# Introduction to Information Security
# 14-741/18-631 Fall 2020
# Unit 1: Lecture 3: Basic properties

**Limin Jia** liminjia@andrew

# Overview

- **Agenda**
  - Introduce basic properties of a secure system
- **Goal**
  - Set up the theoretical background for our in-class case studies

# Secrecy, privacy, and confidentiality

- **Keeping information secret from all but those who are authorized to see it**
  - Alice wants to talk to Bob without Eve or Mallory being able to listen to the conversation
- **Slight differences in terminology**
  - Privacy = preserving own personal information secret
    - Alice protects her privacy by not revealing her age to anyone
  - Confidentiality = obligation to preserve someone else’s information secret
    - Trent ensures confidentiality of Alice’s credit card numbers
  - Secrecy = effect of mechanisms used to limit the number of principals who can access information

# Data integrity

- **Ensuring that information has not been altered by unauthorized or unknown means**
  - Alice and Bob ensure the integrity of their communication by using a secure physical channel that prevents Mallory from changing the contents of the messages they exchange
  - Trent performs bit-parity checking after downloading a file from the server to ensure the integrity of the downloaded file, i.e., that the contents are correct

# Identification

- **Corroboration of the identity of an entity**
  - By showing her driver's license, Alice identifies herself to the poll worker at the voting place
  - By logging in using her Andrew ID and password, Alice identifies herself to canvas system.
  - Also sometimes called "entity authentication"
- **Note that identification can be pseudonymous**

# Anonymity

- **Concealing identity of a protocol participant**
  - Alice decided to use Tor to browse websites anonymously (More on this later this semester)

# (Message) Authentication

- **Corroborating the source of information**
- **Also known as “data origin authentication”**
  - Bob authenticates that the letter he is receiving is from Alice by checking Alice’s signature

# Non-repudiation

- Assurance that someone cannot deny something
- In the context of security it is often mentioned together with digital signature (more later)

# Authorization, certification, access control, revocation, witnessing

- **Authorization**
  - Conveyance to another entity of official sanction to **do** or **be** something (someone)
- **Certification**
  - Endorsement of information by a trusted entity
- **Access control**
  - Restricting access to resources to privileged entities
- **Witnessing**
  - Verifying the creation or existence of information by an entity other than the creator
- **Revocation**
  - Retraction of certification or authorization

# Freshness & Age

- **Freshness**
  - Proof that an event occurred after a given point in time
  - The bank only accepts to cash a check from Alice if she has endorsed it within 90 days of its issuance date
- **Age**
  - Proof that an event occurred before a given point in time
  - Bob can only receive his purchase, 5 days after his check for payment is cleared by the sellers' bank.
- **Mechanisms to achieve freshness and age**
  - Timestamps

# Availability

- **Services/resources are available to rightful entities**
- **Example:**
  - Alice can access the internet once she pays the COMCAST
  - PNC customers can do online banking on pnc.com 24/7

# List of properties

- Secrecy
- Integrity
- Identification
- (Message) Authentication
- Authorization, certification, access control, revocation, witnessing
- Non-repudiation
- Anonymity
- Freshness & Age
- Availability

# Before class exercises

- **Connect properties to attacks (as outlined in STRIDE)**
- **STRIDE: Six categories**
  - Spoofing of user identity
  - Tampering
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service (D.o.S)
  - Elevation of privilege