SMARTHOME DEUTSCHLAND

TeleTrusT Pioneers in IT security.

IT-Sicherheit in smarten Gebäuden

Bundesverband IT-Sicherheit e.V. (TeleTrusT) in Kooperation mit SmartHome Initiative Deutschland e.V.

Berlin, 29.10.2019

Sicherheit bei Smart-Home-Funksystemen

Prof. Dr.-Ing. Christian Pätz, Z-Wave Europe

Fahrplan

- Warum Sicherheit ?
- Wo liegt das Problem ?
  - Wahrnehmung
  - Spezielle technische Herausforderungen bei SH
- Welche technischen Anforderungen
  - Allgemein aus der IT Welt
  - Speziell bei Smart Home Funk

Begriffsdefinition und Abgrenzung

- Smart Home: Funktionen und Installationen im Haus kommunizieren digital. d.h. Sensorik, Aktorik, keine Sprachassistenten, in der Regel keine Kameras
- Smart Home Funk: Drahtlose Kommunikation zwischen Aktorik und Sensorik im Haus von und zu einer zentralen Steuerung und untereinander.

Was sollte im Smart Home nicht möglich sein

- Information, wer wann zu Hause ist, Entferntes Öffnen der Tür
- Informationen über Lufthygiene, Körperhygiene
- Informationen über Mediennutzung
- Entfernte Sabotage (Heizung, hoch, Heizung, runter, Licht nachts an im Minutentakt, ...)
- Abweichungen von der typischen Wohnungsnutzung

Claudia Pechstein (5*Olympia-Gold)

- 2009: Sperre durch ISU wegen Indizien zu Blutdoping (Retikulozyten sind mit 3.5 % ca. 1.1 % über der festgelegten Norm).
- 2009: Klage vor CAS abgelehnt
- 2010: Hausdurchsuchung durch das BKA
- 2010: Die Dt. G. für Hämatogolie (DGHO) bestätigt, das C.P. eine vererbte Blutanomalie hat, welche die Werte erklären
- 2010: Schweizer Bundesgericht bestätigt Sperre aus formalen Gründe (keine neuen Beweise)
- 2011: Selbstanzeige durch Claudia Pechstein, Anti-Doping Agentur eröffnet kein Verfahren
- 2014. Schadenersatzklage in München abgelehnt.

Wie wichtig ist die Sicherheit beim Feldbus

Argument: Man muss ja quasi im Haus sein, um Smart Home Funk abzuhören. **ABER**: Mit Drohnen ist es leicht möglich, größere Wohngebiete abzuscannen.

Licht an, Licht aus: ZigBee-Wurm befällt smarte Glühbirnen

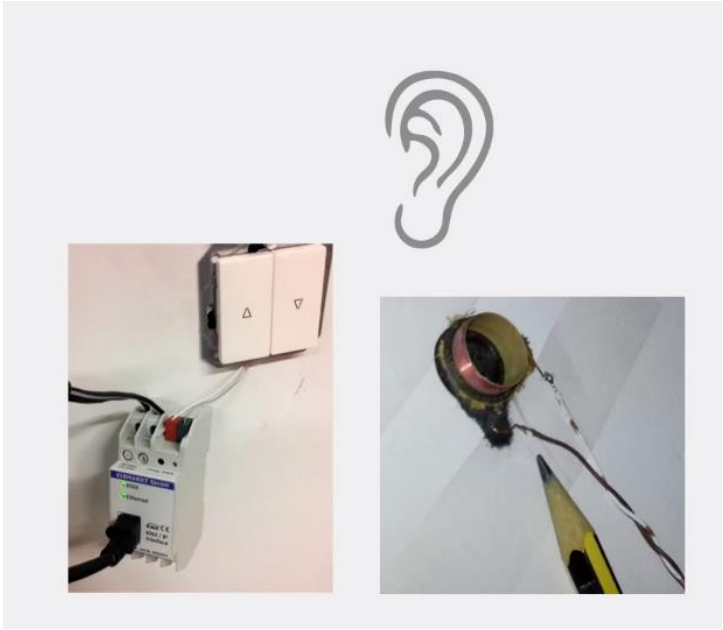
heise Security 08.11.2016 15:40 Uhr – Fabian A. Scherschel vorlesen

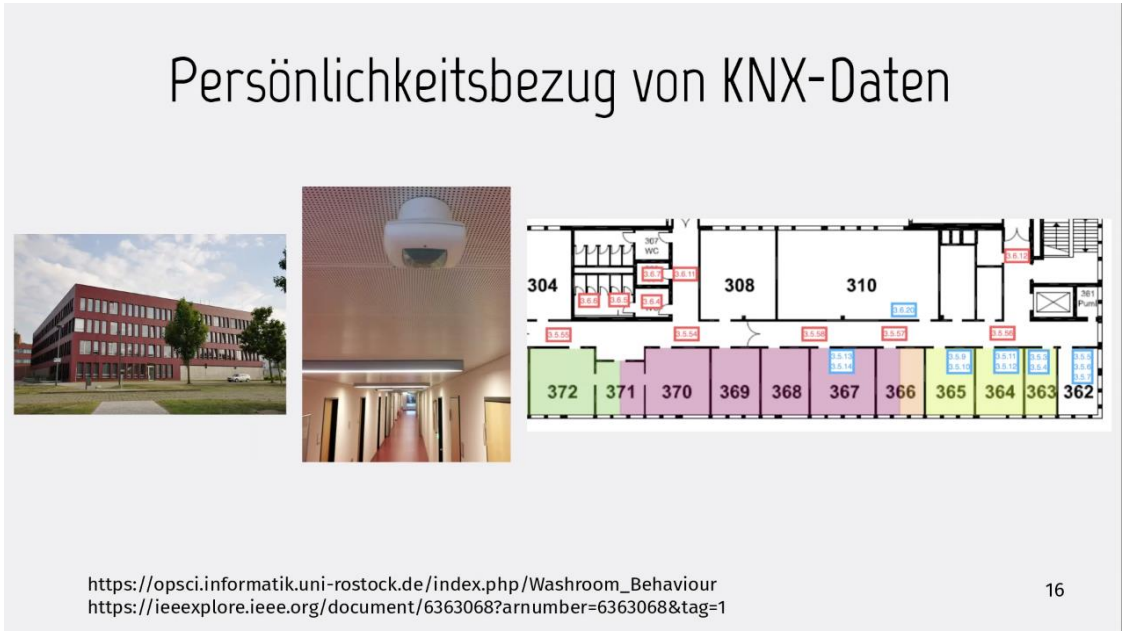
(Bild: Ronen et al.)

Das Internet der Dinge (IoT) sorgt mal wieder für eine skurrile Sicherheitslücke: Diesmal haben Forscher einen Wurm programmiert, der von einer Philips-Hue-Birne zur anderen springt und diese mit bösartiger Firmware bespielt.

Draht ist sicher und KNX ist für Profis

- Vortrag von Simeon Wiedenmann,Uni Rostock, gehalten auf dem CCC 2019 in Zedenick
- Net-Net: KNX ist perfekt unsicher, KNX secure nicht unbedingt die Lösung





Zusammenfassung bisher

- Daten aus dem Smart Home sind definitiv interessant, sowohl für Privatpersonen als auch für Regierungen oder NGOs
- Die Funkverbindung auf „der letzten Meile“ ist mit heutigen Mitteln durchaus angreifbar und muss damit genau so gut geschützt sein wie der Rest der Infrastruktur.
- Leider ist die Realität mitunter anders!

Warum ist SH-Funk mitunter so schlecht (gemacht)

- Hersteller implementieren (aus Kosten oder ‚Usability' Gründen) nur ein Minimum an Sicherheit
- Sicherheit ist nicht die Kern-Kompetenz der Hersteller
- Rückwärtskompatibilität über mehr als 20 Jahre
- Öffentliche Wahrnehmung != Realität
- Smart Home Funk ist speziell

Homematic versus PlusMinus

Soweit für uns ersichtlich, wurde für die Hacks im Videobeitrag der Umstand genutzt, dass ein Standard-Gerätekennwort nicht geändert oder der Zugang vom Anwender aktiv ohne Kennwortschutz freigegeben wurde. Glücklicherweise vergeben die meisten Hersteller von Routern und sonstigen Geräten mit Internet-Anbindung heutzutage per Zufall generierte Kennwörter oder zwingen den Endnutzer, bei der Erstinstallation ein eigenes Kennwort zu vergeben. Auf diese Weise werden Einfallstore wie im Film gezeigt geschlossen. Hersteller, die für extern erreichbare Geräte tatsächlich noch standardisierte Anmeldedaten vergeben gehören dagegen sehr wohl namentlich genannt, hier wäre in der Tat auch politischer Druck wünschenswert.

Z-Wave versus Forbes

- Z-Wave S2 ist inhärent sicher aber erst seit 4 Jahren im Markt
- Für Rückwärts-Kompatibilität schaltet Z-Wave auf Security S0 (von 2007), bei dem der Schlüssel als erstes Paket unverschlüsselt übertragen wird
- Der Controller muss vor diesem Vorgang warnen
- Die Journalisten nutzten den Textcontroller aus der Entwicklungsumgebung, der als Testwerkzeug keine Endkundenwarnungen hat.
- Sie schließen aus der fehlenden Warnung beim Rückschalten des Sicherheitsmodus im Textcontroller, dass 100 Mio. Geräte „exposed“ sind.

34,638 views | May 24, 2018, 07:10am

A Basic Z-Wave Hack Exposes Up To 100 Million Smart Home Devices

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

The Z-Shave attack detailed by British researchers exposes Z-Wave smart home devices to hacker... [+]

PEN TEST PARTNERS

Welche Techniken

- WLAN (Saugroboter, Apple Homekit, ...) ?
- Bluetooth?
- Zigbee, Z-Wave, EnOcean, ULE, Bidcos, LORA, Thread, Proprietäre Protokolle

Besonderheiten

- „*Command and Control*“, d.h. Steuerung vom Aktorik, Auslesen von Sensorik
- Sehr kleine Datagramme und Inhalt ist weitgehend bekannt
- Sehr unterschiedliche Sicherheitsanforderungen inner-halb der verwendeten Geräte
- Recht häufig ist die Nachricht die Nachricht und nicht der Nachrichteninhalt

Kompromisse im Smart Home Funk

1. Sicherheit und Energieverbrauch sind gegenseitig ausschließend
   1. Beispiel: WIFI bietet hohe Sicherheit (WPA2) braucht dafür aber zu viel Energie für Batteriebetrieb
   2. Beispiel: EnOcean braucht extrem wenig Energie (4 Byte Datagramme), ist aber dafür in Bezug auf Sicherheit ... Nunja
2. Sicherheit und Bequemlichkeit sind gegenseitig ausschließend
   1. Komplexer Setup, persönliche Schlüssel, „Zwei-Faktor-Authentifizierung“
   2. Latenz bei Bedienung (z.B. Licht schalten)

Allgemeine Sicherheitsprobleme in der IT

1. Ein unbefugter Dritter bekommt Zugriff auf vertrauliche Daten. [**Verschlüsselung, sichere und gültige Schlüssel**]
2. Ein unbefugter Dritter führt im Netz im Namen des Angegriffenen unerwünschte Aktionen durch, entweder indem er die Daten des Angegriffenen manipuliert oder sich gleich erfolgreich als eine andere Person ausweist. [**Authentifizierung**]
3. Die gewünschte Funktion des Netzes ist vorsätzlich gestört (Denial of Service). [**Robustheit**]

Typische Sicherheitsprobleme im SH-Funk

Verschlüsselung
Sichere Schlüssel
Authentifizierung
Robustheit

1. Ein korrekt gesendete Nachricht wird zu einem späteren Zeitpunkt nochmals gesendet (Replay Attack) [**Sequenznummern**]
2. Es gibt Geräte mit sehr geringem Schutzstatus (z.B. Regenmelder außen), mit normalem Schutzstatus (z.B. Lichtschalter) oder mit sehr hohem Schutzstatus (Türschloss) [**kein Zentralschlüssel**]
3. Paralleles Pairing erzwingt Authentifizierung [**Authentifizierung**]
4. Firmwares sind leicht/schwer zu bauen [**Firmware-OTA**]

Verschlüsselung/Sequenznummern

1. AES-128 ist der heute in standardisierten Smart Home Funksystemen verwendete Verschlüsselungsstandard. AES gilt als sicher, die Schlüssellänge von 128 Bit als ausreichend
2. Rolling Codes sind nur bei 2 Punkt-Verbindungen brauchbar. Die Alternative „Nonces“ (Einmal-Transaktionsnummer) ist komplex und erfordert gegebenenfalls Zusatzkommunikation.
3. Gültigkeit von Nonces kann zeitlich begrenzt werden und damit zusätzliche Sicherheit schaffen. Nachteil: Mehr Kommunikation.

~~Verschlüsselung~~
Sichere Schlüssel
Authentifizierung
Robustheit

~~Sequenznummern~~
Individuelle Keys
Authentifizierung
Firmware-OTA

Schlüsselmanagement

1. Schlüssel werden entweder über sichere Kryptographie (Diffi-Hellman) oder *Out-of-Band* ausgetauscht, d.h. weder statisch (Beispiel Philips Hue Hack) noch voreingestellt.
2. Schlüssel müssen hinreichend lang sein.

~~**Verschlüsselung**~~
~~**Sichere Schlüssel**~~
Authentifizierung
Robustheit

~~**Sequenznummern**~~
Individuelle Keys
Authentifizierung
Firmware-OTA

Mehrere Schlüssel für mehrere Geräte

1. Unterschiedliche Geräte brauchen unterschiedliche Schlüssel
2. Lösungen
   1. Verschiedene Schlüsselzonen (Z-Wave), Nachteil: Verständlichkeit
   2. Grundsätzlich verbindungsindividuelle Schlüssel (LORA: Nachteil: sehr schwierige Device/Device-Kommunikation

~~**Verschlüsselung**~~
~~**Sichere Schlüssel**~~
Authentifizierung
Robustheit

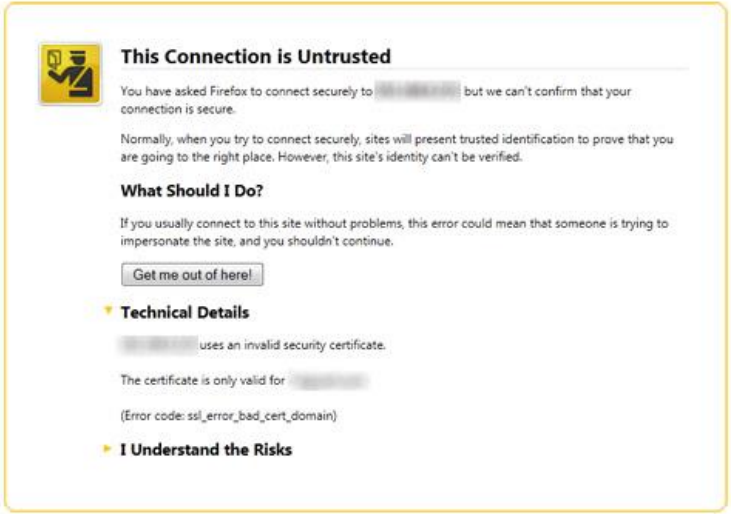
~~**Sequenznummern**~~
~~**Individuelle Keys**~~
Authentifizierung
Firmware-OTA

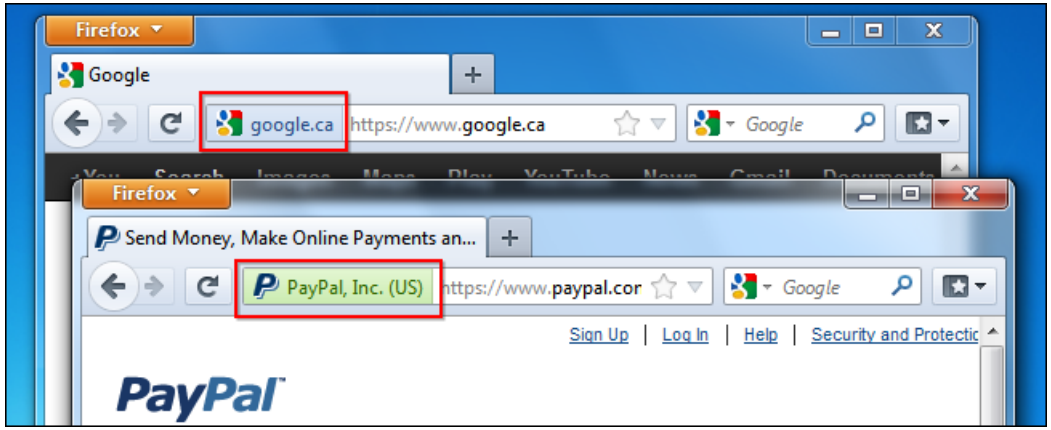
Authentifizierung – mit wem rede ich eigentlich ?

1. Standard und unverzichtbar bei Webseiten
2. Installation von Smart Home Geräten in größeren Einheiten ?

~~Verschlüsselung~~
~~Sichere Schlüssel~~
~~Authentifizierung~~
Robustheit

~~Sequenznummern~~
~~Individuelle Keys~~
~~Authentifizierung~~
Firmware-OTA





OTA- Aber richtig

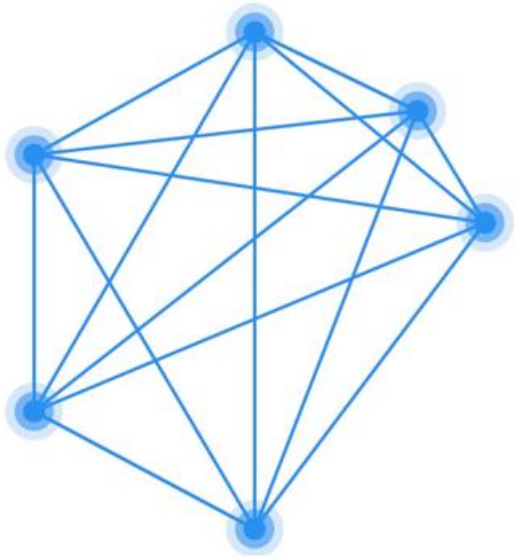
1. Da SH Geräte fest eingebaut werden, muss es zwecks nachträglichem Fix von Problemen die Möglichkeit geben, neue Firmwares „*inband*“ und „*over the air*“ zu übertragen.
2. FW-Update ist eine wunderbare Backdoor, daher :
    1. Immer physische Bestätigung am Gerät
    2. FW Binaries verschlüsselt mit einem Schlüssel, der bereits auf dem Gerät ist

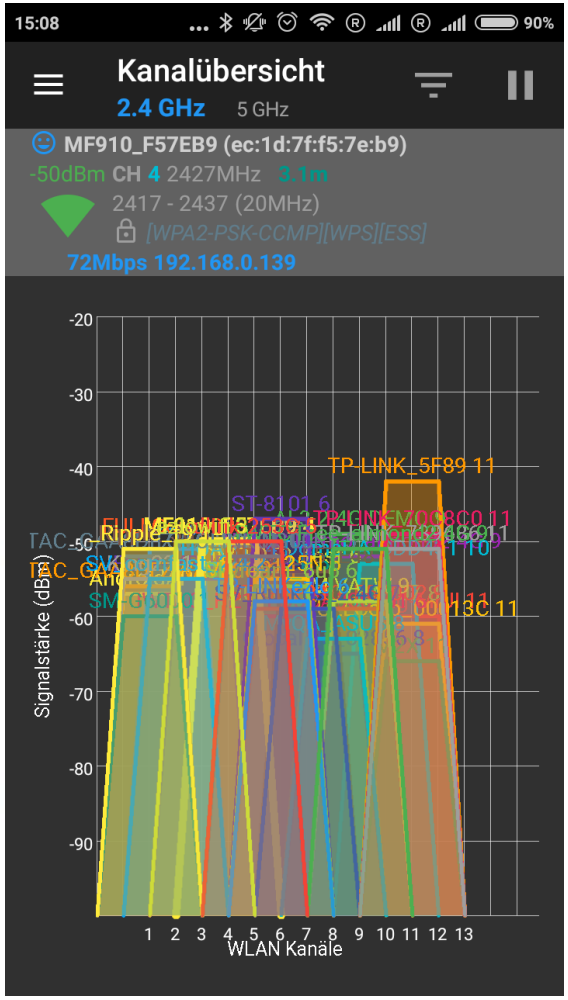
~~Verschlüsselung~~
~~Sichere Schlüssel~~
~~Authentifizierung~~
Robustheit

~~Sequenznummern~~
~~Individuelle Keys~~
~~Authentifizierung~~
~~Firmware-OTA~~

Robustheit

1. Frequenz-Agilität
2. Rückbestätigung
3. Funkvermaschung





~~Verschlüsselung~~
~~Sichere Schlüssel~~
~~Authentifizierung~~
~~Robustheit~~

~~Sequenznummern~~
~~Individuelle Keys~~
~~Authentifizierung~~
~~Firmware-OTA~~

Zusammenfassung II und Thesen

- Für die sichere Funkkommunikation im Smart Home existieren *Best Practise*, die alle relevanten Aspekte der Funksicherheit abdecken.
- Leider werden diese *Best Practise* in der Praxis nicht überall korrekt implementiert. Besondere „anfällig“ sind
  - Protokolle, die schon lange im Markt sind
  - Proprietäre Protokolle auf Basis standardisierter Hardware
- Hohe Sicherheit fordert seinen Preis in Bezug auf Energieeffizienz und/oder Nutzerfreundlichkeit. Sind Sie bereit, diesen Preis zu zahlen?