Examen: concepten uitleggen is belangrijk bv: wat is steganografie, wat is caesar 7

Figuur van DES uitleggen

Hybride cryptografie

belangrijkste schema van het vak

kunnen tekenen & uitleggen op het examen

bijna alles van veilige combinatie op het internet is op deze techniek gebaseerd

grote file door snel algoritme (dus DES)

de DES key is klein bestand dus traag algoritme (RSA)

des key encrypteren met public key van ontvanger (zodat alleen hij het kan openen)

van groot origineel bestand maken we een hash (MD-5)

hash is klein bestand dus traag algoritme (RSA)

hash encrypteren met private key van verstuurder

ontvanger is enige die de DES key kan decrypteren, dus je bent zeker dat alleen hij het kan decrypteren

de hash kan enkel ontsleuteld worden met de public van de verstuurder, dus je bent zeker dat enkel de verstuurder het verzonden kan hebben (= digitale handtekening)

Mogelijke examenvraag: geef de 4 belangrijke categorieen van public key crypto en leg uit

Mogelijke hoofdvraag op examen: securing van het e-mail verkeer

Wat is het principe van veilig e-mail verkeer: = hybride cryptografie

* PGP = hybride cryptografie met een certificaat gesigneerd via Web Of Trust
* S/Mine = hybride cryptografie met een certificaat uitgeleverd door een CA
* Certificaat was nodig om security flaw van hybride op te lossen: public key linken aan een ID
* Geldigheid certificaat controleren via OCSP

Leg uit wat een CA is, vergeet beleidsdocumenten niet uit te leggen (CP, CPT)

Zkeer kunnen uitleggen op het examen, de 2 beveiligingssystemen (van e-mails)

Belangrijk:

De handshake + figuur kunnen uitleggen (figuur = slide 27) Je krijgt de pijlen, uitleg moet je invullen (op examen)

De 3 protocollen: SSL alert protocol, Change Cipher Spec, SSL handshake

Mogelijke bijvraag op examen: wat is een replay attack

Belangrijk voor examen: VPN’s worden via Ipsec gemaakt

Belangrijk: promiscous mode & selectief

Mogelijke vraag: wat is ARP poisoning

Te kennen voor examen

Syn-flooding

Smurf attack

Ping of death

Verschillende manieren om webserver plat te krijgen

DDOS: Distributed Denial of Service

Belangrijk voor examen:

Same Origin principe kunnen uitleggen

Mogelijke bijvraag: webbugs: 1x1 transparante img op een site (met een href) voor tracking