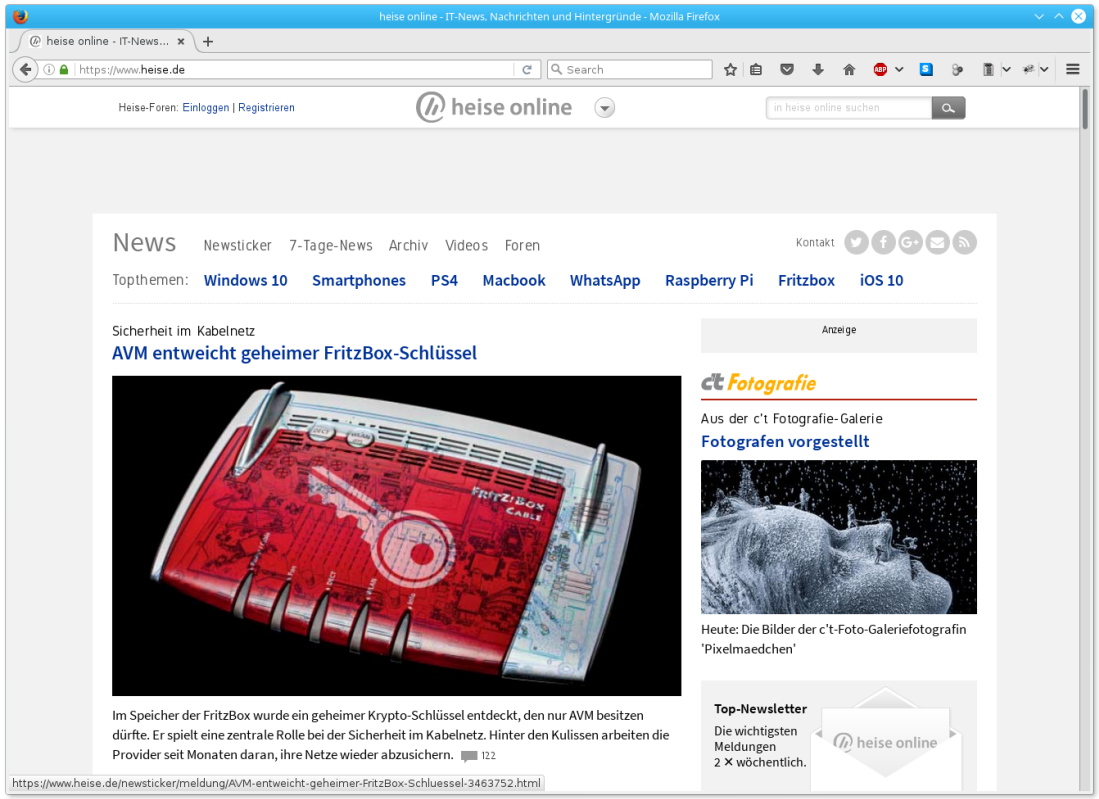
Hacking DOCSIS

Joel Stein

FRITZ!Box Keyble

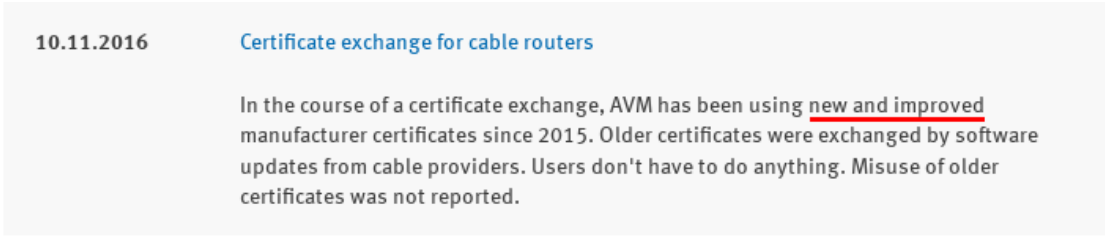


SRC: `https://www.heise.de` (11.11.2016)

FRITZ!Box Keyble

- AVM ships private key for Euro-DOCSIS-signed intermediate CA on Router.
- On-the-fly generation of VALID modem certificates.
- Presumably trusted by many CMTS around the world (Trusting the Euro-DOCSIS Root-CA)

FRITZ!Box Keyble



10.11.2016 Certificate exchange for cable routers

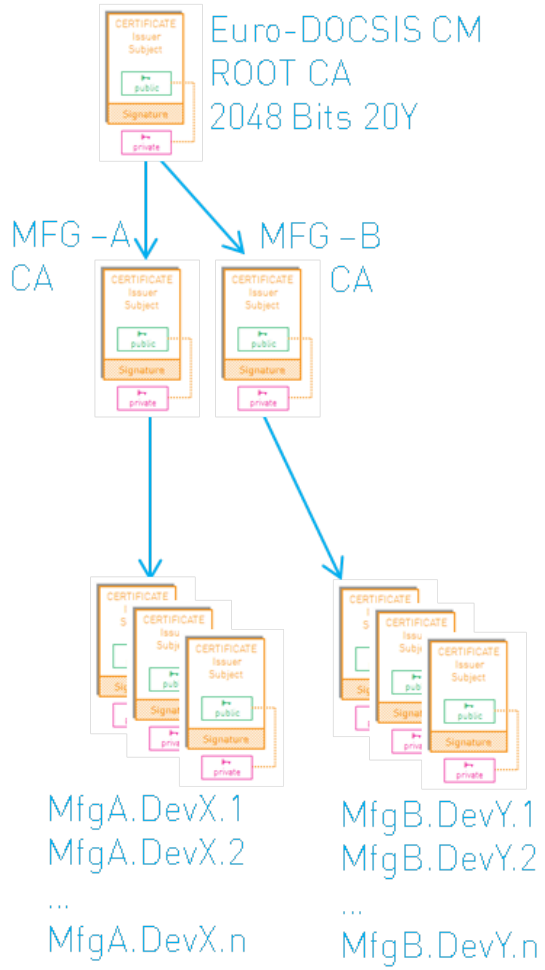
In the course of a certificate exchange, AVM has been using new and improved manufacturer certificates since 2015. Older certificates were exchanged by software updates from cable providers. Users don't have to do anything. Misuse of older certificates was not reported.

1

- German ISPs and AVM working on updating old devices and blocking compromised CA in their CMTS.
- What about the rest of the (Euro)-DOCSIS world?

[1] https://en.avm.de/service/current-security-notifications/

Euro-DOCSIS PKI



SRC: `https://www.excentis.com/blog/certificates-and-different-pkis-docsis-31`

AVM Intermediate CA

Listing 1: AVM Cable Modem Root CA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:d9:3d:04:72:8f:ce:2f:ba:a7:81:a8:1f:92:6a:43
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BE, O=tComLabs - Euro-DOCSIS, OU=Cable
            Modems, CN=Euro-DOCSIS Cable Modem Root CA
        Validity
            Not Before: Jul 30 00:00:00 2009 GMT
            Not After : Jul 29 23:59:59 2029 GMT
        Subject: C=DE, ST=Berlin, L=Berlin, O=AVM GmbH, OU=
            Euro-DOCSIS, OU=Germany, CN=AVM GmbH Cable
            Modem Root Certificate Authority
```

"Revocation"

"My CMTS is not using that certificate, am I safe now?

No, because (Euro)DOCSIS is designed to accept any correctly signed cable modem by default, the certificate might be used by a hacked modem in the future without you noticing it. Hence, it is important to configure ALL your CMTSs not to accept the revoked certificate anymore!"[2]

[2] https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates/revoked-certificates

"Revocation"

"Two centralized methods are defined in the specifications (CRL and OCSP). None of these are required to be supported. No public CRL or OCSP service for (Euro)DOCSIS exists."[3]

[3] https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates/revoked-certificates

"Revocation"

snmpset –v 2c –c <community> <cmts_ip>

docsBpi2CmtsCACertStatus.<index> i 4 docsBpi2CmtsCACertTrust.<index> i 2

docsBpi2CmtsCACert.<index> x <hexString>[4]

[4] https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates/revoked-certificates

"Revocation"

33c3@joel-stein.de