Week 2 - Friday

COMP 4290

Last time

- What did we talk about last time?
- Biometrics
- Tokens
- Started access control

Questions?

Assignment 1

Project 1

Security tidbit of the day

- AI hiring bots are growing common
- To get a job at McDonald's, you might have to talk to their AI chatbot, Olivia
- Some white hat hackers discovered that the password for the Paradox.ai account that runs Olivia was … "123456"
  - (Not secure)
- They accessed a database containing as many as 64 million chat records, many of which contained personal data
- Follow the story:
  - https://www.wired.com/story/mcdonalds-ai-hiring-chat-bot-paradoxai/

Back to Access Control

Extended Unix example

- Unix has users, groups, and processes
- A user has a unique UID
- A group has a unique GID
- A process has a unique PID
- Each user can belong to many groups
- Access is controlled on:
  - Files
  - Directories

File permissions

- Reading
- Writing
- Executing
- Ownership is also important

Directory permissions

- Reading
- Execution allows moving through the directory
- Writing and executing are needed to create and delete files in a directory
- There is also a "sticky bit" for directories
  - If the sticky bit is set, only the directory owner can rename, move, or delete files owned by other people

Permission example

```
drwxr-xr-x
```

- **First character:** directory or not
- **Next three characters:** owner permissions
- **Next three characters:** group permissions
- **Next three characters:** other permissions

chmod example

- We can change permissions using the Linux command **chmod**
- Examples:
  - **chmod a+r wombat.txt**
  - **chmod g+rw combat.txt**
  - **chmod 664 ramjet.txt**
- Whoa! 664? What's that?
  - Would it help if I pointed out that 664 can be written 110110100?

Role-based access control

- Role-based access control makes an effort to abstract away from specific subjects
- The idea is that you should have access based on your role
- Examples:
  - Secretaries have access to mailboxes
  - Department heads have access to performance reports
  - Provosts have access to salaries

RBAC definitions

- A role is a collection of job functions
- Each role is authorized to perform one or more transactions
- The active role of a subject is the role that subject is currently performing
- The authorized roles of a subject make up the set of roles that the subject is authorized to assume

Cryptography

Cryptography

- "Secret writing"
- The art of encoding a message so that its meaning is hidden
- **Cryptanalysis** is breaking those codes

Encryption and decryption

- **Encryption** is the process of taking a message and encoding it
- **Decryption** is the process of decoding the code back into a message
- A **plaintext** is a message before encryption
- A **ciphertext** is the message in encrypted form
- A **key** is an extra piece of information used in the encryption process

Notation

- A plaintext is M (sometimes P)
- A ciphertext is C
- The encryption function $E(x)$ takes M and converts it into C
  - $E(M) = C$
- The decryption function $D(x)$ takes C and converts it into M
  - $D(C) = M$
- We sometimes specify encryption and decryption functions $E_k(x)$ and $D_k(x)$ specific to a key k

Attacks

- Cryptography is supposed to prevent people from reading certain messages
- Thus, we measure a **cryptosystem** based on its resistance to an **adversary** or **attacker**
- Kinds of attacks:
  - **Ciphertext only:** Attacker only has access to an encrypted message, with a goal of decrypting it
  - **Known plaintext:** Attacker has access to a plaintext and its matching ciphertext, with a goal of discovering the key
  - **Chosen plaintext:** Attacker may ask to encrypt any plaintext, with a goal of discovering the key
  - Others, less common

Terminology

- A **sender** *S* wants to send a message to a **recipient** *R*
- If *S* gives the message to *T* who gives it to *R*, *T* is a **transmission medium**
- If an outsider *O* wants to access the message (to read, change, or destroy it), we call *O* an **interceptor** or **intruder**
- The fear is that O will cause one of the four security failures we discussed earlier:
  - Blocking the message
  - Intercepting the message
  - Modifying the message
  - Fabricating a false message

Terminology remix

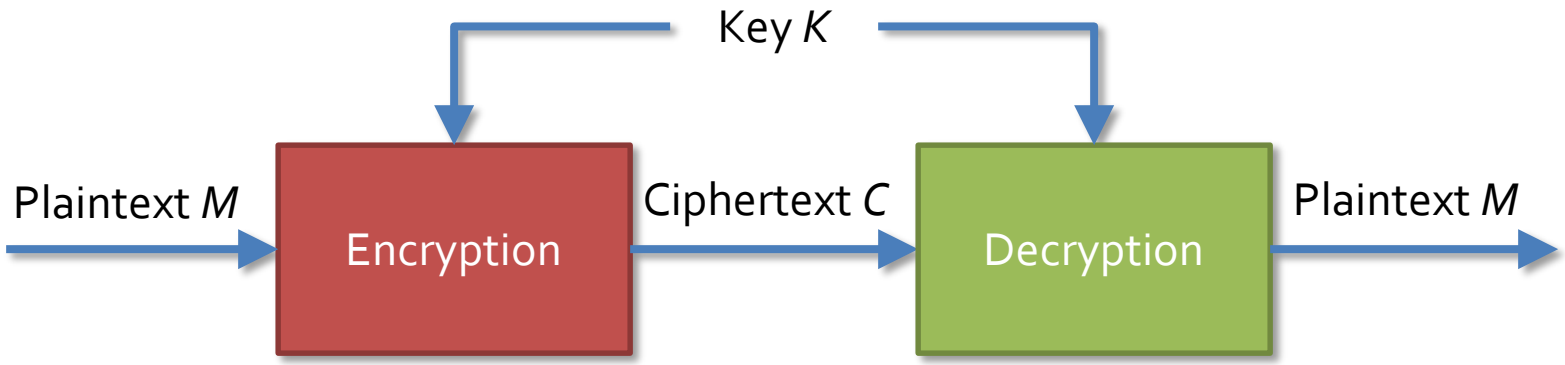
- The previous slide gives traditional, formal terminology
- Rather than use letters, a system popularized by Ron Rivest is to use **Alice** and **Bob** as the two parties communicating
  - **Carl** or another "C" name can be used if three people are involved
- **Trent** is a trusted third party
- **Eve** is used for an evil user who often eavesdrops
- **Mallory** is used for a malicious user who is usually trying to modify messages

Encryption algorithms

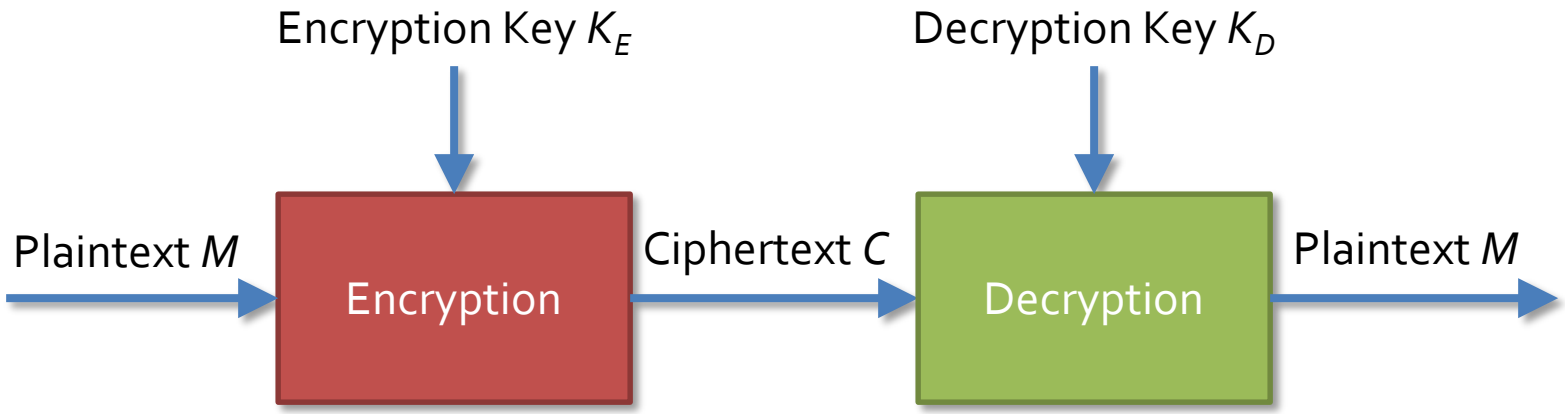
- The algorithms for encryption often rely on a secret piece of information, called a key
- We can notate the use of a specific key in either of the two following ways:
  - $C = E_K(M)$
  - $C = E(K, M)$
- In symmetric (or private key) encryption, the encryption key and the decryption key are the same
- In asymmetric (or public key) encryption, the encryption key and the decryption key are different

Symmetric vs. asymmetric

Symmetric Encryption



Asymmetric Encryption



Cryptanalysts

- A **cryptanalyst** is someone who is trying to break the cryptography and discover the plaintext or the key
- A cryptanalyst could:
  - Break a single message
  - Find patterns in the encryption that allow future messages to be decrypted
  - Discover information in the messages without fully decrypting them
  - Discover the key
  - Find weaknesses in the implementation of the encryption
  - Find weaknesses in the encryption that may or may not be able to lead to breaks in the future

Cryptanalysis

- There are two kinds of security for encryption schemes
  - **Unconditionally secure**
    - No matter how much time or energy an attacker has, it is impossible to determine the plaintext
  - **Computationally secure**
    - The cost of breaking the cipher exceeds the value of the encrypted information
    - The time required to break the cipher exceeds the useful lifetime of the information
- We focus on computationally secure, because there is only one practical system that is unconditionally secure

- "I want them to remain secret for as long as men are capable of evil" -Avi from *Cryptonomicon*

Modular Arithmetic Overview

Review of Modular Arithmetic

- Modulo operator takes the remainder
- Two numbers are said to be congruent modulo n if they have the same remainder when divided by n
- For example,

  $39 \equiv 3 \pmod{12}$
- Addition, subtraction, and multiplication:
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Divided and Conquered

- We can't actually divide
- Instead, we have to find the multiplicative inverse
- The multiplicative inverse of x exists if and only if x is relatively prime to n
- $13 \cdot 5 \equiv 65 \equiv 1 \pmod{16}$
- So, 13 and 5 are multiplicative inverses mod 16
- But, 0, 2, 4, 6, 8, 10, and 12 do not have multiplicative inverses mod 16

Upcoming

Next time…

- Shift ciphers
- Substitution ciphers
- One-time pads

Reminders

- **No class Monday!**
- Read Sections 2.3 and 12.1
- Work on Project 1
- Start Assignment 1
  - Due next Friday