Lektion 22

Onsdag d. 19. april 2023

Læsestof til denne lektion:

[Kurose og Ross] 8.6 og 8.9

Emner

Netværkssikkerhed

- Grundig genopfriskning af det, vi havde sidst
- TLS (SSL version 3)
- Firewalls og IDS-systemer

Sikkerhed i netbanker og NEMID

Pensumsoversigt

Opgaver:

Opgave 28 og opgave 29

Læsestof til næste lektion:

Overheads om Web-sikkerhed

Bemærkninger:

Opgave 28

Denne opgave handler om de vigtigste begreber fra sidste gang

1. Der er typisk fire ting, man gerne vil opnå med netsikkerhed – nævn de fire ting.
2. Hvilken af de fire ting vil en god kryptering sikre?
3. Hvad er den væsentligste fordel og den væsentligste ulemper ved symmetrisk kryptering?
4. Hvad er den væsentligste fordel og den væsentligste ulemper ved public key kryptering?
5. Hvilken nøgle bruges når man vil kryptere med public key kryptering?
6. Hvilken nøgle bruges når man vil dekryptere med public key kryptering?
7. Hvordan kan man sikre message integritet?
8. Hvad er forskellen på de hash-funktioner man bruger til at opdage transmissionsfejl og de hash-funktioner, der anvendes til message integritet?
9. Hvad sikrer en digital signatur?
10. Hvad bruger man når man laver en digital signatur?
11. Hvad er et CA og hvad gør det godt for?
12. Hvad er et certifikat?
13. Hvad er replaying og hvordan er det farligt?
14. Hvordan kan man sikre mod replaying?

Opgave 29

Denne opgave er en meget kort repetitionsopgave i netsikkerhed.

Du skal binde nedenstående tal sammen med nedenstående bogstaver.

1. Fortrolighed
2. Beskedsintegritet .
3. Digital signatur
4. Certifikation Authority
5. Autentifikation
6. TLS

A. TDC er et eksempel på dette
B. Kan sikres alene med kryptering
C. I dette begreb indgår både at teksten ikke er ændret og man ved hvem, der har signeret det.
D. Fortrolighed og beskedsintegritet sikres af denne mekanisme
E. SHA 1 og MD5 er teknikker, der ofte anvendes til at sikre dette
F. Skal sikre at man kan stole på hvem der har en bestemt public key
G. Findes tit omtalt både som client- og server-.
H. Begrebet dækker at man ved, hvem det er man kommunikerer med
I. Den service, der anvendes af HTTPS