Network sniffing with Wireshark

Ingo Blechschmidt

35th Chaos Communication Congress

December 29th, 2018

Sniffing network traffic

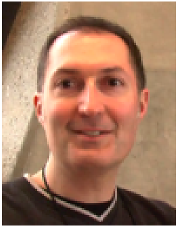
Key question:
How does the traffic which my computer sends and receives look like?

Why be interested in this question?

- To learn how network protocols work.
- To diagnose network problems.
- To sharpen one's security awareness.
- To uncover hidden background communication.

On Wireshark

- Wireshark: free tool for network sniffing
- first release in 1998 by Gerald Combs
- `$ apt install wireshark`
- no magic – the traffic exists either way
- be careful: security problems in Wireshark
- alternatives: tcpdump;
  partially also Firefox, Chrome



Gerald Combs

Networking basics

- Network traffic is sent and received in individual packets.
- A typical maximal packet size is 1500 bytes.
- Ways of addressing target computers:

global:	domain names,	e. g. `events.ccc.de`
global:	IP addresses,	e. g. `195.54.164.66`
lokal:	MAC addresses,	e. g. `00:16:76:7d:00:c2`

Live demo

1. First steps: Ping
   (DNS, ICMP)
2. Starting a browser
   (DNS prefetching)
3. Loading a website
4. Logging in to a website
5. ARP spoofing (Debian-Paket dsniff)