



openHPI: **Web-Technologien** Privatsphäre und Sicherheit in einer hochvernetzten Welt

Prof. Dr. Christoph Meinel

Hasso-Plattner-Institut

Universität Potsdam

Smart Cars – ein spektakulärer Angriff

Spektakuläre Angriffsdemonstration aus 2015:
Hacker übernehmen **über das Internet**
ein Auto während der Fahrt



Sicherheitsforscher Miller und Valasek demonstrieren für WIRED Magazin Übernahme eines modernen SUV

1. Angreifer können Internet-Adresse des Autos feststellen und verbinden sich damit über dessen Internetanbindung
2. Über verschiedene Sicherheitslücken und Schwächen im Design gelingt es ihnen, das Car Entertainment System zu übernehmen und von dort auf internes Bordnetzwerk zuzugreifen
3. Weitergehende Manipulation der Software des Fahrzeugs erlaubt umfassende „Fernsteuerung“



Den Angreifern war es möglich:

- Klimaanlage zu manipulieren
- Soundsystem zu bedienen
- Wischer, Lichter, etc. zu steuern
- GPS-Position und Geschwindigkeit auszulesen
- **Gaspedal und Bremse zu bedienen**
- Motor abzuwürgen
- Lenkung teilweise zu bedienen
(derzeit nur im Rückwärtsgang)

(Vernetzte) Computersysteme haben Schwachstellen und können über das Internet massiv manipuliert werden!



- Früher zielten Hacker-Angriffe meist auf rein digitale Systeme oder auf Nutzer des Webs ab
- Integration digitaler Komponenten in physikalische Systeme (etwa bei Smart Factory oder im Smart Home) macht auch Cyberangriffe auf physikalische Systeme möglich
 - unberechtigtes An-/Abschalten
 - Auslesen von Daten oder Veränderung von Konfigurationen
 - Beschädigung oder Zerstörung der Systeme
 - ...
- Angriffe können nicht mehr „nur“ Daten, Reputation oder finanzielle Ressourcen treffen, sondern auch Maschinen oder gar die Unversehrtheit von Menschen – wie im Fall des Auto-Hacks – werden zu direkten oder mittelbaren Zielen von Cyberattacken

Risiken für das Smart Home

SmartHome-Controller, die Fernsteuerung der Haustechnik erlauben, bieten (noch) zahlreiche **gefährliche Angriffspunkte**

Beispiel:

- MiCasaVerde VeraLite hat Schwachstellen, die es Angreifer erlauben
 - **beliebige Daten** aus Dateisystem auszulesen (inklusive gehashter Passwörter)
 - **Firmware zu ändern** und **Einstellungen herunterzuladen**
 - aus dem LAN heraus **als Administrator jede Art von Schadsoftware** auszuführen
 - mit Kenntnis einer gültigen GeräteID **vollständigen Zugriff** auf den SmartHome-Controller zu erlangen

Risiken für das Smart Home – Smart-TV

Nicht nur SmartHome-Controller, sondern auch andere „Smart“ Geräte haben **Probleme mit Privacy** und **Sicherheit**

■ Samsung Smart-TV

- hört alle Gespräche (und andere Geräusche) im Raum mit, falls Sprachsteuerungsfunktion aktiviert ist
- gesprochene Worte werden “an Drittanbieter übertragen”

■ LG Fernseher

- senden verschiedene Nutzer-Daten an Hersteller, um Smart Ad (gezielte Werbung) zu zeigen
- Informationen werden auch übertragen, wenn entsprechende Einstellung deaktiviert ist (!)
- übertragene Daten: angesehene TV-Kanäle, Datei-Listen von angeschlossenen USB Sticks und Festplatten, Suchanfragen, ...

Risiken für das Smart Home – Smart Meter

Smart Meter sind Verbrauchsmesser („Meter“) für Strom, Gas, Wasser mit Netzanschluss

- Analoge Verbrauchsmesser werden 1-2 mal pro Jahr abgelesen
- Smart Meter sind ständig mit Energie-Anbieter verbunden und schicken ihm Messwerte zu
- Anbieter erkennt zeitnah Energiebedarf und kann diesen z.B. über Tarifgestaltung optimieren (Strom in der Nacht günstiger, ...)
- Bilanzierungsprozesse, Prognosen, Rechnungserstellung, ... werden erleichtert
- Typischerweise eröffnen Smart-Tarife dem Verbraucher auch Sparmöglichkeiten



EVN Energie AG, via Wikimedia Commons

Risiken für das Smart Home – Smart Meter

- Detaillierte Informationen über Energie-Nutzung in einem Haushalt sagt viel über Bewohner aus
 - Schlafzeiten
 - Waschzeiten
 - wie viele Personen sind gerade zu Hause
 - Kochzeiten
 - ...
- Polizei in Texas (USA) nutzt Strom-Daten, um Marihuana-Plantagen zu erkennen
- In Australien wurden solche Daten an Inkasso-Unternehmen weitergegeben
- Smart Meter ermöglicht dem Energie-Anbieter – und damit auch Angreifern – auch Fernabschaltung der Energieversorgung

Risiken für Smart Factory und Industrie 4.0

Industrielle Anlagen waren bisher **isolierte Systeme**

- Steuerungsanlagen (PLCs) für physikalische Maschinen und industrielle Netzwerke auf Zuverlässigkeit und sicheren Betrieb ausgelegt
- Keine Verbindung mit anderen Unternehmensnetzwerken und dem Internet

Industrie 4.0 und Smart Factory bedingen **hochvernetzte Anlagen**

→ dadurch **anfälliger für Cyberattacken**

- Datendiebstahl
- Spionage
- DoS-Attacken (Denial of Service – Ziel: Betriebsschädigung und Außerbetriebnahme von Anlagen)
- Malware (Viren, Würmer, Trojaner)
- ...

Risiken für Smart Factory und Industrie 4.0

Beispiel für cyber-physikalischen Angriff: **Stuxnet**

- **Stuxnet** ist **Schadsoftware**, die 2010 auf den Computern von iranischen Anlagen zur Urananreicherung entdeckt wurde
- Schlägt in zwei Phasen zu:
 - Infektion von Windows-Systemen
 - Stuxnet verbreitet sich über Netzwerk und USB-Sticks
 - Ist Windows-Rechner infiziert, prüft Stuxnet, ob Software zur Programmierung von Steueranlagen installiert ist
 - Wenn ja, modifiziert Stuxnet diese Software
 - Infektion von PLCs (Programmable Logic Controller, Steueranlagen)
 - Schadsoftware verändert einzelne Codeblöcke in den Steueranlagen
 - ...

Risiken für die Smart Factory und Industrie 4.0

Beispiel für cyber-physikalischen Angriff: **Stuxnet**

- **Stuxnet** ist **Schadsoftware**, die 2010 auf den Computern von iranischen Anlagen zur Urananreicherung entdeckt wurde
- Schlägt in zwei Phasen zu:
 - Infektion von PLCs (Programmable Logic Controller, Steueranlagen)
 - ...
 - Zusätzlich verschleiert Stuxnet Manipulationen, dem Betreiber werden keinerlei Abweichungen im Betriebsablauf gemeldet
→ so blieb Stuxnet lange unentdeckt ...
- 2010 waren Angriffe auf Steuerungsanlagen nur Fiktion, die in einigen Forschungspapieren behandelt wurde
- Zunehmende Vernetzung, auch mit Internet und Web Services, **vergrößert Angriffsflächen** deutlich

Identitätsdiebstahl – ein spektakulärer Fall (1/3)

Angriff auf Mat Honan, Autor bei Wired.com:

- Wired.com: Bekanntes US-amerikanisches Technologiemagazin
- Mat Honan (@mat) ist Senior Staff Writer bei Wired
- 2012: Angreifer haben mit einer mehrstufigen Attacke erreicht, dass alle Daten sowohl auf Honans MacBook, iPhone und iPad sowie den Online-Backups gelöscht wurden
- Als Warnung veröffentlichte Honan Ablauf der Ereignisse in einem Artikel



Identitätsdiebstahl – ein spektakulärer Fall (2/3)

Angriff auf Mat Honan, Autor bei Wired.com:

- Angreifer wollten Twitter-Konto von Mat Honan übernehmen
- Twitter-Konto enthält Information über persönliche Webseite
- Mithilfe des „Whois“-Dienstes finden Angreifer Honans Postadresse und private Gmail-Adresse heraus
 - „Whois“ erlaubt Auslesen hinterlegter Daten der Domaininhaber (hier: von Honans persönlicher Website)
- Durch Passwort-Wiederherstellung im Gmail-Account finden Angreifer Email-Adresse der Apple ID heraus
 - Gmail: „Wir haben eine Email an [m****n@me.com](#) gesendet“
 - Angreifer rät vollständige Email-Adresse ...

Identitätsdiebstahl – ein spektakulärer Fall (3/3)

Angriff auf Mat Honan, Autor bei Wired.com:

Angreifer kennen nun Name, Postadresse, private Gmail-Adresse und Email der Apple ID

- kontaktieren Amazon und lassen eine Kredit-Karte mit Honans Konto verbinden
- kontaktieren Amazon erneut und lassen Passwort wiederherstellen (möglich durch Kenntnis der zuvor hinterlegten Kreditkarten-Nummer)
- finden im Amazon-Konto letzte vier Ziffern echter Kreditkarte von Honan
- kontaktieren Apple, erhalten Zugang zur Apple ID (durch Kenntnis von Name, Adresse, Email und letzten vier Ziffern der Kreditkarte)
- mit Apple ID bzw. Zugriff auf Apple-Mailkonto setzten Angreifer Gmail-Passwort (und anschließend auch Twitter-Passwort) zurück und löschen alle Daten von Honan's iPhone, iPad und MacBook...

Zusammenfassung

- IoT, Smart World, hochgradige Vernetzung und weitergehende Durchdringung unserer Gesellschaft mit (Web-)Anwendungen läuten **neues technologisches Zeitalter** ein (4. industrielle Revolution)
- Digitale Transformation birgt aber gleichzeitig **hohes Gefahrenpotential** für Industrie und Gesellschaft
 - neue Arten von Angriffen, nicht nur auf digitale Systeme
 - inhärent Verletzung der (digitalen) Privatsphäre, bis hin zu deren faktischer Abschaffung
- Sicherheit und Datenschutz sind **zentrale Herausforderungen**, denen sich Forschung, Politik, Wirtschaft – aber auch **jeder einzelne** – stellen muss
 - Schaffung geeigneter politischer Rahmenbedingungen
 - Bereitstellung technischer Hilfsmittel
 - Sicherheitsbewusstsein → openHPI-Kurs „**Sicherheit im Internet**“