CSE 484 / CSE M 584: Computer Security and Privacy

Cryptography
[Symmetric Encryption]

Spring 2019

Franziska (Franzi) Roesner
franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
Reminder: Block Ciphers

- Operates on a single chunk ("block") of plaintext
  - For example, 64 bits for DES, 128 bits for AES
  - Each key defines a different permutation of possible outputs
  - Same key is reused for each block (can use short keys)
Electronic Code Book (ECB) Mode

- Identical blocks of plaintext produce identical blocks of ciphertext
- No integrity checks: can mix and match blocks
Information Leakage in ECB Mode

[Wikipedia]
Cipher Block Chaining (CBC) Mode: Encryption

- Identical blocks of plaintext encrypted differently
- Last cipher block depends on entire plaintext
  - Still does not guarantee integrity
CBC Mode: Decryption

Initialization vector

plaintext

ciphertext

decrypt

decrypt

decrypt

decrypt

key

key

key

key
ECB vs. CBC

AES in ECB mode

Similar plaintext blocks produce similar ciphertext blocks (not good!)

AES in CBC mode

[Picture due to Bart Preneel]
Initialization Vector Dangers

Found in the source code for Diebold voting machines:

```
DesCBCEncrypt((des_c_block*)tmp, (des_c_block*)record.m_Data, totalSize, DESKEY, NULL, DES_ENCRYPT)
```
Counter Mode (CTR): Encryption

Initial ctr (random) → ctr → ctr+1 → ctr+2 → ctr+3

- block cipher
- block cipher
- block cipher
- block cipher

pt → + → pt → + → pt → + → pt → + → ciphertext

• Identical blocks of plaintext encrypted differently
• Still does not guarantee integrity; Fragile if ctr repeats
Counter Mode (CTR): Decryption

Initial ctr

ct

ctr

ctr+1

ctr+2

ctr+3

block cipher

Key

Key

Key

Key

ct

ct

ct

ct

ct

pt

pt

pt

pt
When is an Encryption Scheme “Secure”? 

• Hard to recover the key?
  – What if attacker can learn plaintext without learning the key?

• Hard to recover plaintext from ciphertext?
  – What if attacker learns some bits or some function of bits?
How Can a Cipher Be Attacked?

• Attackers knows ciphertext and encryption algthm
  – What else does the attacker know? Depends on the application in which the cipher is used!

• Ciphertext-only attack

• KPA: Known-plaintext attack (stronger)
  – Knows some plaintext-ciphertext pairs

• CPA: Chosen-plaintext attack (even stronger)
  – Can obtain ciphertext for any plaintext of his choice

• CCA: Chosen-ciphertext attack (very strong)
  – Can decrypt any ciphertext except the target
Chosen Plaintext Attack

Crook #1 changes his PIN to a number of his choice

PIN is encrypted and transmitted to bank

cipher(key,PIN)

Crook #2 eavesdrops on the wire and learns ciphertext corresponding to chosen plaintext PIN

... repeat for any PIN value
Very Informal Intuition

• Security against chosen-plaintext attack (CPA)
  – Ciphertext leaks no information about the plaintext
  – Even if the attacker correctly guesses the plaintext, he cannot verify his guess
  – Every ciphertext is unique, encrypting same message twice produces completely different ciphertexts
    • Implication: encryption must be randomized or stateful

• Security against chosen-ciphertext attack (CCA)
  – Integrity protection – it is not possible to change the plaintext by modifying the ciphertext
So Far: Achieving Privacy

Encryption schemes: A tool for protecting privacy.
Now: Achieving Integrity

Message authentication schemes: A tool for protecting integrity.

Integrity and authentication: only someone who knows KEY can compute correct MAC for a given message.