Eric Clausing

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

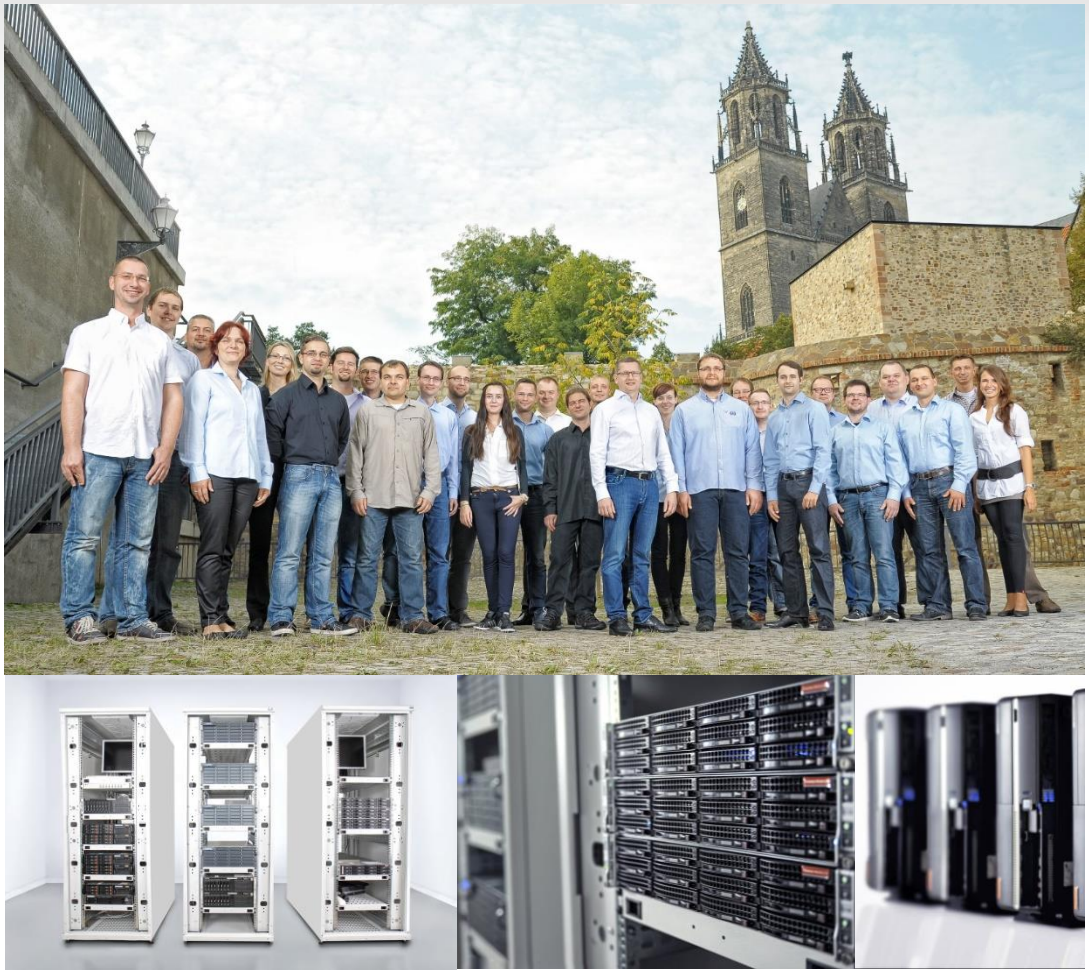
Sicheres Design im Internet of Things

Über das AV-TEST Institut

- Mehr als 35 IT-Spezialisten
- Mehr als 15 Jahre Expertise im Bereich Antivirenforschung
- Unternehmensgründung 2004

- Eine der weltweit größten Virendatenbanken
- 500 Client- und Server-Systeme
- Mehr als 2.500 Terabyte Testdaten
- Mehr als 5.000 Einzel- und Vergleichstests pro Jahr

- Analyse, Testing, Development, Consulting & Services für AV-Hersteller, Fachmagazine, Behörden & Unternehmen



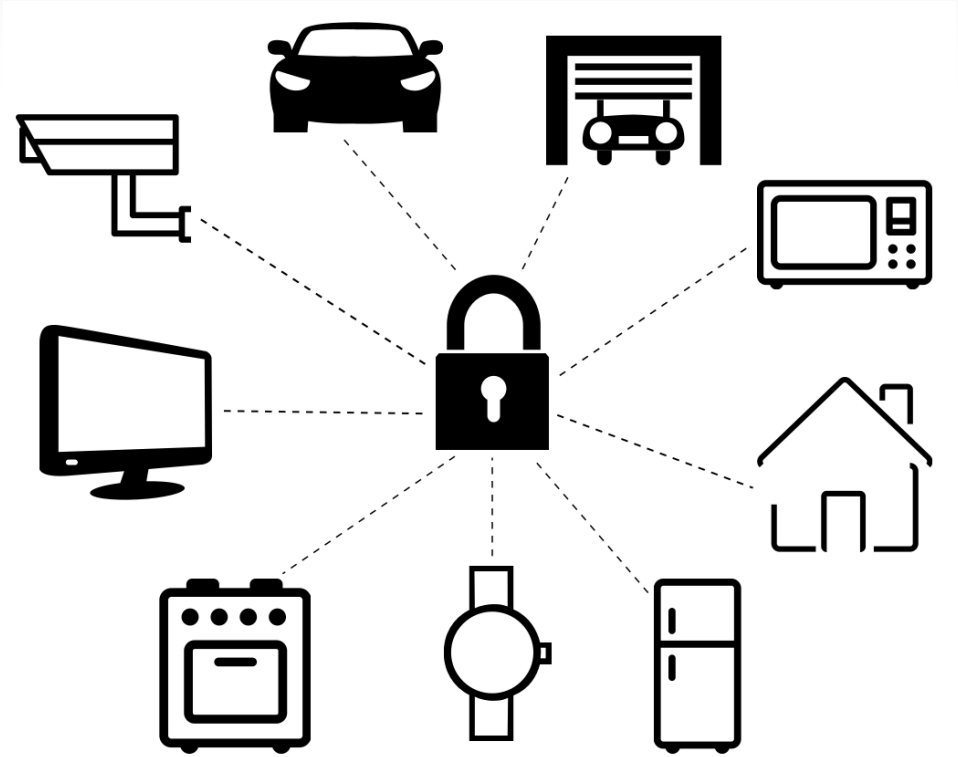
Über das AV-TEST Institut

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

- Transparente Veröffentlichung aller Testergebnisse auf https://www.av-test.org
- Vergabe der AV-TEST Qualitätssiegel „Certified“ und „Approved“
- 1.686 AV-TEST Zertifikate seit 2010 vergeben
- Der AV-TEST Award für die jahresbesten Schutzlösungen in den Bereichen Heimanwender, Unternehmen und Mobile Security.
- Der AV-TEST Innovation Award für innovative IT-Schutzlösungen

Agenda

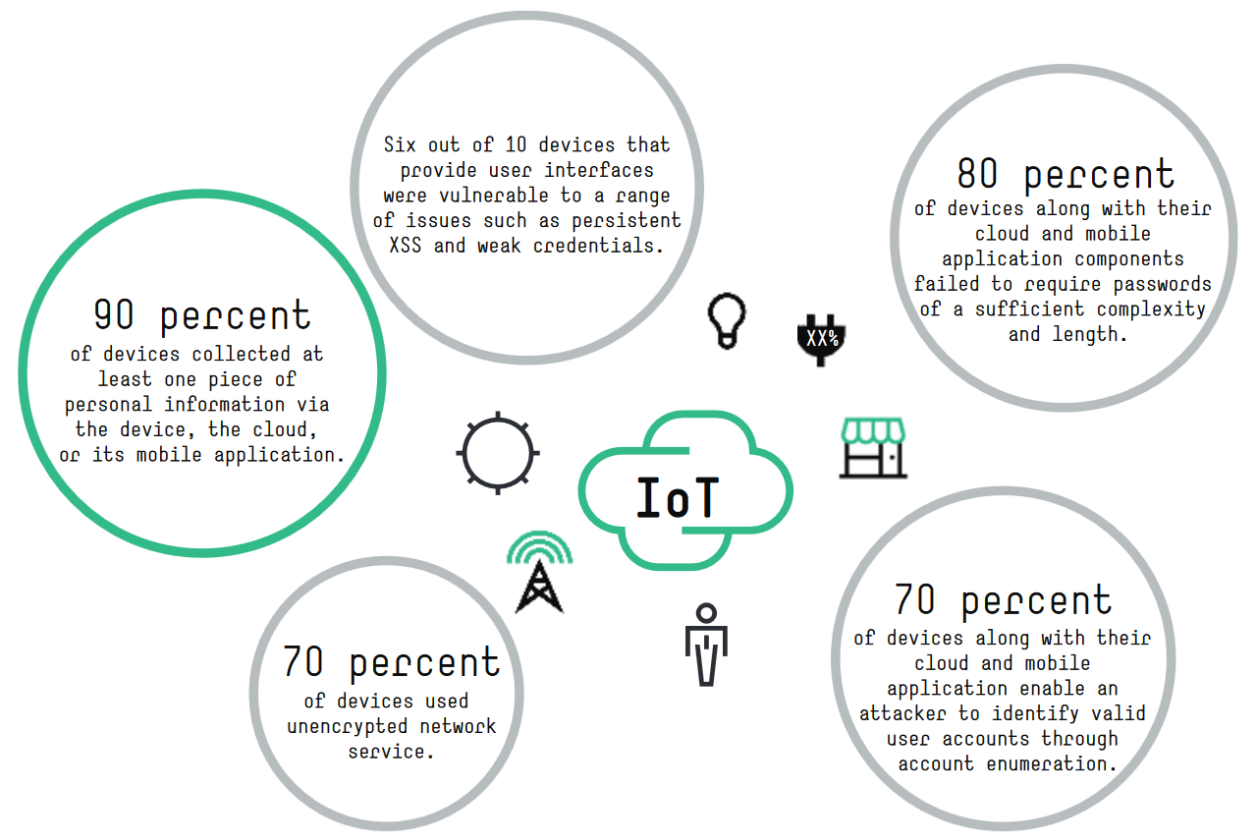
- Motivation
- Grundgedanken
- Kritische Bereiche
  - Authentifizierung
  - Online-Kommunikation
  - Lokale Kommunikation
  - Firmware / Hardware
  - Behandlung sensibler Daten
- Schlussfolgerungen und Empfehlungen



Motivation

- Das Internet of Things wächst ständig, unglaublich schnell und hält dabei in beinahe jedermanns Leben Einzug
  - Immer **neue Hersteller, Produkte und Produktsparten** bilden sich heraus
  - Der **Sicherheit** wird dabei oft **nicht die gebührende Aufmerksamkeit** geschenkt
- Unsere Tests zeigen, dass das **Sicherheitsniveau** zwar wachsend ist, aber zum Teil immer noch **unnötig niedrig**
  - Klassische, eigentlich „ausgestorbene“ **Fehler** werden **wiederholt**
  - Sicherheit in **kritischen Bereichen nicht adressiert**
  - Existierende **Lösungen nicht verwendet**
  - **Sicherheitsbewusstsein** bei vielen Herstellern **nicht ausreichend ausgeprägt**
- **Kaum Sicherheitsrichtlinien** und Empfehlungen speziell für den Bereich des Internet of Things

Motivation



Quelle: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=eny

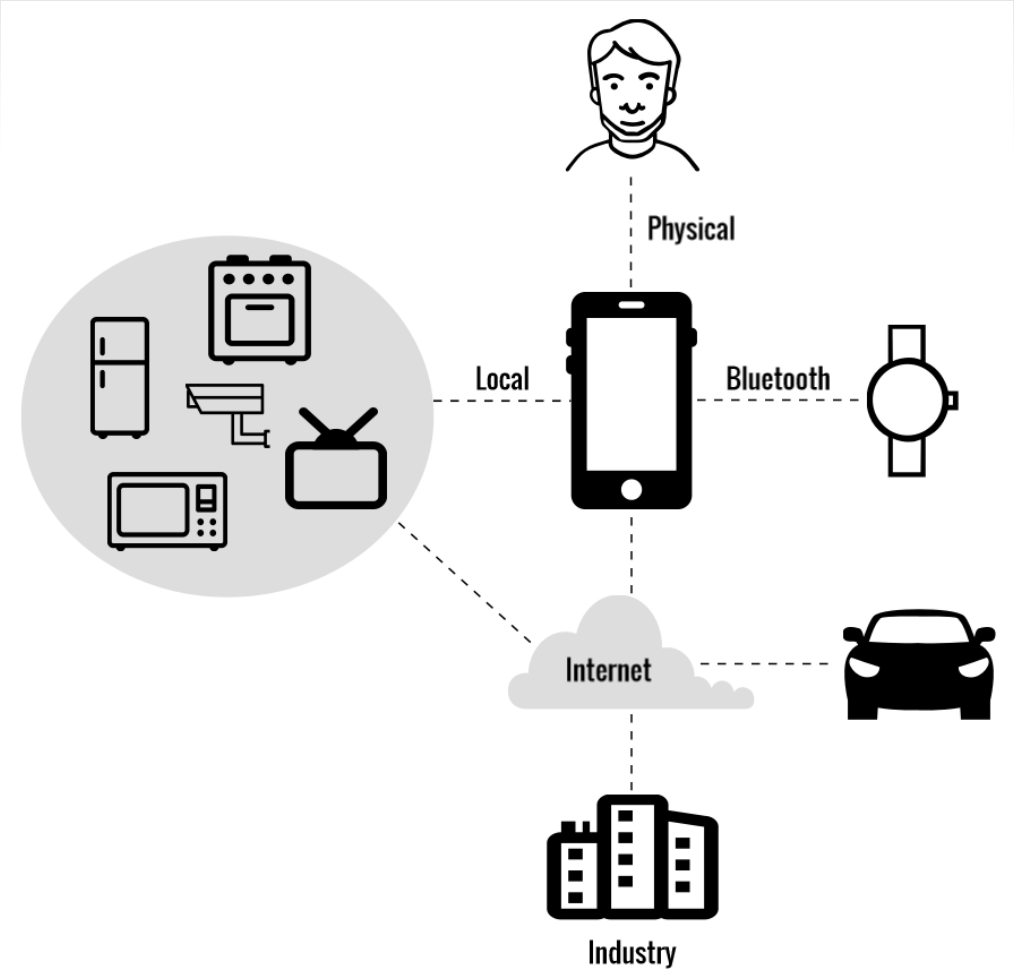
Grundgedanken

- **Angreifermodell**
  - **Essentiell** für adäquates Sicherheitskonzept
  - Auch für IoT sind **Standardmodellierungssansätze anwendbar** (bspw. *Dolev-Yao-Modell*)
  - Häufig festgestelltes Problem: Keine Berücksichtigung des eigentlich **legitimen Nutzers als Angreifer**!
    - Einige Anwendungsszenarien in denen kriminelle Energie vom Nutzer ausgehen kann (Beispiel Fitness-Tracker)
    - Oftmals **unzureichende Integritäts- und Authentizitätssicherung** gegenüber dem Nutzer ermöglicht einfach Manipulationen

Grundgedanken

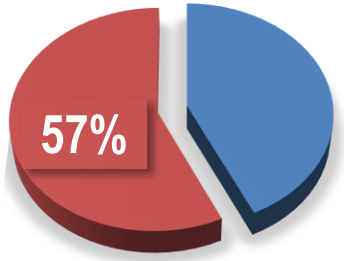
- **Kerckhoffs‘sches Prinzip**
  - Eines der ältesten und immer noch **essentiellen Prinzipien** der Kryptographie:
    - Die Sicherheit eines Algorithmus darf nicht von der Geheimhaltung seiner Funktionsweise abhängen. (im **Gegensatz** zum Prinzip **„Security by Obscurity“**)
  - Ursprünglich nur auf kryptographische Algorithmen bezogen, kann es aber generell **für jeden Sicherheitsmechanismus** angewendet werden
  - Häufigste Verletzungen des Prinzips:
    - Passwörter, Schlüssel oder Zertifikate **„hard coded“**
    - Algorithmen mit **schlüsselunabhängiger** Funktionsweise
    - Algorithmen **ohne begutachtete** Funktionsweise

Kritische Bereiche



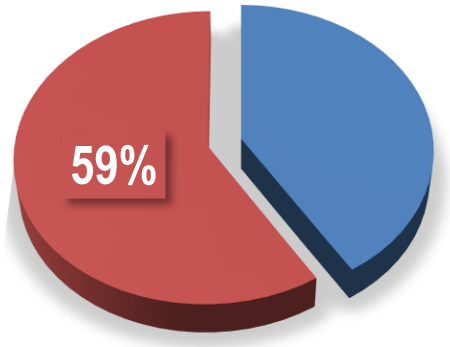
Kritische Bereiche

- **Authentifizierung**
  - Einer der **wichtigsten Punkte** für ein sicheres Konzept
  - Ein **Großteil** der in der Praxis gefundenen konzeptionellen **Schwachstellen** haben **Ursprung in einer unzureichenden Authentifizierung** und ließen sich durch adäquate Umsetzung verhindern
  - Häufigste Probleme:
    - **Fehlende** Authentifizierung
    - **Einseitige** Authentifizierung
    - Authentifizierung mit **statischen Daten und/oder ohne zeitlichen Bezug**
    - Authentifizierung mit **öffentlich zugänglichen Daten**
    - Nichtbeachtung des Kerckhoffs'schen Prinzip und **mangelnde Geheimhaltung** der Funktionsweise
    - Nichtbeachtung N:N **Nutzer-Anwendungs-** und transitiver **Besitzverhältnisse**



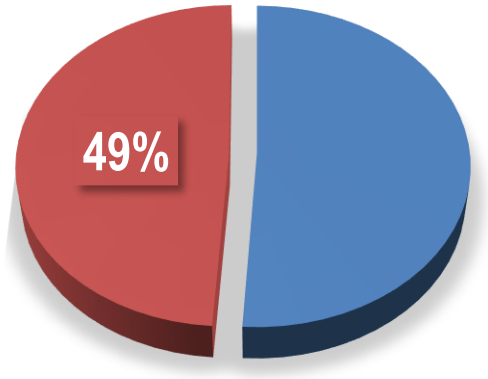
Kritische Bereiche

- **Online-Kommunikation**
  - Naturgemäß besitzt jedes IoT-Gerät einen **Kanal ins Internet**
  - Dieser Kanal muss penibel abgesichert werden, da eine **Schwachstelle** in diesem Bereich potentiell **alle** anderen **Sicherheitsmechanismen aushebeln** kann
  - Häufigste Probleme:
    - Fehlende **Verschlüsselung**
    - Verschlüsselung mit **veraltetem Algorithmus**
    - Verschleierung mit **nicht begutachtetem Algorithmus** \ Missachtung Kerckhoffs‘sches Prinzip
    - Keine oder unzureichende **Validierung der Zertifikate**



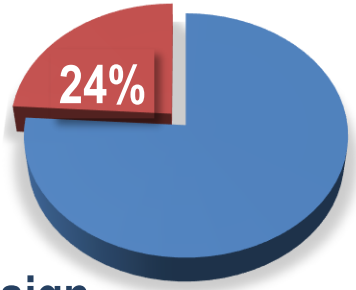
Kritische Bereiche

- **Lokale Kommunikation**
  - Vielzahl von IoT-Geräten verfügen auch über eine Möglichkeit offline lokal zu kommunizieren (bspw. über Bluetooth)
  - **Zugang zu sensiblen Daten** auch über diesen Weg möglich
  - Häufigste Probleme:
    - Fehlende **Authentifizierung**
    - Fehlende **Verschlüsselung**
    - Out of the Box-Verwendung von Kommunikationsprotokollen **ohne sicherheitstechnische Anpassung**



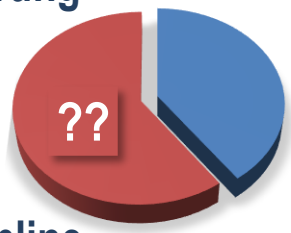
Kritische Bereiche

- **Hard- und Firmware-Design**
  - Einfachste und **wirkungsvollste Methode** Produktfunktionen vor **ungewolltem Zugriff** zu schützen:
    - Beschränkung / Beseitigung der Zugriffsmöglichkeit nach außen
  - Kann immensen **Aufwand** für die Implementation von Sicherheitsmechanismen **einsparen**
  - Erfordert allerdings vorausschauendes und **ausgeklügeltes Design**
  - Häufigste Probleme:
    - **Offene Ports**, die nicht (mehr) für die eigentliche Funktionalität benötigt werden
    - **Aktivierte Zusatzprotokolle**, die für finale Nutzung nicht (mehr) benötigt werden
    - Keine / Unzureichende Möglichkeiten der **Adaption / Aktualisierung** des Sicherheitssystems
    - Unzureichender Schutz des **Firmware-Update-Mechanismus**



Kritische Bereiche

- **Behandlung sensibler Daten**
  - **Kritischer Aspekt** für den Bereich des IoT
    - Erfasste Daten erlauben immer **Einblick** in einen oder mehrere Aspekte des **Lebens der Nutzer**
    - Daten eines Gerätes isoliert betrachtet in vielen Fällen noch unkritisch, aber **Gesamtheit aller Daten aller Geräte** stellen in jedem Fall **sensible Information** dar → Alle Daten absichern, so wird auch die Gesamtheit geschützt
    - **Schutz** der Daten **lokal**, bei der **Übertragung** und der finalen **Lagerung** notwendig
  - Häufigste Probleme:
    - Kein sicheres **Speicherkonzept** für sensible Daten **lokal**
    - Unzureichende Absicherung des **Übertragungsweges lokal und online**
    - Unverhältnismäßige / Unnötige **Datensammlung**



Schlussfolgerungen und Empfehlungen

1. **Authentifizierung**
   - **Lokal und Online**
   - User ←→Device
   - **Dynamische** Authentifizierung (Challenge-Response + Zeitstempel!)
   - Potentiell komplexe **Besitz- und Nutzerverhältnisse** beachten
2. **Verschlüsselung**
   - Man kann nicht zu viel verschlüsseln!
   - Man kann schlecht verschlüsseln!
   - **Online-Kommunikation** in jedem Fall, aber auch **lokal** wichtig
   - Ohne Überprüfung der **Zertifikate** und Absicherung der **Schlüssel** ist Verschlüsselung (nahezu) nutzlos
3. **Datenerfassung und –haltung**
   - **Umfang, Detail und Verhältnismäßigkeit** der Erfassung
   - Erfasste Daten sind eigentlich **immer schützenswert**
   - Wahrer **Informationsgehalt** erfasster Daten direkt nur **schwer einzuschätzen**

Schlussfolgerungen und Empfehlungen

4. Umsetzung

- Ein **etablierter, begutachteter Algorithmus** ist in nahezu allen Fällen einem neu entwickelten vorzuziehen
- „Security by Obscurity“ vermeiden
- Kerckhoffs‘ Prinzip anstreben
- **Eignung** von Standardlösungen **überprüfen**

5. Angreifermodell

- Erstellung eines **szenarioabhängigen Angreifermodells**
- Standard Angreifermodelle auch im IoT anwendbar (bspw. *Dolev-Yao-Modell*)
- **Nutzer** ist auch **potentieller Angreifer**!

6. Review

- Des **Sicherheitskonzeptes**
- Der **Implementation**
- Des **fertigen Produktes**

@avtestorg (Englisch) & @avtestde (Deutsch)

Folgen Sie uns auf facebook.com/avtestorg

Aktuelle Testergebnisse unter https://www.av-test.org

Vielen Dank für Ihre Aufmerksamkeit!