

CS 465

# Terminology

# Is This System Secure?

Common question, but the wrong question to ask

Security begins by understanding the attackers and the threats

- Secure from whom?
- Secure from what?

# Context

Who are the players?

Good guys trying to communicate securely

- Alice
- Bob

Bad guys trying to break the system

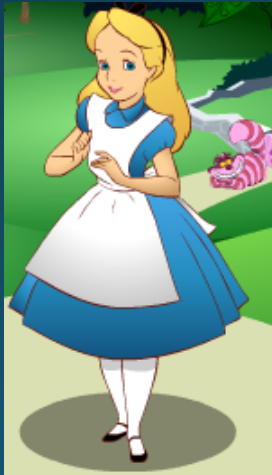
- Eve
- Mallory
- Trudy

# Good Guys – Alice and Bob

Traditional names used in the security literature

Alice and Bob attempt to share information

- Exchange secure email or chat messages
- A customer at a website



# Bad Guys

Eve

- Eavesdropper – passive attacker

Mallory

- Active attacker

Trudy

- Intruder

# What Kinds of Attacks?

- STRIDE Threat Model (Microsoft)
  - Spoofing user identify
  - Tampering
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service (DoS)
  - Elevation of privilege

# What Kinds of Defenses?

CIA

Confidentiality

- Prevent unauthorized access to data

Integrity

- Detect unauthorized modification/creation of data

Availability

- Prevent a denial of service attack
- Data is delivered in a reasonable time frame
- System is available when a service is requested

# Example: Secure Email

Who are the attackers?

What kind of attacks?

- Confidential - from eavesdroppers, email server, active attackers
  - End-to-end encryption
- Integrity - cannot change the message, who is it from?
  - Digital signature
- Availability - DDoS mail server, START/TLS downgrade attack



# Threat Model

Decide on the threats that are relevant in a given scenario

Analyze how well the system thwarts those threats

## Example

- Email
- Attack
  - Eavesdropping
- Solutions
  - HTTPS
  - End-to-end encryption (PGP)

# Access Control

## Authentication

- Determining if this is really Alice or Bob

## Authorization

- Does the user have authorization to complete a requested action?

# Non-repudiation

Prevent the ability to later deny that an action took place

Usually involves cryptographic evidence that will stand up in court

# Deniability

Ability to later deny that an action took place

# Three Facets to Security

Prevention

Detection

Reaction



# Weakest Link Property

A security system is only as strong as its weakest link

# Principle of Least Privilege

A process should have enough permissions to do just what it needs to do and no more

# Security Through Obscurity

Reliance on the secrecy of the design or implementation as the main method of providing security for a system or component of a system

## Examples

- Key under the door mat
- Obscure URL
- Don't open source the code

Related concept: Security Through Minority

- Use an unpopular tool



# Attack Trees

An ad-hoc method to reasoning about the threats to a system

Hierarchical tree with the root node as the goal of an attacker

- Child nodes contain all the ways to accomplish the goal of the parent node
- Probability associated with each node