CS 591: Introduction to Computer Security

Lecture 5: Identity, Fraud, and Data Mining

James Hook

10/18/10 16:39

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

Anderson Chapter 10

- Banking and Bookkeeping
  - Long history
  - Strong motivation for fraud
  - Early adoption of computing technology

Integrity

- Double-entry bookkeeping
  - At least 12th Century Cairo
- Two separate books
  - Each transaction recorded in both, one as credit one as debit

Example

- XYZ sells Amy $100 of widgets on credit
  - Posts:
    - +$100 to Sales
    - -$100 to Receivables
- Amy pays $100 on account
  - Posts
    - +$100 to Receivables
    - -$100 to Cash
  - “Debit the receiver, credit the giver”

Double-Entry

- Books are kept by different clerks
- Balanced periodically (daily; monthly)
- Designed so that each shop, branch balanced separately
- Fraud requires collusion of two or more staff
- Dual control provided by audit (periodic and random)

Clark-Wilson in context

RA’s CW criticisms

- Maintains state
  - Problematic for partially completed transactions
  - Mixes user state and security state
- Doesn’t do everything
  - Preserves invariants, but “ok” to deposit in wrong account
- Duck’s “hardest question”
  - How do we control dishonest staff

Designing “Internal Controls”

- Can you say “banking crisis”?
- “It’s also important to check that [the books] correspond to external reality. That was brought home … turned out that 20% of the recorded assets and inventory were nonexistent”

Separation of Duty policy

- Dual control
  - Two or more staff members must act together to authorize a transaction
- Functional separation of duties
  - Two or more staff members act on a transaction at different points in its path

Objective

- Prevent – Detect – Recover
- Timing, risks, costs suggest balance of these “legs”

Risks

- Too many sysadmins

War Stories

- Password reset clerk makes new password for AT&T, transfers $20M to offshore companies
- Suspense accounts used in rotation to avoid audit trigger (employee not taking required vacations)
- Invented fictitious school
- Insider notices address changes not audited; sends self ATM card and PIN for idle account

Volume Crime

- Subject to incentives of liability rules
- Auditors also problem (Arthur Andersen failure)

Eroding controls

- “Changing technology also has a habit of eroding controls, which therefore need constant attention and maintenance.”

RA “lessons learned”

- It’s not always obvious which transactions are security sensitive
- Maintaining a working security system can be hard in the face of a changing environment
- If you rely on customer complaints to alert you to fraud, you had better listen to them
- there will always be people in positions of relative trust who can get away with a scam for a while

RA lessons (cont)

- No security policy will ever be completely rigid. There will always have to be workarounds…
- These workarounds naturally create vulnerabilities. So the lower the transaction error rate, the better

ATMs

- Over 1,500,000 machines world wide
- Excellent discussion of mechanisms in text

ATM discussion

- “The engineers … assumed that criminals would be relatively sophisticated, fairly well-informed about the system design, and rational in their choice of attack methods. … agonized over … encryption algorithms … tamper resistance … random number generators …”

Phantom withdrawls

- Simple processing errors
  - Even with an error rate of 1 in 10k to 1 in 100k you get a lot of disputes
- Thefts in the mail
  - 30% of all UK card losses
- Frauds by bank staff
  - Not investigated if customer paid fraudulent charges

Discussion

- “These failures are all very much simpler and more straightforward than the ones we’d worried about.”

- “the first thing we did wrong … was to worry about criminals being clever, when we should rather have worried about our customers [banks] … being stupid”
- “… as correspondingly little attention is paid to the ‘boring’ bits such as training, usability, standards, and audit, it’s rare that the bad guys have to break the crypto to compromise a system.”