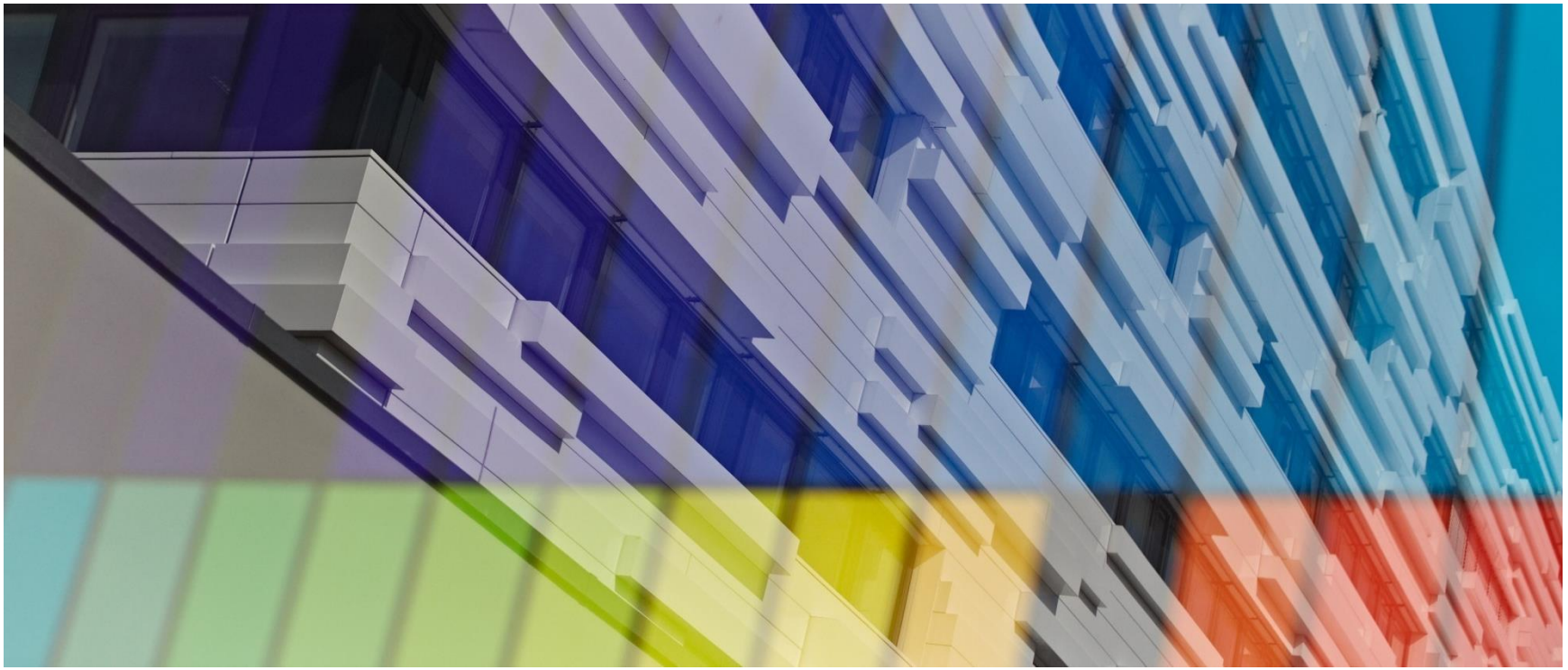
Cybersicherheit und Digitalisierung in der Energiewirtschaft

Dr. Michael Kreutzer
Fraunhofer SIT
Center for Research in Security and Privacy CRISP



Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Fraunhofer Institut für Sichere Informationstechnologie SIT

Führende Einrichtung für angewandte Cybersicherheitsforschung

Fraunhofer SIT

- **Geschichte**
  - Gegründet **1961** als »Deutsches Rechenzentrum«, seit **1992** Schwerpunkt auf **Cybersicherheit,** seit **2001** **Fraunhofer**
- **Fakten**
  - **170** Mitarbeiter/innen, **6** Professor/innen, **11M€** Budget
  - Mitarbeiter in **Darmstadt, Birlinghoven, Mittweida, Jerusalem** (w/ HUJI, seit 2015), **Singapur** (w/ NTU, seit 2017)

TECHNISCHE UNIVERSITÄT DARMSTADT

האוניברסיטה העברית בירושלים THE HEBREW UNIVERSITY OF JERUSALEM

NANYANG TECHNOLOGICAL UNIVERSITY

- **Forschungszentren**

CRISP Center for Research in Security and Privacy

Fraunhofer-Leistungszentrum Sicherheit und Datenschutz in der digitalen Welt

Center for Research in Security and Privacy

Größtes Kompetenzzentrum Cybersicherheit in Europa

TECHNISCHE UNIVERSITÄT DARMSTADT
CYSEC

Fraunhofer SIT
Fraunhofer IGD
Fraunhofer-Leistungszentrum Cybersicherheit

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

2008 gegründet und seitdem gefördert vom Land Hessen

seit 2011 vom BMBF gefördert

seit 2015 CRISP gefördert von BMBF + Hessen

seit 2016 Fraunhofer-Leistungszentrum

2017 Nationales Forschungszentrum für angewandte Cybersicherheit vereinbart

500+ Wissenschaftler/innen

aus 40+ Ländern,

2000+ Studierende

Bundesministerium für Bildung und Forschung

HESSEN Hessisches Ministerium für Wissenschaft und Kunst

50+ »Distinguished Speakers«

50+ Konferenzen

80+ Auszeichnungen

@Politik

CRISP-Sprecher wird Chief Digital Officer für die Digitale Stadt Darmstadt

Bundeskanzlerin Angela Merkel informiert sich über Leuchtturmprojekt "Secure Internet-Infrastructure"

DIGITALGIPFEL 2017 DER BUNDESREGIERUNG

Der Digital-Gipfel am 12.-13. Juni 2017 (ehemals Nationaler IT-Gipfel) und sein ganzjähriger Prozess bilden die zentrale Plattform für die Zusammenarbeit von Politik, Wirtschaft, Wissenschaft und Gesellschaft bei der Gestaltung des digitalen Wandels.

Positionspapier für Cybersecurity veröffentlicht im Februar 2017

CRISP ist ein Haupt-Akteur der neuen Werbekampagne von "Hessen schafft Wissen"

Michael Waidner wird Mitglied im Fachbeirat des Nationalen Cybersicherheitsrat

IT und Netzpolitik | IT- und Cybersicherheit | Artikel

Cyber-Sicherheitsrat

Sichtbare Stärkung der Zusammenarbeit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft: Der Cyber-Sicherheitsrates als wichtiger Baustein der Cyber-Sicherheitsstrategie für Deutschland.

HESSISCHER LANDTAG

Öffentliche Anhörung zu "Digitalisierung in Hessen"
Michael Waidner spricht im Hauptausschuss des Hessischen Landtags: Dringlichkeitsantrag bezügl. Hessen 4.0 – Agenda Digitales Hessen. Öffentliche Anhörung am 16.08. im Hessischen Landtag.

In 2017 zweimal ausgezeichnet!

DIGITAL HUB CYBERSICHERHEIT DARMSTADT

Bundesministerium für Wirtschaft und Energie

DE.DIGITAL

21. April

Bundeswirtschaftsministerium: Darmstadt ist führendes deutsches Ökosystem für Cybersicherheits-Start-Ups und Internationalisierung

Digitale.Stadt by bitkom

STADT | WIRTSCHAFT | BÜRGERSCHAFT | WISSENSCHAFT

DIGITALSTADT DARMSTADT

12. Juni

Europa schaut auf das Innovationslabor Darmstadt mit "Fokus auf hochprofessionelle Cybersicherheit" (Bitkom)

Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Energiewende und Digitalisierung

Rahmenbedingungen Energiewende

Ziele Energiewende: Umweltverträglichkeit, Wirtschaftlichkeit, Versorgungssicherheit

Dezentralität: Strukturmerkmale der Strom- und Wärmemärkte der Energiewende

Energiewende + Digitalisierung = Prosumer 4.0 (Udo Sieverding Verbraucherzentrale NRW)

Aus einer Studie des Fraunhofer ISI:

- Fluktuierende erneuerbare Energien
- Flexibel reagierende komplementäre Stromerzeugung & Nachfrage nach Strom
- Hinzukommende Stromanwendungen im Bereich der Gebäude und des Verkehrs
- Speicher und Anlagen zur Erzeugung synthetischer Energieträger
- Verbrennungstechniken werden durch elektrische Maschinen ersetzt, die die Endenergie Strom effizienter in Nutzenergie (Wärme, Traktion) wandeln

Vgl.: https://www.ise.fraunhofer.de/de/veroeffentlichungen/studien/was-kostet-die-energiewende.html

Energiewende und Digitalisierung

Rahmenbedingungen Energiewende

Ziele Energiewende: Umweltverträglichkeit, Wirtschaftlichkeit, Versorgungssicherheit

Dezentralität: Strukturmerkmale der Strom- und Wärmemärkte der Energiewende

Energiewende + Digitalisierung = **Prosumer 4.0** (Udo Sieverding Verbraucherzentrale NRW)

Aus einer Studie des Fraunhofer ISI:

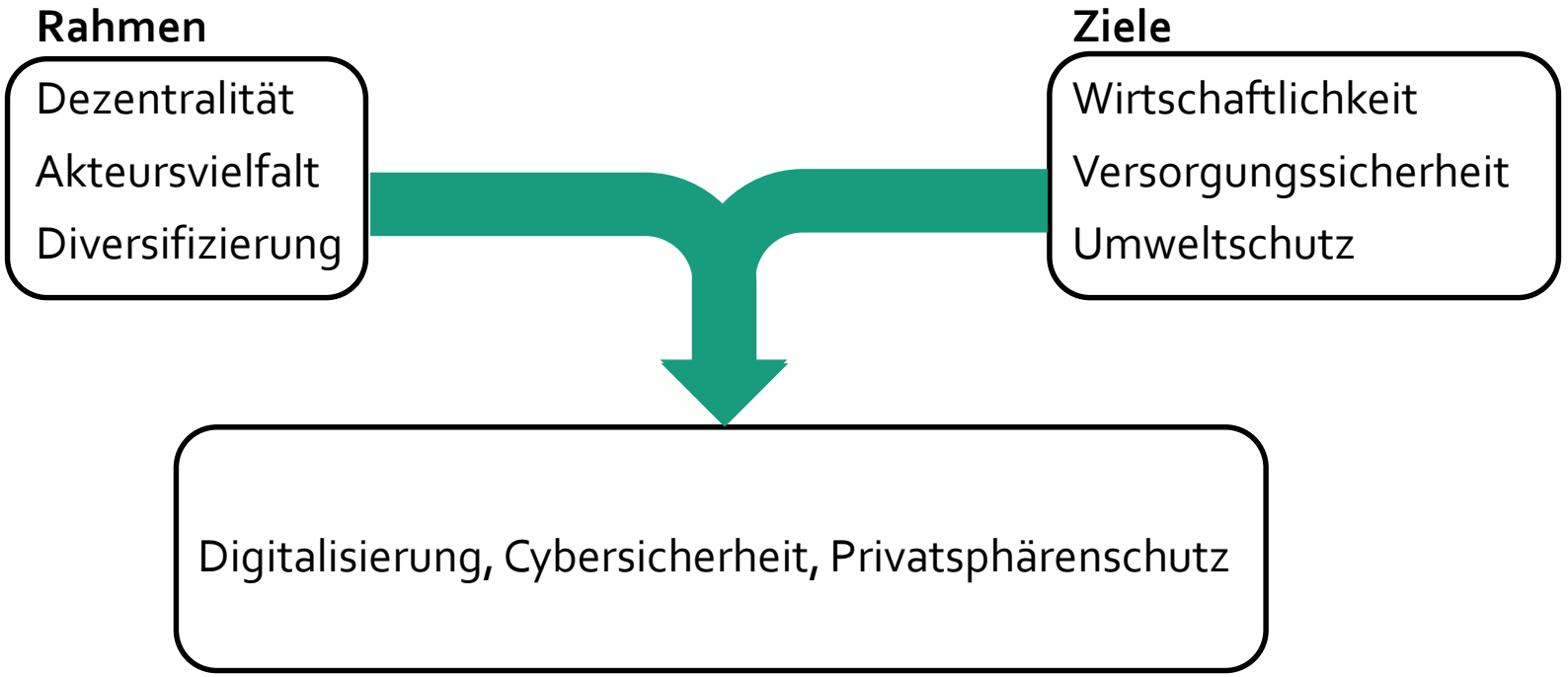
- **Fluktuierende** erneuerbare Energien
- **Flexibel** reagierende komplementäre Stromerzeugung & Nachfrage nach Strom
- **Hinzukommende** Stromanwendungen im Bereich der Gebäude und des Verkehrs
- **Speicher und Anlagen** zur Erzeugung **synthetischer Energieträger**
- Verbrennungstechniken werden **durch elektrische Maschinen ersetzt**, die die Endenergie Strom effizienter **in Nutzenergie (Wärme, Traktion) wandeln**

= > **Dezentralität, Akteursvielfalt und Diversifizierung**

Vgl.: https://www.ise.fraunhofer.de/de/veroeffentlichungen/studien/was-kostet-die-energiewende.html

Energiewende und Digitalisierung

Rahmen und Ziele der Energiewende
=> Digitalisierung, Cybersicherheit und Privatsphärenschutz



Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Prototypische Angriffe

Ökonomisch oder politisch motiviert, organisiert, gezielt, automatisiert

Zeus Trojan and Botnet (2007)

Anonymous (2008)

Jérôme Kerviel vs. Société Générale (2008)

False Flag Operations: “Iranian Cyber Army” vs. “Baidu” Search Engine (2010)

DigiNotar (2011), RSA/Lockheed-Martin (2011), Saudi Aramco (2012), EADS (2012), ...

Stuxnet (2010)

PRC Unit 61398, Shanghai (2013), NSA/GCHQ Programs (2013/14)

German Steel Mill (2014)

Jeep Cherokee (2015)

German Bundestag (2015), US Democratcs National Committee (2016)

Mirai (2016)

XCodeGhost (2015)

Pegasus iOS Spyware (2016)

Ransomware (2016)

DTAG/Speedport (2016)

Yahoo lost 500M/1B passwords (2016)

Various attempts to influence US Presidential Elections (2016)

Wannacry (2017)

Prototypische Angriffe

Ökonomisch oder politisch motiviert, organisiert, gezielt, automatisiert

Zeus Trojan and Botnet (2007)

Anonymous (2008)

Jérôme Kerviel vs. Société Générale (2008)

False Flag Operations: “Iranian Cyber Army” vs. “Baidu” Search Engine (2010)

DigiNotar (2011), RSA/Lockheed-Martin (2011), Saudi Aramco (2012), EADS (2012), ...

Stuxnet (2010)

PRC Unit 61398, Shanghai (2013), NSA/GCHQ Programs (2013/14)

German Steel Mill (2014)

Jeep Cherokee (2015)

German Bundestag (2015), US Democratcs National Committee (2016)

Mirai (2016)

XCodeGhost (2015)

Ransomware (2016)

Pegasus iOS Spyware (2016)

DTAG/Speedport (2016)

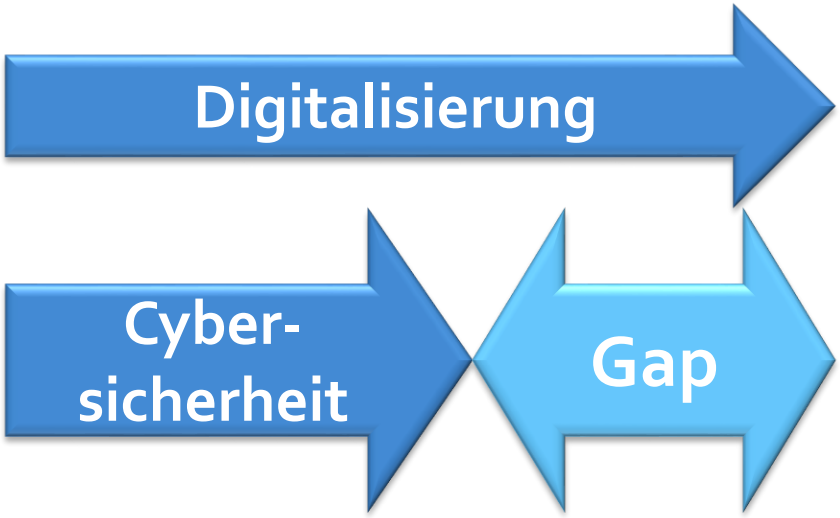
Yahoo lost 500M/1B passwords (2016)

Various attempts to influence US Presidential Elections (2016)

Wannacry (2017)

Cybersicherheit und Schutz der Privatsphäre

hinken – real und gefühlt – der Digitalisierung hinterher



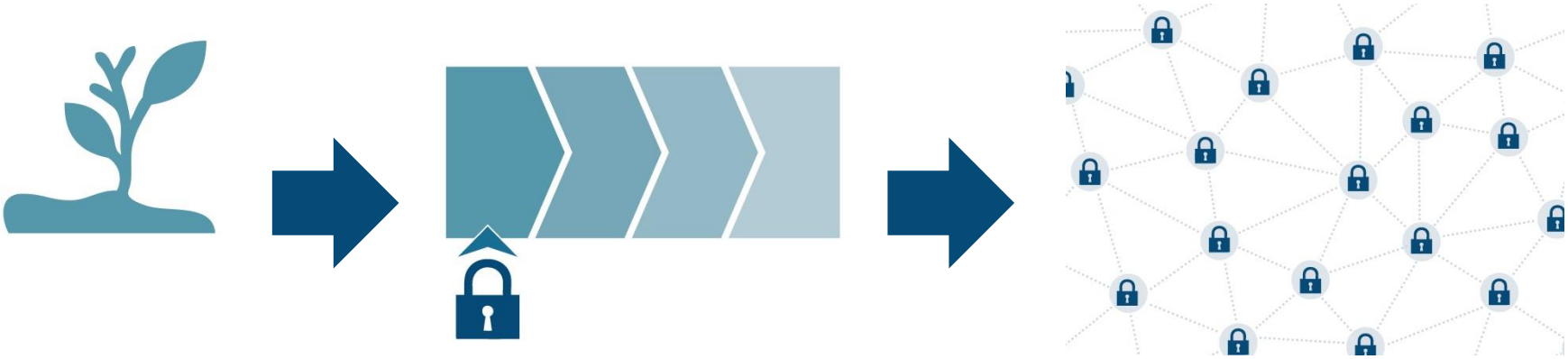
- **Staat und Gesellschaft**
  Snowden, Bundestag, US Wahlen, ...
- **Wirtschaft und Industrie**
  Stuxnet, Hochofen, …
  >51% Betroffene, Milliardenschäden
- **Privatsphäre**
  Yahoo: 1,5 Mrd. Nutzerdaten, …
- **Infrastruktur**
  DDoS-Angriffe, …
- **Wertekonflikte**
  Überwachung + Datenwirtschaft
  vs. Sicherheit und Datenschutz

Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Das Ziel von CRISP: Security at Large

Cybersicherheit für große, reale IT-basierte Systeme



Sicherheit Ad Hoc, primär reaktiv

Schritt 1:
»Security & Privacy by Design«
Systematische Sicherheit, proaktiv & angriffstolerant

Schritt 2:
»Cybersecurity at Large«
Systematische Sicherheit für große, reale Systeme wie z.B. »Industrie 4.0« und »IT der Energiewende«

Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Smart Grid Scenario

Risks and threats

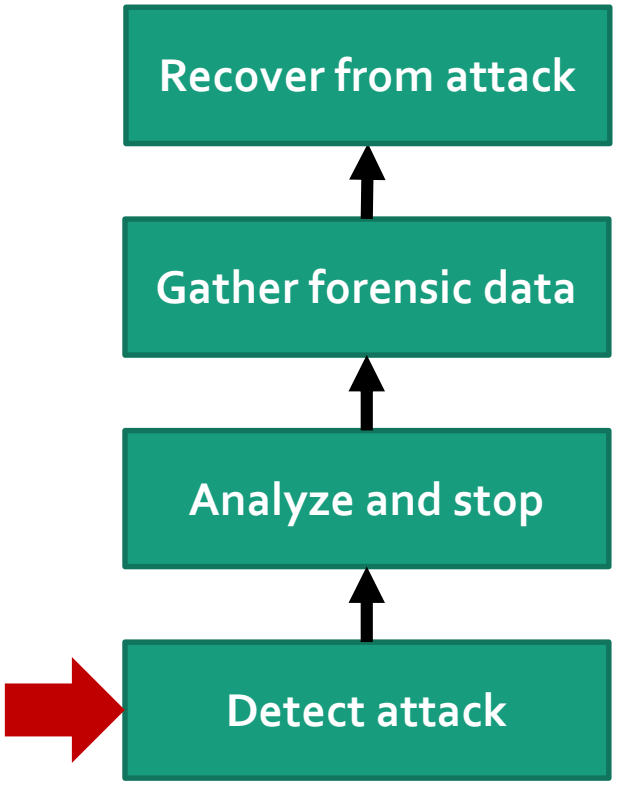
- Targeted attacks on energy distribution
  → **Denial of Service / Blackout**
- Corruption of business processes → **Fraud**
- Placement of dormant Trojans and APTs as **Cyber Weapons**

Security Technology Stack for Distributed Infrastructures

Prevention	Secure Coding Static and Dynamic Analysis Access-Authentication *Many more …*
Mitigation	Process Isolation Compartmentalization Redundancy Mandatory Access Control *Many more …*
Detection	Intrusion Detection Anomaly Detection Runtime Integrity Monitoring *Many more …*
Recovery	Software Updates Factory Reset Trustworthy Remote Integrity Assessment

All Systems need Recovery Capabilities

All software is flawed, hence all systems can be hacked



Recover from attack

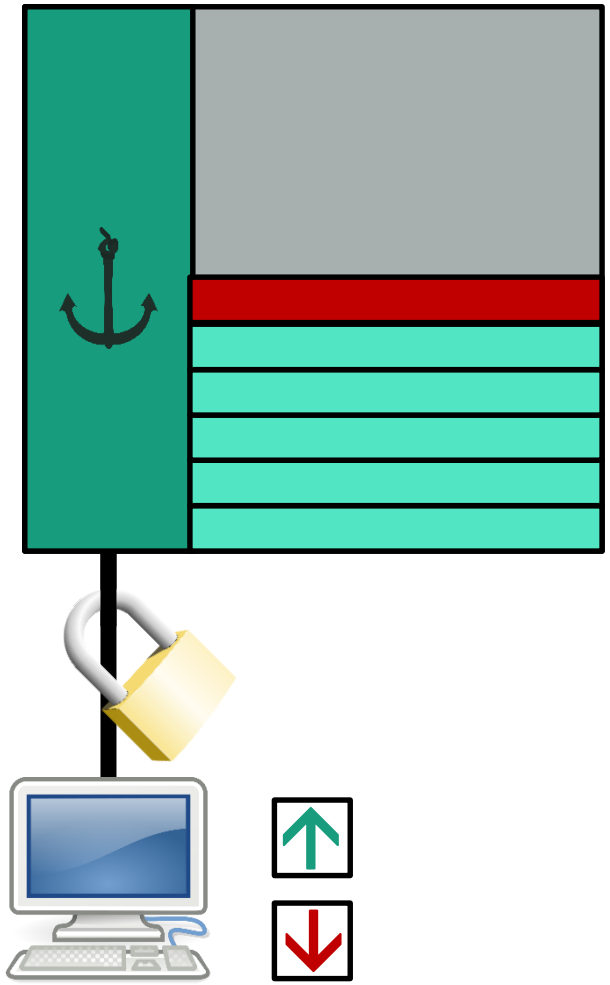
- Reboot (on/off)
  → Maintains vulnerability
- Update / patch software and firmware, reset system remotely
  → Challenge: Any vulnerability may have enabled hidden Trojan, »simulating« an update
- Solution for the challenge
  → Provably security hardware anchor which can remotely attest correct patching and reboot
  → Detects Trojan (reboot must be enforced)

TRUSTED COMPUTING GROUP®

IETF®

Trusted Remote Attestation Solutions by Fraunhofer SIT

Trusted »agent« assists in remotely assessing the integrity of a device



TPM-based integration into control plane protocols

- Time-based Uni-Directional Attestation (TUDA)
- Proposed to IETF for adoption as standard
- Support for TPM 1.2 and extension in development for TPM 2.0

DICE-based attestation for »tiny« devices

- Device Identity Composition Engine based attestation
- Design for attesting of Aduino-class microcontrollers

embeddedworld2017 Exhibition&Conference ...it's a smarter world

HANNOVER MESSE 24–28 April 2017 Hannover • Germany

Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Schutz der Privatsphäre?

Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Was macht Blockchain attraktiv?

Verteilte Einigung in einem Netzwerk, keine zentrale Instanz
- – für viele Anwendungen Einigung schneller
- – robust selbst bei nicht kooperativen / bösartigen Akteuren

Automatisierungspotenzial durch Smart Contracts
- – Abbildung von Werten und Rechten

Nachvollziehbarkeit und irreversibles Protokoll des Transfers (technisch)

Ist die Technologie für die Energiewende relevant?

- Intermediäre
- Daten- und Prozessintegrität
- Dezentrales Netzwerk
- Übermittlung von Werten und Wahrung von Rechten
- Automatisierungspotenzial

=> Distributed Ledger Technology

Überblick

- Cybersicherheit in Darmstadt
- Energiewende und Digitalisierung
- Energiewende und Cybersicherheit
  - Cybersicherheitsparadigmen
  - Beispiel: Trusted Remote Attestation for Smart Grids
  - Beispiel: Schutz der Privatsphäre
  - Blockchain
- Thesen

Thesen

- Angriff lohnt sich → Angriff findet statt
- Digitalisierung der Energiewende setzt Cybersicherheit voraus
- Dezentralisierung und Diversifikation
  => Schutzmechanismen für alle Akteure
- Software, Dienste und Geräte der Energiewende nach Paradigma „Security and Privacy by Design"
- „Security at Large": IT-Sicherheit und Privatsphärenschutz des großen, realen Gesamtsystems Energieversorgung mit seinen hohen Anforderungen an Verfügbarkeit. Neben den Ingenieursmethoden auch empirische Methoden.
- Anwendungsorientierte Forschung: Entscheidende Rolle bei der evolutionären Verbesserung der Cybersicherheit für die Energiewende
- Vorteil von Darmstadt: CRISP am Standort!

תודה רבה!

çok teşekkürler

Merci beaucoup!

谢谢

Thank you very much!

Dank je wel!

Vielen Dank!

Muchas gracias

ありがとうございます

Dziękuję!

zor spas

شكرا لك

Grazie mille!