DSL

Dismantling Secret Layers

Brian Butterly

Independent Security Researcher
@BadgeWizard
www.security-bits.de

10.2018 / H2HC 2018

Outline

Outline

About me

"Hacker"

- Hello! My name is Brian!
- It's my fourth H2HC in a row
- I dropped out off Pentesting beginning of the year and have switched to incident response in a simply epic environment
  - Creating detection mechanisms for crazy devices requires the same skills, and often even deeper knowledge & I finally have my own turf to look after
  - I now have much more time to break fun stuff :)

Why DSL?

And why talk about it?

- Over the past few years, together with Hendrik, we've given multiple talks on giving insights into not trivial areas
  - Embedded / Hardware Security, LTE, VoLTE, general cellular
  - P.S.: A short hello to Hendrik!
- The aim always being: To make sure the community (>YOU<) can skip wasting time doing background research and can simply dive into the topic!

Why DSL?

And why talk about it?

- large parts of our everyday lives rely on being online and being connected
- DSL is one of the typical connection types / channels we use
- As such it's critical to have secure DSL infrastructure and environments
- And to achieve this, we need to able to research this technology

Why DSL?

Because we need to!

- In some countries/with some providers you do not have a choice which router you want to use
- The provider patches, or doesn't and secures the device, or doesn't
- It's crucial for us to be able to oversee the devices and ensure their and our security

That's why!

- There has been a significant history of home routers being owned

DSL History

Digital Subscriber Line

- Also known as Digital Subscriber Loop
- Current approach to providing internet via 2-wire copper (phone lines)
- Patented in 1988

ADSL

Asymmetric Digital Subscriber Line

- Asymmetric -> Larger downstream than upstream (customer perspective)
- Using Frequency-Division duplex, Echo-Canceling-Duplex or Time-Division-Duplex
- Initially as ANSI T1.413-1998 Issue 2 from 1998
  - With 8Mbit/s down and 1Mbit/s up
- Later as ADSL2+ / ITU G.992.5 Annex M
  - With 24Mbit/s down and 3.3Mbit/s up

VDSL

Very-high-bit-rate Digital Subscriber Line

- Very fast ;-)
- Using Quadrature Amplitude Modulation or Discrete Multi-Tone Modulation
- Initially as ITU G.993.1
  - With 55Mbit/s down and 3 Mbit/s up
- Since 2015 as VDSL2-Vplus / ITU G.993.2 Amendment 1 (11/15)
  - With 300Mbit/s down and 100Mbit/s up

DSLAM

DSL Components

- Digital Subscriber Line Access Modem
  - The part the modem connects to
- In areas with slow DSL you'll have one for a part of a town
- In ares with fast DSL you'll have Outdoor DSLAMs basically on every street block
- DSLAM controls the link with the modem and sets the DSL parameters

Splitter

DSL Components

- Splitters are used when a two-wire line is used in multiple ways
  - i.e. Analog calling, ISDN & DSL
- The Splitter splits the frequency band into two parts
  - Lower band: Phone calls & ISDN
  - Upper band: DSL
- For modern lines (Annex J / I) the whole spectrum is used for DSL

Annex

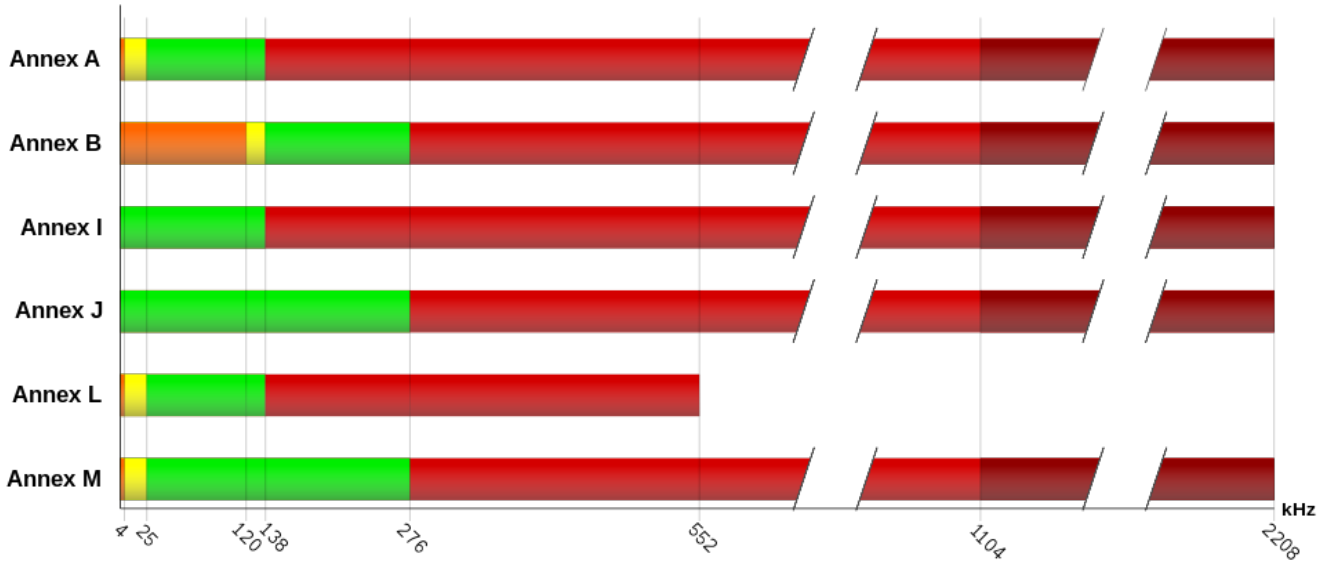

Figure: Exemplary Annex

The Annex describes the practical usage of frequencies / band plan on the copper wires

Annex

- The Annex describes the practical frequency usage on the phone lines
- Modems & DSLAMs support different Annexes based on internal splitter (uplink/downlink)
- And of course the used chipset

Modem

DSL Components

- Modem in the classical sense
- Slave device towards the master modem
- Basically just a converter between the DSL lines on the one side and Ethernet on the other

Client

DSL Components

- Whatever actually has the modem in it or controls it

Outline

DLSAM / Master Modem

ALLNET 126AM2

- Supports ADSL
- Looks like a small home router
- 4 Ethernet ports, 1 Line port (DSL), 1 Phone Port
- Serial console (just in case)
- Price: $230us, half on eBay if you're lucky

CPEs

Home Routers

- What ever you have or need or want!

PPP Server

PPP-over-Eternet

- Small Software package by Roaring Penguin Software Inc.
- All you need to do is configure the IP address ranges and credentials
- And create a TUN interface

ACS

Auto Configuration Server

- Remote management & provisioning system for CPEs and other components
- ISP uses these to push new firmware & configuration
  - And initial setup
- This is the thing that uses TR-069
- Today's setup does not contain an ACS ... but....

ACS

...is real fun

- The ACS is usually pushed to the client via DHCP paramters
  - Using defined vendor options
- Usually, on initial setup, secrets are exchange (i.e. user & password)
- The ACS then needs these when connecting to the client
- Obviously some use SSL, some don't. Some use Digest Auth, some don't...

ACS

...can be broken

- Some CPEs during start, actively initiate a connection the the ACS
- And use credentials to sign in
- And fetch configuration
- What could possibly go wrong?

Basics

- Modern DSL connections use VLANs
  - So we need VLAN tools
- Some routers use raw DHCP
  - So we need a DHCP server
- We want to reroute traffic
  - So we need a DNS server, IPTables, EBtables

Above that...

Tools...

- Everything from here is plain IP :)

Making life easier

- High can just highly recommend automatic most things in scripts
  - Especially configuration of interfaces etc.
- Also, extend the DSLAM ;-)
  - DSLAM sets the DSL parameters, but sometimes you don't have enough information about the modem
  - So I wrote a short bash script starting and killing the DSL connection and using new settings everytime

Three Stages of the Lab

1. Basic setup for testing a CPE
2. MitM setup
3. Dev setup für MiTm

Level 1 Setup

DSLAM & CPE

- Blue VM is the target VM
- Running a PPPoE server
- The green VM is simply the user

Level 1

Options

- We know have raw and direct network access to the CPE
- From the DSL side
- We can now scan, fuzz and have a closer look at the communication

Level1

A quick insight

- Let's get it running

Level 2

DSLAM, CPE and Modem

- Basic MitM setup
- The Modem supports PPPoE passthrough
- This is the approach that I travel with when looking and things

Level 3

DSLAM, CPE, Modem and another DSLAM

- Aim is to emulate a complete DSL MitM setup
  - Including internet access
- Having the ISP on the one side, the CPE on the other
- And the MitM actually in the middle

- I use this setup, because I don't want to loose my connection or break something by accident

Demo Setup

On the table

- Blue DSLAM
  - ISP - Connected to ISP VM (Blue)
- FritzBox
  - In PPP pass through mode, converting the intercepted date back into line signals
  - Data coming from Attacker VM (Red)
- Grey DSLAM
  - Providing line signal for victim
  - Sending signals into Attacker VM (Red)
- $CPE
  - Our Victim
  - Data coming from User VM (Green)

Outline

The full setup

- Time for a short Demo

Telekom DSL Router

- Model from a few years back
- Used to be the standard device Deutsche Telekom gave to their customers
  - I got this from eBay, and am actually using a custom setup at home ;-)
- DSL Router with VoIP, WiFi and (I think) DECT

Telekom DSL Router

Sniffing it

- PCAP or It didn't happen

Telekom DSL Router

Results

- PPP Authentication is in Plaintext
- Fetching firmware information is in Plaintext
- Fetching the firmware is, too
  - But they’re signed....

Telekom DSL Router

VoIP

- Credentials are sent encrypted
  - Simple but effective Digest Auth
- Phone calls are unencrypted

O2 DSL Router

Sniffing it

- PCAC or it didn't happen

Telekom DSL Router

Above that...

- I have not taken a closer look at the DHCP request the router sends out
- But I guess I might be able to squeeze in an ACS here

O2 DSL Router

Results

- PPP Authentication is in Plaintext

O2 DSL Router

VoIP

- Credentials are sent encrypted
  - Simple but effective Digest Auth
- Not sure about phone calls, yet
- But there is a second account configured by default which obviously isn't configured

What we have seen is...

not too bad

- Usually these services are only exposed and used within the "ISP's network"
- They should not be exposed to the public internet
  - Should be filtered at boarder gateways

Sometimes they aren't

- I.e. Big router outage in 2016 in Germany
- A buggy worm accidentally crashing routers via TR-069

Summary

- Hacking DSL devices is fun
  - And it's easy
- There are many things to have a look at
- We are relying on networks we have never had a look at

Questions?

Questions?

- Questions?

Sources

- Annexes: https:///en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line#/media/File:ADSL_annex_overview.svg