SYMMETRIC-KEY CRYPTOGRAPHY

NOTICES

- Lab #2 servers now available
- Start those dictionary attacks early! If your search has been going for ~4 days or more, let me (or a TA) know and you might get a hint
- In the meantime, teach yourself to smash stacks!
- It takes a lot of work to pull off a buffer overflow attack successfully!
- Homework #2 due 23:59 Jan 31st

SYMMETRIC-KEY CRYPTOGRAPHY

LAST TIME: WEB SECURITY

- Formats and protocols
  - HTTP/ HTML / CSS / Javascript
  - Cookies
- Web security goals / policies
  - Same Origin Policy
  - Attacks and Defenses
- SQL Injection / Code injection
- Cross Site Request Forgery (CSRF)
- Cross Site Scripting (XSS)

TODAY

- Introduction to cryptography
- Definitions and goals
- Historic Symmetric-Key Encryption
  - Caesar Cipher
  - One-Time Pad
- Modern Symmetric-Key Encryption
  - Block Ciphers

WHAT IS CRYPTOGRAPHY?

- Cryptography is the study and practice of secure communication over insecure channels
- A channel is any medium of communication: written messages, network protocols, digitally stored files, electromagnetic signals, sound, etc.
- A channel generally has a sender and an intended recipient (or recipients), but may also be observed by an adversary

CRYPTOGRAPHY GOALS

- Confidentiality
  - Prevent adversaries from reading data
- Integrity
  - Prevent attackers from altering data
- Authentication
  - Determining who created a given message
EVE'S POWER (PASSIVE ATTACKERS)

1. Cipher text only
   - Eve sees every cipher text $C_i$
   - Variant: partial knowledge about $M$
   - Language, or space of possible words (yes/no, true/false, buy/sell)

2. Known plaintext
   - Eve knows part of $M$, and has (complete) previous messages
   - Known protocol: HTTP request will start with GET
   - Known patterns in previous messages: "Dear Bob," or "Date: 1/3/2019"

THE CRYPTO GAME

- Attacker's goal:
  - Gain any knowledge about $M$, beyond an upper bound on length
  - Even slightly better than 50% probability at guessing 1 bit => attacker wins

- Defender's goal:
  - Ensure attacker has no basis to think any other (for $M$ beyond of length $n$)

Confidentiality
- Prevent adversaries from reading data

Integrity
- Prevent attackers from altering data

Authentication
- Determining who created a given message

SYMMETRIC-KEY CRYPTOGRAPHY
- EVE'S POWER
- No knowledge of $K$:
  - Assume $K$ is selected by a truly random process
  - For $b$-bit key, any $K \in \{0,1\}^b$ is equally likely
  - Success is recognizable:
    - Eve can recognize a fully recovered message $M$
    - But not a partial solution, such as whether a particular bit in $M$ was correct
    - Doesn't apply if Eve can examine all possible messages in $\{0,1\}^n$ (why?)
**CIPHER DESIGN**

- **Caesar cipher**: rotate each letter in M by K places in the alphabet
  
  \[ E(M, K) = \text{ROT}_K(M) \]
  
  \[ D(C, K) = \text{ROT}_K^{-1}(C) \]
  
  Examples:
  
  - \( E(\text{DOG}, 3) = \text{GRJ} \)
  
  - \( D(\text{GRJ}, 3) = \text{DOG} \)

**CHOSEN PLAINTEXT ATTACK SECURITY (IND-CPA)**

- **Chosen plaintext**
  
  - Eve gets Alice to send \( M \) of Eve’s choosing
  
  - Example: In WWII, Allies would plant mines to induce German ships to send “warning” and “all clear” messages with the location of the mines.

**INDISTINGUISHABILITY GAMES**

**CHOSEN CIPHERTEXT ATTACK SECURITY (IND-CCA1/CCA2)**

- **Ciphertext chosen**
  
  - Eve tricks Bob into decrypting some \( C_i \)’s of her choice and he reveals something about the result
  
  - Example: A webserver that responds with different-sized messages depending on whether ciphertext decrypts to a valid message or not

**ATTACKING THE CAESAR CIPHER**

- **Possibly effective in 50 BC, but not many people could even read back then.**

- **Brute force**: try every possible value of \( K \)

- **Analysis**:
  
  - Analyze letter frequencies (most common is “e”)
  
  - Known plaintext: guess likely words (“JCKN ECGUCT” = “HAIL CAESAR”)
  
  - Chosen plaintext:
    
    - get a general to send “ALL QUIET”, observe “Y JJ OSGCR”, infer \( K = 24 \)
SYMMETRIC-KEY CRYPTOGRAPHY

KERCKHOFFS'S PRINCIPLE
- Cryptosystems should remain secure even when an attacker knows all internal details
  - OR: Don’t rely on security by obscurity
  - Key should be the only thing that must stay secret
  - It should be easy to change the key

Find K!

SYMMETRIC-KEY CRYPTOGRAPHY

ROT BETTER
- Consider $E(M,K) = \text{Rot-}(K_1, K_2, ..., K_n)(M)$
  - Rotate first character by $K_1$, second by $K_2$, up through $n$th character. Then start over with $K_1$
  - $K = (K_1, K_2, ..., K_n)$
  - How well do the previous attacks work now?
    - Brute force: key space is factor of $26^{(n-1)}$ bigger
    - Frequency analysis: need way more ciphertext
  - Known/Chosen plaintext: still effective! Why?

SYMMETRIC-KEY CRYPTOGRAPHY

ONE-TIME PAD
- Requirement 1: Use a different key for each message $M$
  - Keys must be completely independent
  - Defeats known plaintext, chosen plaintext – Why?
- Requirement 2: Make the key as long as $M$
  - $E(M,K) = M \oplus K$ ($\oplus$ = XOR)
  - $D(C,K) = C \oplus K = M \oplus K \oplus K = M \oplus 0 = M$

SYMMETRIC-KEY CRYPTOGRAPHY

ONE-TIME PAD: PROVABLY SECURE!
- Suppose Eve has some partial information about $M'$ and $M''$
- We want to show Eve does not gain any additional information given $C$
- Formalization
  - Alice sends either $C = M' \oplus K$ or $C = M'' \oplus K$
  - Eve tries to guess which one based on $C$
- Proof sketch
  - For random, independent $K$, probability that $C[i] = 0$ or $C[i] = 1$ is $\frac{1}{2}$ for all $i$. Regardless of whether Alice chose $M'$ or $M''$!
SYMMETRIC-KEY CRYPTOGRAPHY

ONE-TIME PAD: LIMITATIONS
▸ One-time pads are still used for some extremely sensitive communication but they have some drawbacks
▸ Key generation
   ▶ Generating truly random, independent keys at scale is challenging
▸ Key length
   ▶ Keys must be at least as long as the message sent
   ▶ Requires anticipating message sizes in advance
▸ Key distribution
   ▶ Sender and receiver must have matching pads

SYMMETRIC-KEY CRYPTOGRAPHY

TWO-TIME PAD?
▸ What if we reuse a key $K$ just one more time?
▸ Alice sends: $C = E(M, K)$ and $C' = E(M', K)$
▸ Eve observes $M \oplus K$ and $M' \oplus K$
   ▶ Can Eve learn anything about $M$ and/or $M'$?
▸ Eve computes:
   
   
   $$C \oplus C' = (M \oplus K) \oplus (M' \oplus K)$$
   
   $$= (M \oplus M') \oplus (K \oplus K) = (M \oplus M') \oplus 0$$
   
   $$= M \oplus M'$$

   Learns which bits match in $M$ and $M'$!
   
   If Eve knew $M$, she can recover $M'$!

SYMMETRIC-KEY CRYPTOGRAPHY

TWO-TIME PAD EXERCISE
▸ Two volunteers
   ▶ Flip a coin 4 times (write down the results on two pieces of paper)
   ▶ Go to separate sides of the room
   ▶ Pick a number between 0-15 and encrypt it
   ▶ “Send” the encrypted numbers
   ▶ Everyone else:
   ▶ What pairs of numbers are possible?

(OTHER SLIDE DECK)

SYMMETRIC-KEY CRYPTOGRAPHY

NEXT TIME
▸ Public Key Cryptography