CS 591: Introduction to Computer Security

Lecture 6: Identity and Data Mining

James Hook

(Some material from Bishop, 2004)

4/16/09 21:17

Topics

- Clark-Wilson
- Identity
- Data mining

Clark Wilson Model

“Essentially, there are two mechanisms at the heart of fraud and error control: the well-formed transaction, and separation of duty among employees.”

A Comparison of Commercial and Military Computer
Security Policies, Clark and Wilson, 1987

CW Criteria

1. The system must separately authenticate and identify every user
2. The system must ensure that specified data items can be manipulated only by a restricted set of programs
3. The system must associate with each user a valid set of programs to be run (controls must ensure .. Separation of duty)
4. System must maintain an auditing log that records every program executed and the name of the authorizing user

Additional Criteria

1. System must contain mechanisms to ensure that the system enforces is requirements
2. System must be protected against tampering or unauthorized change.

Clark-Wilson Integrity Model

- Integrity defined by a set of constraints
  - Data in a *consistent* or valid state when it satisfies these
- *Well-formed transaction* move system from one consistent state to another
- Issue: who examines, certifies transactions done correctly?

Entities

- CDIs: constrained data items
  - Data subject to integrity controls
- UDIs: unconstrained data items
  - Data not subject to integrity controls
- IVPs: integrity verification procedures
  - Procedures that test the CDIs conform to the integrity constraints
- TPs: Transformation procedures
  - Procedures that take the system from one valid state to another

Certification Rules 1 and 2

CR1 When any IVP is run, it must ensure all CDIs are in a valid state

CR2 For some associated set of CDIs, a TP must transform those CDIs in a valid state into a (possibly different) valid state

- Defines relation *certified* that associates a set of CDIs with a particular TP
- Example: TP balance, CDIs accounts, in bank example

Enforcement Rules 1 and 2

ER1 The system must maintain the certified relations and must ensure that only TPs certified to run on a CDI manipulate that CDI.

ER2 The system must associate a user with each TP and set of CDIs. The TP may access those CDIs on behalf of the associated user. The TP cannot access that CDI on behalf of a user not associated with that TP and CDI.

- System must maintain, enforce certified relation
- System must also restrict access based on user ID (*allowed* relation)

Users and Rules

CR3 The allowed relations must meet the requirements imposed by the principle of separation of duty.

ER3 The system must authenticate each user attempting to execute a TP

- Type of authentication undefined, and depends on the instantiation
- Authentication *not* required before use of the system, but *is* required before manipulation of CDIs (requires using TPs)

Logging

CR4 All TPs must append enough information to reconstruct the operation to an append-only CDI.

- This CDI is the log
- Auditor needs to be able to determine what happened during reviews of transactions

Handling Untrusted Input

CR5 Any TP that takes as input a UDI may perform only valid transformations, or no transformations, for all possible values of the UDI. The transformation either rejects the UDI or transforms it into a CDI.

- In bank, numbers entered at keyboard are UDIs, so cannot be input to TPs. TPs must validate numbers (to make them a CDI) before using them; if validation fails, TP rejects UDI

Separation of Duty In Model

ER4 Only the certifier of a TP may change the list of entities associated with that TP. No certifier of a TP, or of an entity associated with that TP, may ever have execute permission with respect to that entity.

- Enforces separation of duty with respect to certified and allowed relations

Discussion

- How can we apply CW to Voting Machine?
  - Constrained Data Items:
  - Integrity Constraints:
  - Unconstrained Data Items:
  - Transaction Procedures:
  - Integrity Verification Procedures:

Constrained Data Items:

- Boot loader
- Operating System and Trusted Applications
- Voting Application
- Ballot Definition
- Vote Tally
- Completed Ballot

Integrity constraints:

- New images of the boot loader, OS, Trusted Applications, and Voting Applications must include a certificate of origin signed by a trusted party. The certificate must include a message digest of the image.
- The OS, Trusted Applications, and Voting Applications must pass an integrity check based on their certificate of origin before being executed.
- The Ballot Definition must be signed digitally by an election official distinct from the official operating the voting machine.

Transaction processes (TPs):

- Update Boot Loader
- Update OS and Trusted Applications
- Update Voting Application
- Define Ballot
- Start Election
- End Election
- Vote

Comparison to Biba

- Biba
  - No notion of certification rules; trusted subjects ensure actions obey rules
  - Untrusted data examined before being made trusted
- Clark-Wilson
  - Explicit requirements that *actions* must meet
  - Trusted entity must certify *method* to upgrade untrusted data (and not certify the data itself)

Sources

- News stories on Surveillance
  - NY Times article on NSA spying, Dec 2005, http://www.commondreams.org/headlines05/1216-01.htm
  - USA Today article on NSA phone records, May 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm
- Readings on Telephone Fraud detection
  - Gary M. Weiss (2005). Data Mining in Telecommunications. http://storm.cis.fordham.edu/~gweiss/papers/kluwer04-telecom.pdf
  - Corinna Cortes, Daryl Pregibon and Chris Volinsky, "Communities of Interest", http://homepage.mac.com/corinnacortes/papers/portugal.ps
- Anderson 20 and 24 (17 and 21 in 1st edition)

Identity

- Mapping from abstract subjects and objects to real people and things

Principal

- A *principal* is a unique entity
- An *identity* specifies a principal
- Authentication binds a principal to a representation of identity internal to a computer system

Uses of Identity

- Access Control
- Accountability

Unix Users

- UNIX uses UID (User identification number) for Access Control
- UNIX uses Username for Accountability
- Users provide a username and password to authenticate
- Password file maps usernames to UIDs
- Common for one principal to have multiple usernames (and UIDs)

Object identity

- Object sharing
- E.g. unix files
  - file names map to inodes
  - inodes map to “real” files

Identity in distributed systems

jghook@pdx.edu	PSU OIT	windows boxes across campus
hook@cs.pdx.edu	PSU CS	unix boxes in CS department
hook@linux.cecs.pdx.edu	PSU MCECS/CAT	linux boxes in Engineering
hook@beethoven.cs.pdx.edu	laptop (owned by PSU)	user administered laptop

Phone Systems

- Phone fraud
  - Attacks on metering
  - Attacks on signaling
  - attacks on switching and configuration
  - insecure end systems
    - dial-through fraud
  - feature interaction

Fraud detection problem

- Subscription fraud
  - customer opens account with the intention of never paying
- Superimposition fraud
  - legitimate account; some legitimate activity
  - illegitimate activity “superimposed” by a person other than the account holder

Fraud detection as identity

- Both Subscription fraud and superimposition fraud are asking if we can identify a principal by their behavior (and without their cooperation)

Communities of Interest

- On the telephone you are who you call
- Coretes, Pregibon and Volinsky paper
  - use “top 9 lists” of ingoing and outgoing calls to characterize a user’s Community of Interest (COI)
  - Define Overlap of two COIs to be a distance measure
- Overlap is highly effective at identifying fraudsters
  - “Record Linkage Using COI-based matching”
- NB: Application not limited to phone networks

Phone Fraud

- Where does the data come from?
- Phone switches generate call detail records (Weiss paper)
- These records can be harvested to yield CPV’s top 9 lists
  - Hancock is a DSL for writing code to read large volumes of data

Telephone fraud detection

- Historically, COI-based matching is used to detect a deadbeat customer who has assumed a new network identity
- Is this a legitimate business use?
- Is there a potential privacy issue?
- Discuss potential abuses

Credit Card Fraud detection

- Credit Card companies have done nearly real-time analysis of card usage
- Anomalies are flagged; card holder is contacted
- Customers have come to expect this service
  - It is considered a protection and an added value
- Discuss:
  - Abuse potential
  - Does government have a role? Why or why not?

NY Times Story

- Revealed content of international phone calls between “persons of interest” were monitored outside of FISA
  - What not use FISA?
  - What if identity is a surrogate, not a name?
- [Note: I don’t know if the COI papers and the news stories reference in this lecture are related.]

USA Today Story

- Several telephone companies providing call detail data to NSA
- “Largest database ever”
- Asserts no content being monitored
- Discussion/Conjecture:
  - What if they are calculating COI? Or COI-like data?
  - Could this serve as the source of the “surrogate identities” used for non-FISA wiretaps
  - If it is reasonable for business to use this technology for fraud detection is it reasonable for the government to exploit it as well?
  - What other personal information could be obtained from this data?

US Constitution
Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Discussion

- Is a COI a sufficient description to meet the requirement:
  - particularly describing the place to be searched, and the persons or things to be seized