PURDUE UNIVERSITY

CS52600: Information Security

Course Overview

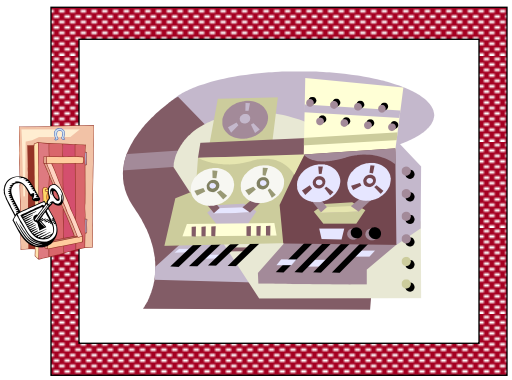
8/23/2010

Prof. Chris Clifton

Portions of the material courtesy Professor Matt Bishop

What is Information Security?

- Confidentiality
  - *Is this all?*
  - *Why not?*
- Availability
  - *To whom?*
- Authentication
  - Still not there
- Integrity



It's about more than network security!

2

Course Outline

1. Introduction: Role of security, Types of security, Definitions.
2. Access Control Matrix model
3. Protection Models
4. Policy: Risk Analysis, Policy Formation, Role of audit and control.
5. Formal policy models.
6. Information Flow
7. Authentication and Identity
8. TBD (probably basics of Cryptography
9. System Design principles. TCB and security kernel construction, Verification, Certification issues.

Midterm. Most likely date: 10/18.

Let me know of bad dates this week

10. System Design principles. TCB and security kernel construction, Verification, Certification issues.
11. Network Security. Distributed cooperation and commit. Distributed authentication issues. Routing, flooding, spamming. Firewalls.
12. Audit Mechanisms.
13. Malicious Code: Viruses, Worms, etc.
14. Vulnerability Analysis.
15. Physical threats, operational security, Legal and Societal Issues

Final Exam

December 18, 9pm – earliest you should count on leaving campus before you see the exam schedule

3

Course Administration

www.cs.purdue.edu/homes/clifton/cs526/

- Teaching Assistant:
  - Ashish Kundu
- Course Announcements
  - Mailing list (directed to *you*@purdue.edu)
  - http://www.cs.purdue.edu/~clifton/cs526/
  - Discussion, grades, assignment submission through blackboard
- Evaluation/Grading
  - Midterm 25%, Final 36%
  - Exercises, projects 36%
    - 1-2 programming projects
    - 9-11 written assignments (similar to exercises in the book)
- Let me know if you will be taking the qual1
  - See web page for more

4

© 2010 Chris Clifton

Course Text

- Recommended Text:
  - Matthew Bishop
    Computer Security: Art and Science
    Addison-Wesley, 2003
    ISBN 0-201-44099-7
    http://nob.cs.ucdavis.edu/book/
  - *If you don't have the latest printing, see the above link for Errata pages*
- Not required, but easier than finding/reading original papers

Waiting List / Registration

- Send me "background information" as follows:

  Career ID, Infosec Masters , Expected graduation , Research focus , Had CS555 , Will take CS555 , Taking CS626 , likely TA next year
- Sample:

  clifton, no , 6/1991 , Privacy and Data Mining , no , no , no , no
- *Course is planned for spring as well*

© 2010 Chris Clifton

Introduction

- Components of computer security
- Threats
- Policies and mechanisms
- The role of trust
- Assurance
- Operational Issues
- Human Issues

7

Basic Components

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources

8

© 2010 Chris Clifton

Classes of Threats

- Disclosure
  - Snooping
- Deception
  - Modification, spoofing, repudiation of origin, denial of receipt
- Disruption
  - Modification
- Usurpation
  - Modification, spoofing, delay, denial of service

9

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines “security” for the site/system/*etc*.
  - Policy definition: Informal? Formal?
- Mechanisms enforce policies
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities

10

© 2010 Chris Clifton

Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

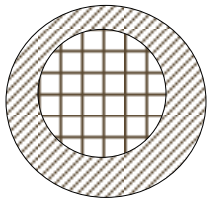
11

Trust and Assumptions

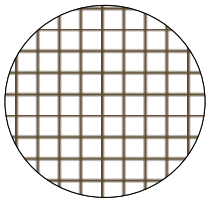
- Underlie *all* aspects of security
- Policies
  - Unambiguously partition system states
  - Correctly capture security requirements
- Mechanisms
  - Assumed to enforce policy
  - Support mechanisms work correctly

12

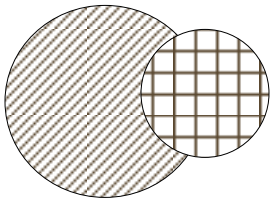
Types of Mechanisms



secure



precise



broad

set of reachable states

set of secure states

13

Assurance

- Specification
  - Requirements analysis
  - Statement of desired functionality
- Design
  - How system will meet specification
- Implementation
  - Programs/systems that carry out design

14

Operational Issues

- Cost-Benefit Analysis
  - Is it cheaper to prevent or recover?
- Risk Analysis
  - Should we protect something?
  - How much should we protect this thing?
- Laws and Customs
  - Are desired security measures illegal?
  - Will people do them?

15

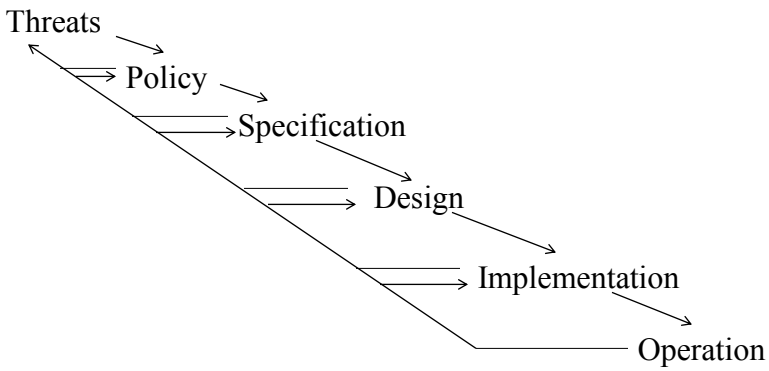
Human Issues

- Organizational Problems
  - Power and responsibility
  - Financial benefits
- People problems
  - Outsiders and insiders
    - *Which do you think is the bigger problem?*
  - Social engineering

16

© 2010 Chris Clifton

Tying the Definitions Together



17

Key Points

- Policy defines security, and mechanisms enforce security
  - Confidentiality
  - Integrity
  - Availability
- Trust and knowing assumptions
- Importance of assurance
- The human factor

18

Models: Access Control

- What is access control?
  - Limiting who is allowed to do what
- What is an access control model?
  - Specifying who is allowed to do what
- What makes this hard?
  - Interactions between types of access

19

Basics

- State: Status of the system
  - Protection state: subset that deals with protection
- Access Control Matrix
  - Describes protection state
- Formally:
  - Objects O
  - Subjects S
  - Matrix $A \subseteq S \times O$
- Tuple (S, O, A) defines protection states of system

20

© 2010 Chris Clifton

Student Choice Topics

- Trusted Computing Systems
  - How does software know underlying system can be trusted?
  - Case study of trusted system / verification
  - Validation process
- Forensics
  - Recovery/Prevention
  - Tracing/Prosecution
- Digital Rights Management
- Legal issues
- …

21

PURDUE UNIVERSITY

CS526: Information Security Access Control Matricies

Prof. Chris Clifton

August 25, 2010

Access Restriction Facility

- Subject: attributes (name, role, groups)
- Verbs: possible actions
  - Default rule for each verb
- Objects associated with set of verbs
  - Rule for each (object, verb) pair
  - Rule may be function of subject attributes
- Can be converted to Access Control Matrix

23

Access Control Matrix: Boolean Evaluation Example

	Internal	Local	State University	Long Distance	International
Public	CR T		R		
Student	CR T	CR T	R	R	R
Staff	CR Transfer	CR T	CR T	R	R
Account	CR T	CR T	CR T	CR T	CR T

24

What Else Might We Add?

- Default Rule
  - General default: Receive
  - Object default: Call Internal
  - Requires ability to override with negative and positive access
- Time-based access
  - Allow students to call on State University system after hours?
- History-based access

25

Access Control by History

- Example: Statistical Database
  - Allows queries for general statistics
  - But not individual values
- Valid queries: Statistics on 20+ individuals
  - Total salary of all Deans
  - Salary of Computer Science Professors
- See a problem coming?
  - Salary of CS Professors who aren't Deans

26

Solution: Query Set Overlap Control (Dobkin, Jones & Lipton '79)

- Query valid if intersection of query coverage and each previous query < *r*
- Given *K* minimum query size, r overlap:
  - Need *1 + (K-1)/r* queries to compromise
- Can represent as access control matrix
  - Subjects: entities issuing queries
  - Objects: *Powerset* of records
  - $O_s(i)$: objects referenced by *s* in queries *1..i*
  - *A*[*s,o*] = read iff $\forall_{q \in \cup_s} \cap \; <$

27

Next

- Optional reading: Dobkin, Jones, and Lipton (TODS 4(1), see course web site)
- Basic theorems on protection states
  - Decidability of safety of a state with respect to a right
- More Protection Models

28

Protection Study: Your Homework

- What does it take to make sure your homework is secure?
  - Let's assume a Unix system (mentor.ics)
  - Issues?
- *Participation Expected!*

30