Historikken til dokumentet

2017-04-25

Formål

Lære overfladisk om hvordan data “reiser” gjennom nettverk (Internett i dette tilfelle).
Gi mer mening til OSI-modellen.

Ofte, når man jobber med datasystemer, trenger man å sette seg inn i hvordan nettverk fungerer. Motivasjon kan være å diagnostisere og løse nettverks-kommunikasjonsproblemer, planlegge et nytt nettverksoppsett, gjennomføre optimalisering av nettverk eller å implementere og konfigurere applikasjoner som tilfredstiller grunnleggende sikkerhetskrav for en gitt kontekst.

Med mindre man jobber som systemadmistrator, er kanskje den mest nødvendige kunnskapen i dag relatert til datasikkerhet. Hvordan beskytte data fra å bli lest av andre (kryptering, AES128-GCM), hvordan beskytte systemer fra påloggінger i andres navn (digital signatur, RSA), hvordan utveksle hemmelige nøkler på en sikker måte (Diffie-Hellman) og hvordan sørge for at ingen endrer data på veien fra sender til mottaker (SHA256).

Lesestoff relevant for hele oppgavesettet:

Internet Protocol:
https://en.wikipedia.org/wiki/Internet_Protocol
https://en.wikipedia.org/wiki/IPv4#Packet_structure
https://en.wikipedia.org/wiki/IP_address

UDP (User Datagram Protocol):
https://en.wikipedia.org/wiki/User_Datagram_Protocol
https://en.wikipedia.org/wiki/QUIC

TCP (Transmission Control Protocol):
https://en.wikipedia.org/wiki/Transmission_Control_Protocol

Oppgave 1

Relevant lesestoff: http://www.minaandrawos.com/2016/05/14/udp-vs-tcp-in-golang/
Søk selv etter lesestoff med søkeuttrykk som “udp server client in golang” og lignende.

a) Lag en UDP klient og en UDP tjener
b) Send over “hemmelig” melding “Møte Fr 5.5 14:45 Flåklypa”
c) Studer kommunikasjon i Wireshark
    i) på det lokale grensesnittet (obs! windows brukere kan eventuelt droppe det)

1) Hvor mange prosent av data, som blir sendt over en nettverksforbindlese, er protokoll-data, dvs. data, som er nødvendig for å transportere meldingen fra bruker over nettverksforbindelsen?
2) Hvor stror kan en UDP pakke være? Begrunn.

ii) over NIC

1) Hvor mange prosent av data, som blir sendt over en nettverksforbindlese, er protokoll-data, dvs. data, som er nødvendig for å transportere meldingen fra bruker over nettverksforbindelsen?
2) Hvilken filter må du bruke for å filtrere ut relevante meldinger?
3) Hva er forskjell mellom data som ble sendt over NIC (ditt nettverkskort, mest sannsynlig trådløst) og de som ble sendt innenfor din lokale node? Illustrer gjerne med “screenshots” eller log-filer. Forklar.

Oppgave 2

a) Lag en TCP klient og en TCP tjener
b) Studer i Wireshark (vinduer og andre parametre)
   i) Hva er forskjellig fra UDP?
   ii) Hvor stor kan en TCP pakke være?
   iii) Hva er fragmentering, hvorfor oppstår det og hvordan håndterer man det?
   iv) I hvilke brukerscenarier bruker man UDP og i hvilke TCP?

Oppgave 3

Relevant lesestoff: https://golang.org/src/crypto/cipher/example_test.go,
https://golang.org/pkg/crypto/aes/
https://github.com/monnand/dhkx
https://github.com/wsddn/go-ecdh

Relevant AV-media:
https://www.oreilly.com/learning/https-is-coming-are-you-prepared?imm_mid=0f114b&cmp=em-webops-na-na-newsltr_20170421

a) Implementer kryptering for eksemplet fra Oppgavene 1 og 2
b) Implementer Diffie-Hellman (sikker nøkkelutveksling)
c) Eventuelt se på implementasjon av signatur og sjekk for dataintegritet (frivillig)

Oppgave 4 (frivillig)

“Å studere” betyr og finne ut hvilke protokoller som brukes i streaming av video fra forskjellige kilder.

a) Studer kommunikasjon med direkte TV fra NRK over NIC i Wireshark
b) Studer kommunikasjon med YouTube-video over NIC i Wireshark
c) Eventuelt studer kommunikasjon med et “online” spill

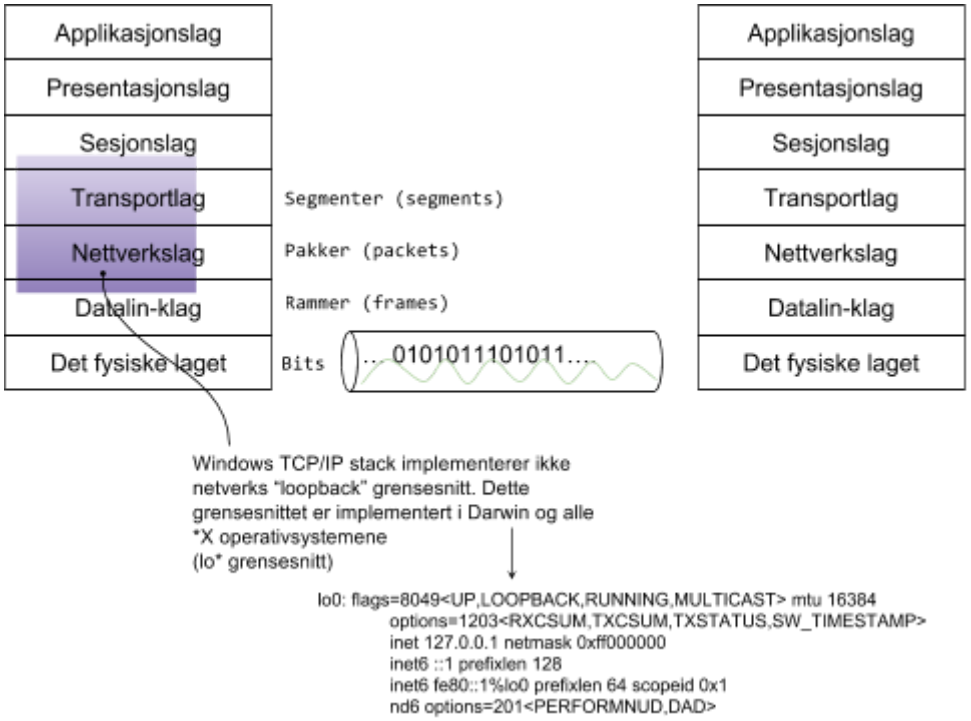
Tillegg

Wireshark prosjekter

http://www.ece.rutgers.edu/~marsic/books/CN/projects/

Wireshark i Windows

https://www.wireshark.org/
For loopback grensesnittet:
http://www.netresec.com/?page=RawCap



Phishing

https://www.xudongz.com/blog/2017/idn-phishing/

Lykke til!

SLUTT.
JG/2017-04