Lecture for January 25, 2016

ECS 235A

UC Davis

Matt Bishop

Example English Policy

- Computer security policy for academic institution
  - Institution has multiple campuses, administered from central office
  - Each campus has its own administration, and unique aspects and needs
- Deals with electronic communications
  - Policy
  - User Advisories
  - Implementation at University of California Davis

Background

- University of California
  - 10 campuses (including UC Davis), each run by a Chancellor
  - UC Office of the President (UCOP) runs system, and is run by President of University of California
- UCOP issues policies that apply to all campuses
- Campuses implement the policy in a manner consistent with directions from UCOP

Electronic Communications Policy

- Begins with purpose, to whom policy applies
  - Includes email, video, voice, other means
  - Not to printed copies of communications
  - Not to Dept. of Energy labs that UC manages, or to Dept. of Energy employees
- Gives general implementation guidelines

Use of Electronic Communications

- University does *not* want to deal with contents of these!
  - But all communications relating to University administration are public records
  - Others may be too
- Allowable users
  - Faculty, staff, students, others associated with UC
  - Others authorized by the Chancellors or UCOP
  - Others participating in programs UC sponsors

Allowable Uses

- University business
  - Classes, research, *etc*.
- Incidental personal use OK
  - But can’t interfere with other uses
- Anonymous communications OK
  - But can’t use a false identity

Non-Allowable Uses

- Endorsements not OK
- Running personal businesses not OJK
- Illegal activities not OK
  - Must respect intellectual property laws, US DMCA
- Violating University of campus policies or rules not OK
- Users can't put "excessive strain" on resources
  - No spamming, DoD or DDoS attacks

Privacy, Confidentiality

- General rule: respected the same way as is for paper
- Cannot read or disclose without permission of holder, except in specific circumstances
- To do so requires written permission of:
  - A designated Vice Chancellor (campus)
  - A Senior Vice President, Business and Finance (UCOP)

Privacy, Confidentiality

- Written permission not required for:
  - Subpoena or search warrant
  - Emergency
    - But must obtain approval as soon as possible afterwards
  - In all these cases, must notify those affected by the disclosure that the disclosure occurred, and why

Limits of Privacy

- Electronic communications that are public records will not be confidential
- Electronic communications may be on backups
- Electronic communications may be seen during routine system monitoring, etc.
  - Admins instructed to respect privacy, but *will* report "improper governmental activity"

Security Services, Practices

- Routine monitoring
- Need for authentication
- Need for authorization
- Need for recovery mechanisms
- Need for audit mechanisms
- Other mechanisms to enforce University policy

User Advisories

- These are less formal, give guidelines for the use of electronic communications
  - Show courtesy and consideration as in non-electronic communications
  - Laws about privacy in electronic communications are not as mature as laws about privacy in other areas
  - University provides neither encryption nor authentication
    - Easy to falsify sender

UC Davis Implementation

- Acceptable Use Policy
  - Incorporates the UCD Principles of Community
  - Requires respect of rights of others when using electronic communications
  - Use encouraged for education, university business, university-related activities

UC Davis Implementation

- UC Davis specific details
  - Only Chancellor-approved charitable activities may use these resources
  - Cannot be used to create hostile environment
    - This includes violating obscenity laws
  - Incidental personal use OK under conditions given in Electronic Communications Policy

UC Davis Implementation

- Unacceptable conduct
  - Not protecting passwords for University resources
  - Not respecting copyrights, licenses
  - Violating integrity of these resources
  - Creating malicious logic (worms, viruses, *etc*.)
    - Allowed if done as part o an academic research or instruction program supervised by academic personnel; and
    - It does not compromise the University's electric communication resource

UC Davis Implementation

- Allowed users
  - UCD students, staff, faculty
  - Other UCD academic appointees and affiliated people
    - Such as postdocs and visiting scholars
- People leaving
  - Forwarding email allowed
  - Recipient must agree to return to the University any email about University business

Exceptions Allowing Disclosure

- Required by law;
- Reliable evidence of violation of law, University policies;
- Failure to do so may result in:
  - Significant harm
  - Loss of significant evidence of violations;
  - Significant liability to UC or its community;
- Not doing so hampers University meeting administrative, teaching obligations

Confidentiality Policy

- Goal: prevent the unauthorized disclosure of information
  - Deals with information flow
  - Integrity incidental
- Multi-level security models are best-known examples
  - Bell-LaPadula Model basis for many, or most, of these

Bell-LaPadula Model, Step 1

- Security levels arranged in linear ordering
  - Top Secret: highest
  - Secret
  - Confidential
  - Unclassified: lowest
- Levels consist of *security clearance* $L(s)$
  - Objects have *security classification* $L(o)$

Example

security level	*subject*	*object*
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	Ulaley	Telephone Lists

- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- Ulaley can only read Telephone Lists

Reading Information

- Information flows *up*, not *down*
  - "Reads up" disallowed, "reads down" allowed
- Simple Security Condition (Step 1)
  - Subject s can read object o iff $L(o) \le L(s)$ and s has permission to read o
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called *no reads up rule*

Writing Information

- Information flows up, not down
  - "Writes up" allowed, "writes down" disallowed
- *-Property (Step 1)
  - Subject *s* can write object *o* iff $L(s) \le L(o)$ and *s* has permission to write *o*
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Sometimes called *no writes down rule*

Basic Security Theorem, Step 1

- If a system is initially in a secure state, and every transition of the system satisfies the simple security condition, step 1, and the *-property, step 1, then every state of the system is secure
  - Proof: induct on the number of transitions

Bell-LaPadula Model, Step 2

- Expand notion of security level to include categories
- Security level is (*clearance*, *category set*)
- Examples
  - (Top Secret, { NUC, EUR, ASI })
  - (Confidential, { EUR, ASI })
  - (Secret, { NUC, ASI })

Levels and Lattices

- (A, C) *dom* (A', C') iff $A' \leq A$ and $C' \subseteq C$
- Examples
  - (Top Secret, {NUC, ASI}) *dom* (Secret, {NUC})
  - (Secret, {NUC, EUR}) *dom* (Confidential,{NUC, EUR})
  - (Top Secret, {NUC}) $\neg$*dom* (Confidential, {EUR})
- Let C be set of classifications, K set of categories. Set of security levels $L = C \times K$, *dom* form lattice
  - $lub(L) = (max(A), C)$
  - $glb(L) = (min(A), \emptyset)$

Levels and Ordering

- Security levels partially ordered
  - Any pair of security levels may (or may not) be related by *dom*
- "dominates" serves the role of "greater than" in step 1
  - "greater than" is a total ordering, though

Reading Information

- Information flows *up*, not *down*
  - "Reads up" disallowed, "reads down" allowed
- Simple Security Condition (Step 2)
  - Subject *s* can read object *o* iff $L(s)$ *dom* $L(o)$ and *s* has permission to read *o*
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Again, sometimes called *no reads up rule*

Writing Information

- Information flows up, not down
  - "Writes up" allowed, "writes down" disallowed
- *-Property (Step 2)
  - Subject *s* can write object *o* iff $L(o)$ *dom* $L(s)$ and *s* has permission to write *o*
    - Note: combines mandatory control (relationship of security levels) and discretionary control (the required permission)
  - Again, sometimes called *no writes down rule*

Basic Security Theorem, Step 2

- If a system is initially in a secure state, and every transition of the system satisfies the simple security condition, step 2, and the *-property, step 2, then every state of the system is secure
  - Proof: induct on the number of transitions
  - In actual Basic Security Theorem, discretionary access control treated as third property, and simple security property and *-property phrased to eliminate discretionary part of the definitions — but simpler to express the way done here.

Problem

- Colonel has (Secret, {NUC, EUR}) clearance
- Major has (Secret, {EUR}) clearance
  - Major can talk to colonel ("write up" or "read down")
  - Colonel cannot talk to major ("read up" or "write down")
- Clearly absurd!

Solution

- Define maximum, current levels for subjects
  - *maxlevel*(*s*) *dom curlevel*(*s*)
- Example
  - Treat Major as an object (Colonel is writing to him/her)
  - Colonel has *maxlevel* (Secret, { NUC, EUR })
  - Colonel sets *curlevel* to (Secret, { EUR })
  - Now *L*(Major) *dom curlevel*(Colonel)
    - Colonel can write to Major without violating "no writes down"
  - Does *L*(*s*) mean *curlevel*(*s*) or *maxlevel*(*s*)?
    - Formally, we need a more precise notation

Principle of Tranquility

- Raising object's security level
  - Information once available to some subjects is no longer available
  - Usually assume information has already been accessed, so this does nothing
- Lowering object's security level
  - The *declassification problem*
  - Essentially, a "write down" violating *-property
  - Solution: define set of trusted subjects that *sanitize* or remove sensitive information before security level lowered

Types of Tranquility

- Strong Tranquility
  - The clearances of subjects, and the classifications of objects, do not change during the lifetime of the system
- Weak Tranquility
  - The clearances of subjects, and the classifications of objects, do not change in a way that violates the simple security condition or the *-property during the lifetime of the system

Declassification Principles

- Semantic consistency
  - As long as semantics of parts of system not involved in declassification do not change, they can be altered without affecting security of system
- Occlusion
  - Declassification operation cannot conceal *improper* lowering of security levels
  - *Robust declassification* property says attacker cannot use declassification channels to obtain information not properly declassified

Declassification Principles

- Conservativity
  - Absent any declassification, system is secure
- Monotonicity of release
  - When declassification done in an authorized manner by authorized subjects, system remains secure

Integrity Models

- Requirements
  - Very different than confidentiality policies
- Biba's model: Strict Integrity Policy
- Clark-Wilson model

Requirements of Policies

1. Users will not write their own programs, but will use existing production programs and databases.
2. Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.
3. A special process must be followed to install a program from the development system onto the production system.
4. The special process in requirement 3 must be controlled and audited.
5. The managers and auditors must have access to both the system state and the system logs that are generated.