Grand Challenges in Authorization Systems

Prof. Ravi Sandhu
Executive Director and Endowed Chair

November 14, 2011

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
Mutually Supportive Technologies

AUTHENTICATION
CRYPTOGRAPHY
ASSURANCE

RISK ANALYSIS
ACCESS CONTROL

INTRUSION DETECTION

SECURITY ENGINEERING & MANAGEMENT

World-Leading Research with Real-World Impact!

© Ravi Sandhu
Cyber Security Objectives

INTEGRITY modification

CONFIDENTIALITY disclosure

AVAILABILITY access
Cyber Security Objectives

- CONFIDENTIALITY
  - disclosure

- INTEGRITY
  - modification

- USAGE
  - purpose

- AVAILABILITY
  - access
Cyber Security Objectives

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Grand Challenge arena → Dynamics Agility

Policy Specification → Enforcement
Access Control Models

- Discretionary Access Control (DAC)
  - Owner controls access
  - But only to the original, not to copies

- Mandatory Access Control (MAC)
  - Same as Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels propagate to copies

- Role-Based Access Control (RBAC)
  - Access based on roles
  - Can be configured to do DAC or MAC
  - Generalizes to Attribute-Based Access Control (ABAC)

Numerous other models but only 3 successes: SO FAR
Discretionary Access Control

A trusted not to copy F to G

B cannot read file F
Discretionary Access Control

Program Goodies

Trojan Horse

File F

File G

ACL

A:r
A:w

B:r
A:w

But trusting A does not stop Trojan Horses
Mandatory Access Control

High User

Information is leaked unknown to the high user

High Trojan Horse Infected Subject

COVERT CHANNEL

Low Trojan Horse Infected Subject

Low User
Role-Based Access Control

- Access is determined by roles
- A user’s roles are assigned by security administrators
- A role’s permissions are assigned by security administrators

Is RBAC MAC or DAC or neither?

- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

RBAC is neither MAC nor DAC!
Server Pull Enforcement Model

Client

User-role Authorization Server

Server
Tough Challenges

- Trojan Horse
- Covert Channels
- Inference
- Analog Hole
- Assured Enforcement
- Privelege Escalation
- Policy Comprehension and Analysis

Tough Challenges NOT EQUAL TO Grand Challenges
How can we be “secure” while being “insecure”?

What is the value of access control when we know that ultimately it can be bypassed?
Grand Challenge arena

Dynamics Agility

Policy Specification

Enforcement
How do we determine the balance between too much and too little?

How do we enforce policies across multiple layers of the software stack?

How do we build dynamics into policy specifications and enforcement mechanisms?

How do we understand and control what we have done?
Computer scientists could never have designed the web because they would have tried to make it work.

- But the Web does “work.”
- What does it mean for the Web to “work”?