Zukünftige Herausforderungen an die Sicherheit smarter Gebäude

Dr. Steffen Wendzel,
Head of Secure Building Automation

steffen.wendzel@fkie.fraunhofer.de

Fraunhofer FKIE

Agenda

Es handelt sich um eine Zusammenfassung der verwendeten Präsentationsfolien.

- Einleitung
- Gefahren:
  - Angriffe aus der TCP/IP-Welt
  - Data Leakage
  - „Smart Building Botnets“
- Unsere neue Gegenmaßnahme:
  - Traffic Normalization
- Literatur

Smart Buildings

- Gebäude verfügen über Sensoren und Aktoren
- Gebäude sind remote steuer- und überwachbar
- Gebäudeautomation bereits seit den 1950‘er Jahren (pneumatische Elemente)

Gefahr #1:
Bekannte TCP/IP-Angriffe

- Bisherige Schutztechniken aus dem Bereich Betriebssystemforschung und der Netzwerksicherheitsforschung wurden kaum auf die Gebäudetechnik übertragen.
- Daraus ergibt sich eine klare Verwundbarkeit gegenüber selbst grundlegenden Angriffen (etwa Spoofing, Fuzzing-Angriffe gegen schlecht implementierte Netzwerkstacks, inkonsistente Re-Transmissions, Angriffe gegen das dynamsiche Routing), die insb. aus der TCP/IP-Welt bekannt, jedoch für Protokolle der Gebäude-Automation neu sind.
- Es gibt keine nennenswerte Lösung zum Schutz von Gebäude-Netzwerkprotokollen gegen derartige Angriffe.

Gefahr #2:
Data Leakage

- Sensorrdaten in Gebäuden übertragen vielerlei Informationen, etwa
  - Electronic Health-Daten im Kontext von Ambient Assisted Living
  - Aufenthaltsdaten (durch Anwesenheitssensoren)
- Werden diese sensitiven Daten geleaked, so entstehen diverse Szenarien, die Angriffe motivieren, etwa
  - Verkauf von Gesundheitsdaten an Krankenkassen
  - Nutzung von Bewegungsmustern durch Kriminelle zur optimalen Planung von Einbrüchen
- Es gibt keine Lösung für Data Leakage, die speziell für die Bedarfe der Gebäudeautomation zugeschnitten ist.

Gefahr #3:
Smart Building Botnets

- *Smart Building Botnets* wurden von uns jüngst als zukünftige Bedrohung zur Diskussion gestellt *(s. letzte Folie)*
- Im Unterschied zu bisherigen Botnets nutzen Smart Building Botnets die physikalischen Eigenschaften von Gebäuden aus, d.h. sie nutzen Sensoren und Aktoren, und sie können ganze Regionen/Smart Cities angreifen.
- *Beispiel-Szenario:* Ein Öl-Lieferant möchte seine Lieferungen innerhalb einer Region steigern. Durch Angriff auf diverse Smart Homes der Region werden Räume stärker beheizt. Dadurch wird mehr Öl verbraucht und die Kunden müssen früher neue Öllieferungen bestellen.
  - *Für weitere Szenarien s. letzte Folie.*

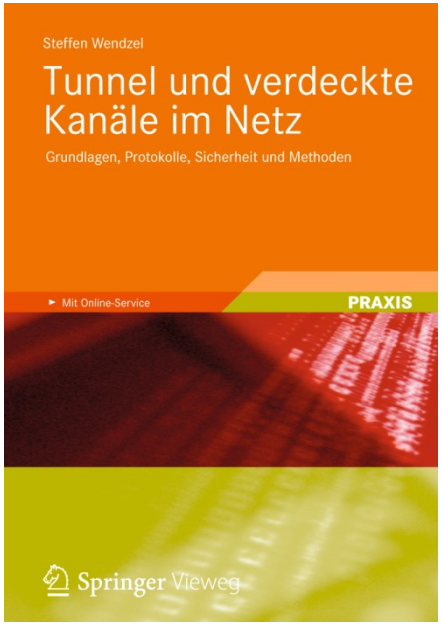
Eine Lösung: Traffic Normalization

- Traffic Normalization (TN) entfernt Mehrdeutigkeiten und teils Angriffe aus Netzwerktraffic. Zudem stellt TN eine höhere Standardkonformität von vorliegendem Traffic sicher.
- Diverse Angriffe (etwa simplere verdeckte Kanäle und Adressspoofing) können verhindert oder limitiert werden.
- TN bietet einen Schutz für teils schlecht implementierte Netzwerkstacks in Gebäudeequipment
- Wir haben einen ersten **Prototyp als Snort-Extension für das BACnet-Protokoll** entwickelt.
- Vorteile der Traffic Normalization:
  - Integrierbar in legacy-Systeme, die nicht nachrüstbar/patchable sind
  - Integrierbar in bestehende Netzwerkprotokolle (etwa BACnet)

Vielen Dank für Ihre Aufmerksamkeit

Unsere Themen:

- Data Leakage Protection
- IT-Sicherheit für Gebäude
- Network Steganography



Dr. Steffen Wendzel

Head of Secure Building Automation
der Cyber Defense Research Group
Fraunhofer FKIE
steffen.wendzel@fkie.fraunhofer.de

http://www.wendzel.de

Fraunhofer FKIE

Unsere Publikationen zum Thema

Vorstellung von Smart Building Botnets:

S. Wendzel, V. Zwanger, M. Meier, S. Szlósarczyk: Envisioning Smart Building Botnets, in Proc. GI Sicherheit, Wien, GI, 2014 (to appear).

Traffic Normalization für Gebäude-Netze:

S. Szlósarczyk, S. Wendzel, J. Kaur, M. Meier, F. Schubert: Towards Suppressing Attacks on and Improving Resilience of Building Automation Systems – An Approach Exemplified Using BACnet, in Proc. GI Sicherheit, Wien, GI 2014 (to appear).