SySS
THE PENTEST EXPERTS.

SCHWACHSTELLEN VON HEIMNETZROUTERN

Typische Fehler von Herstellern

AGENDA

- Wer greift an? Mit welchem Ziel?
- Wer ist Schuld? Hersteller oder Benutzer/Betreiber?
- Unsere Untersuchung und allgemeine Arbeitserfahrung
- Typische Schwachstellen
- Empfehlungen zur Konfiguration

VORSTELLUNG

Gerhard Klostermeier

- Pentester / Expert IT Security Consultant
- Seit 2014 bei SySS GmbH
- Teammanager „Embedded Security"
- Interessen: Hardware-Hacking, IoT, Automotive, Funktechnologien, NFC/RFID, Android usw.
- E-Mail-Adresse: gerhard.klostermeier@syss.de

WER GREIFT AN? WESHALB?

- Nicht alle Angreifer sind gleich motiviert, besitzen dieselben Möglichkeiten, denselben Wissensstand oder dasselbe Ziel
- Beispiele für Angreiferpositionen:
  - Extern (aus dem Internet)
  - Im Gäste-WLAN bzw. WLAN
  - Im LAN
  - Physischer Zugriff auf das Gerät
- Motivation bzw. Ziele: Botnet, finanzieller Schaden (z. B. Erpressung), Image-Schaden, persönliche Motive etc.
- Wissensstand: Laie, Script Kiddie, Profi, etc.

HERSTELLER VS. BETREIBER

THE PENTEST EXPERTS.

- Schwachstellen in Heimnetzroutern sind meist vom Hersteller verursacht, manchmal aber auch vom Betreiber
- Beispiele für Routeranforderungen an Hersteller:
  - Sollten mit „Security by Design“ entwickelt werden
  - Sollten eine gute Konfiguration für den Auslieferungszustand aufweisen
  - Sollten lange mit Sicherheitsupdates versorgt werden
  - Sollten regelmäßig auf Schwachstellen hin untersucht werden
- Beispiele für Anforderungen an Betreiber:
  - Sichere Passwörter wählen
  - Fehlkonfigurationen vermeiden

UNTERSUCHUNG & ARBEITSERFAHRUNG

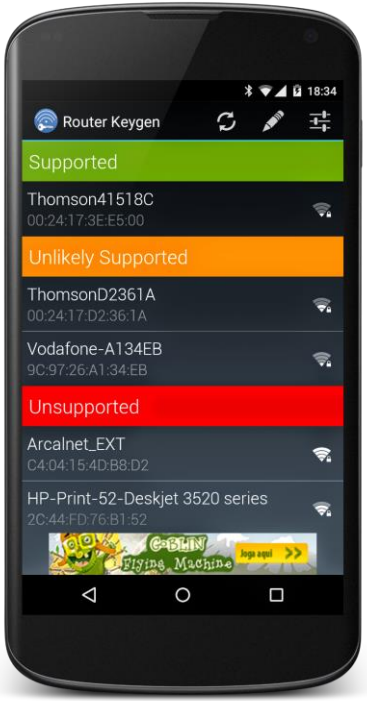
- Untersuchung in Kooperation mit CHIP.de
  - Frage: Ist die Sicherheit von Heimnetzroutern einfach bewertbar?
  - Tiefgreifende Analyse wirtschaftlich nicht durchführbar
  - Wir untersuchten vier Router beispielhaft
  - Artikel: https://www.syss.de/fileadmin/bilder/04_Pentest_Blog/2022/CHIP_WLAN-Router.pdf
- Unsere Arbeitserfahrung
  - Fachteam für Security in Embedded Systems
  - Viel Erfahrung durch die Untersuchungen zahlreicher Router und ähnlicher Komponenten
  - Labor für hardwarenahe Tests

Typische Schwachstellen

AUFGEDRUCKTE PASSWÖRTER

- Hersteller drucken oftmals Zugangsdaten auf das am Router befindliche Etikett
- Manchmal werden die Passwörter nicht zufällig gewählt, sondern berechnet
- Mache Passwörter werden aus bekannten Daten berechnet, z. B. der BSSID/MAC-Adresse

AUFGEDRUCKTE PASSWÖRTER



WI-FI PROTECTED SETUP

- Wi-Fi Protected Setup (WPS)
- Verhältnismäßig alt, aber immer noch häufig anzutreffen
- Typischerweise mit Knopf (Push Button Configuration (PBC)) oder PIN
- 8-stellige PIN → maximal 10^8 Versuche, aber:
  - Die letzte Ziffer ist eine Prüfziffer
  - Die PIN wird in zwei Hälften an den AP übermittelt
  - Nachrichten werden individuell quittiert
- Reduzierte Angriffskomplexität: $10^4 + 10^3$ = maximal 11.000 Versuche
- Mache Geräte verfügen über keinen Brute-Force-Schutz → WPS-PIN kann erraten werden

MEDIA SERVER / NAS

- Viele Heimnetzrouter verfügen über eine USB-Schnittstelle, an die ein Speichermedium (Festplatte/USB-Stick) angeschlossen werden kann
- Die Daten können oftmals über verschiedene Technologien (Netzwerkfreigabe, Media Streaming-Server etc.) freigegeben werden
- Der Zugriffschutz auf die Daten ist nicht immer optimal geregelt
  - Beispiel: Netzwerkfreigabe vs. Streaming bei FritzBox 7530ax
- Der Scope der Daten ist nicht immer optimal geregelt
  - Beispiel: Link auf USB-Speichermedium bei Linksys Velop MR9600

Demo:
Authentifizierung Mediaserver/NAS

Demo:
Scope Mediaserver/NAS

EINRICHTUNGSPROZESS

- Heimnetzrouter können durch zusätzliche Einrichtungsschritte weiter abgesichert werden
- Häufig wird auf eine komplexere Einrichtung verzichtet:
  - Über Features wie UPNP wird nicht aufgeklärt
  - Einstellungen bei der ersten Einrichtung werden nicht angeboten
  - etc.
- Manchmal wird auf eine einfache Einrichtung verzichtet:
  - Keine Passwortänderung nach erster Anmeldung
  - Nutzer bleiben bei unsicheren Anmeldedaten → Benutzer: „admin“, Passwort: „admin“
  - etc.

FIRMWARE-UPDATEPROZESS

- Heimnetzrouter sind vollständige Computer, auf denen ein Betriebssystem bzw. eine Vielzahl von Anwendungen läuft
- Veraltete Software mit bekannten Schwachstellen ist ein häufiges Sicherheitsproblem
- Hersteller sollten Firmware-Updates bereitstellen
- Updates sollten automatisch und sicher installierbar sein
- Typischer Fehler: Updates werden vor dem Installieren nicht ausreichend geprüft
  - Download über unsichere Verbindung
  - Keine kryptografischen Signaturen
  - Beispiel: Edimax BR-6473AX

FIRMWARE-UPDATEPROZESS: EDIMAX BR-6473AX

- Firmware-Update herunterladen
- Firmware „entpacken“
- Relevante Dateien finden (Script für automatische Firmware-Updates)
- Updateprozess analysieren

```
36      done
37  }
38
39  #Control
40  DO_WHAT=$1
41  STATUS_CODE="/opt/lantiq/www/ErrorCode"
42  PRODUCT="BR-6473AX"
43  AUTOFW_DIR="/tmp/autofw"
44  G_DEF_FW_DISCOVER_SERVER_DOMAIN="www.edimax.com" #Official Server IP
45  G_DEF_FW_DISCOVER_SERVER_FILE="BR-6473AX_info.txt"
46  AUTOFW_TIMEOUT=600
47  AUTOFW_DISCOVERY_FILE="$AUTOFW_DIR/BR-6473AX_info.txt"
48  AUTOFW_FINAL_FW="$AUTOFW_DIR/fw.bin"
49  AUTOFW_DOWNLOAD_CHECK_RESULT="$AUTOFW_DIR/downloadCheckResult"
50
51  #Detect WPS
52  if [ "$DO_WHAT" = "DoUpg" ]; then
53      isWPSrunning
54  fi
55
56  doUpgrade=0
57  rm -rf $AUTOFW_DIR
58  mkdir -p $AUTOFW_DIR
59
60  curl -k -m 5 -s -o $AUTOFW_DISCOVERY_FIL http:/${G_DEF_FW_DISCOVER_SERVER_DOMAIN}/fw/wifirouter/${PRODUCT
    }/${G_DEF_FW_DISCOVER_SERVER_FILE}
61  if [ "`cat $AUTOFW_DISCOVERY_FILE | grep Forbidden`" != "" ] || [ "`cat $AUTOFW_DISCOVERY_FILE | grep -w "4
    04 Not Found"`" != "" ] || [ ! -f $AUTOFW_DISCOVERY_FILE ]; then
62      # echo  "[Auto Upgrade] Download Fail! (login failed, server is not exist)"
63      echo 1 > $STATUS_CODE
64      exit
65  else
```

FIRMWARE-UPDATEPROZESS: EDIMAX BR-6473AX

THE PENTEST EXPERTS.

```
    done
}

#Control
DO_WHAT=$1
STATUS_CODE="/opt/l
PRODUCT="BR-6473AX"
AUTOFW_DIR="/tmp/autofw"
G_DEF_FW_DISCOVER_SERVER_DOMAIN="www.edimax.com" #Official Server IP
G_DEF_FW_DISCOVER_SERVER_FILE="BR-6473AX_info.txt"
AUTOFW_TIMEOUT=600
AUTOFW_DISCOVERY_FILE="$AUTOFW_DIR/BR-6473A
AUTOFW_FINAL_FW="$AUTOFW_DIR/fw.bin"
AUTOFW_DOWNLOAD_CHECK_RESULT="$AUTOFW_DIR/d

#Detect WPS
if [ "$DO_WHAT" = "DoUpg" ]; then
    isWPSrunning
fi

doUpgrade=0
rm -rf $AUTOFW_DIR
mkdir -p $AUTOFW_DIR

curl -m 5 -s -o $AUTOFW_DISCOVERY_FILE https://${G_DEF_FW_DISCOVER_SERVER_DOMAIN}/fw/wifirouter/
${PRODUCT}/${G_DEF_FW_DISCOVER_SERVER_FILE}
if [ "`cat $AUTOFW_DISCOVERY_FILE | grep Forbidden`" != "" ] || [ "`cat $AUTOFW_DISCOVERY_FILE |
 grep -w "404 Not Found"`" != "" ] || [ ! -f $AUTOFW_DISCOVERY_FILE ]; then
    # echo  "[Auto Upgrade] Download Fail! (login failed, server is not exist)"
    echo 1 > $STATUS_CODE
    exit
else
```

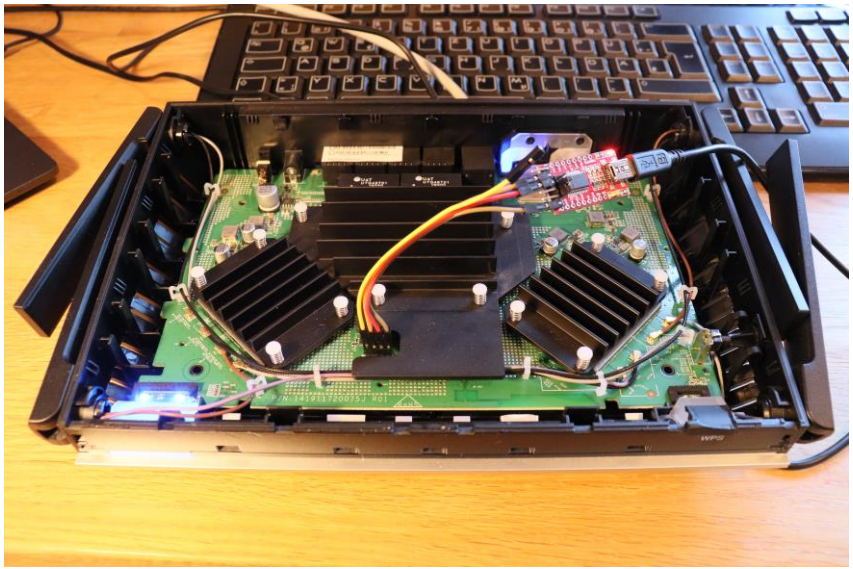
```
-k, --insecure
       (TLS  SFTP  SCP)  By default, every secure connection curl makes is verified to be secure
       before the transfer takes place. This option makes curl skip the  verification  step  and
       proceed without checking.
```

File: **/tmp/autofw/BR-6473AX_info.txt**

```
1  BR-6473AX
2  1.0.24
3  dbe3bb7dbee7ddd73cd73794516e9e1b
4  http://www.edimax.com/fw/wifirouter/BR-6473AX/BR-6473AX_v1.0.24.bin
```

HARDWARENAHE ANGRIFFE

- Heimnetzrouter besitzen oft interne Schnittstellen (z. B. JTAG oder UART)
  - Ursprünglich für Entwickler gedacht
  - Erlauben oftmals Kompromittierung des Geräts
- Speicher kann ausgelesen und manipuliert werden
- Speicher wird beim Zurücksetzten auf Werkseinstellungen nicht immer richtig/vollständig gelöscht



EMPFEHLUNGEN ZUR KONFIGURATION

- Passwörter ändern (Gerätezugang und WLAN)
  - Länge schlägt Komplexität
- WPS deaktivieren
- Mindestens WPA2 (mit AES/CCMP) nutzen
  - Besser: WPA3 nutzen und auf Mischbetrieb mit WPA2 verzichten
- UPNP deaktivieren (Gäste-WLAN verwenden)
- Unterstützung für Protected Management Frames (802.11w) aktivieren
- Automatische Updates aktivieren bzw. regelmäßig manuell auf Updates prüfen
- Airbnb/Ferienwohnung: Router unzugänglich machen

Fragen & Diskussion

E-Mail: gerhard.klostermeier@syss.de
Twitter: @iiiikarus
YouTube: https://www.youtube.com/c/SySSPentestTV
Blog: https://blog.syss.com

THE PENTEST EXPERTS

WWW.SYSS.DE