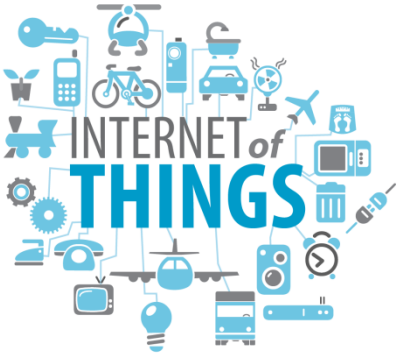
Artemij Voskobojnikov und Benjamin Swiers
Seminar IT-Sicherheit, 2015

Freie Universität Berlin



Absicherung des Internets der Dinge

Welche Mechanismen können auf limitierten Geräten verwendet werden?

Überblick

1. Was ist das Internet der Dinge?
2. Sicherheitsaspekte im IoT
   - Probleme
   - Lösungsansätze
3. Smart Home
4. Industrie 4.0

Was ist das Internet der Dinge (IoT)

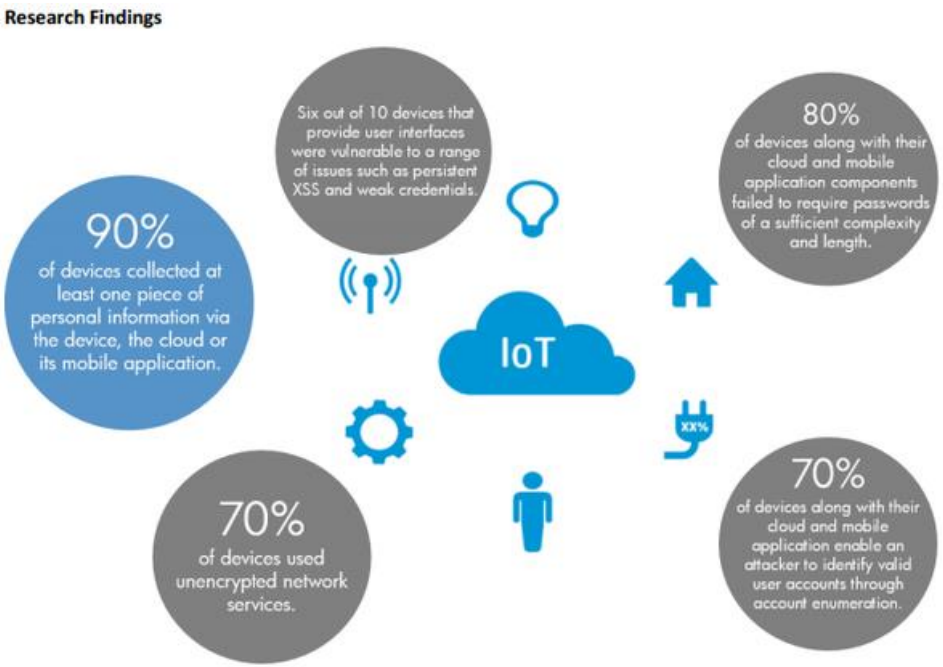
- **Verknüpfung der virtuellen mit der dinglichen Welt**
- **Dezentralität/ Modularität** der Systeme und deren **umfassende Vernetzung**
- **Einbettung** von Hardware und Software **in Geräte** und Gegenstände **des täglichen Gebrauchs**
- Mobile Unterstützung des Nutzers mit Informationsdiensten **an jedem Ort** und **zu jeder Zeit**
- Anpassung des Systems an die aktuellen Informationserfordernisse
- automatische Erkennung und **autonome Bearbeitung** wiederkehrender Aufgaben ohne Nutzereingriff
- **Limitierte Geräte** (Leistung, Energie, Speicher)

Zeitleiste

1997	1999	2001	2005	2010	2008	2011	2014
Smartcards in der Metro von Hongkong	Begriff „Internet der Dinge“ wird geprägt	Drahtloses Tagging in Bibliotheken der Niederlande	Drahtloses Tagging von Chips in den Casinos von Las Vegas	Aufschwung der RFID-Chip-Herstellung	In Japan werden Schuluniformen mit einem integrierten Ortungschip versehen, der verlinkt ist mit einem SMS-Info-Service	Der neue Adidas-Fußballschuh erfasst und analysiert die Bewegungsdaten seines Trägers	An Gebäuden befindliche Sensoren erfassen die Klimawerte innen und außen

Sicherheitsstudie von Hewlett-Packard (2014)

- **10** führende IoT-Geräte → **250** Schwachstellen!
- Untersucht wurden: Fernseher, Webcams, Thermostate, fernsteuerbare Steckdosen, Löschanlagen, Türschlösser, Waagen und Garagenöffner



Beispiele für mögliche Angriffe

Heizungsanlage
Webinterface mit Sicherheitsproblem
Auslesen der Passwörter

Smart TV
Ausspähen von Bild und Ton über integrierte Kamera/ Mikrofon

Hauptgründe für Sicherheitsprobleme im IoT

1. Unsichere Web Interfaces
2. Unzureichende Authentifikation
3. Unsichere Netzwerk Services
4. Mangelnde Transportverschlüsselung
5. Datenschutz/ Privatsphäre
6. Unsichere Cloud-Schnittstellen
7. Unsichere Mobile-Interfaces
8. Unzureichendes Maß an Sicherheitskonfiguration
9. Unsichere Software/ Firmware
10. Mangelnde physische Sicherheit

1) Unsichere Web Interfaces

Potentielle Probleme

- Account Enumeration
- Cross-site Scripting (XSS)
- SQL-Injection
- Schwache Anmeldedaten

Sicherheitsmechanismen

- Validierung der Eingaben
- Passwort-Recovery-Mechanismus robust (kein Hinweis auf gültigen Account)
- Anmeldedaten nicht offen darlegen (Netzwerkverkehr)
- Account-Sperre nach 3-5 falschen Anmeldeversuchen

2) Unzureichende Authentifikation

Potentielle Probleme

- Unzureichende Passwortkomplexität
- Schwacher Schutz der Anmeldedaten
- Unrechtmäßige Erhöhung von Rechten

Sicherheitsmechanismen

- Hohe Passwortkomplexität
- Verschlüsselung der Anmeldedaten
- Zwei-Faktor-Authentifizierung wo möglich
- Sichere Passwort-Recovery Mechanismen
- Public Key Infrastructur (PKI)
- Prüfe Sicherheitsrichtlienien

3) Unsichere Netzwerk Services

Potentielle Probleme

- Angreifbare Services
- Offene Ports als Angriffspunkt
- Denial-of-Service (DoS)

Sicherheitsmechanismen

- Transportverschlüsselung (z.B. AES)
- Nur notwendige Ports offen → Portscanner
- Bestimmte Ports und Services sollten nicht über Internet (z.B. Universal Plug and Play (UPnP)) zugänglich sein
- (PUFS, PKI, …)

Aber: Spagat zwischen Erreichbarkeit und Angreifbarkeit

4) Mangelnde Transportverschlüsselung

Potentielle Probleme

- Unverschlüsselte Services
- Führt potentiell zur Verletzung aller Schutzziele

Sicherheitsmechanismen

- Nutzung von Verschlüsselungsprotokollen(SSL,TLS)
  → Besser: Lightweight Kryptography
- Wenn nicht möglich, nutze andere (industrielle) standardisierte Verfahren
- Sicherer Austausch von Schlüsseln über unsicheren Kanal → z.B. Diffie-Hellman

Aber: Verschlüsselung der Daten kostet Energie → oft Dilemma

5) Datenschutz/ Privatsphäre

Potentielle Probleme

- Verletzung der informationellen Selbstbestimmung
- Sammeln von personenbezogenen Daten

Sicherheitsmechanismen

- Privacy by Design
- Datenvermeidung und Datensparsamkeit
- Anonymisierung und Pseudonymisierung
- Wenn Speicherung erforderlich → Verschlüsselung
- Nur autorisierte Subjekte dürfen Zugriff haben

6) Unsichere Cloud-Schnittstellen

Potentielle Probleme

- Account Enumeration
- Zugriff auf Anmeldedaten → Daten

Sicherheitsmechanismen

- Validierung der Eingaben
- Anmeldedaten nicht offen darlegen (Netzwerkverkehr)
- Account-Sperre nach 3-5 falschen Anmeldeversuchen
- Zwei-Faktor-Authentifizierung, wo möglich

7) Unsichere Mobile-Interfaces

Potentielle Probleme

- Account Enumeration
- Zugriff auf Anmeldedaten

Sicherheitsmechanismen

- Validierung der Eingaben
- Anmeldedaten nicht offen darlegen (Netzwerkverkehr)
- Account-Sperre nach 3-5 falschen Anmeldeversuchen
- Zwei-Faktor-Authentifizierung, wo möglich

8) Unzureichendes Maß an Sicherheitskonfiguration

Potentielle Probleme

- Mangelnde Granularität
- Mangelnde Passwort-Sicherheitsoptionen
- Kein Sicherheits-Monitoring
- Kein Sicherheits-Logging

Sicherheitsmechanismen

- Trennung zwischen User und Admin
- Möglichkeit der Datenverschlüsselung bieten
- Starke Passwort-Richtlinien
- Logging von sicherheitsrelevanten Ereignissen
- Monitoring von Handlungen

9) Unsichere Software/ Firmware

Potentielle Probleme

- Einspielen von Schadsoftware bei Updates
- Firmware enthält sensitive Daten
- Probleme durch veraltete Versionen

Sicherheitsmechanismen

- Privacy by Design
- Update-Funktionalität
- Verschlüsseltes Update-File
- Übertragung der Updates über verschlüsselten Kanal
- Update sollte signiert und verifiziert sein

10) Mangelnde physikalische Sicherheit

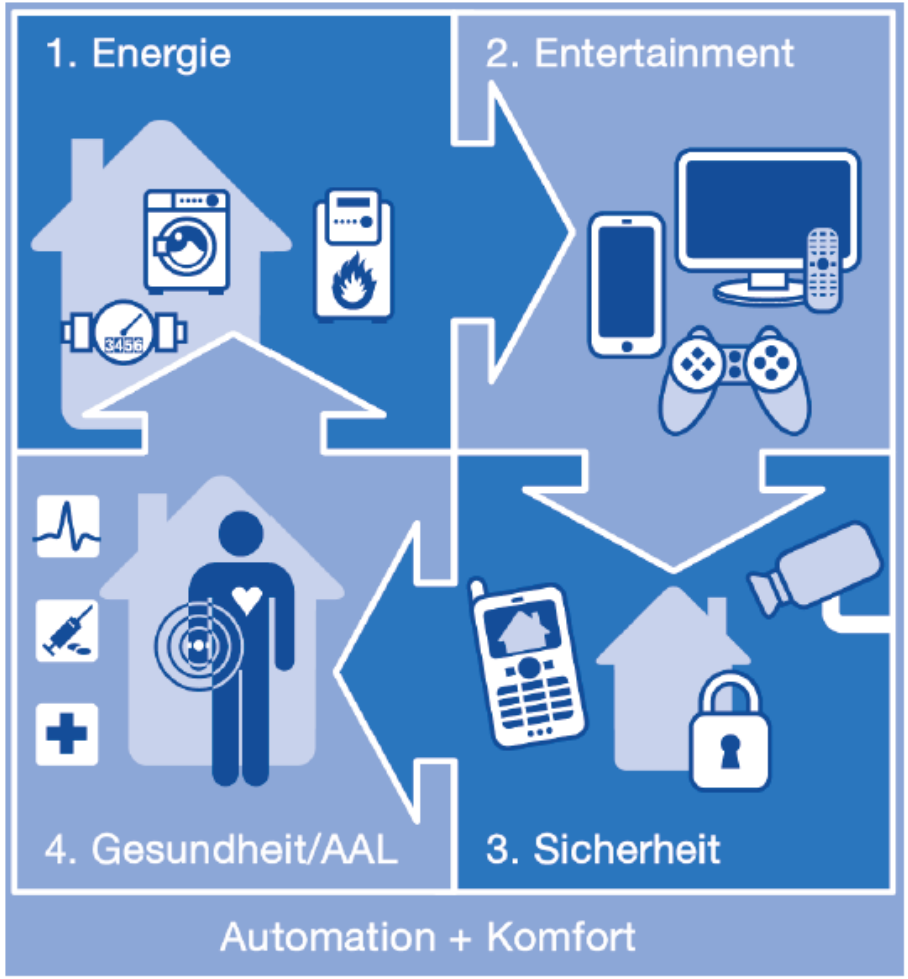
Potentielle Probleme

- Zugang zu Daten über z.B. USB
- Entwendung von Speichermedien

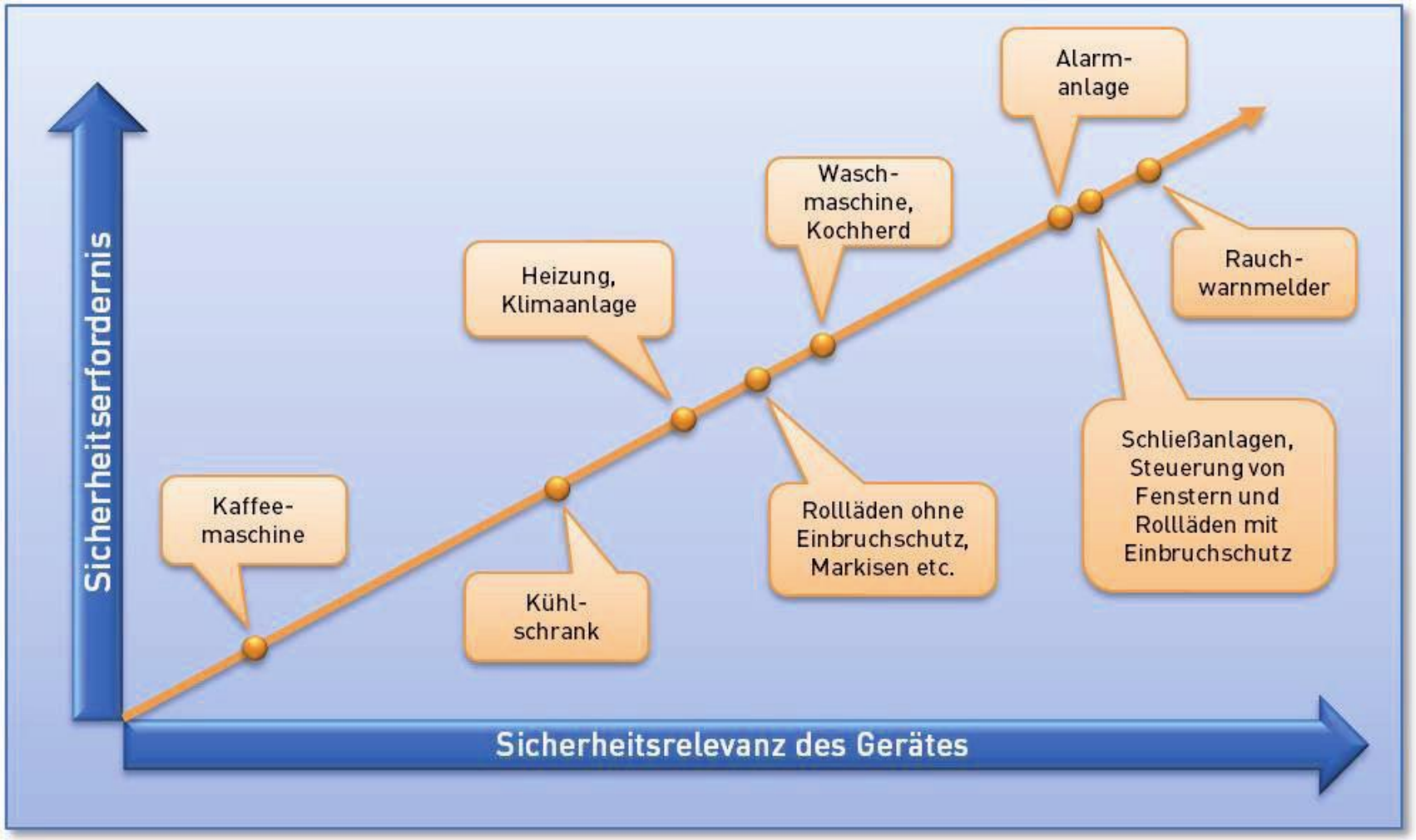
Sicherheitsmechanismen

- Speichermedium darf nicht leicht entfernbar sein
- Daten auf diesem sollten verschlüsselt sein
- Schnittstellen nur für autorisierte Handlungen verwendbar
- Device muss schwer auseinandernehmbar sein

Smart Home - Anwendungsbereiche



Sicherheitsrelevanz von Smart Home-Geräten



Sicherheitsmechanismen im Smart Home

Software

- Sicherheit schon in Planung berücksichtigen (im Nachhinein oft schlecht)
- Verschlüsselungen nach dem Stand der Technik (z.B. AES)

Zugang

- PUF
- PKI
- Gegenseitige Prüfung der Sicherheitsrichtlinien

Sicherheitsmechanismen im Smart Home

Übertragung

- leitungsgebundener Übertragung dem WLAN oder anderen Funk-Übertragungs-wegen vorzuziehen
- Andernfalls in jedem Fall Verschlüsselung und lange, komplexe Passwörter
- Intrusion Detection: Erkennung aktuell laufender Angriffe
- Firewalls(z.B. mit Application Filter)

Hardware

- Bei Erkennung von Gefahr (unberechtigter Fremdzugriff, Manipulation, Sabotage etc.) → Trennung vom Internet
- PUFS

Welche Anwendung findet das IoT im industriellen Bereich?

IKT-Bereiche in Unternehmen

Übliche Unterscheidung zwischen zwei Bereichen:

- Produktions-IT (Controller o.ä.)
- Business-IT (CMS, allgemeine Datenerfassung etc.)

Was ist Industrie 4.0?

Industrie 4.0 vernetzt beide IT-Bereiche, es entstehen cyberphysikalische Systeme (CPS)

CPS sind:

- Beschränkt in ihrer Rechenfähigkeit
- Beschränkt in ihrem Energieverbrauch
- Müssen rund um die Uhr ihre Aufgaben erfüllen (zeitlicher Druck)
- Sind oftmals zertifiziert!

Was für Probleme verbergen sich dahinter?

Vernetzung beider „Welten“ beherbergt Probleme aus beiden Bereichen

→ Neue Verwundbarkeiten und Probleme

- Computerviren der Desktop-PCs bereiten sich auf Produktionsanlagen aus
- Sicherheitspatches können nicht ohne weiteres aufgespielt werden (zertifiziert)
- Verschiedene Anforderungen an jeweiliges Untersystem

Was bedeutet dies genau?

Insbesondere Sicherheitsanforderungen verschieden (Umsetzung nicht trivial):

Firewalls, VPNs oder SSL/TLS nicht im Produktionsumfeld anwendbar, da dies möglicherweise einen Eingriff in die Komponenten benötigt

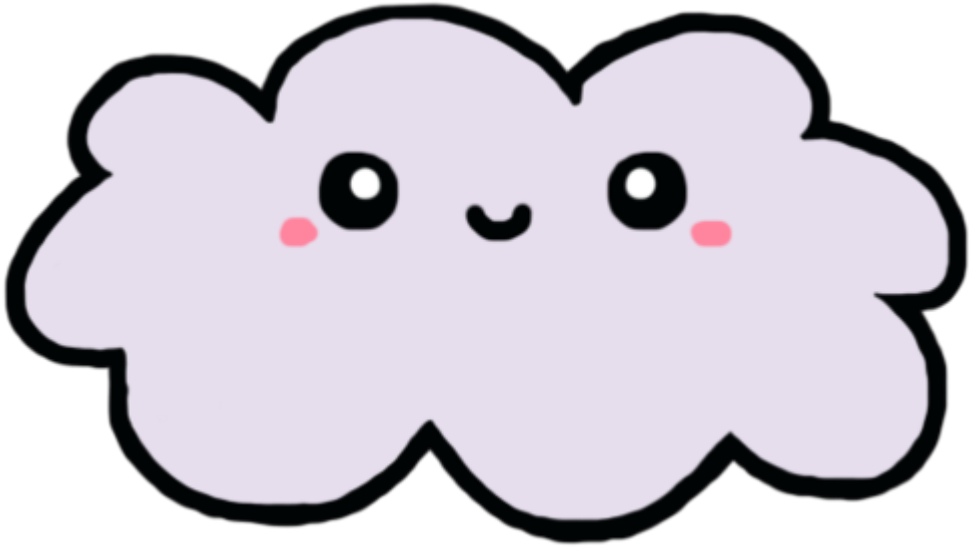
→ Zertifizierung unter Umständen ungültig!

Zusätzlich können dadurch Latenzen entstehen, was in vielen Fällen nicht akzeptabel ist

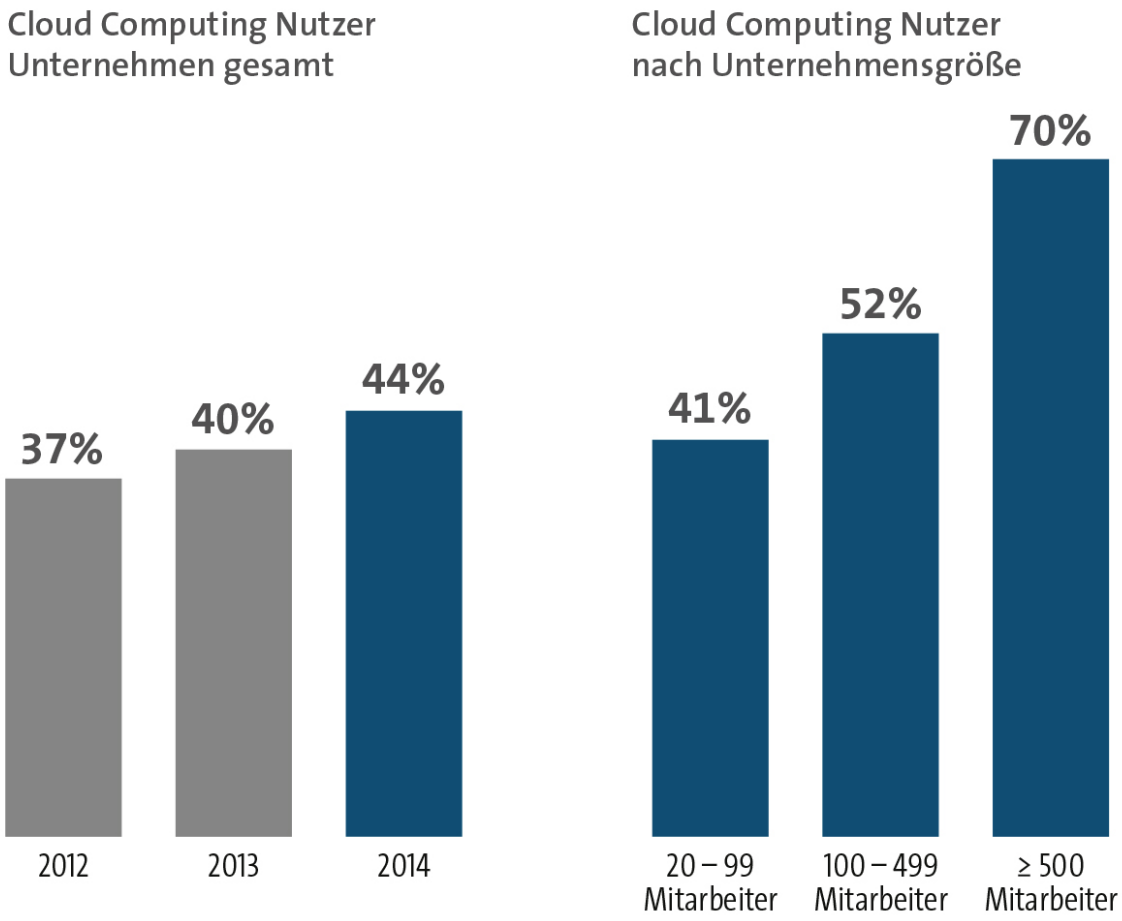
Angreifer können hier sogar physikalischen Zugriff auf die Geräte haben

Industrie 4.0 in einem Bild

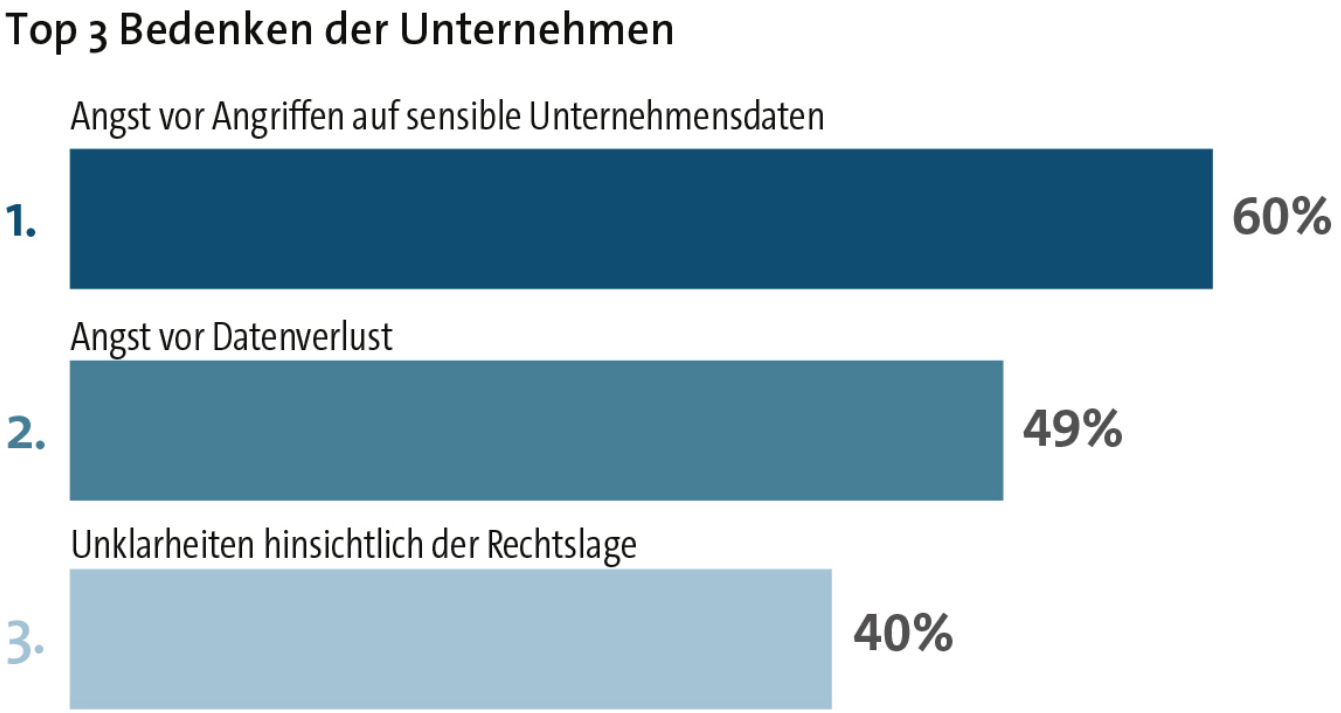
Die Cloud



Cloud-Computing ist in...

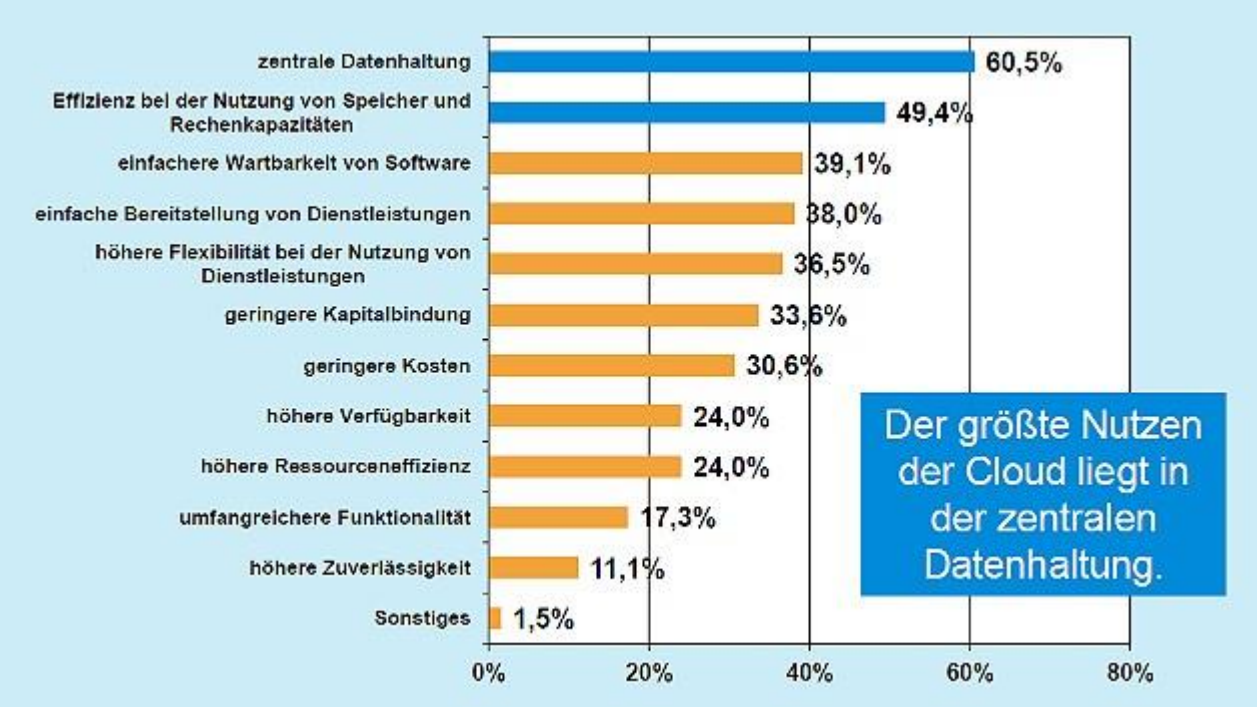


...es gibt aber auch Bedenken

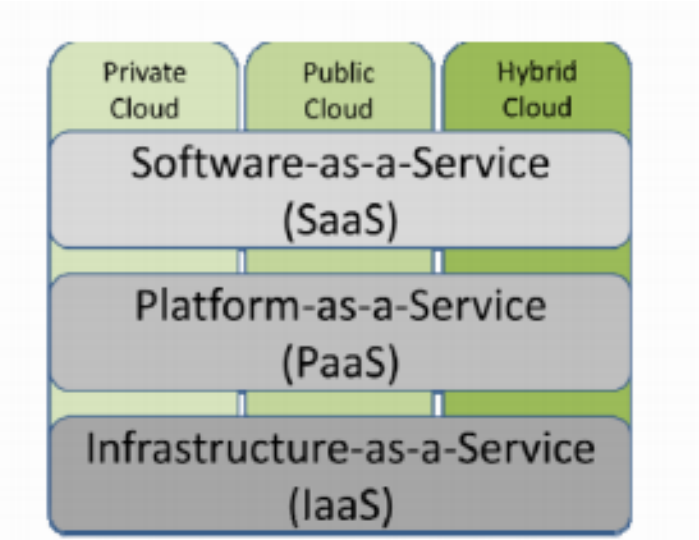


Die Cloud

- Verteilung auf mehrere Server bietet eine hohe Verfügbarkeit
- Cloud-Computing spart Kosten ein (Fernwartung)



Welche Clouds gibt es?

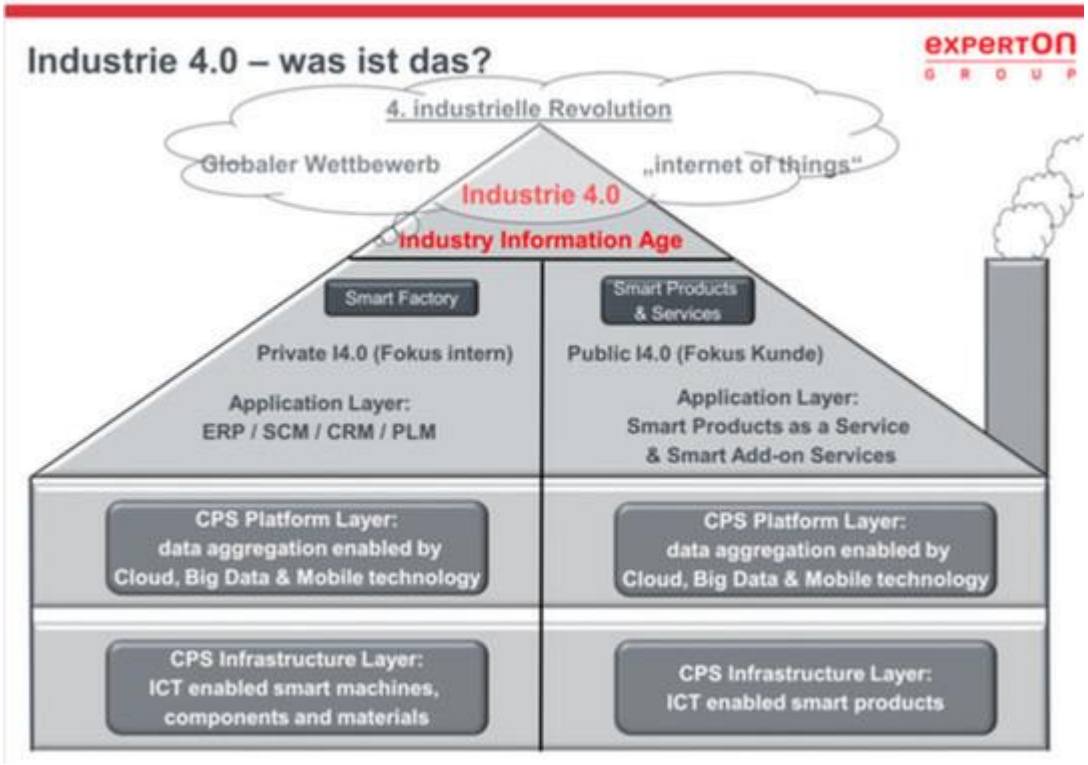


SaaS: komplette Systeme beispielsweise via Browser verfügbar

PaaS: Nutzer können eigene Applikationen deployen

IaaS: Nutzer hat viele Möglichkeiten (OS, Netzwerk, Speicher), der Betreiber kontrolliert das darunterliegende Cloud-Netzwerk

Private vs Public Cloud



Herausforderungen in der Industrie 4.0

- Schutz der Daten bereits dort ansetzen, wo diese erhoben werden (Sensoren)
- Die Übertragung zur Cloud muss sicher sein
- Zugriffskontrolle in der Cloud
- Datenschutz!

→ „Sicher vom Sensor bis in die Cloud!“

Wir konzentrieren uns auf

- Einführung in die Cloud-Sicherheit, Vorstellung der grundlegenden Konzepte
- Absicherung von Komponenten mit beschränkten Ressourcen (wie beispielsweise Controller)

Absicherung der Cloud

Was muss alles abgesichert werden?

- Übertragung der Daten zwischen Cloud-Service und Maschine
- Speicherung der Daten in der Cloud
- Nutzung, Verarbeitung und Weitergabe der Daten
- Kommunikation mit der Cloud über das Internet (viele Knotenpunkte zwischen Sender und Empfänger)

„Trusted Cloud“

- Vom Bundesministerium für Wirtschaft und Energie
- Böswillige Systemadministratoren sollen nicht auf Daten in der Cloud zugreifen können

- Speziell gesicherte Serverschränke
- Verschlüsselte Speicherung in Datenbanken
- Bei der Verarbeitung nur im flüchtigen Speicher
- Server fahren runter, falls Unberechtigten den Schrank aufschließen
- Auch verschlüsselte Speicherung auf den Datenträgern

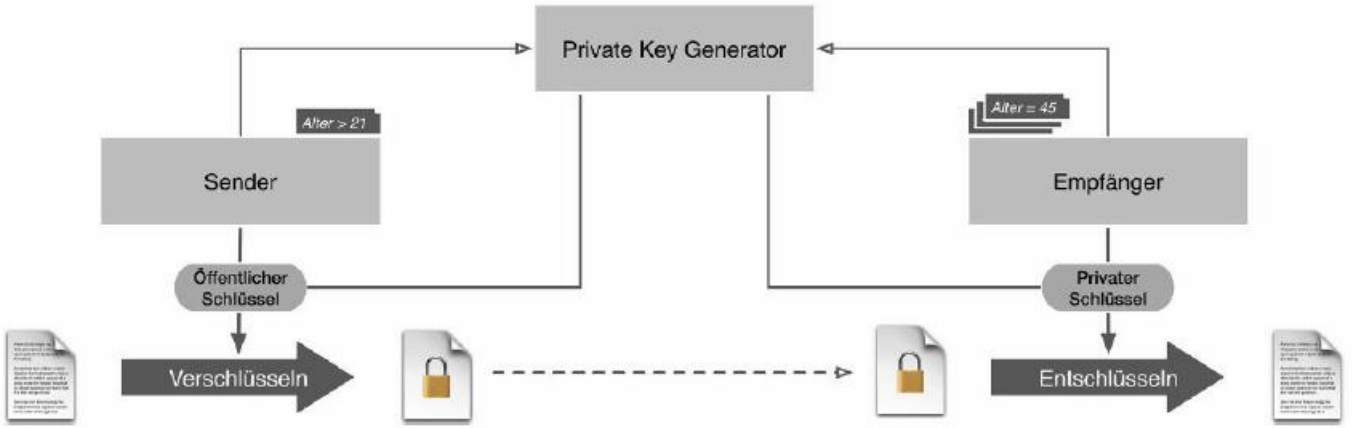
Zugriffsbeschränkungen für Cloud-Dienste

Rollenbasierte Zugriffskontrolle denkbar, aber bei möglicher Schwachstelle könnten die Softwarekontrollen umgangen werden

→ besser: Attributbasierte Verschlüsselungssysteme

- Diese erlauben es, dass nur Schlüssel verwendet werden können, die gewisse Attribute besitzen
- Diese Attribute ermöglichen es Zugriffsberechtigungen direkt in die verschlüsselten Daten oder kryptografischen Schlüssel zu kodieren

Attributbasiertes Verschlüsselungssystem



- Öffentlicher Schlüssel von einer Dritten Instanz ausgestellt (PKG)
- Ein Empfänger kann nur entschlüsseln, wenn er die nötigen Attribute besitzt
- PKG stellt auch den privaten Schlüssel aus
- Beim Verlassen der Gruppe → Schlüssel entziehen, erneute Verschlüsselung der Daten mit neuem Schlüssel

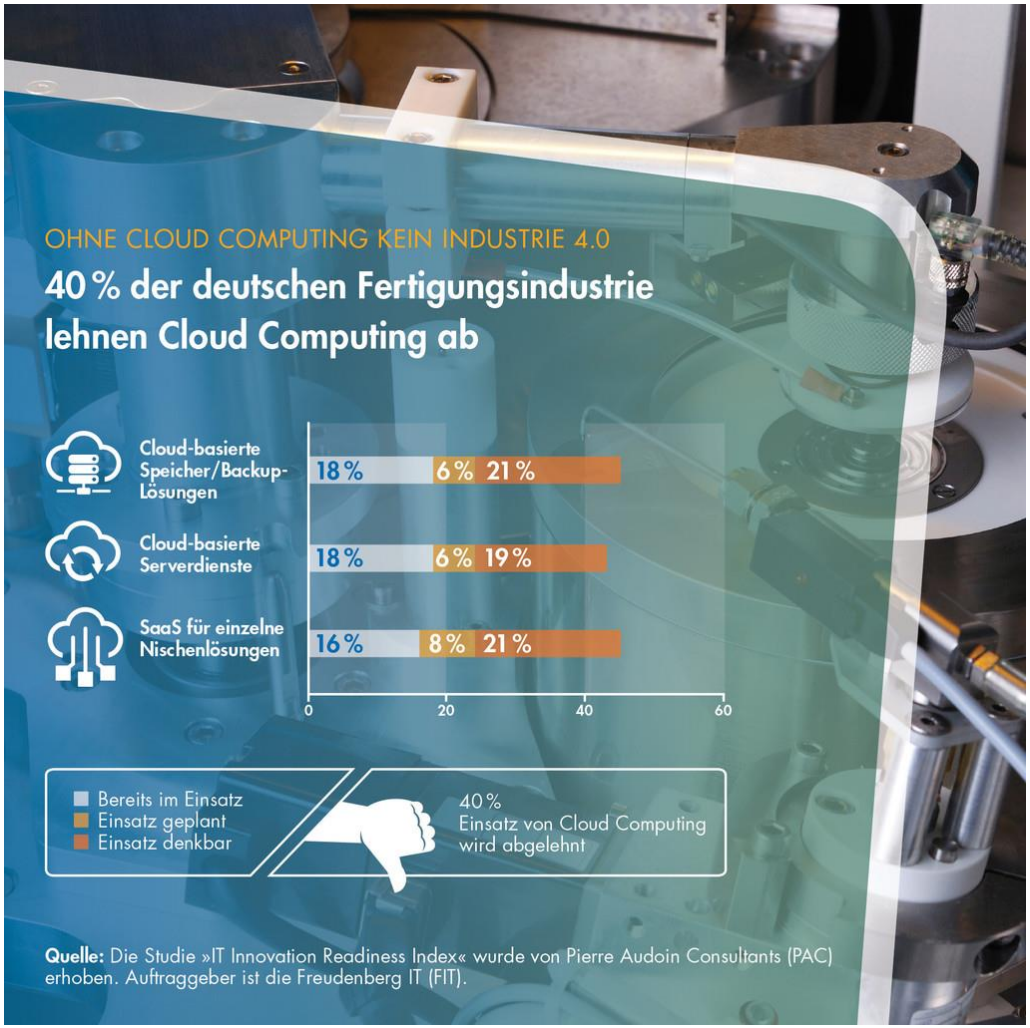
Suchen nach Daten

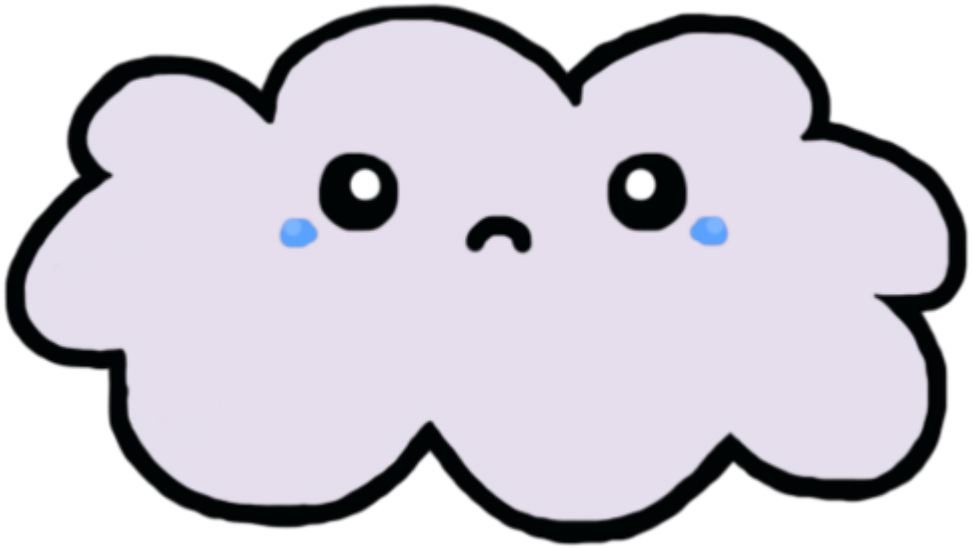
Daten nur verschlüsselt vorzufinden, Problem bei der Suche!

Lösung: Searchable Encryption

- Verwendung von kryptografischen Verfahren, welche die Suche auf verschlüsselten Daten zulassen (**SSE** oder **ASE**)
- Nach Finden → Übertragung der verschlüsselten Daten zum Anwender, welcher die Daten nun entschlüsseln kann

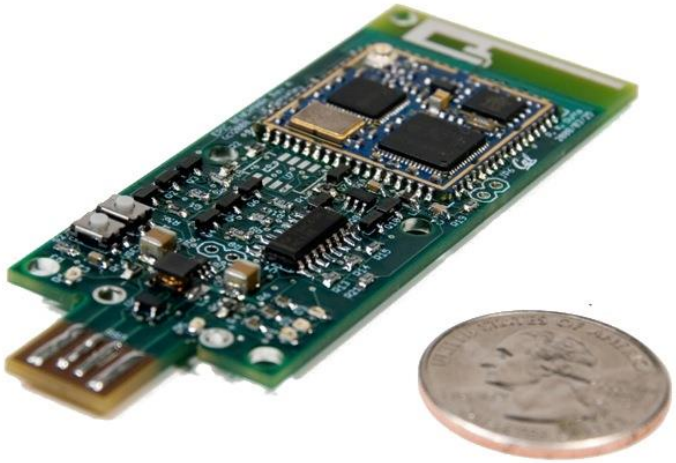
Ohne Cloud Computing kein Industrie 4.0





Komponenten mit beschränkten Ressourcen

Was ist ein Gerät mit beschränkten Ressource



- Besitzen nicht immer ein Betriebssystem
- Beschränkt in Größe und Leistung
- Müssen sparsam sein
- Müssen dabei schnell bleiben
- Müssen zuverlässig sein

Sicherheit eines solchen Geräts

Zwei verschiedene Sicherheitsbereiche:

- Sicherheit bei der Datenübertragung
- Absicherung des Gerätes selbst

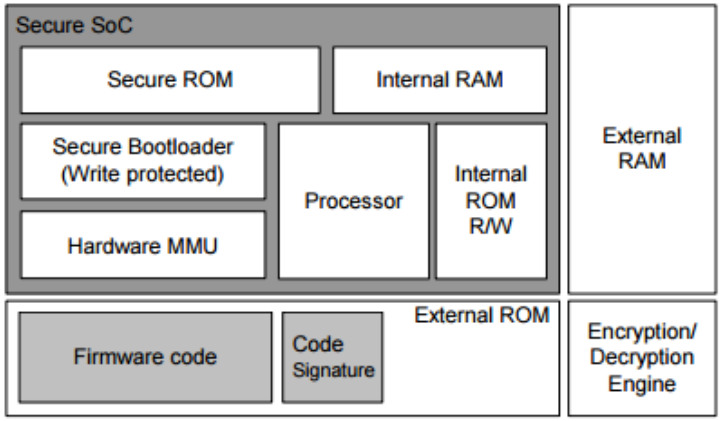
Die Verschlüsselung der Datenströme unterscheidet sich nur bedingt von bekannten Systemen, wir konzentrieren uns auf die Absicherung des Gerätes selbst

Warum muss man das Gerät absichern?

Ein Arbeiter könnte ein Gerät manipulieren, was tun?

PUFs (Physical Unclonable Functions) können verwendet werden um Produktteile zu identifizieren

Ebenfalls werden Schlüssel sicher im System gespeichert (**SoC)**



Auf Secure ROM kann physisch nicht zugegriffen werden

Die Buse des SoC können nicht abgehört werden

Physical Unclonable Function

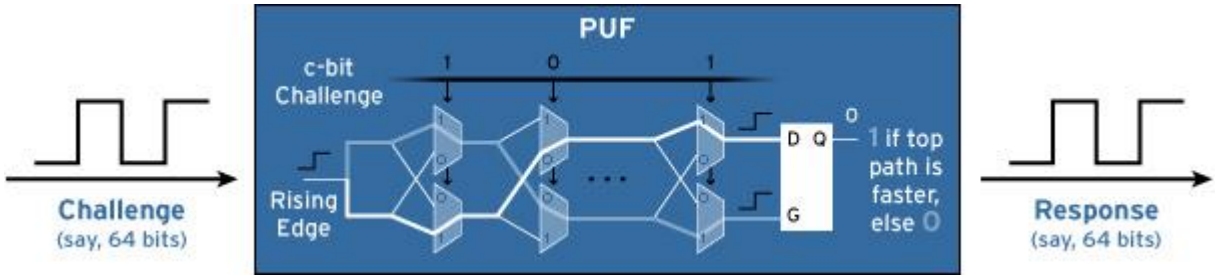
- Idee: keine zwei Stromkreise sind identisch!
- Eine PUF erzeugt ein Geheimnis, welches ein Produktteil identifizieren/ authentifizieren kann
- Sie muss einfach durchzuführen sein, aber schwer zu fälschen
- Hardwareversion einer Einwegfunktion (will man erreichen)

PUF – Ein Beispiel

Challenge: c

Response r = f(c)

Hier MUX-PUF:



- Für jede Challenge hat ein (integrierter) Schaltkreis die gleiche Respone
- Für jede Challenge haben unterschiedliche (integrierte) Schaltkreise unterschiedliche Responses

Was bedeutet dies für das Gerät?

- Ein Gerät könnte mit PUFs die eigenen Komponenten im besten Fall identifizieren
- Es entstehen also Geräte, die in der Produktion auf Verwendung von originalen Teilen geprüft werden können
- Diebstahl oder Manipulation wird dadurch erschwert!

Fazit

- Probleme auf Grund der beschränkten Ressourcen und massiven Vernetzung nicht einfach zu lösen
- Industrie 4.0 erbt Schwachstellen aus den beiden IT-Bereichen
- Neue Sicherheitsanforderungen müssen beide schützen
- Schutz der Bauteile, der Kommunikation und der Cloud als zentrale Verwaltung
- Viele Bereiche müssen noch optimiert werden, Forschungsbedarf!

Quellen

1) E. Eppinger et al. (Hrsg.), Dienstleistungspotenziale und Geschäftsmodelle in der Personalisierten Medizin, © Springer Fachmedien, Wiesbaden 2015.
2) R. Watson, 50 Schlüsselideen der Zukunft, © Springer-Verlag Berlin Heidelberg, 2014
3) R. Roman, P. Najera, J. Lopez, Securing the Internet of Things, Article published in IEEE Computer, vol. 44, no. 9, pp. 51-58, 2011.
4) M. Friedewald, O. Raabe, P. Georgieff et al.: Ubiquitäres Computing: Das „Internet der Dinge“ – Grundlagen, Anwendungen, Folgen, Berlin: Edition Sigma (Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, 31), 2010.
5) ZDFNet, HP findet 250 Schwachstellen in zehn Geräten fürs Internet der Dinge, Online unter URL: http://www.zdnet.de/88200176/hp-findet-250-schwachstellen-zehn-geraeten-fuers-internet-der-dinge/
6) Open Web Application Security Project (OWASP), OWASP Internet of Things Top 10, 2014, Online unter URL: https://drive.google.com/file/d/0B52IUvO0LP6ON2VzZVFkNGF6aVE/view?pli=1
7) Landeskriminalamt Nordrhein-Westfalen, Smart Home und Connected Home, Sicherheitsempfehlungen für Hersteller, Fachhändler und Handwerker, Düsseldorf 2014.
8) Eckert C. & Fallenbeck N. (2015): „Industrie 4.0 meets IT-Sicherheit: eine Herausforderung!“, Berlin Heidelberg 2015.

Quellen

9) Devadas, S.: Physical Unclonable Functions and Applications, online unter: http://people.csail.mit.edu/rudolph/Teaching/Lectures/Security/Lecture-Security-PUFs-2.pdf

10) Wind River Systems (2015): Security in the Internet of Things, online unter: http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

11) Anoop MS (2008): Security needs in Embedded Systems, online unter: https://eprint.iacr.org/2008/198.pdf

12) Channelpartner: http://www.channelpartner.de/a/security-services-fuer-industrie-4-0,3044992

13) Eckert C. (2014): IT-Sicherheit und Industrie 4.0, online unter: http://www.i40.de/wp/wp-content/uploads/2015/04/IT-Sicherheit-und-Industrie-4.0.pdf

14) MUX-PUF: online unter: http://studiopresence.com/client/verayo/technology

Quellen – Bilder (1)

- http://www.n-droid.de/wp-content/uploads/2015/01/Internet-der-Dinge.png
- http://www.heise.de/newsticker/meldung/Vaillant-Heizungen-mit-Sicherheits-Leck-1840919.html
- http://www.stern.de/digital/homeentertainment/samsung-fernseher--smart-tv-kann-via-dvb-t-gehackt-werden-6190476.html
- http://www.zdnet.de/88200176/hp-findet-250-schwachstellen-zehn-geraeten-fuers-internet-der-dinge/
- http://imagescdn.tweaktown.com/news/3/9/39828_01_fbi_investigates_reported_theft_of_1_2_billion_internet_credentials.jpg
- http://i.wfcdn.de/teaser/660/11753.jpg
- http://www.androidmag.de/wp-content/uploads/2013/05/Biometrics.jpg
- http://www.nano-itdesign.de/imgs/netzwerke_1.jpg
- https://detektiv-lux.de/achtung-email-anbieter-stellen-ab-heute-auf-transportverschluesselung-um/
- http://www.fruehgeborene-bildung.de/fotos/mainTitle/bi_neuesweb.png
- http://us.cdn4.123rf.com/168nwm/stokkete/stokkete1204/stokkete120400163/13410590-futuristische-anzeige-cloud-computing-touchscreen-schnittstelle.jpg
- http://designshack.net/wp-content/uploads/lesson1.jpg
- Landeskriminalamt Nordrhein-Westfalen, Smart Home und Connected Home, Sicherheitsempfehlungen für Hersteller, Fachhändler und Handwerker, Düsseldorf, 2014

Quellen – Bilder (2)

- http://praxisit.net/tl_files/inhalte/bilder/hardnsoftware.png
- http://acadtech.gwu.edu/sites/acadtech.gwu.edu/files/image/13030015p3-app%20icons.jpg
- http://www.computerbetrug.de/wp-content/uploads/2011/07/Fotolia_30881854_S.jpg
- https://fasab.files.wordpress.com/2012/05/image023.jpg
- http://www.renewbl.com/wp-content/uploads/2009/03/werkiii_70.jpg
- http://s.hswstatic.com/gif/hammer-1.jpg
- http://images.channelpartner.de/images/computerwoche/bdb/2506412/890x.png
- https://www.bitkom.org/Presse/Pressegrafik/2015/M%C3%A4rz/150306_CloudMonitor/BITKOM-Grafik_Cloud_Computing(1).jpg
- TREND MICRO, Addressing Data Security Challenges in the Cloud
- http://29.media.tumblr.com/tumblr_lqgee1v5fj1qaiwhyo2_500.png
- http://images.vogel.de/vogelonline/bdb/732400/732402/26.jpg
- http://www.elektroniknet.de/typo3temp/pics/c_54ab7e406b.jpg
- http://www.cloud-tresor.de/wp-content/themes/tresor/images/logo_trusted_cloud.jpg
- Eckert C. & Fallenbeck N. (2015)
- http://images.vogel.de/vogelonline/bdb/615200/615209/4.jpg
- http://30.media.tumblr.com/tumblr_lqgee1v5fj1qaiwhyo1_500.png
- http://www.cs.berkeley.edu/~prabal/research/embedded/epic.jpg
- Anoop MS (2008)
- MUX-PUF