Velkommen til

Data misbrug 2018

Ulovlig logning møde

Henrik Lund Kramshøj hlk@zencurity.dk

slides are available on Github

Målet: data kan misbruges, men hvilke

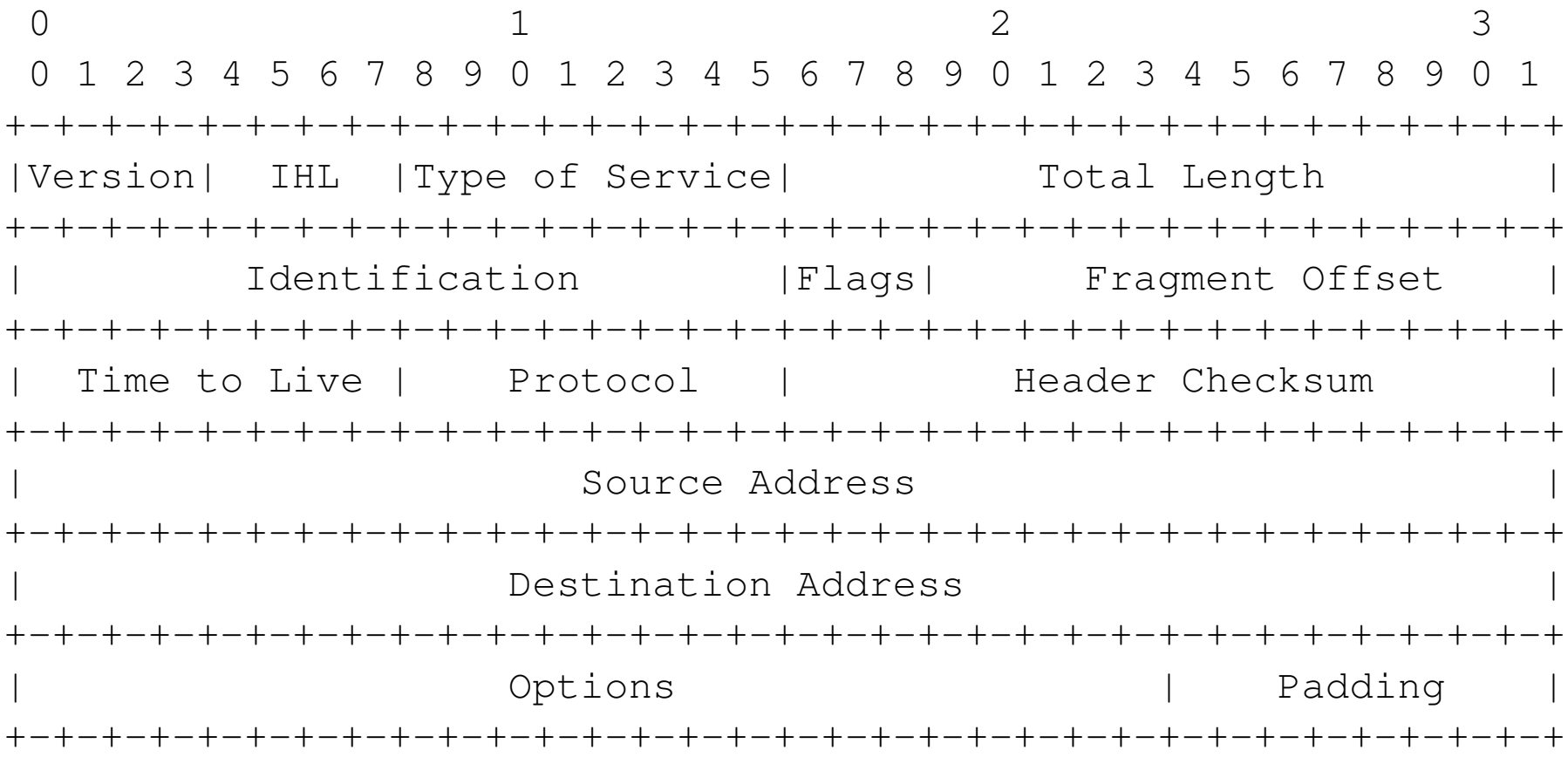
Der tales om data misbrug og data logning

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

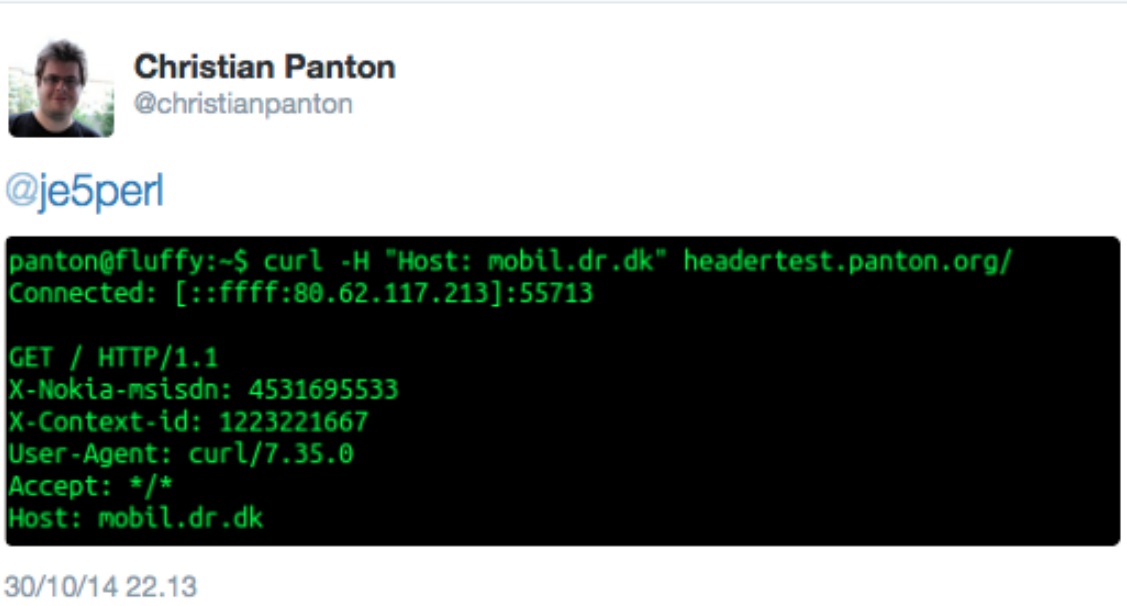
Lufthavns wifi

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

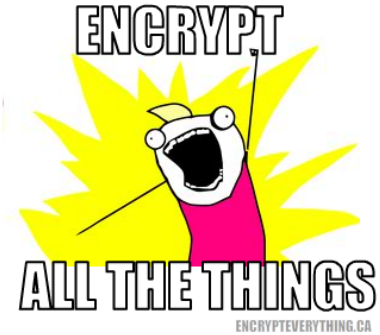
Telefonnumre



- Christian Panton 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

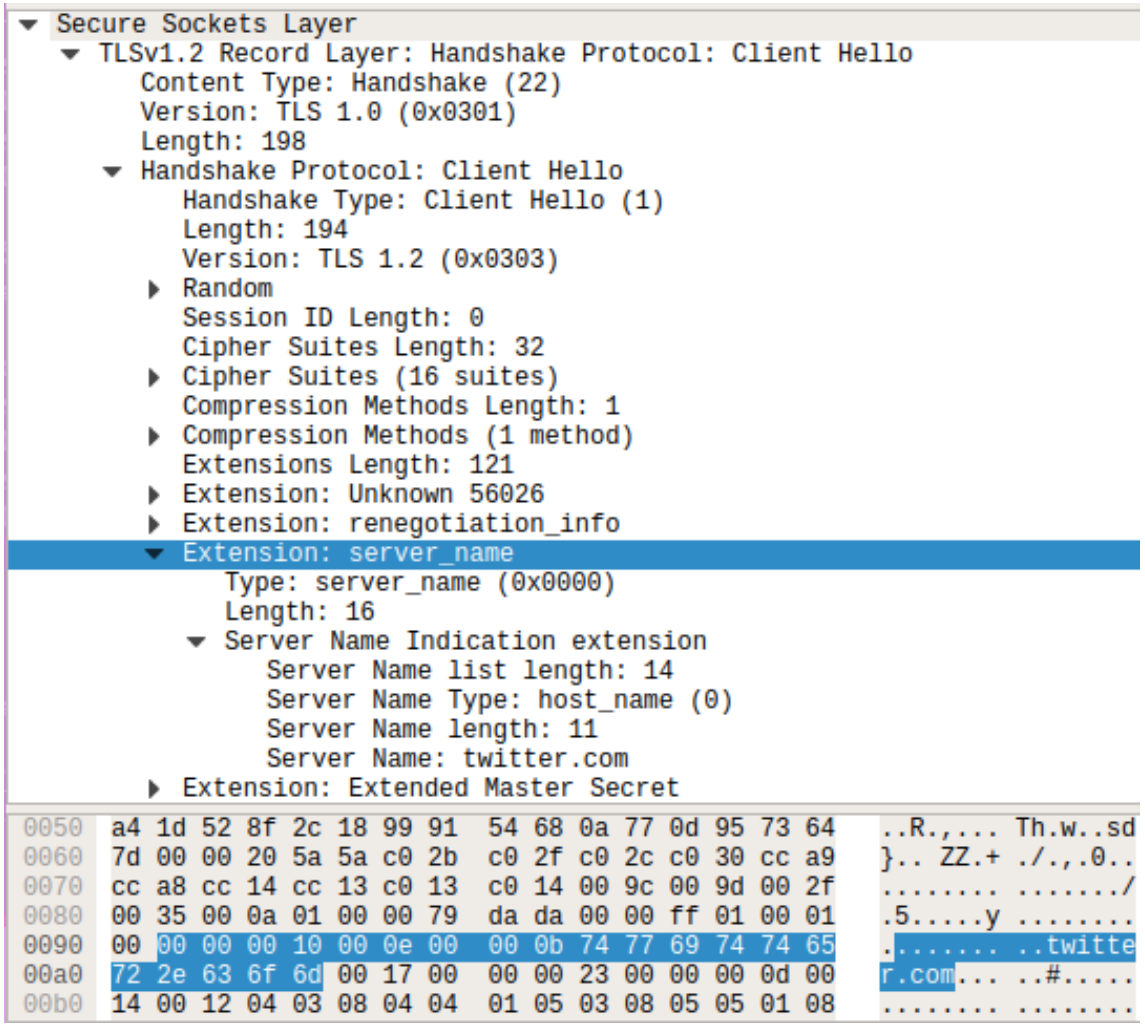
HTTPS skal der til!



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



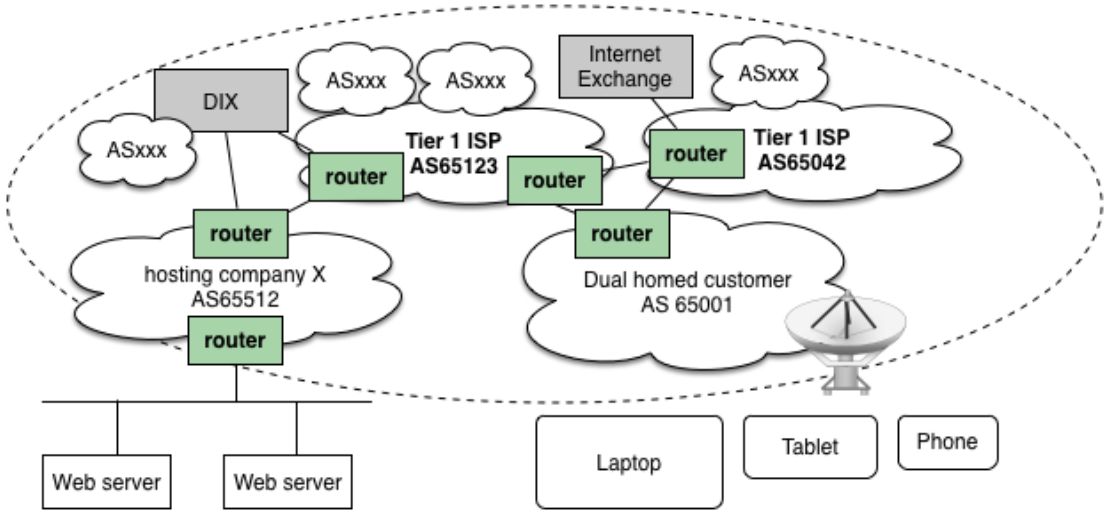
Metadata

- 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)

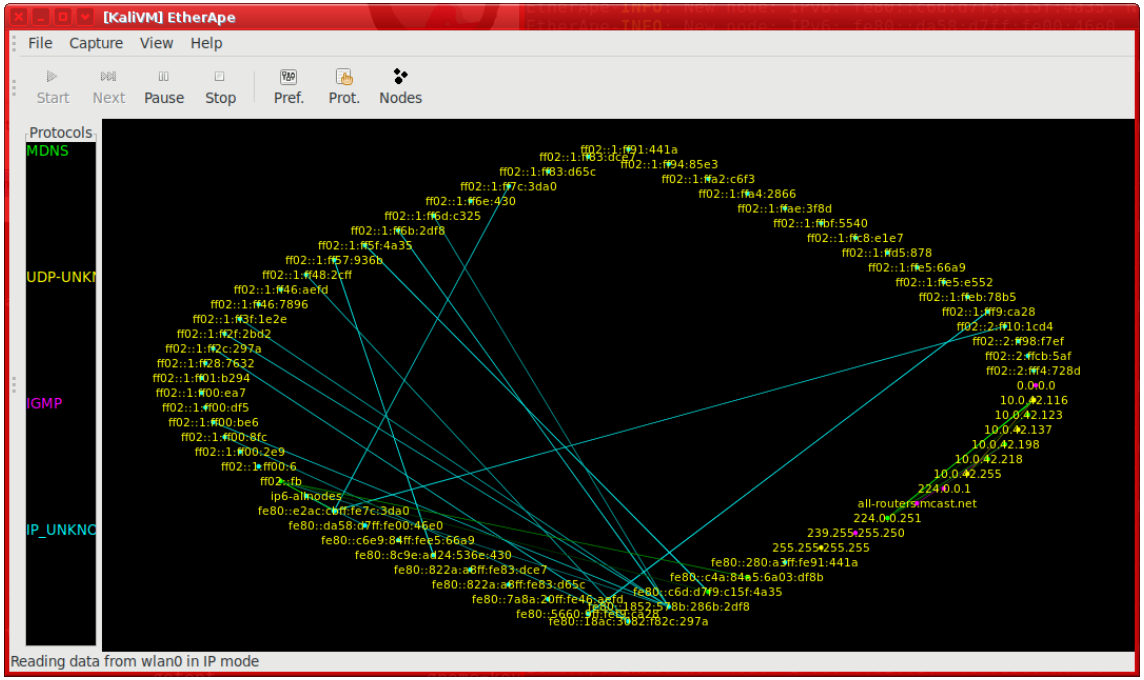
Hosting og internet-udbydere



- 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

"On the Internet, nobody knows you're a dog."

Henrik Lund Kramshøj hlk@zencurity.dk