



Velkommen til

Data misbrug 2018

Ulovlig logning møde

Henrik Lund Kramshøj hk@zencurity.dk

slides are available on Github

Målet: data kan misbruges, men hvilke



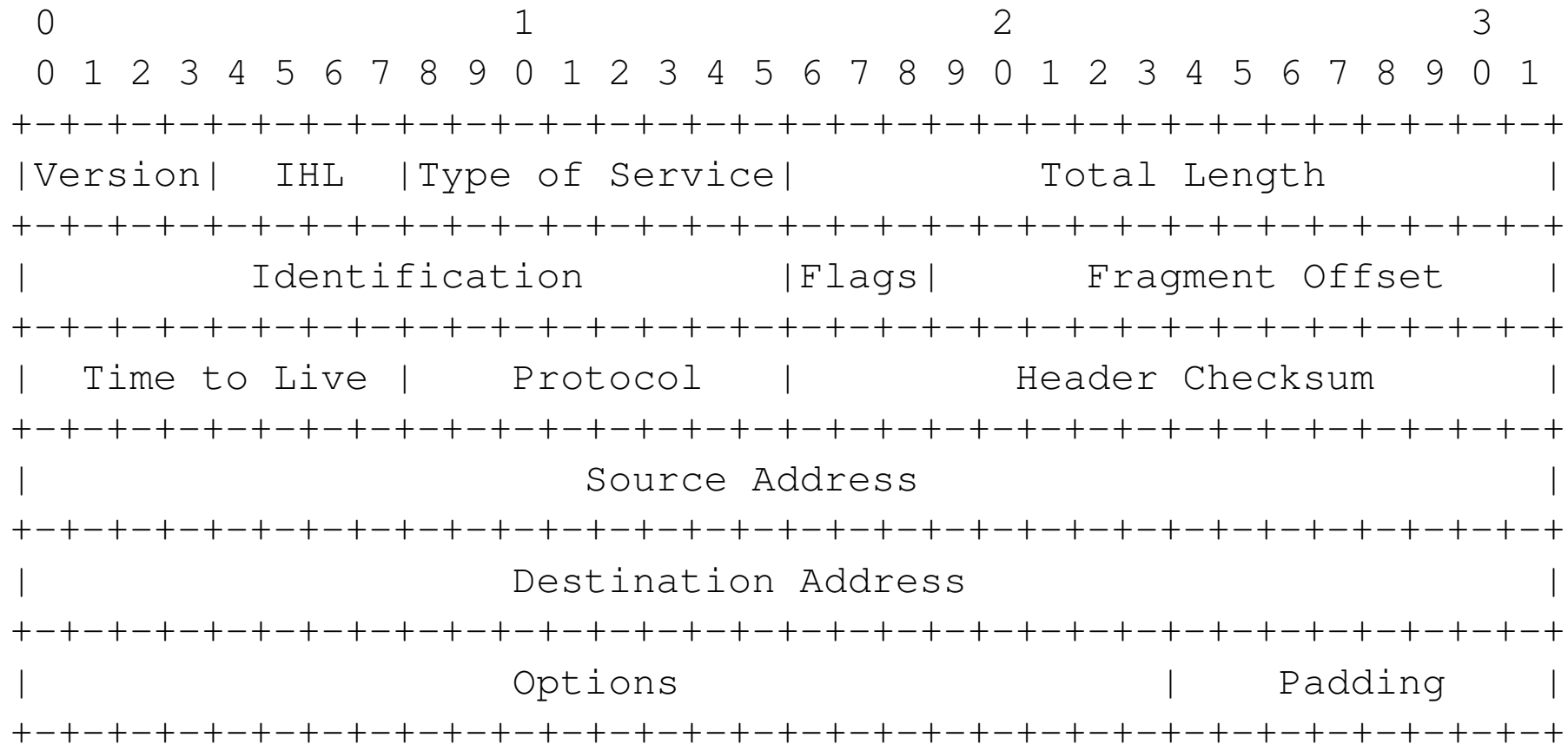
Der tales om data misbrug og data logning

Planen for idag:

- Fokus på bestemte typer data, netværksdata
- Eksempelvis åbne trådløse netværk
- ... det er de samme data din internetudbyder har adgang til

Hvis du har lyst kan du være med til at vise data

IPv4 pakken - header - RFC-791



Example Internet Datagram Header

Eksempler



Jeg vil nu gennemgå nogle få eksempler på information som man kan samle op.

Det hele starter eksempelvis med:

- IP-adresser - den adresse som din enhed har
- Eksterne IP-adresse, oftest har du en privat adresse internt, lokalnummer og så går du på internet ud igennem en router - med ekstern/offentlig IP.
Kan være flere niveauer med Carrier Grade NAT, som Interpol er kede af!
- Operativsystemer, bruger du Windows fremgår det af dine internetpakker
- Applikationer, dine browsere og andre programmer fortæller gerne hvad version det er



Åbne trådløse netværk er dejlige, vi bruger dem allesammen.

```
http://wifi.aal.dk/fs/customwebauth/login.html?  
switch_url=http://wifi.aal.dk/login.html&ap_mac=70:db:98:73:e5:a0&  
client' mac=30:10:b3:XX:YY:ZZ&wlan=AALfree&redirect=www.gstatic.com/generate'204
```

- Når du forbinder til netværket, bruger din enhed sin MAC adresse
- Denne indeholder en OUI som er den første halvdel af de 48-bit
- Dette ID er gemt i din enhed, fra fabrikken, kan sjældent ændres
- Alle i nærheden kan se denne MAC, og dermed din enheds unikke hardwareadresse.
- Kendere ved at man kan skifte sin MAC midlertidigt, og det gør telefoner ofte når de scanner efter netværk idag - hvis de overhovedet scanner

Telefonnumre



Christian Panton
@christianpanton

@je5perl

```
panton@fluffy:~$ curl -H "Host: mobil.dr.dk" headertest.panton.org/  
Connected: [::ffff:80.62.117.213]:55713  
  
GET / HTTP/1.1  
X-Nokia-msisdn: 4531695533  
X-Context-id: 1223221667  
User-Agent: curl/7.35.0  
Accept: */*  
Host: mobil.dr.dk
```

30/10/14 22.13

- Christian Panton har tidlige vist hvordan telefonnummer blev sendt med
- Applikationer kan snildt sende data med
- ... men gør de det sikkert - med kryptering

TLS Server Name Indication extension



HTTPS skal der til!



Vi skal kryptere, men desværre så skjuler vores HTTPS ikke hvad site vi tilgår.

- HTTPS er idag TLS Transport Layer Security
- Verifikation sker med certifikater der præsenteres af server
- Der kan være flere sites på en enkelt IP - med SNI
- Desværre vælges det rigtige certifikat før krypteringen starter

TLS Server Name Indication example



▼ Secure Sockets Layer		
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello		
Content Type: Handshake (22)		
Version: TLS 1.0 (0x0301)		
Length: 198		
▼ Handshake Protocol: Client Hello		
Handshake Type: Client Hello (1)		
Length: 194		
Version: TLS 1.2 (0x0303)		
▶ Random		
Session ID Length: 0		
Cipher Suites Length: 32		
▶ Cipher Suites (16 suites)		
Compression Methods Length: 1		
▶ Compression Methods (1 method)		
Extensions Length: 121		
▶ Extension: Unknown 56026		
▶ Extension: renegotiation_info		
▼ Extension: server_name		
Type: server_name (0x0000)		
Length: 16		
▼ Server Name Indication extension		
Server Name list length: 14		
Server Name Type: host_name (0)		
Server Name length: 11		
Server Name: twitter.com		
▶ Extension: Extended Master Secret		
0050	a4 1d 52 8f 2c 18 99 91 54 68 0a 77 0d 95 73 64	..R.,... Th.w..sd
0060	7d 00 00 20 5a 5a c0 2b c0 2f c0 2c c0 30 cc a9	}.. ZZ.+ ./,..0..
0070	cc a8 cc 14 cc 13 c0 13 c0 14 00 9c 00 9d 00 2f /
0080	00 35 00 0a 01 00 00 79 da da 00 00 ff 01 00 01	.5.....y
0090	00 00 00 00 10 00 0e 00 00 0b 74 77 69 74 74 65twitte
00a0	72 2e 63 6f 6d 00 17 00 00 00 23 00 00 0d 00	r.com... ..#.....
00b0	14 00 12 04 03 08 04 04 01 05 03 08 05 05 01 08

Metadata



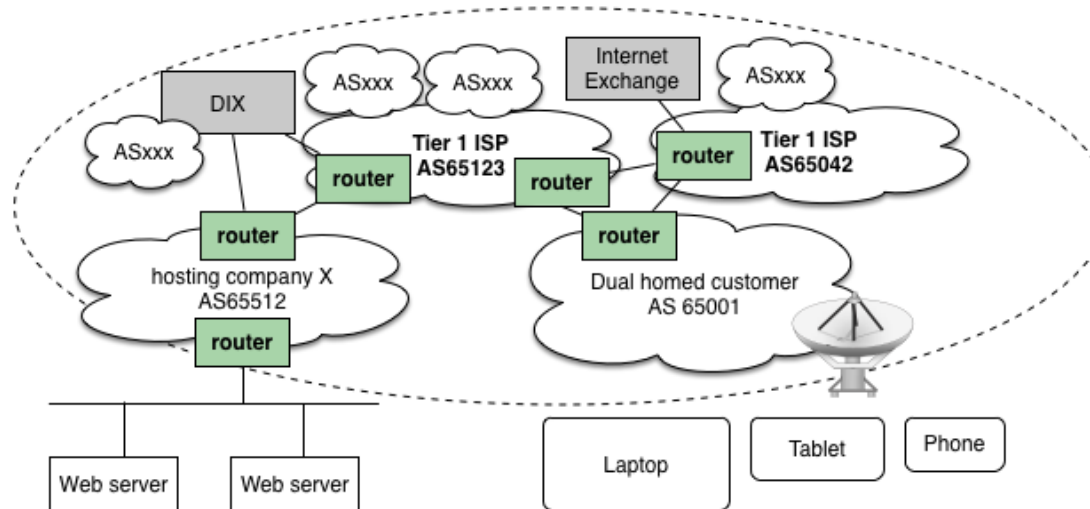
- Data er det vi udveksler
- Meta data er data om data, nødvendige data for kunne sende eksempelvis IP-adresser

Enhederne er forskellige



- Mine enheder er selvfølgelig forskellige
- MAC adresser er forskellige
- De data mine enheder er også forskellige
- Qubes spørger fedora.pool.ntp.org, min Turris router openwrt.pool.ntp.org
- Et TV spørger måske efter opdateringer fra Samsung, mens en laptop henter fra Apple (via CDN)

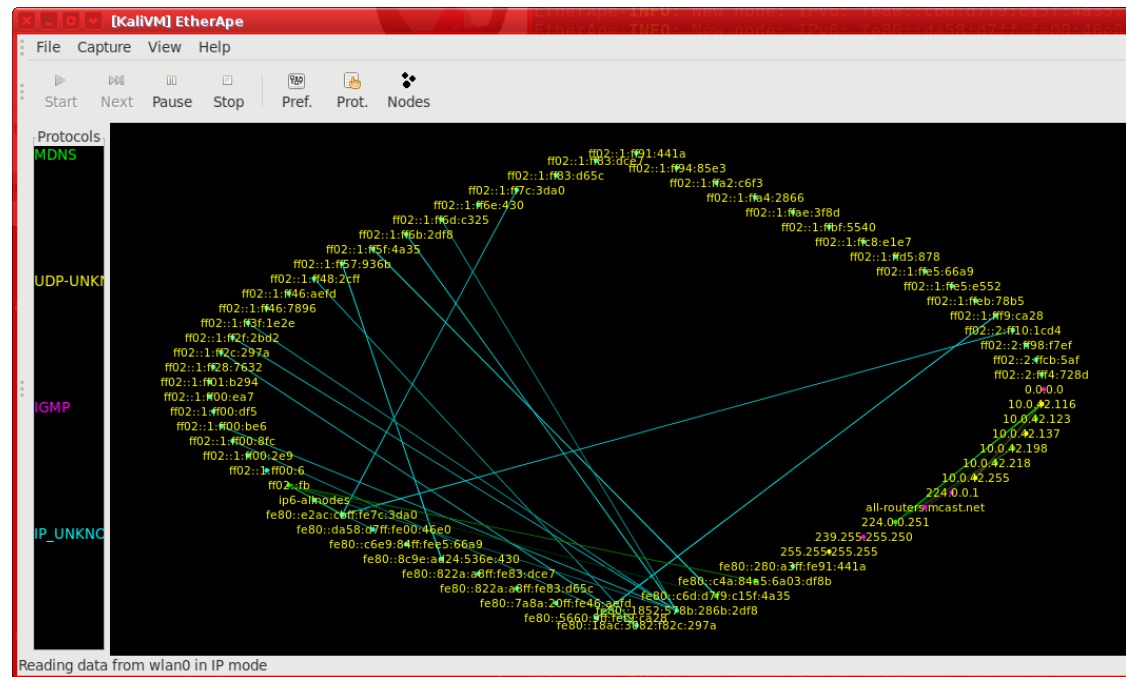
Hosting og internet-udbydere



- Jeg var engang i en position hvor vi transporterede data for mange kunder
- Det var data som information, just eat, kino.dk
- ... er vi trygge ved snifferbokse foran vores allesammens statslige netværk?

Var data fra kun een hosting udbyder, med mange kunder/portaler

Etherape demo, hvis vi har tid



- Etherape er et smart demoprogram
- men tcpdump er virkelig også *sjovt*

Spørgsmål og mere debat



Henrik Lund Kramshøj hik@zencurity.dk