Security+

Teacher : Fallahzadeh

Link : https://www.youtube.com/watch?v=geDkUSjfKu0&list=PL-mrTgDRWNRU3YALjzV_cruqYKyhDDfEB

Date : 1404/05/31

دیتا میتونه به دو شکل باشه :

Public.1

Private.2

اضافه کردن امنیت به اطلاعاتی که داریم information Security نامیده میشه

Security triangle —> CIA

Confidentiality.1 : محرمانگی اطلاعات یا دیتا

Data should not sniff

Data should encrypt

دو مدل رمزنگاری داریم:

same key : sym ALG.1

public key and private key <--- key pair : Asym ALG.2

دیتایی که رمز نشده میگن Clear Text

به اطلاعات رمز شده Cipher میگن

SYM Encryption ALG: دیتا توسط مبدا با یک کلید رمزنگاری میشه و دیتا در مقصد با همون کلید رمزگشایی میشه

DES,3DES,AES مدل هایی از این رمزنگاری هستند

DES=56bit, 3DES=168bit, AES=256bit

ASym Encryption ALG: هر نودی public key خودش رو در اختیار بقیه میزاره تا با اون دیتا رو رمزنگاری کنن و سپس دیتارو با private key خودش باز میکنه.

یه مرجع باید برای تایید نودها باشن چون ما نمیدونیم public key مال کیه

PKI: Public Key Infrastructure <-- CA <-- Certificate Authority

هر نودی میاد اطلاعات خودش رو که باید توی cert قرار بگیره واسه CA میفرسته (به این عمل که درخواست cert هست Certificate Enrollment میگن) CA میاد cert رو با public key خودش امضا میزنه و نود دریافت کننده امضای CA رو داره پس میگه این cert معتبره بعد میاد با public key ارسال کننده دیتارو رمزنگاری میکنه. مثل:

RSA, Diffie Hellman

Integrity.2 : صحت دیتا، یعنی کسی دیتارو تغییر نداده باشه.

Malware : بدافزارها

هکر میاد اون بدافزار رو اضافه میکنه به یه سری فایل دیگه مثل پی دی اف ها و.. برای گرفتن دسترسی از قربانی

Hash کردن دیتارو رمزنگاری نمیکنه، hash اون فایل به مقصد داده میشه و گفته میشه پس از دریافت دیتارو دوباره hash کنه و خروجی رو با خروجی که بهش داده شده مقایسه کنه
hash یک طرفه هستش یعنی نمیتونیم از هش اون دیتا به خود دیتا برسیم. الگوریتم هایی مثل MD5, SHA