

# Sicherheit bei der Gebäudeautomation

## 11. Linux-Informationstag der LUGA

Steffen Wendzel

# Agenda



IT4SE

- Vorstellung IT4SE-Projekt
- Überblick BAS-Security
- IT4SE Building Automation-Projekte
- Verdeckte Kanäle und Seitenkanäle in BAS



- IT4SE – IT for **S**mart renewable **E**nergy generation and use  
<http://www.it4se.net>
- BMBF-gefördert
- Kooperation zwischen
  - Hochschule Augsburg (Projektleitung, Prof. Rist)
  - University of Waikato (Neuseeland)
  - Universität Augsburg



# Was ist Gebäudeautomation?



IT4SE

- engl. Building Automation System (BAS)
- Früher hauptsächlich HVAC (heating, ventilation, air-conditioning)
- Heute: Alles :-)
  - Von: Komfort für das Heim durch die Steuerung von praktisch **allem**
  - Über: benutzerorientiertes Energiesparen
  - Bis: Vitalfunktionen alter Menschen überwachen; Haus meldet Notfall an Arzt
  - *Ambient Assisted Living, AAL*



# Building Automation Security: SotA



IT4SE

- erst ab Ende der 90er Thema
- Wie sieht es heute aus?
  - Hersteller: Sicherheit << Funktionalität
  - viel verschiedene Hardware (Bus-Systeme, Funk)
  - eigene embedded Systeme (tw. Linux-basiert)

# Building Automation Security: SotA



IT4SE

- **Hersteller: Sicherheit << Funktionalität**
  - Bewusstsein für Sicherheitsproblematik kommt nur langsam
  - teilweise unverschlüsselte Funkprotokolle
  - alte Hardware verbaut (Kryptografie-Probleme!)
  - unsichere Web-Interfaces

# Building Automation Security: SotA



IT4SE

- **verschiedene Hardware/Protokolle**

- Bus-Systeme/Funk
- Interoperabilitätsprobleme (schon seit frühen 90'ern bekannt)
- closed (Low-level) Interfaces, etwa bei HomeMatic :(

# Building Automation Security: SotA



IT4SE

- **eigene embedded Systems**
  - HomeMatic-System (eq-3)
    - Linux-Image zum freien Download  
... aber tw. closed source Programme!
    - Security-Problem im August gemeldet → noch nicht behoben

# Einbrecher ...



IT4SE

... können das BAS hacken und einfach das Kellerfenster per Befehl öffnen.



# Inhouse-Problem



IT4SE

Angestellter prüft vor Dokumenten-Entwendung,  
ob Vorgesetzter gerade in seinem Büro ist → BAS  
Sensor(en) abfragen



# Security-Ansätze aus der Forschung



IT4SE

- Verschlüsselung in verschiedenen Systemen vorhanden (teilweise proprietäre Algorithmen)
- EIBSec
  - EIB/KNX (TU-Wien)
  - Inkl. Key Distribution-Funktionalität
- Security-Analyse der bestehenden Protokolle (Schwaiger/Treytl 2003)
- Analyse sonstiger Aspekte (etwa: Beleuchtungs-Angriff über Nacht → Kosten)



- Middleware stellt einheitliche, hardware-unabhängige API für BAS bereit
- mehrere Middleware-Implementierungen durchgeführt, aktuell ist Version 3 in Arbeit mit Fokus auf Security
  - Vorherige Projekte:
    - HASI (Arbeitsgruppe der HS-Augsburg)
    - USEM (Gemeinschaftsprojekt der Uni Augsburg und der University of Waikato)



# HASI-basierte Apps: Energiesparen mit BJ Fogg



IT4SE

- Design-Mantra von Fogg: „Put triggers in the path of motivated people.“, d.h.
  1. Benutzer muss motiviert sein
  2. Benutzer muss zum passenden Zeitpunkt auf Verbesserungsmöglichkeit hingewiesen werden
  3. Benutzer muss in der Lage sein, Verbesserung umzusetzen
- Im Kontext des Energiesparens:
  1. Benutzer zum Energiesparen motivieren
  2. Gelegenheiten ausfindig machen, bei denen der Benutzer Energie einsparen kann
  3. Benutzer in die Lage versetzen, die Einsparungen möglichst einfach vorzunehmen

# HASI Augmented Calendar



IT4SE

## HASI

Home Analytical System Interface

Home Hausübersicht Kalender Achievements Regeln Nachrichten

### Filter

Bitte wählen Sie einen Filter aus.

Gebäude  Raum

Typ	Bezeichnung	Standort	Status	
	tmpr	HSA-Fakl / J2.12a	24.4 °C	
	1_ch1	HSA-Fakl / J2.12a	68 W	
	1_ch2	HSA-Fakl / J2.12a	34 W	
	1_ch3	HSA-Fakl / J2.12a	23 W	
	Zimmertemperatur	HSA-Fakl / J2.12a	23.6 °C	
	Fenster	HSA-Fakl / J2.12a	zu	
	Schalt Nespresso	HSA-Fakl / J2.12a	an	
	Schalt Soundanlage	HSA-Fakl / J2.12a	an	

## Kalender

← August 2011 →  
Dieser Monat

Montag	Dienstag	Mittwoch	Donnerstag
1	2	3	4
<b>7:00</b> Project Meeting	<b>7:00</b> Travel: Conference in Vienna	<b>7:30</b> Project Meeting	<b>7:30</b> Project Meeting
<b>9:00</b> Dev. Process Planning		<b>9:00</b> Meeting (Mr. J. Doe)	<b>9:20</b> Project Workgroup
<b>13:30</b> Annual Employ. Discussion		<b>10:30</b> Product Presentation	<b>13:30</b> Deadline: Project Progress Report
<b>15:00</b> Monthly Marketing Meeting		<b>11:30</b> Meeting (Lunch w. Mrs. Smith)	<b>15:30</b> Project Workgroup
		<b>12:30</b> Going Home Earlier	

# Smart Garden und elektr. Schlüsselboard



IT4SE

IAM-Gruppe von Prof. Rist



# Prototyp IT4SE Secure Middleware



IT4SE



## Privatsphäre im Kontext des Energiesparens

- Etwa: Person X darf nur die eigenen Energiespardaten einsehen
- Lösung: Einführung von Role-based Access Control (RBAC) in Middleware

# Der Weg zur Middleware



IT4SE

- HASI im SS-2011, USEM im Sommer '11
- Neues HSA-Projektgruppe zur Security Requirements Analyse und zum Entwurf des Systems (ggf. Implementierung) im SS-2012
- HSASec Building Automation-Gruppe (hsasec.de)
- Labor für Gebäudeautomation an der HSA
  - EIB/KNX, BACnet, ZigBee, HomeMatic, CurrentCost + Industrie-Automatisierung

# Forschung im Bereich Covert/Side Channels



IT4SE

- Side Channel in BAS = nicht explizit gesendet
- Covert Channel in BAS = explizit gesendet, quasi Ausnutzung eines Seitenkanals
- Beispiel:
  - Angestellter überwacht Räume im Gebäude
  - Geheime Absprachen über BAS

# MLS-Middleware



IT4SE

Ziel: Keine Side Channels  
und keine Covert Channels  
in BAS





- Covert Channels und Side Channels sind verhinderbar durch RBAC, aber umständlich
- Einführung von Security Levels wesentlich geeigneter → Multilevel Security (MLS)
- High-Level SC/CC in Form von Storage Channels völlig verhinderbar
  - Sicherstellung von NRU, NWD

Mehr dazu: IEEE SFCS Workshop im Juni



Themenspezifische Fragen/Anregungen:  
Steffen Wendzel (<http://www.wendzel.de>)

Bzgl. IT4SE:

Prof. Dr. Thomas Rist ([www.it4se.net](http://www.it4se.net))

# Weitere Informationen zur Thematik (ab 2011)



IT4SE

- S. Wendzel: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden, First IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012), Ottawa, Canada, 2012 (to appear).
- S. Wendzel, J. Keller: Design and Implementation of an Active Warden Addressing Protocol Switching Covert Channels, 7th International Conference on Internet Monitoring and Protection (ICIMP 2012), Stuttgart, 2012 (to appear).
- S. Wendzel, J. Keller: Low-attention forwarding for mobile network covert channels, in Proc. 12th Conference on Communications and Multimedia Security (CMS 2011), International Federation for Information Processing (IFIP), Ghent (Belgium), B. de Decker et. al. (Eds.), LNCS vol. 7025, pp. 122-133, Springer, 2011.
- S. Wendzel: The Problem of Traffic Normalization Within a Covert Channel's Network Environment Learning Phase, in Proc. Sicherheit 2012 (6. Jahrestagung des Fachbereichs Sicherheit), Darmstadt, N. Suri and M. Waidner (Eds.), LNI vol. 195, pp. 149-161, Gesellschaft für Informatik (GI) / Bonn, 2012.
- S. Wendzel, T. Rist, E. André, M. Masoodian: A Secure Interoperable Architecture for Building-Automation Applications, in Proc. 4th Int. Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), pp. B:1-B:5, Barcelona, Spain, 2011.
- T. Rist, S. Wendzel, M. Masoodian, P. Monigatti, E. André: Creating Awareness for Efficient Energy Use in Smart Homes, In Proc. Intelligent Wohnen. Zusammenfassung der Beiträge zum Usability Day IX, Dornbirn, Austria, F. Gerhild, R. Walter (Hrsg.), pp. 162-168, 2011
- S. Wendzel, J. Keller: Einführung in die Forschungsthematik der verdeckten Kanäle, Magdeburger Journal zur Sicherheitsforschung, S. Schumacher (Editor), Vol. 2, pp. 115-124, 2011.
- S. Wendzel: Bewusstsein für die Sicherheit im Bereich der Gebäudeautomatisierung, Hakin9 (de) 03/2011, pp. 11-12, 2011.
- S. Wendzel: Mikroprotokolle in verdeckten Netzwerkkanälen, In: G. A. Fink, J. Vahrenhold (Eds.): Informatik Ruhr: Doktorandenkolleg 2011, Oct 6-7, Meinerzhagen Valbert, p. 35, Germany, 2011.
- T. Rist, S. Wendzel, M. Masoodian, E. André: Next-Generation Home Automation Systems, In Proc. Usability Day X, Dornbirn, Austria, 2012 (to appear).
- S. Wendzel, T. Rist, E. André, M. Masoodian, R. Wirth: Sicherheit beim Energiesparen durch Abstraktion, BusSysteme Magazin 2/12, 2012 (to appear).
- S. Wendzel: Tunnel und verdeckte Kanäle im Netz, Springer-Vieweg, August 2012 (to appear).