Computer Security

Reagan Shirk

September 15, 2020

Feistel Cipher

- Why is this important? Fundamental block for a lot of modern ciphers like DES
  - AES is **not** a feistel cipher
    - He's said this three times, **we will be asked this on the midterm**
- What makes feistel cipher so cool? Encryption and decryption take the same amount of time
  - How is this possible? Decryption is just the reverse of encryption
- You can do multiple rounds of feistel ciphers
  - In the **last round** of encryption, you swap the two halves of the output block

DES

- Type of feistel cipher
- Not secure *anymore*, was fine back in the late 70s
- Official criteria:
  - missed it because I needed my laptop charger but I'll go back and check it
- Hard to implement in software, easy in hardware
  - This is because we don't have an operation for permutation

DES Basics

- The plaintext input and ciphertext output are both 64 bits
- Every 8^{th} bit of they key is a parity bit, so the key size really 56 bits long
  - just want to make sure you know why some people say 64 and others say 56
- There are 16 rounds
- Initial and Final Permutations of plaintext/ciphertext:
  - Initial permutation outline is: input bit 58 turns into output bit 1, input bit 50 turns into output bit 2...
  - The initial permutation is fully specified, independent of the key, which means it doesn't improve security
  - If it doesn't improve security, why do we need it?
    - didn't catch the answer I was buying my halloween costume...
    - Someone in the groupme said: Shuffling bits around like you'd need for the permutation is hard to do in software, CPUs don't have an operation for moving bits around like that, you'd have to do it bit by bit. It's easy to do in hardware though, you just cross the wires in the right pattern.
  - Why is the final permutation needed?
    - we want to make it a feistel cipher so the decryption is the reverse of the encryption
- Initial and Final Permutations of key:
  - I got distracted again... oops
  - There's something significant about 48... the output key is 48 bits?
- I'm so zoned out today, I'll watch the recording (if he uploads them?) and look back over the slides to buff out my notes sorry fam
- We will be asked about S-Box, part of the Mangler Function for DES
- Substitution part of DES is important as well, we will be asked about it

DES Operations

- Permutation
- Swapping Halves
- Substitution (S-box, table lookup)
- Bit discard
- Bit replication
- Circular Shift
- XOR

S-Box

- Very important
- Only non-linear part of DES
- Each row should be a permutation of the possible output values
- Output of one S-box should affect other S-boxes in the following rounds

Desirable Property: Avalanche Effect

- A small change in the plaintext will cause a big change in the ciphertext
- It would be better to have an output where any bit should be flipped with a probability of 0.5 if any input bit is changed
  - I'm interpreting this as there's a 50/50 chance of the output changing if an input bit changes, someone please correct me

DES Keys to Avoid

- Weak keys are keys which, after the first permutation are:
  - All 0's
  - All 1's
  - Half 0 and half 1
  - Half 1 and half 0
- Weak keys are susceptible to brute force attacks, have 16 identical subkeys, and encrypting twice returns the original plaintext

AES

- Not feistel cipher
- Selected from an open competition that was organized by the NSA
- Shares similar properties to DES
- Block size is 128, 192, or 256 bits
- Key sizes are 128 for 10 rounds, 192 for 12 rounds, or 256 for 14 rounds