CLOUD COMPUTING CONCEPTS

with Indranil Gupta (Indy)

SECURITY

Lecture A

BASIC SECURITY CONCEPT

Security Threats

- **Leakage**
  - Unauthorized access to service or data
  - E.g., someone knows your bank balance
- **Tampering**
  - Unauthorized modification of service or data
  - E.g., someone modifies your bank balance
- **Vandalism**
  - Interference with normal service, without direct gain to attacker
  - E.g., denial-of-service attacks

Common Attacks

- **Eavesdropping**
  - Attacker taps into network
- **Masquerading**
  - Attacker pretends to be someone else, i.e., identity theft
- **Message tampering**
  - Attacker modifies messages
- **Replay attack**
  - Attacker replays old messages
- **Denial-of-service**: bombard a port

ADDRESSING THE CHALLENGES: CIA PROPERTIES

- Confidentiality
  - *Protection against disclosure to unauthorized individuals*
  - Addresses leakage threat
- Integrity
  - *Protection against unauthorized alteration or corruption*
  - Addresses tampering threat
- Availability
  - *Service/data is always readable/writable*
  - Addresses vandalism threat

Policies vs. Mechanisms

- Many scientists (e.g., Hansen) have argued for a separation of policy vs. mechanism
- A security policy indicates *what* a secure system accomplishes
- A security mechanism indicates *how* these goals are accomplished
- E.g.,
  - Policy: in a file system, only authorized individuals allowed to access files (i.e., CIA properties)
  - Mechanism: Encryption, capabilities, etc.

Mechanisms: Golden A's

- **Authentication**
  - Is a user (communicating over the network) claiming to be Alice, really Alice?
- **Authorization**
  - Yes, the user is Alice, but is she allowed to perform her requested operation on this object?
- **Auditing**
  - How did Eve manage to attack the system and breach defenses? Usually done by continuously logging all operations.

DESIGNING SECURE SYSTEMS

- Don’t know how powerful attacker is
- When designing a security protocol need to

1. Specify attacker model: Capabilities of attacker

 (Attacker model should be tied to reality)

2. Design security mechanisms to satisfy policy under the attacker model

3. Prove that mechanisms satisfy policy under attacker model

4. Measure effect on overall performance (e.g., throughput) in the common case, i.e., no attacks

Next

- Basic cryptography