Computer Security

Reagan Shirk

September 29, 2020

Padding

- How to pad may appear on our exam
- 14 pad 0e. . . ?
- 11 bytes, need 16, pad 05

Triple DES

Meet in the Middle Attack

- Choose a plaintext P and generate ciphertext C using double DES with $K_1 + K_2$
- Encrypt P using single DES for all possible 2^{56} K_1 values to generate all possible single DES ciphertexts for P
- Decrypt C using single DES for all possible 2^{56} K_2 values to generate all possible single DES plaintexts for C
- For each value, check the table
- He be blowing through these slides now, I'll come back to these later

Attack Complexity

- How many DES encryptions and decryptions are needed for the attacker to compute? $2 \times 2^{56} + 2 \times 2^{48}$
- It's an expensive attack in terms of computation and storage but is still enough of a threat to discourage double DES

Triple Encryption (DES-EDE)

- You can use $k_1 = k_3$, using three unique keys doesn't increase security
- Why apply DES thrice?
  - Taking $k_1 = k_2 =$ key, Triple DES becomes a single DES with key; Triple DES communicates with single DES
- Bummer because this is inefficient and expensive
  - One third as fast as DES and DES is already slow af
- How is block chaining used in DES?
  - Very similar to CBC

MAC/MIC

- Message authentication/integrity code
- Easily provides confidentiality of messages, only the "key partner" (the party sharing the key) can decrypt the ciphertext
- How can we use encryption to authenticate messages and verify integrity?

  - prove the message was created by the key partner and not modified by anyone else

Integrity

- Approach 1: if the decrypted text "looks plausible", then it was probably produced by the key partner
  - Modified ciphertext or ciphertext encrypted with the wrong key will decrypt to some random ass shit
- Approach 2: sending the plaintext and ciphertext to verify the integrity of the message upon decryption
  - Why tf would you bother sending a ciphertext if you're just going to send the plaintext with it