Computer Security

Reagan Shirk

October 1, 2020

MAC/MIC

- Message authentication/integrity code
- Not taking notes on what he's talking about rn because I don't know the context but I'll come back and figure it out

Message Authentication Codes

- MAC
- Has requirements but he's moving pretty quickly so I'll have to come back for this too

Attempt #1 - Does this work or not?

- Compute residue using Key k
- Attach MAC to the plaintext P
- Encrypt the concatenated quantity P | MAC using the same key K to produce C
- Transmit C to receiver
- Receiver decrypts received C' with K to get P' | MAC'
- Receiver computers MAC(P') using K and compares to received MAC'
- A better explination (I think?)
  - You have $M_1,\ M_2,\ M_3,\ M_4$
  - You create Residue R using MAC
  - Your ciphertext $C = E(M_1||M_2||M_3||M_4||R)$
    - E = encrypt
  - C goes to Bob
  - I don't entirely get how he said decryption works
  - Probably important to mention that the encryption is CBC, I think he said DES-CBC but I'm not sure
- Residue will always be the last block of ciphertext
- Need something stricter to guarantee security

Attempt #2

- I missed the details, but the gyst: good cryptographic quality but it's too expensive. Requires two separate, full encryptions with different keys

Attempt #3

- Sender computers an **error detection code** $F(P)$ of plaintext P
- Sender concatenates P and $F(P)$ and encrypts it, $C = E(P|F(P))$
- You need a long CRC, whatever the fuck that is

Secret Key Cryptography Summary

- Last lecture on secret key cryptography
- ECB is not secure
  - CBC is most commonly used mode of operation
- Triple-DES (with 2 keys) is much stronger than normal DES
  - Usually uses EDE in outer chaining mode
- MACs use crypto to authenticate messages at a small cost of additional storage/bandwidth, but this has a high computational cost