CS 558: Network Security (2/2)

Defining encryption scheme security

Last Lecture

- encryption schemes
  - one time pad (1-bit encryption)
  - AES-CBC mode (arbitrary length message encryption)
- possible attacks (most to least difficult for adversary)
  - key recovery (adversary obtains secret key)
  - recovery of plaintext (adversary obtains plaintext)
  - distinguishing attack (adversary can pick between two messages given the corresponding ciphertext)
- defend against the *easier* attack to ensure protection against harder ones

More Attacks (most to least difficult)

- know ciphertext attack (KCA): attacker able to observe ciphertexts (network snooping, etc)
- known plaintext attack (KPA): attacker able to observe plaintext and ciphertext pairs
- chosen plaintext attack (CPA): attacker can choose plaintext input and can see ciphertext output
- *note* m0 and m1 may be queried during the learning phase of an attack! e.g. CPA will be possible if the same message produces the same ciphertext if encrypted multiple times - recall penguin picture encryption under electronic codebook mode (ECB)
- this is why in CBC mode we XOR the random IV and then the next

ciphertext in block ciphers (to make sure the same message will look different)

Realworld Attack Example

- laptop <--- encryption ---> google
- adversary can see encrypted traffic
- adversary can also inject an ad
- this allows the attacker to know part of the plain text (the ad) and also the ciphertext (the encrypted traffic)
- now attacker can do a chosen plaintext attack (CPA)

Chosen Ciphertext Attack (CCA) - even easier attack

- adversary can obtain for ciphertext from plaintext (like CPA)
- adversary can *also* obtain plaintext from ciphertext (reverse direction)
- however, *cannot* obtain the plaintext for c* (the specific ciphertext of the target)

Order of difficulty for adversary (most to least difficult) (e.g. lower to higher tiers of security if protected)

- KCA
- KPA
- CPA
- CCA

AES

- if AES is a secure PRP, then AES-CBC and AES-CTR are CPA secure (but not CCA)

- in order to be CCA secure, we need *integrity* (preventing attacker from modification of the message/ciphertext)
- malleability: altering the ciphertext still produces valid plaintext upon decryption
- AES CBC and CTR *are* malleable, so we need something more...