Fundamentals of Information & Network Security ECE 471/571

Lecture #2: Security Objectives, Modular Arithmetic
Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Information & Network Security

Information Security

Information: Commodity distributed via a network

Protection of the information has to do with information security

E.g.: Encryption prevents unauthorized users from eavesdropping data

Network Security

Network: An infrastructure for distributing information

Protection of the network availability to enable information delivery

E.g.: Adversary launches a Denial-of-Service attack on a website server that becomes unavailable

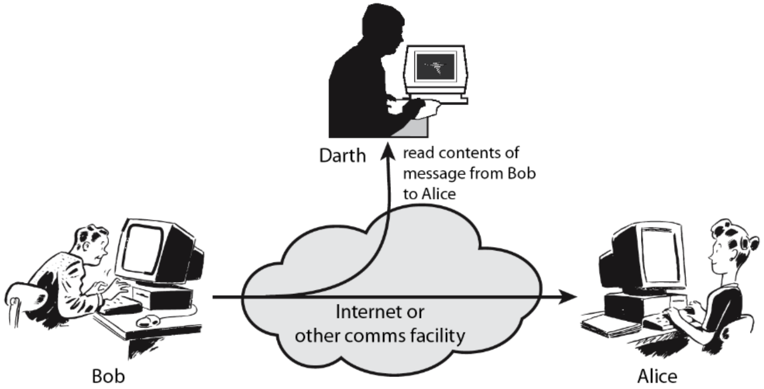
Threats, Vulnerability, Attacks

“The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Sun Tzu – Art of War

Security Attacks

- Passive attacks
  - Eavesdropping
  - Traffic analysis


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

- Active attacks
  - Masquerade, modification, insertion, delay, replay, deletion

Security Objectives (Services)

Confidentiality

Restricting access to information only to authorized entities

Id Authentication

Association of an identity to an entity

Message Authentication

Association of a message to an entity, i.e. verifying the source of a message

Data Integrity

Ensuring that the information has not been altered by an unauthorized entity

Non-repudiation

Preventing the denial of previous commitments or actions (think of a contract)

Access Control

Preventing unauthorized use of a resource (e.g., systems and applications)

Availability

Ensuring the accessibility and usability of a system or resource by an authorized entity

Objectives of Information Security

Certification

Endorsement of information by a trusted entity.

Privacy & Anonymity

Keeping, data, whereabouts, associations, identity, etc. private

Freshness

Ensure that the information sent is fresh

Revocation

Retraction of certification or authorization

A Model of Secure Communication

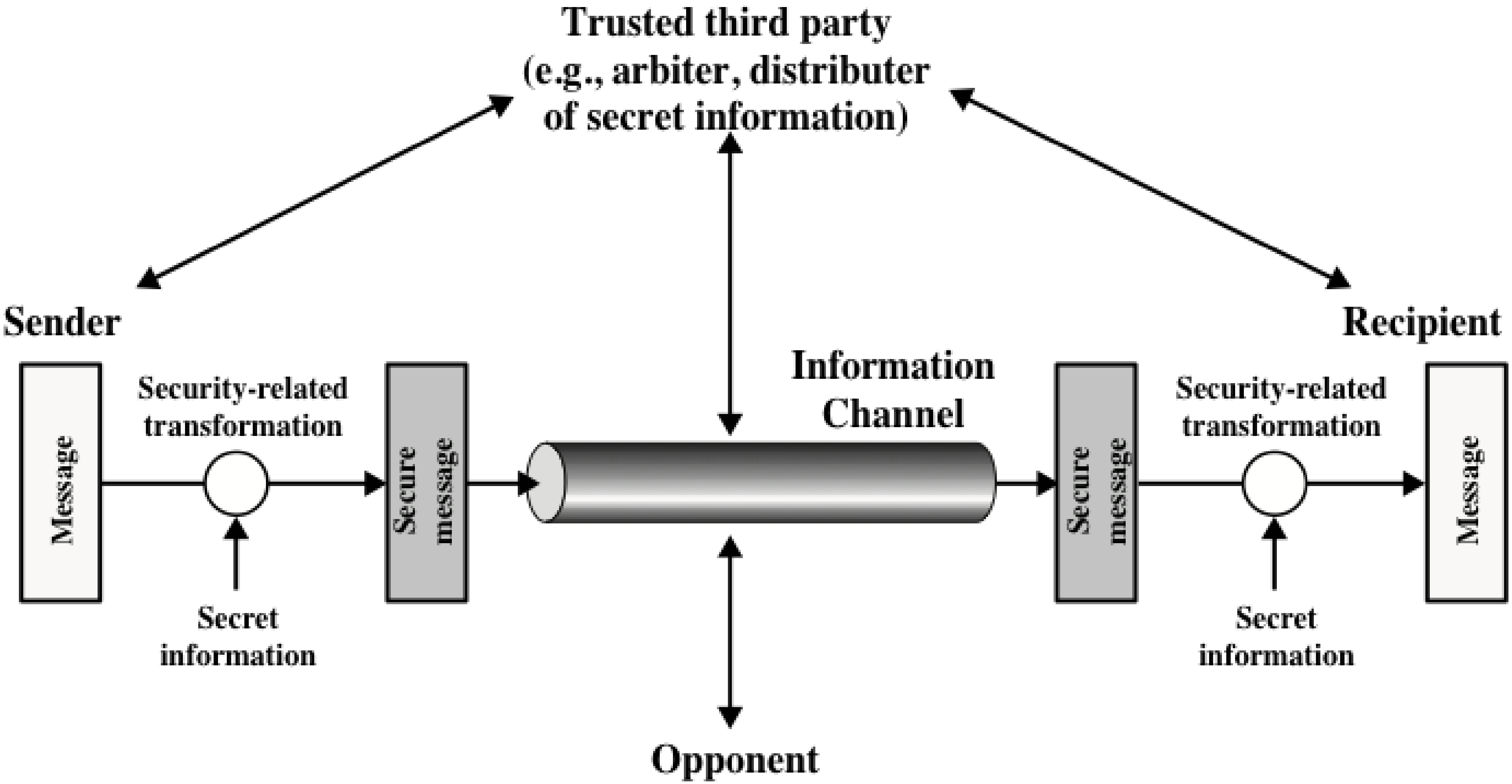


Figure 1.5 Model for Network Security

A Model of Network Security

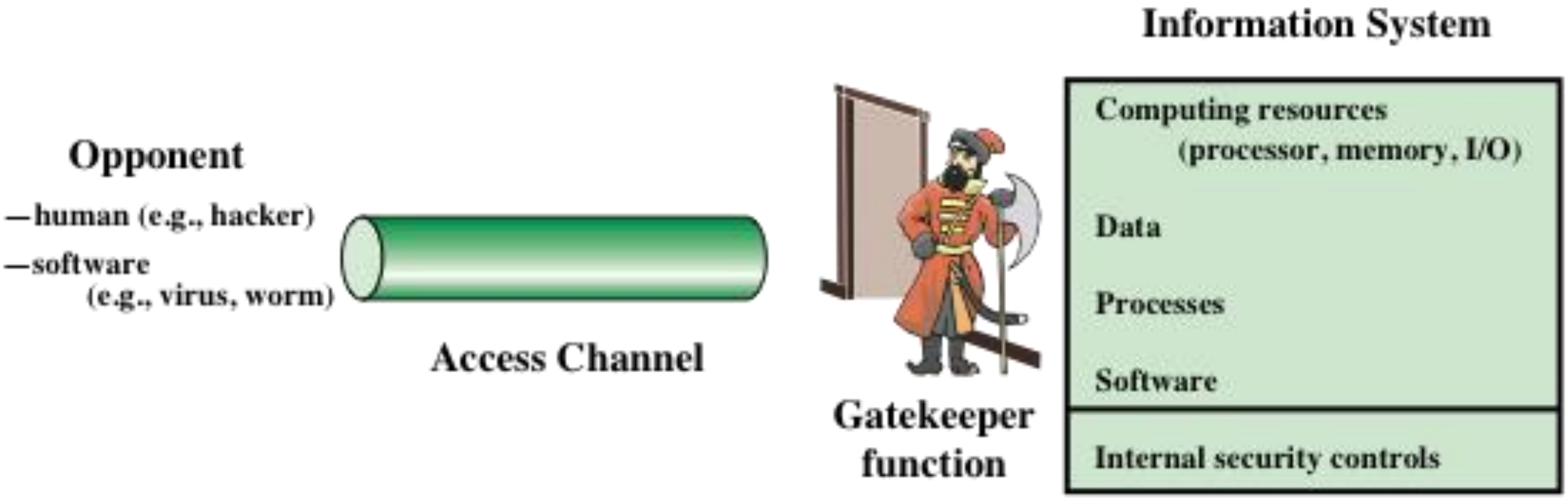


Figure 1.6 Network Access Security Model

Basic Modular Arithmetic

- Divisibility
  - A nonzero b divides a, if a=mb for some m (all are integers)
  - If b|a, then b is a divisor of a

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
13 | 182; - 5 | 30; 17 | 289; - 3 | 33; 17 | 0

- Properties of divisibility
  - If *a* | *b* and *b* | *c*, then *a* | *c*
  - If *b* | *g* and *b* | *h*, then *b* | (*mg* + *nh*) for arbitrary integers *m* and *n*

11 | 66 and 66 | 198 = 11 | 198

- Division algorithm
  - Given any positive integer n, integer a,

    a = qn+r, 0≤ r<n, q=floor(a/n) ---- q: quotient; r: residue

Basic Modular Arithmetic

- Modulus
  - a mod n: the remainder when a is divided by n
  - n is a positive integer and is called the modulus

11 mod 7 = 4; - 11 mod 7 = 3

- Congruence
  - Integers a and b are congruent modulo n, if (a mod n)=(b mod n)
  - Written as a ≡ b (mod n)

73 ≡ 4 (mod 23); 21 ≡ - 9 (mod 10)

- Properties
  - a ≡ b (mod n) ⇔ n |(a – b)
  - a ≡ b (mod n) ⇔ b ≡ a (mod n)
  - a ≡ b (mod n) and b ≡ c (mod n) → a ≡ c (mod n)

23 = 8 (mod 5) because 23 - 8 = 15 = 5 * 3
- 11 = 5 (mod 8) because - 11 - 5 = - 16 = 8 * (- 2)
81 = 0 (mod 27) because 81 - 0 = 81 = 27 * 3

Basic Modular Arithmetic

- Modular Addition and Multiplication
  - Arithmetic operations within the set Z_n={0,1,…,(n-1)}
  - Examples: (5+7) mod 10 =? (5*7) mod 10 = ?

- Properties:
  - (a + b) mod n = [(a mod n) + (b mod n)] mod n
  - (a - b) mod n = [(a mod n) - (b mod n)] mod n
  - (a * b) mod n = [(a mod n) * (b mod n)] mod n

- More examples
  - (978 + 1047) mod 10 =?
  - (111 * 112) mod 10 =?

- Modular Exponentiation
  - Can be done by repeated multiplication
  - 11^7 mod 13 =?

Reading Assignment for Next Class

- Finish Chapter 2 of Stallings, and Chapter 3 (3.1, 3.2).