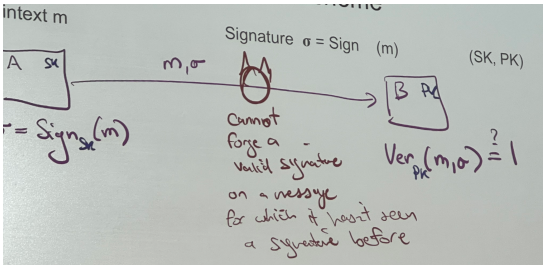
CAS CS 357

InClass Note 13

1. Asymmetric cryptography aka public key crypto
    a. Alice has key pair (Sk, Pk)
    b. PK is Alice's public key; everyone (including adversary) knows Pk
    c. Public key algorithm generates a public key and a secret key
    d. SK is Alice's secret key. Only Alice knows SK
    e. Having knowledge about the public key refers nothing regarding the secret key
    f. Even dictionary attack will not be helpful due to the randomness of the characters
    g. Ex) RSA → 1024 or 2048 bit secret keys, ECDSA → 512 bits secret key
2. Defining a digital signature scheme
    a. 

    b. Plaintext m Signature o = Sign (m) (SK, PK)

       Alice generates a message with the secret key

       Receiver check whether the verification of message and the sign equals 1 by using the public key
    c. Guarantees that the man in the middle cannot forge valid signature on a message for which it hasn't seen a signature before
    d. Correctness: (Ver (m, Sign (m)) = 1 [A validly signed message verifies correctly]

e. Security: The adversary cannot forge the signature without SK

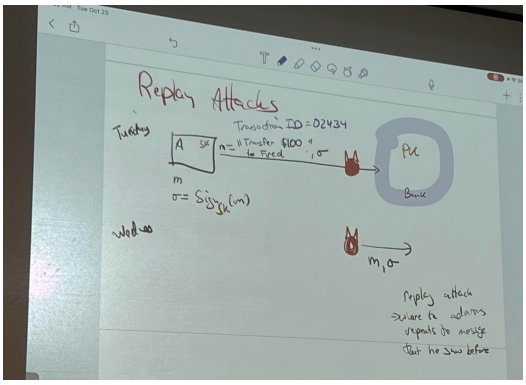
3. Replay attacks

   a. Alice sends a message to a bank where m = “Transfer $100 to Person C”

   b. Alice signs the message with the secret key

   c. The adversary, for example the next day, sends the same message “Transfer $100 to Person C” to the bank

   d. Replay attack → where the adversary repeats the message that he saw before (Nothing that stops from sending the message over and over again)

   e. 

   f. If the message included the transaction ID and the bank deletes the repetition of transaction ID before transferring the money, we can prevent such happening

   g. Other types of replay protection: timestamp, transaction ID, Sequence numbers

4. Application of signatures: code signing with well-known signer

   a. Me (owns windows laptop) Microsoft (developer of windows operating system)

   I own a microsoft account

   Know the public key of microsoft Microsoft has a secret key

   There exist a software update that exist in microsoft

   The code is c, the time is t, and the signature o is sent to the users

   $O = sign_{SK}(c,t)$

$Ver_{PK}(c||t,o) = 0$ or 1

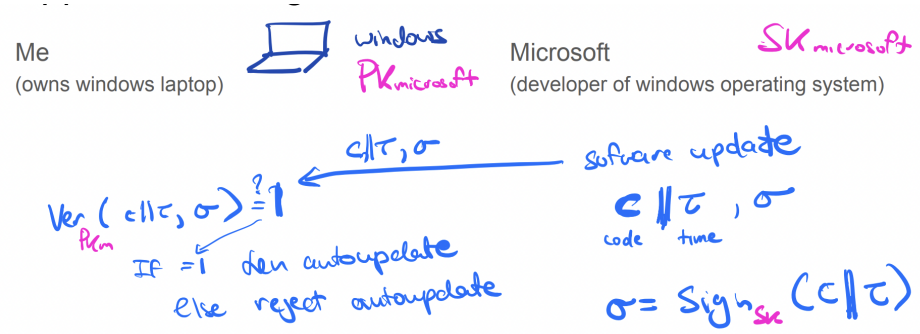
If 1, autoupdate

If 0, reject the autoupdate

b. Public key is baked into the laptop (Trust on First Use (TOFU): security arrangement that pertains to when a device is connecting to a server it has not before, one for which no earlier trust relationship exists)

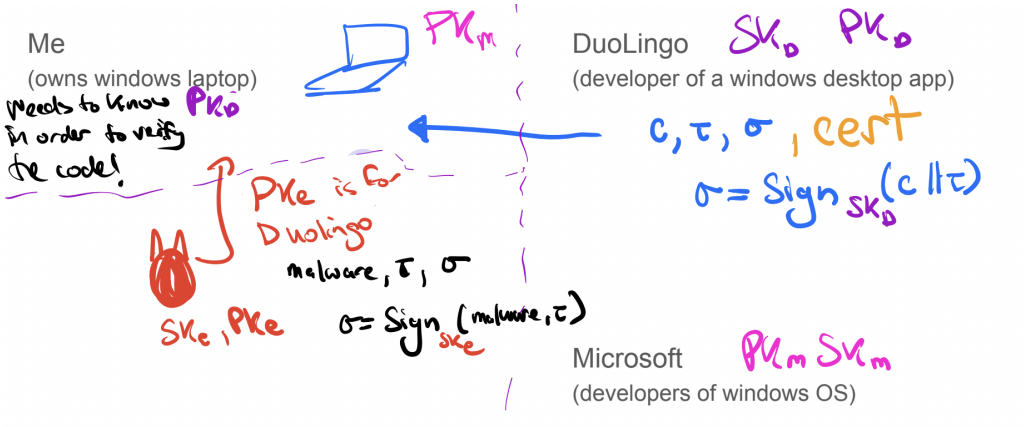
c. This example is assuming that the security of your computer is secure when purchasing the items from Microsoft

d. Without the timestamp within the signature, adversary can take an old piece of the code that was signed previously and replace it with the current code(reinforces the notion that everything has to be signed within the code)



e.

5. Application of signatures: Code signing, signer unknown

a. 

b. We need to somehow know that we are downloading the correct DuoLingo

c. Me (owns windows laptop)

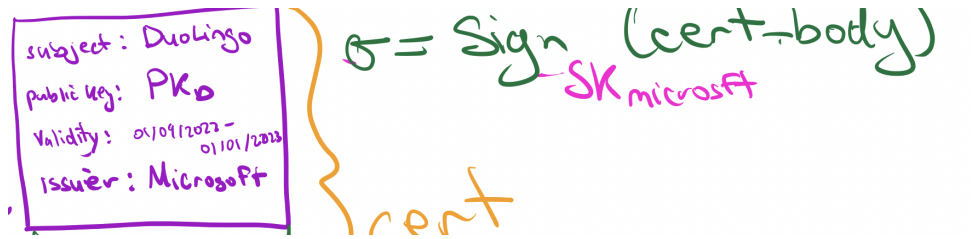
- Has the public key of microsoft (PK_m)
- In order to verify the signature, we need to know the public key of DuoLingo
- Gets the public key of DuoLingo (you have to get the right public key from DuoLingo, not from an adversary)
- Problem: which key belongs to which identity (we can get completed valid message but from a completely wrong person)
- We must bind the public key to the current identity
- How? We use certificates (if we trust microsoft because we know the key, microsoft can validify DuoLingo for us)

d. DuoLingo

- Has its own Secret key and Public Key (SK_D, PK_D)
- Has c, t, o, where o = $Sign_{SK_D}(c||t)$
- Has cert (code signing certificate)

e. Microsoft

- Has its own Secret key and Public Key (PK_m, SK_m)

6. Certificate from the example above (DuoLingo)
   a. 

   b. Certificate:

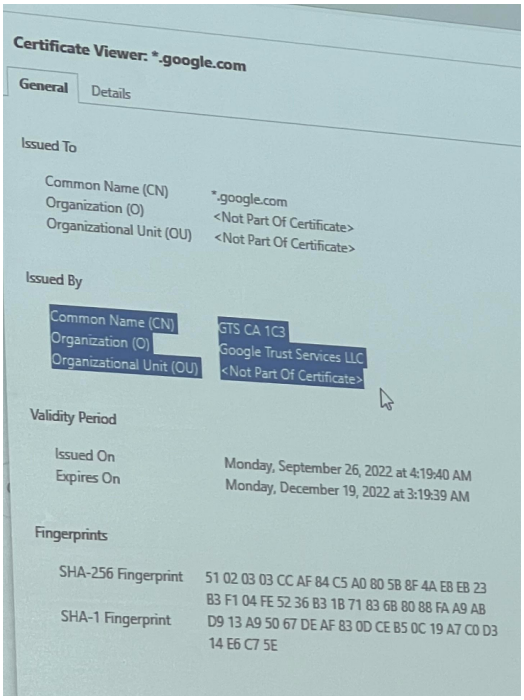
      Subject: DuoLingo

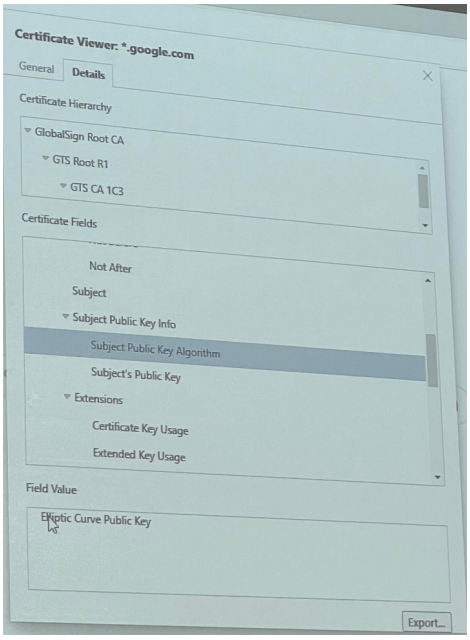
      Public key: PKD

      Validity: 01/09/2022 - 01/10/2022

      Issuer: Microsoft

   c. The information above should be protected (needs integrity)
   d. Microsoft needs to sign the information so that adversary cannot modify the information
   e. $O = Sign_{SKmicrosoft}(certificate)$
   f. DuoLingo includes the cert(code signing certificate) – this signature can be verified the public key and is approved by microsoft
   g. As long as microsoft secret key is not forged, then we have integrity of the code
7. Certificate examples

a. 

b. 

c. Issued To: who is the certificate for (DuoLingo)

d. Issued By: Entity issuing the certificate (Microsoft)