# Protocol Design

csci 7000-001 f01-08

Antonio Carzaniga

## Protocol Design: Assumptions

- Alice initiates a conversation with Bob
- Alice has various pieces of information, some secret, some not
- Bob has various pieces of information as well

## Threats: Eavesdrop

Trudy reads messages between Alice and Bob

Trudy *should not* be able to

- impersonate either Alice or Bob in another exchange between Alice and Bob
- impersonate either Alice or Bob in an exchange with another party
- guess Alice's or Bob's secrets

## Threats: Spoofing Alice

Trudy initiates an exchange pretending to be Alice

Trudy *should not* be able to

- convince Bob she is Alice
- learn info that allows her to guess either Alice's or Bob's secrets
- learn info that allows her to impersonate either Alice or Bob in another exchange
- trick Bob into signing or decrypting something

## Threats: Spoofing Bob

Trudy accepts connections (messages) pretending to be Bob

Trudy *should not* be able to

- convince Alice she is Bob
- learn info that allows her to guess either Alice's or Bob's secrets
- learn info that allows her to impersonate either Alice or Bob in another exchange
- trick Alice into signing or decrypting something

## Threats: Reading Alice's Secrets

Trudy gains access to Alice's private data

Trudy *should not* be able to

- impersonate Bob to Alice
- decrypt a previous conversation between Alice and Bob

## Threats: Reading Bob's Secrets

Trudy gains access to Bob's private data

Trudy *should not* be able to

- impersonate Alice to Bob
- decrypt a previous conversation between Alice and Bob

## Threat: Man-in-the-Middle

Trudy can intercept, destroy, modify, or forge messages between Alice and Bob

Trudy *should not* be able to

- learn info that allows her to guess either Alice's or Bob's secrets
- read the conversation between Alice and Bob
- hijack a conversation
- cause Alice and Bob to misinterpret one-another (e.g., Bob ends up rejecting a valid conversation)

## General Principles

- Exactly symmetrical protocols are bad
  - replay attacks

  ⇒always have Alice do something a bit different from Bob
- Invariant exchanges are bad
  - deferred replay

  ⇒introduce some random numbers or time-dependent quantities or counters
- Encrypting known plaintext is a bad idea
  - password-guessing attacks

  ⇒add random padding

## General Principles

- Self-enforcing authentication with symmetric cipher
  - vulnerable to man-in-the-middle attacks
- The security of a public-key schema can be reduced to
  - integrity (authenticity) of public keys, and
  - confidentiality of secret keys

# Formal Analysis of Protocols

- Traditional software verification
- Expert system
- Logic of beliefs and knowledge (BAN)
- Algebraic methods