

## Principles of Information Security CS 5323 Lecture Four

Prof. William Winsborough  
September 9, 2008

## Business

- Read chapters 3, 4, and 5 by Thursday
  - In chapter 3, I want you to understand the basic structure of how we can prove safety is undecidable in the Harrison, Ruzzo, and Ullman model
  - You don't have to be able to recreate the reduction itself
- Questions from previous lectures?

9 September 2008

Winsborough CS 5323 Lecture 4

2

## Modeling Computer Systems

- We can view a computer system as a finite state machine (FSM)
  - Set of states, one of which is the *initial state*
  - A set of events to which the FSM responds
  - A set of actions the FSM can initiate
  - A transition relation indicating how the FSM can transit from one state to another, based on events and defining actions initiated by the transition
- In this context, policy can be viewed as defining which states are secure and which are not
  - Many, but not all system properties of interest to security can be categorized this way

9 September 2008

Winsborough CS 5323 Lecture 4

3

## Secure Systems

- Under the FSM model
  - A secure system starts in a secure state and cannot enter an insecure state
  - A *breach of security* occurs if a system transits from a secure state to an insecure state

9 September 2008

Winsborough CS 5323 Lecture 4

4

## Three Fundamental Properties

- Confidentiality
  - Information I has *confidentiality* with respect to entity set X if no member of X can obtain information about I
  - Tells you where the information could go
- Integrity
  - I has *integrity* with respect to X if members of X trust I
  - Tells you where the information came from and how it got to you
- Availability
  - I has *availability* with respect to X if all member of X can access
  - Tells you where the information must be able to go
  - Can include *quality of service* requirements

9 September 2008

Winsborough CS 5323 Lecture 4

5

## Integrity

- Example: Unix write permission
- Example: separation of duty requirements
- Information integrity versus system integrity
  - Data can be modified by flawed or compromised system components
  - A system is *compromised* if it has been maliciously altered
- Example: Execute permission

9 September 2008

Winsborough CS 5323 Lecture 4

6

## Confidentiality

- Example: Unix read permission
- Access control versus Information-flow control
  - How to enforce confidentiality policy in a distributed system?
  - Can you trust other hosts?
  - How much of your own host can you trust, or do you have to trust to enforce confidentiality policy?
- Is it possible to have confidentiality without having any integrity guarantees?
  - If the system is compromised, it may not correctly enforce confidentiality policies

9 September 2008

Winsborough CS 5323 Lecture 4

7

## Availability

- Example attack: denial of service (DOS)
  - In a distributed denial of service attack (DDOS), an attacker uses lots of compromised hosts to send service requests to a victim service, thus preventing the victim from being able to provide service to legitimate clients
- Availability can also be compromised by mis-configured security mechanisms

9 September 2008

Winsborough CS 5323 Lecture 4

8

## Policies, Mechanisms and Models

- A *mechanism* (or *enforcement mechanism*) is an entity or procedure that enforces some part of a security policy
  - Just because the mechanism doesn't prevent something doesn't mean it is authorized
- A model is a conceptual framework that can be used to represent policy
  - Often the model can be configured to express various policies

9 September 2008

Winsborough CS 5323 Lecture 4

9

## A Word About Words

- Many of these terms are used in different ways in different contexts
- Sometimes "policy" is used to refer to a precise specification in a formal language
- Sometimes "model" is used to refer to a finite state machine

9 September 2008

Winsborough CS 5323 Lecture 4

10

## Types of Access Control

- Discretionary Access Control (DAC)
  - Object owner control who can access
  - Based on subject and object identity
- Mandatory Access Control (MAC)
  - Institution controls who can access
  - Typically based on
    - Clearance level of subject
    - Confidentiality label of object
  - Canonical example: Bell-LaPadula model

9 September 2008

Winsborough CS 5323 Lecture 4

11

## Usage Control

- Generalizes access control
  - May require that remote hosts are part of the *trusted computing base* (TCB)
    - Providing mechanisms that provide assurance of trustworthiness is an active research area today
  - Considers usage that consists of more than just one operation
  - Can require that actions be taken by the resource user before, during, and after the period of usage
  - Usage can modify the state of the security system
    - Resource consumption
  - Rights can depend on environmental factors, such as where the user is or the time of day

9 September 2008

Winsborough CS 5323 Lecture 4

12