructures is vital and their failure can have severe impacts up to the loss of human lives.
Security refers to the fact that protection goals are achieved in the presence of malicious attacks and system failures. Typical security goals can be confidentiality, integrity, accountability, and availability. Security and privacy in information systems addresses both technical and organizational aspects, such as building and establishing security concepts and security infrastructures as well as risk analysis and risk management.
Privacy can be a conflicting goal to security, but they can also benefit from each other. Hence, it is necessary to balance both when developing secure information systems.

Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

federrath@informatik.uni-hamburg.de

https://svs.informatik.uni-hamburg.de