Flurfunk

Building sovereign network infrastructure

in a real-world government agency

Bundesamt
für Sicherheit in der
Informationstechnik

What is it all about?

The network gear in your typical office

- **Switches**
- **Routers**
- **Wireless (WLAN) access points**

Agenda

- Management-level Overview
- Technical implementation
- Arguments why this is a good idea (Slides after the end)

01. Management-level Overview

Structure

- My task
  - Celebrate how far we've come
  - Show you how easy it is to run sovereign network infrastructure solely with FOSS firmware/software
- Your task (should you choose to accept it)
  - Copy and enjoy!

Who am I?

Carl-Daniel Hailfinger

- **Working for BSI (Federal Office for Information Security, Germany) on operating system security**
- **FOSS developer since at least 2002 (first Linux kernel patch)**
- **Former maintainer of flashrom project**
- **Current maintainer of hai-end-streaming project**
- **Occasional contributor to various projects**
- **Take apart, understand, rebuild better**

The State of Sovereign <thing>

Building Europe’s Public Digital Infrastructure

- **Sovereign software on the client? Solved.**
- **Sovereign cloud infrastructure? Solved.**
- **Sovereign software on servers? Solved.**
- **Sovereign networks? Wait a minute.**

A sovereign office network running only FOSS?

We tried it. Surprisingly, it works well enough.

- **Usability is on par with proprietary commercial offerings.**
- **Reliablity is fit for critical infrastructure.**
- **Features: You lose some, you win some.**
- **Hardware choice:**
  - **Limited (not all devices supported)**
  - **Extended (no vendor lock-in, same user interface everywhere)**
- **Overall: Enterprise ready (at least with OpenWrt)**

Goals

Making COTS network hardware trustworthy with very little effort

Have all the network gear in your office run trustworthy FOSS

Definitions

- **Easy installation: No opening the case, no soldering, 5 minutes max per device**
- **Easy management: GUI or text mode, your choice**
- **Trustworthy: You have full control over the code running on your network gear**
- **Firmware: (in this context) Combination of bootloader and operating system**

Measurable benefits

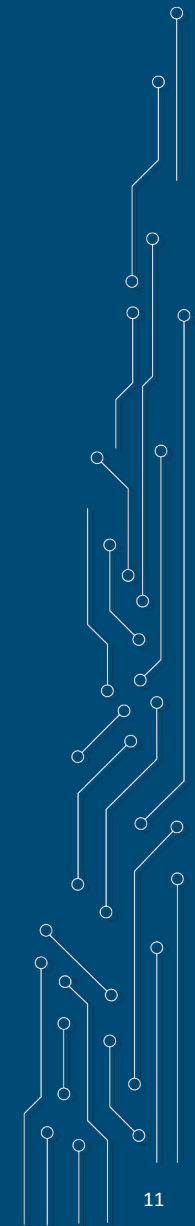
- Security: Backdoor in vendor firmware? Not your problem anymore.
- Security: Hardware is EOL? FOSS network OS has updates, usually >10 years.
- Cost: Extra features at no cost
- Cost: No rip-and-replace when switching hardware vendors
- Ease of use: Same user interface for all hardware vendors
- CRA: You get a complete SBOM
- Ecological: Continue using hardware after end-of-support from manufacturer
- Missing feature/bugfix? Pay someone to develop + integrate it in the next version

Management Summary

TL;DR

Replace the firmware of your network gear with OpenWrt.

It’s secure and works well.



02. Technical implementation

Bild: © AdobeStock/Azazul

Disclaimers

- Management wants me to emphasize that we're not using this in production. Officially, it is a PoC.
- The network operating system (OpenWrt) of this PoC has been chosen for broad hardware support, usability, longevity and a helpful community.
- The hardware of this PoC was from multiple vendors, but we converged on few devices offering easy installation of OpenWrt, realiability and good price.
- Depending on your needs / OpenWrt development, other hardware may be better
- This is not an endorsement or recommendation of any hardware/software vendor.

Most COTS network hardware

Extremely limited control, lots of blind trust

You choose the vendor based on

- **Politics**
- **Habit (which UI do you know)**
- **Already deployed gear**
- **Price**
- **Features**
- **Perceived security**

Run a Linux-based NOS on COTS hardware

But... is it enterprise-ready?

- **Yes! (At least OpenWrt is)**
- **Many switches, routers (home/office/datacenter), wifi access points run Linux**
- **Hidden behind a vendor-specific user interface**
- **Linux not preinstalled? Can be installed on many devices**

Architecture

Typical office network

- **Router towards the internet**
- **Switches for the internal network**
- **WLAN (Wi-Fi) access points**
- **(Network monitoring: May exist, but mostly unused)**
- **(Servers and clients not part of this talk)**

Security considerations

Target environment

- **Average office**
- **Users/Guests have no management access to network gear**
- **Wired (LAN) access needs no further authentication**
- **Separate Guest network (wired+wireless) is desired**
- **Separating networks with VLAN (management/users/guests) is good enough for the use case**
- **Off-boarding people/devices should not require a wireless password change**
- **Wireless User authentication via WPA3 Enterprise with certificates**

Technical implementation (1)

- Management network: no VLAN tag
- User network: VLAN 1, untagged wherever users connect
- User WLAN authentication
  - WPA2/WPA3-EAP-TLS, separate key per device
  - AP asks RADIUS server if authentication is OK
- Guest network: VLAN 3, untagged wherever guests connect
- Guest WLAN authentication
  - WPA2/WPA3-PSK, same password for everyone
  - AP verifies WLAN password directly

Technical implementation (2)

- RADIUS server checks user certificates
  - APs do not directly communicate with RADIUS server
  - AP/RADIUS server communication via central radsecproxy
- User Certificate generation: script invoking OpenSSL or step-ca
- Heavily inspired by Eduroam and the documentation provided by DFN
- You could easily hook up the user network to Eduroam

WLAN access points: Preparing the image

Example: Zyxel NWA50AX Pro, procedure is the same for other devices

1) Preparing the image (only once)

a) Go to https://firmware-selector.openwrt.org/

b) Select "Zyxel NWA50AX Pro" and Version "24.10.5" (current version)

c) Click on "Customize installed packages and/or first boot script"

d) Add luci-ssl and luci-app-attendedsysupgrade to the list of installed packages

e) Click "Request build", wait 5 Minutes

f) Download "Factory" and "Sysupgrade" images, verify checksums

WLAN access points: Installation

Example: Zyxel NWA50AX Pro. (See https://openwrt.org/toh/zyxel/nwa50ax_pro)

1) Create a separate provisioning network for installing ("flashing") OpenWrt
    a) Have a DHCP server active on a separate machine
    b) No internet connection needed/advisable
2) Attach AP to this network and power it on, AP will get an IP from the DHCP server
3) Connect web browser to AP, log in with default credentials
    a) Choose standalone mode
    b) You will be forced to change the password and re-login
    c) Log in with the changed password, exit the setup wizard, do not upgrade firmware

WLAN access points: Installation

6) On the main screen, check if any firmware update has been installed

    a) If no firmware update has been installed previously, skip to next step

    b) If another firmware update has been installed, consult OpenWrt wiki

7) Navigate to Maintenance → File Manager → Firmware package

8) Upload the previously prepared factory firmware

9) Wait for the device to reboot

10) Disconnect the DHCP server, reconnect your local workstation

11) Connect web browser to 192.168.1.1 (user: root, no password)

WLAN access points: Installation

12) Navigate to System→Backup/Flash Firmware, upload archive (config) file

13) Click proceed. The AP will reboot.

14) Connect DHCP server again and reconnect your local workstation

15) AP will get an IP from the local DHCP server

16) Connect web browser to AP (user: root, no password)

17) Set password and any other configuration

18) Navigate to System→Backup/Flash Firmware, download current configuration

19) Use the new configuration for all other APs

Routers/switches: Installation

Same as APs, but without the complicated DHCP dance

Routers need one additional package: radsecproxy

RADIUS: Installation

1) Install current Debian

2) Unpack the configuration tarball in root directory

3) Done

CA: Installation

1) Install current Debian

2) Unpack the script tarball in user directory

3) Run generator script

4) Alternative: look at https://smallstep.com/blog/home-network-eap-tls-wifi/

You’re done!

Well, almost…

You need to hook up the cables.

Think about a good wifi password for guests.

That’s it.

Configuration files are in the FOSDEM talk page.

Questions?

Bild: © AdobeStock/Azazul

Thank you for your attention!

Carl-Daniel Hailfinger

Referent, Section Operating Systems

Carl-Daniel.Hailfinger@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: