CS 591: Introduction to Computer Security

Lecture 3: History and Policy

James Hook

Discussion

- NY Times article on Information Warfare
- Nagaraja and Anderson tech report

Discussion Questions

- What is the historical context of the conflict between China and the Dalai Lama?
- Where is Tibet?
- Where is the Tibetan government in exile located?
- How does China regard Tibet? What is the Chinese attitude toward Tibetan language education in Tibet?

Discussion

- Nagaraja and Anderson apply NATO practice to label documents within OHHDL as Confidential, and Secret. What criteria do they use for classification?
- Prior to detection of the attacks, what threats was OHHDL concerned about?
- How did OHHDL learn it was under attack?
- Is it likely that this security failure led to loss of life?

Discussion

- How was the first computer compromised?
- How might this have been avoided?
- What are the conflicts between secure operational practice and the institutional mission of OHHDL?

Is Information Warfare News?

- What is Information Warfare?
- Is information warfare new?
- Why is this newsworthy?

Military Security

- Protection of information has been part of warfare throughout recoded history
- "World War II and the Cold War led to a common protective marking scheme for … documents" [Ross Anderson 8.3.1]
  - Top Secret (many lives lost)
  - Secret (lives lost)
  - Confidential (operational failure)
  - Open

Batch Computing

- Early computers were simple, small machines, with little persistent state
- To run a job for a user, an operator would:
  - Mount the removable media (disks and tapes) requested by the user
  - Completely initialize the computer by pressing an "Initial Program Load" button that read the boot loader from the card deck supplied by the user
  - Execute the operating system loaded by the boot loader, found on the removable media

Secure batch computing

- To make this style of batch computing secure it was only necessary to focus on
  - the physical security of the room,
  - insure that the state was initialized, and
  - handle all removable media according to the rules for handling classified documents

Cold War Computing

- The cold war relied on aircraft capable of dropping nuclear bombs
- Aircraft need to know about weather
- Global weather prediction was one of the most important computational tasks in the cold war

Computers Communicate

- Weather prediction needs input from weather stations
- The batch model of military computing had to be abandoned
- The security perimeter of the weather prediction system was no longer the computer room

Practice beyond Policy

- The weather system evolved to collect data from around the globe and give reports to pilots at Strategic Air Command centers
- Recognizing that this practice was outside of policy doctrine, the Air Force commissioned a study on Computer Security
- James P. Anderson wrote the report: Computer Security Technology Planning Study (1972)

Anderson's study

- Forward looking study focused on driving forces:
  - Time shared computing
  - Communication and Networking

2.3 Requirements Trends and Security Problems

The primary security related operational requirements noted by the users were:

a. Online Multilevel Secure Operation (AFLC, AFDSC, NORAD, AFGWC, SAC, MAC, ECAC)

b. Open Operation (AFDSC, MAC, ECAC, AFGWC)

c. Transaction Systems (AFLC, MAC)

d. General Programming (AFLC, AFDSC, NORAD, AFGWC, SAC, MAC, ECAC)

e. Networks (all)

Air Force Logistics Command	(AFLC)
Air Force Data Services Center	(AFDSC)
Satellite Control Facility	(SAMSO)
NORAD/Aerospace Defense Command	(NORAD)
Air Force Communications Service	(AFCS)
Air Force Global Weather Center	(AFGWC)
Strategic Air Command	(SAC)
Air Force Security Service	(AFSS)
Military Air Lift Command	(MAC)
Electronic Compatibility Analysis Center	(ECAC)

Anderson on networks

The security condition of networks is even less structured than that of most applications. Computer networks that have one or more nodes that can be accessed by users with clearances below the highest level of information in the network, constitute multilevel networks. The security threat posed by such operations is that, in general, the computer to computer communications are accepted as valid on the questionable basis that the other computer has a high security reliability. However, if control of a node can be exercised by a malicious users, the entire network may be compromised. While there are growing requirements for interconnecting computer systems into networks and several networks (Air Weather Network, 465L SACCS, BUIC, and AUTODIN) already exist, the dimensions of the security problem are unknown. More information is needed on both the networks and their security requirements. For this reason we are recommending that network security be included in the exploratory development program.

The Insider Threat

3.1 Requirements For Defense Against a Malicious User

Until now, the principal threat has been seen to be an external penetration. The primary defense against external penetration has been that of preventing access to any part of the system or its data. The malicious user concept on the other hand has bypassed this form of defense by assuming that the malicious user has legitimate access to a system. Taken in the context of open use systems with general program-

The Handbook

The handbook of computer security techniques is envisioned as a collection of system design, implementation, and operation practices covering all aspects of computer security from techniques of user identification through methods of program validation to recommended security policy, practices and procedures in the operation of secure systems. It is intended for use by designers and developers of USAF information systems. Because of anticipated changes in this technology, the handbook should be maintained throughout the indefinite future.

DoD Security Research

- With publication of Anderson's report significant research funds were allocated to Computer Security
- Two goals:
  - Solve aspects of the Security Problem as articulated by Anderson
  - Give guidance to military procurement officers on how to acquire secure computing systems

DoD Research dominates '70's

- Although not all security challenges were related to defense, defense sponsored research dominates publications in 70's and 80's
- In that period Confidentiality was stressed
- The neglect of Availability would bite on September 11, 2001

Policy

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

- Protection of information from a set of principles
- Anderson's use is somewhat non-standard
  - Secrecy: … mechanisms used to limit the … principals who can access information …
  - Confidentiality: … obligation to protect ... other's … secrets …
  - Privacy: … ability and/or right to protect your personal information … and/or to prevent invasions of your personal space …

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

- 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 the users of a system trust the file system does it have integrity?
- Is it reasonable for integrity to be based on user perception?
- If the public loses confidence in voting machines can even a perfect DRE machine have integrity?

Assurance

- Assurance aims to provide intrinsic evidence of integrity
- We trust the integrity of the bank because we 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 the perception of trust in the general case
- If we do not have intrinsic assurance the best we can demand is that no agent can refute integrity

Availability

- A resources is available to a set of principles if they can access it to perform their mission
- 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]

Availability failure

- Operation Redwing in Afghanistan
- Navy SEALS in trouble had secure radios fail
- Ultimately shot while using cell phone to call for help
- End result:

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 Policies

- 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:
    - Bell retrospective
    - Bishop: Chapter 5 (start 6 as well)
    - RA: Chapter 8
- Background
  - What is a lattice?
  - Reading: Chapter 27