CS 591: Introduction to Computer Security

Lecture 3: Policy

James Hook

10/20/07 14:33

Objectives

- Explore what a security policy is;
  develop a vocabulary to discuss policies
- Examine the role of trust in policy

What is a Security Policy?

- Statement that articulates the security goal
- In the state machine model it identifies the *authorized* or *secure* states (which are distinct from the *unauthorized* or *nonsecure* states)
- A *secure system* is one in which the system can only enter authorized states
  - Note: The policy doesn't make the system secure; it defines what secure is

Confidentiality

- *X*: set of entities
- *I*: some information
- *I* has the property of *confidentiality* with respect to *X* if no member of *X* can obtain information about *I*

- What is information?

Confidentiality Scenario

- If an instructor wishes to keep class grades confidential from the students which of the following can the instructor do?
  - – Email the grade file to the class mailing list
  - – Email an encrypted grade file to the class mailing list
  - – Email summary statistics (mean, median, max, and min) to the class mailing list
- What is information? What is data?

Integrity

- *Bishop:*
  - *X*, *I* as before
  - *I* has the property of *integrity* with respect to *X* if all members of *X* trust *I*
- Dictionary (http://www.m-w.com/dictionary/integrity)
  - 1 : firm adherence to a code of especially moral or artistic values : INCORRUPTIBILITY
  - 2 : an unimpaired condition : SOUNDNESS
  - 3 : the quality or state of being complete or undivided : COMPLETENESS

Integrity

- If Alice and Bob trust their horoscopes do horoscopes have integrity?
- What about their elected representatives?
- Does this definition imply that “anything’s legal as long as you don’t get caught” [Traveling Wilburys; *Tweeter and the Monkey Man*]
- If the users of a system trust the file system does it have integrity?
- Is it reasonable for integrity to be an extrinsic property?

Assurance

- Assurance aims to provide intrinsic evidence of integrity
- We trust the integrity of the bank because we intrinsically trust the accounting practices used by banks
- We also trust the bank because
  - The bank is audited for compliance with these trusted practices
  - The bank’s data is scrutinized for signatures of fraud

Integrity

- Although we may desire an intrinsic notion of integrity we must accept an extrinsic notion in the general case
- If we do not have intrinsic assurance the best we can demand is that no agent can refute integrity

Availability

- Let *X* be a set of entities, *I* a resource
- *I* has the property of *availability* with respect to *X* if all members of *X* can access *I*

- What is access?
- Quality of service is not always binary

Setting the bar on access

- Organizational context is critical
- For a person, access sufficient to perform their job function
  - Avionics system: micro-/milli second (some military airframes are aerodynamically unstable; avionics system is required to keep them in the air)
  - Air Traffic control: 100s of milliseconds
  - Airline reservations: 10s of seconds
  - [These numbers are notional]

Access and Quality of Service

- Behavior of service under load may be important
  - Graceful degradation
  - QoS threshold
- When is it better to do a few things quickly than all things slowly?

Dimensions of Policy

- Policy defines security objective:
  - Confidentiality: Protect Information and Resources *I* from *X*
  - Integrity: …in a manner trusted by *Y*
  - Availability: …to be accessible to *Z*

- Mechanisms can be evaluated to determine if they help meet the objective

Does this model match reality?

- Recall PSU AUP
- What facets focus on
  - Confidentiality: what is I? who/what is X?
  - Integrity: I? X?
  - Availability: I? X?
- What facets are outside of this model?

PSU Computer & Network Acceptable Use Policy

- This acceptable use policy governs the use of computers and networks at Portland State University (PSU). As a user of these resources, you are responsible for reading and understanding this document. …
- Portland State University encourages the use and application of information technologies to support the research, instruction, and public service mission of the institution. PSU computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

PSU AUP (cont)

- ***Acceptable use terms and conditions:***
  - The primary purpose of electronic systems and communications resources is for University-related activities only.
  - Users do not own accounts on University computers, but are granted the privilege of exclusive use. Users may not share their accounts with others, and must keep account passwords confidential.
  - Each account granted on a University system is the responsibility of the individual who applies for the account. Groups seeking accounts must select an individual with responsibility for accounts that represent groups.
  - The University cannot guarantee that messages or files are private or secure. The University may monitor and record usage to enforce its policies and may use information gained in this way in disciplinary and criminal proceedings.
  - Users must adhere strictly to licensing agreements and copyright laws that govern all material accessed or stored using PSU computers and networks.
  - When accessing remote systems from PSU systems, users are responsible for obeying the policies set forth herein as well as the policies of other organizations.
  - Misuse of University computing, networking, or information resources may result in the immediate loss of computing and/or network access. Any violation of this policy or local, state, or federal laws may be referred to appropriate University offices and/or, as appropriate, law enforcement authorities.

PSU AUP (cont)

- ***Conduct which violates this policy includes, but is not limited to the following:***
  - Unauthorized attempts to view and/or use another person's accounts, computer files, programs, or data.
  - Using PSU computers, accounts, and/or networks to gain unauthorized access to University systems or other systems.
  - Using PSU computers, accounts, and/or networks for: threat of imminent physical harm, sexual or other harassment, stalking, forgery, fraud, generally offensive conduct, or any criminal activity.
  - Attempting to degrade performance of University computers and/or networks.
  - Attempting to deprive other users of University technology resources or access to systems/networks.
  - Using University resources for commercial activity such as creating products or services for sale.
  - Copying, storing, sharing, installing or distributing software, movies, music, and other materials currently protected by copyright, except as permitted by licensing agreements or fair use laws.
  - Unauthorized mass e-mailings to newsgroups, mailing lists, or individuals, i.e. "spamming" or propagating electronic chain letters.
  - Unauthorized "broadcasting" of unsolicited mail, material, or information using University computers/networks.

Policies and the world

- What about
  - Obey the law
  - Organizational consequences

Policy model vs reality

- Consider password policies (e.g. Sans model policy http://www.sans.org/resources/policies/)
- What dimension of security do password polices primarily address?

Policy informed by experience

- Most organizations have a policy that has evolved
- Reflects understanding of threat environment (or at least threat history)
- Can reveal critical assumptions

Policy vs. Mechanism

- Policy says what is allowed and what isn’t
- Mechanism is an entity or procedure that enforces some part of the policy
- Discuss
  - List some mechanisms
  - Facets of policy for which mechanisms are appropriate
  - Facets of policy for which mechanisms are unlikely to be appropriate

Security Model

- A security model is a model that represents a particular policy or set of policies
- Abstracts from the policy
  - We will see various security models:
  - Bell LaPadula for Confidentiality
  - Clark-Willson Integrity
  - Chinese Wall Model

Families of Policies

- Military Security Policy (Governmental)
  - Primary goal: confidentiality
- Commercial Security Policy
  - Primary goal: integrity
  - Common mechanism: transactions; transaction-oriented integrity security policies
  - When you buy a book from Amazon you want to get exactly what you ordered and pay for it exactly once

Assumptions and Trust

- All policies have assumptions
- Typically something is trusted:
  - Hardware will faithfully execute the program
  - Patch is uncorrupted from vendor
  - Vendor tested patch appropriately
  - Vendor’s environment similar to system being patched
  - Patch is installed correctly

Trust

- What are some assumptions of
  - the PSU AUP?
  - The sans password policy?

Access Control

- Discretionary Access Control (DAC)
  - An individual user can set allow or deny access to an object
- Mandatory Access Control (MAC)
  - System mechanism controls access
  - User cannot alter that access
- Originator Controlled Access Control (ORCON)
  - Access control set by creator of information
  - Owner (if different) can't alter AC
    - Like copyright

Conclusions

- Policy declares security goal
- Policy can be understood in terms of security components:
  - Confidentiality
  - Integrity
  - Availability
- Policy is based on assumptions about the environment
- It is critical to understand what entitie the policy "trusts"

Looking Forward

- Bell-LaPadula Model
  - Military style classification of information
  - Confidentiality
  - Reading:
    - Bishop: Chapter 5 (start 6 as well)
    - RA: Chapter 7
- Background
  - What is a lattice?
  - Reading: Chapter 27

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.

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?

Telephone

- Phone companies have collected “call detail data” for a long time
- Analyze data to build customer profiles
- One useful technique is the “Community of interest”
  - Top k callers in period of study (k is usually 9)
  - Can define a metric on communities
  - Tends to provide a good surrogate for identity (“Record Linkage Using COI-based matching”)

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

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?

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?