

Principles of Information Security CS 5323 Lecture Seven

Prof. William Winsborough
September 23, 2008

Business

- Read chapter 8
- No class Thursday Oct. 2
 - I'm giving a keynote talk that day at PST2008, Sixth Annual Conference on Privacy, Security and Trust, Fredericton, New Brunswick, Canada
- Tuesday October 7 will be devoted to review
 - Bring your questions
- Thursday October 9 will be midterm 1
 - It will cover material from the first 7 chapters and lectures through Thursday 9/25
- Questions from previous lectures?

23 September 2008

Winsborough CS 5323 Lecture 7

2

Chapter 7: Hybrid Policies

- Overview
- Chinese Wall Model
- Clinical Information Systems Security (CISS) Policy
- ORCON
- RBAC

23 September 2008

Winsborough CS 5323 Lecture 7

3

Overview

- Chinese Wall Model
 - Focuses on conflict of interest
- CISS Policy
 - Combines integrity and confidentiality
- ORCON
 - Combines mandatory, discretionary access controls
- RBAC
 - Base controls on job function

23 September 2008

Winsborough CS 5323 Lecture 7

4

Chinese Wall Model

Problem:

- Tony advises American Bank about investments
- He is asked to advise Toyland Bank about investments
- Conflict of interest to accept, because his advice for either bank would affect his advice to the other bank

23 September 2008

Winsborough CS 5323 Lecture 7

5

Organization

- Organize entities into "conflict of interest" classes
- Control subject accesses to each class
- Control writing to all classes to ensure information is not passed along in violation of rules
- Allow sanitized data to be viewed by everyone

23 September 2008

Winsborough CS 5323 Lecture 7

6

Definitions

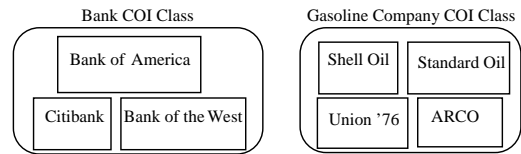
- *Objects*: items of information related to a company
- *Company dataset (CD)*: contains objects related to a single company
 - Written $CD(o)$
- *Conflict of interest class (COI)*: contains datasets of companies in competition
 - Written $COI(o)$
 - Assume: each object belongs to exactly one *COI* class

23 September 2008

Winsborough CS 5323 Lecture 7

7

Example



23 September 2008

Winsborough CS 5323 Lecture 7

8

Temporal Element

- If Anthony reads any CD in a COI, he can *never* read another CD in that COI
 - Possible that information learned earlier may allow him to make decisions later
 - Let $PR(S)$ be set of objects that S has already read

23 September 2008

Winsborough CS 5323 Lecture 7

9

CW-Simple Security Condition

- s can read o iff either condition holds:
 1. There is an o' such that s has accessed o' and $CD(o') = CD(o)$
 - Meaning s has read something in o' 's dataset
 2. For all $o' \in O$, $o' \in PR(s) \Rightarrow COI(o') \neq COI(o)$
 - Meaning s has not read any objects in o' 's conflict of interest class
- Ignores sanitized data (see below)
- Initially, $PR(s) = \emptyset$, so initial read request granted

23 September 2008

Winsborough CS 5323 Lecture 7

10

Sanitization

- Public information may belong to a CD
 - As is publicly available, no conflicts of interest arise
 - So, should not affect ability of analysts to read
 - Typically, all sensitive data removed from such information before it is released publicly (called *sanitization*)
- Add third condition to CW-Simple Security Condition:
 3. o is a sanitized object

23 September 2008

Winsborough CS 5323 Lecture 7

11

Writing

- Anthony, Susan work in same trading house
- Anthony can read Bank 1's CD, Gas' CD
- Susan can read Bank 2's CD, Gas' CD
- If Anthony could write to Gas' CD, Susan can read it
 - Hence, indirectly, she can read information from Bank 1's CD, a clear conflict of interest

23 September 2008

Winsborough CS 5323 Lecture 7

12

CW-^{*}-Property

- s can write to o iff both of the following hold:
 1. The CW-simple security condition permits s to read o ; and
 2. For all *unsanitized* objects o' , if s can read o' , then $CD(o') = CD(o)$
Correction: $o' \in PR(s) \Rightarrow CD(o') = CD(o)$
- Says that s can write to an object if all the (unsanitized) objects it can read are in the same dataset

23 September 2008

Winsborough CS 5323 Lecture 7

13

Compare to Bell-LaPadula

- Fundamentally different
 - CW has no security labels, B-LP does
 - CW has notion of past accesses, B-LP does not
- Bell-LaPadula can capture state at any time
 - Each (COI, CD) pair gets security category
 - Two clearances, S (sanitized) and U (unsanitized)
 - $S \text{ dom } U$
 - Subjects assigned clearance for compartments without multiple categories corresponding to CDs in same COI class

23 September 2008

Winsborough CS 5323 Lecture 7

14

Compare to Bell-LaPadula

- Bell-LaPadula cannot track changes over time
 - Susan becomes ill, Anna needs to take over
 - C-W history lets Anna know if she can
 - No way for Bell-LaPadula to capture this
- Access constraints change over time
 - Initially, subjects in C-W can read any object
 - Bell-LaPadula constrains set of objects that a subject can access
 - Can't clear all subjects for all categories, because this violates CW-simple security condition

23 September 2008

Winsborough CS 5323 Lecture 7

15

Compare to Clark-Wilson

- Clark-Wilson Model covers integrity, so consider only access control aspects
- If “subjects” and “processes” are interchangeable, a single person could use multiple processes to violate CW-simple security condition
 - Would still comply with Clark-Wilson Model
- If “subject” is a specific person and includes all processes the subject executes, then consistent with Clark-Wilson Model

23 September 2008

Winsborough CS 5323 Lecture 7

16

Clinical Information Systems Security Policy

- Intended for medical records
 - Conflict of interest not critical problem
 - Patient confidentiality, authentication of records and annotators, and integrity are
- Entities:
 - Patient: subject of medical records (or agent)
 - Personal health information: data about patient's health or treatment enabling identification of patient
 - Clinician: health-care professional with access to personal health information while doing job

23 September 2008

Winsborough CS 5323 Lecture 7

17

Assumptions and Principles

- Assumes health information involves 1 person at a time
 - Not always true; OB/GYN involves father as well as mother
- Principles derived from medical ethics of various societies, and from practicing clinicians

23 September 2008

Winsborough CS 5323 Lecture 7

18

Access

- Principle 1: Each medical record has an access control list naming the individuals or groups who may read and append information to the record. The system must restrict access to those identified on the access control list.
 - Idea is that clinicians need access, but no-one else. Auditors get access to copies, so they cannot alter records

23 September 2008

Winsborough CS 5323 Lecture 7

19

Access

- Principle 2: One of the clinicians on the access control list must have the right to add other clinicians to the access control list.
 - Called the *responsible clinician*

23 September 2008

Winsborough CS 5323 Lecture 7

20

Access

- Principle 3: The responsible clinician must notify the patient of the names on the access control list whenever the patient's medical record is opened. Except for situations given in statutes, or in cases of emergency, the responsible clinician must obtain the patient's consent.
 - Patient must consent to all treatment, and must know of violations of security

23 September 2008

Winsborough CS 5323 Lecture 7

21

Access

- Principle 4: The name of the clinician, the date, and the time of the access of a medical record must be recorded. Similar information must be kept for deletions.
 - This is for auditing. Don't delete information; update it (last part is for deletion of records after death, for example, or deletion of information when required by statute). Record information about all accesses.

23 September 2008

Winsborough CS 5323 Lecture 7

22

Creation

- Principle: A clinician may open a record, with the clinician and the patient on the access control list. If a record is opened as a result of a referral, the referring clinician may also be on the access control list.
 - Creating clinician needs access, and patient should get it. If created from a referral, referring clinician needs access to get results of referral.

23 September 2008

Winsborough CS 5323 Lecture 7

23

Deletion

- Principle: Clinical information cannot be deleted from a medical record until the appropriate time has passed.
 - This varies with circumstances.

23 September 2008

Winsborough CS 5323 Lecture 7

24

Confinement

- Principle: Information from one medical record may be appended to a different medical record if and only if the access control list of the second record is a subset of the access control list of the first.
 - This keeps information from leaking to unauthorized users. All users have to be on the access control list.

23 September 2008

Winsborough CS 5323 Lecture 7

25

Aggregation

- Principle: Measures for preventing aggregation of patient data must be effective. In particular, a patient must be notified if anyone is to be added to the access control list for the patient's record and if that person has access to a large number of medical records.
 - Fear here is that a corrupt investigator may obtain access to a large number of records, correlate them, and discover private information about individuals which can then be used for nefarious purposes (such as blackmail)

23 September 2008

Winsborough CS 5323 Lecture 7

26

Enforcement

- Principle: Any computer system that handles medical records must have a subsystem that enforces the preceding principles. The effectiveness of this enforcement must be subject to evaluation by independent auditors.
 - This policy has to be enforced, and the enforcement mechanisms must be auditable (and audited)

23 September 2008

Winsborough CS 5323 Lecture 7

27

Compare to Bell-LaPadula

- Confinement Principle imposes lattice structure on entities in model
 - Similar to Bell-LaPadula
- CISS focuses on objects being accessed; BLP on the subjects accessing the objects
 - May matter when looking for insiders in the medical environment

23 September 2008

Winsborough CS 5323 Lecture 7

28

Compare to Clark-Wilson

- CDIs are medical records
- TPs are functions updating records, access control lists
- IVPs certify:
 - A person identified as a clinician is a clinician;
 - A clinician validates, or has validated, information in the medical record;
 - When someone is to be notified of an event, such notification occurs; and
 - When someone must give consent, the operation cannot proceed until the consent is obtained
- Auditing (CR4) requirement: make all records append-only, notify patient when access control list changed

23 September 2008

Winsborough CS 5323 Lecture 7

29