ECS 235B, Lecture 5

January 16, 2019
Example: Take-Grant

• $\sigma_0 = G_0$
• $q$ is $can\cdot share(r, v_1, v_2, G_0)$
• $\tau$ is sequence of take-grant rules
• $\Pi$ is $\exists$
• Security analysis instance examines whether $v_1$ has $r$ rights over $v_2$ in graph with initial state $G_0$
• So safety question is security analysis instance
Comparing Two Models

• Each query in $A$ corresponds to a query in $B$
• Each (state, state transition) in $A$ corresponds to (state, state transition) in $B$

Formally:
• $A = (\Sigma^A, Q^A, e^A, T^A)$ and $B = (\Sigma^B, Q^B, e^B, T^B)$
• $mapping$ from $A$ to $B$ is:
  • $f : (\Sigma^A \times T^A) \cup Q^A \rightarrow (\Sigma^B \times T^B) \cup Q^B$
Image of Instance

• $f$ mapping from A to B

• *image of a security analysis instance*
  
  $(\sigma^A, q^A, \tau^A, \Pi)$ under $f$ is $(\sigma^B, q^B, \tau^B, \Pi)$,
  
  where:
  
  • $f((\sigma^A, \tau^A)) = (\sigma^B, \tau^B)$
  • $f(q^A) = q^B$

• $f$ is *security-preserving* if every security analysis instance in A is true iff its image is true
Composition of Queries

• Let \((\Sigma, Q, e, T)\) be an access control scheme

• Tuple \((\sigma, \varphi, \tau, \Pi)\) is compositional security analysis instance, where \(\varphi\) is propositional logic formula of queries from \(Q\)

• image of compositional security analysis instance defined similarly to previous

• \(f\) is strongly security-preserving if every compositional security analysis instance in \(A\) is true iff its image is true
State-Matching Reduction

• \( A = (\Sigma^A, Q^A, e^A, T^A) \), \( B = (\Sigma^B, Q^B, e^B, T^B) \), \( f \) mapping from \( A \) to \( B \)
• \( \sigma^A, \sigma^B \) equivalent under the mapping \( f \) when
  • \( e^A(\sigma^A, q^A) = e^B(\sigma^B, q^B) \)
• \( f \) state-matching reduction if for all \( \sigma^A \in S^A, \tau^A \in T^A \),
  \( (\sigma^B, \tau^B) = f((\sigma^A, \tau^A)) \) has the following properties:
Property 1

• For every state $\sigma^A$ in scheme $A$ such that $\sigma^A \mapsto^* \sigma'^A$, there is a state $\sigma'^B$ in scheme $B$ such that $\sigma^B \mapsto^* \sigma'^B$, and $\sigma'^A$ and $\sigma'^B$ are equivalent under the mapping $f$
  
  • That is, for every reachable state in $A$, a matching state in $B$ gives the same answer for every query
Property 2

• For every state $\sigma'^B$ in scheme $B$ such that $\sigma^B \mapsto^* \sigma'^B$, there is a state $\sigma'^A$ in scheme $A$ such that $\sigma^A \mapsto^* \sigma'^A$, and $\sigma'^A$ and $\sigma'^B$ are equivalent under the mapping $f$
  • That is, for every reachable state in $B$, a matching state in $A$ gives the same answer for every query
Theorem

Mapping $f$ from scheme $A$ to $B$ is strongly security-preserving iff $f$ is a state-matching reduction
Proof ($\iff$)

- Must show ($\sigma^A, \varphi^A, \tau^A, \Pi$) true iff ($\sigma^B, \varphi^B, \tau^B, \Pi$) true
- $\Pi$ is $\exists$: assume $\tau^A$-reachable state $\sigma'^A$ from $\sigma^A$ in which $\varphi^A$ true
  - By property 1, there is a state $\sigma'^B$ corresponding to $\sigma'^A$ in which $\varphi^B$ holds
- $\Pi$ is $\forall$: assume $\tau^A$-reachable state $\sigma'^A$ from $\sigma^A$ in which $\varphi^A$ false
  - By property 1, there is a state $\sigma'^B$ corresponding to $\sigma'^A$ in which $\varphi^B$ false
- Same for $\varphi^B$ with $\tau^B$-reachable state $\sigma'^B$ from $\sigma^B$
- So ($\sigma^A, \varphi^A, \tau^A, \Pi$) true iff ($\sigma^B, \varphi^B, \tau^B, \Pi$) true
Proof ($\iff$)

- Let $f$ be a map from $A$ to $B$ but not state-matching reduction. Then there are $\sigma^A \in S^A$, $\tau^A \in T^A$, $(\sigma^B, \tau^B) = f((\sigma^A, \tau^A))$ violating at least one of the properties.

- Assume it’s property 1; $\sigma^A, \sigma^B$ corresponding states. There is a $\tau^A$-reachable state $\sigma'^A$ from $\sigma^A$ such that no $\tau^B$-reachable state from $\sigma^B$ is equivalent to $\sigma'^B$.

- Generate $\varphi^A$ and $\varphi^B$ such that the existential compositional security analysis in $A$ is true but in $B$ is false.
  - To do this, look at each $q^A \in Q^A$.
  - If $e(\sigma'^A, q^A) = true$, conjoin $q^A$ to $\varphi^A$; otherwise, conjoin $\neg q^A$ to $\varphi^A$.
  - Then $e(\sigma'^A, q^A) = true$ but for $\varphi^B = f(\varphi^A)$ and all states $\sigma'^B$ that are $\tau^B$-reachable from $\sigma^B$, $e(\sigma'^B, q^B) = false$.

- Thus, $f$ is not strongly security-preserving.

- Argument for property 2 is similar.
Expressive Power

If access control model $MA$ has a scheme that cannot be mapped into a scheme in access control model $MB$ using a state-matching reduction, then model $MB$ is *less expressive than* model $MA$.

If every scheme in model $MA$ can be mapped into a scheme in model $MB$ using a state-matching reduction, then model $MB$ is *as expressive as* model $MA$.

If $MA$ is as expressive as $MB$, and $MB$ is as expressive as $MA$, the models are *equivalent*.

• Note this does not assume monotonicity, unlike earlier definition.
Augmented Typed Access Control Matrix

• Add a test for the *absence* of rights to TAM

command add\cdot right(s:u, o:v)

  if own in a[s,o] and r not in a[s,o]
  then
    enter r into a[s,o]
  end

• How does this affect the answer to the safety question?
Safety Question

• ATAM can be mapped onto TAM
• But will the mapping, or any such mapping, preserve security properties?
• Approach: consider TAM as an access control model
TAM as Access Control Model

• $S$ set of subjects; $S_\sigma$ subjects in state $\sigma$
• $O$ set of objects; $O_\sigma$ objects in state $\sigma$
• $R$ set of rights; $R_\sigma$ rights in state $\sigma$
• $T$ set of types; $T_\sigma$ subjects in state $\sigma$
• $t : S_\sigma \cup O_\sigma \rightarrow T_\sigma$ gives type of any subject or object
• State $\sigma$ defined as $(S_\sigma, O_\sigma, R_\sigma, T_\sigma, t)$
• In TAM, query is of form “is $r \in a[s,o]$”, and $e(s, r \in a[s,o])$ true iff $s \in S_\sigma$, $o \in O_\sigma$, $r \in R_\sigma$, $r \in a_\sigma[s,o]$ are true
ATAM as Access Control Model

Same as TAM with one addition:

• ATAM also allows queries of form “is $r \notin a[s,o]$”, and $e(s, r \notin a[s,o])$
  true iff $s \in S_\sigma$, $o \in O_\sigma$, $r \in R_\sigma$, $r \notin a_\sigma[s,o]$ are true
Theorem

A state-matching reduction from ATAM to Tam does not exist.

Outline of proof: by contradiction

• Consider two state transitions, one that creates subject and one that adds right \( r \) to an element of the matrix

• Can determine an upper bound on the number of answers to TAM query a command can change; depends on state and commands
Proof

- Assume $f$ is state-matching reduction from ATAM to TAM
- Consider simple ATAM scheme:
  - Initial state $\sigma_0$ has no subjects, objects
  - All entities have type $t$
  - Only one right $r$
  - Query $q_{ij} = r \in a[s,o]$; query $q_{ij} = r \notin a[s,o]$
  - 2 state transition rules
    - $\text{make} \cdot \text{subj}(s : t)$ creates subject $s$ of type $t$
    - $\text{add} \cdot \text{right}(x : t, y : t)$ adds right $r$ to $a[x, y]$
Proof

• TAM: superscript $T$ represents components of that system
  • So initial state is $\sigma_0^T = f(\sigma_0)$, transitions are $\tau^T = f(\tau)$
• By definition of state-matching reduction, how $f$ maps queries does not depend on initial state or state transitions of a model
• Let $p, q$ be queries in ATAM and $p^T, q^T$ the corresponding queries in TAM; if $p \neq q$, then $p^T \neq q^T$
• As commands in TAM execute, they can change the value (response) of $q_{ij}$
• Upper bound on the number of values of queries a single command can change is $m$ (number of enter or add•right operations)
Proof

• Choose $n > m$

• In ATAM, construct state $\sigma_k$ such that:
  • $\sigma_0 \rightarrow^* \sigma_k$; and
  • $e(\sigma_k, -q_{1,1} \land q_{1,1} \land \ldots \land -q_{n,n} \land q_{n,n})$ is true

• So $e(\sigma_k, q_{i,j})$ is false, $e(\sigma_k, q_{i,j})$ is true for all $1 \leq i, j \leq n$

• As $f$ is a state-matching reduction, there is a state $\sigma_k^T$ in TAM that causes the corresponding queries to be answered the same way

• Consider $\sigma_0^T \rightarrow \sigma_1^T \rightarrow \ldots \rightarrow \sigma_k^T$; choose first state $\sigma_c^T$ such that $e(\sigma_c^T, q_{i,j}^T \lor q_{i,j}^T)$ is true for all $1 \leq i, j \leq n$
Proof

• In $\sigma_{C-1}^T$, $e(\sigma_{C-1}^T, q_{v,w}^T \lor q_{v,w}^T)$ is false for some $1 \leq v, w \leq n$, so $e(\sigma_{C-1}^T, \neg q_{v,w}^T \land \neg q_{v,w}^T)$ is true

• State $\sigma$ in ATAM for which $e(\sigma, \neg q_{v,w} \land \neg q_{v,w})$ is true is one in which either $s_v$ or $s_w$ or both does not exist

• Thus in that state, one of the following 2 queries holds:
  - $Q_1 = \neg q_{v,1} \land \neg q_{v,1} \land \ldots \land \neg q_{n,v} \land \neg q_{n,v}$
  - $Q_1 = \neg q_{w,1} \land \neg q_{w,1} \land \ldots \land \neg q_{n,w} \land \neg q_{n,w}$

• So in TAM, $e(\sigma_{C-1}^T, Q_1^T \land Q_2^T)$ is true
Proof

• Now consider the transition from $\sigma_{C-1}^{T}$ to $\sigma_{C}^{T}$

• Values of at least $n$ queries in $Q_1$ or $Q_2$ must change from false to true

• But each command can change at most $m < n$ queries

• This is a contradiction

• So no such $f$ can exist, proving the result

Thus, ATAM can express security properties that TAM cannot
Key Points

• Safety problem undecidable
• Limiting scope of systems can make problem decidable
• Types critical to safety problem’s analysis
Security Policies

- Policies
- Trust
- Nature of Security Mechanisms
- Policy Expression Languages
- Limits on Secure and Precise Mechanisms
Security Policy

- Policy partitions system states into:
  - Authorized (secure)
    - These are states the system can enter
  - Unauthorized (nonsecure)
    - If the system enters any of these states, it’s a security violation

- Secure system
  - Starts in authorized state
  - Never enters unauthorized state
Confidentiality

- $X$ set of entities, $I$ information
- $I$ has the *confidentiality* property with respect to $X$ if no $x \in X$ can obtain information from $I$
- $I$ can be disclosed to others
- Example:
  - $X$ set of students
  - $I$ final exam answer key
  - $I$ is confidential with respect to $X$ if students cannot obtain final exam answer key
Integrity

• $X$ set of entities, $I$ information

• $I$ has the *integrity* property with respect to $X$ if all $x \in X$ trust information in $I$

• Types of integrity:
  • Trust $I$, its conveyance and protection (data integrity)
  • $I$ information about origin of something or an identity (origin integrity, authentication)
  • $I$ resource: means resource functions as it should (assurance)
Availability

• $X$ set of entities, $I$ resource

• $I$ has the *availability* property with respect to $X$ if all $x \in X$ can access $I$

• Types of availability:
  • Traditional: $x$ gets access or not
  • Quality of service: promised a level of access (for example, a specific level of bandwidth); $x$ meets it or not, even though some access is achieved
Policy Models

• Abstract description of a policy or class of policies
• Focus on points of interest in policies
  • Security levels in multilevel security models
  • Separation of duty in Clark-Wilson model
  • Conflict of interest in Chinese Wall model
Mechanisms

• Entity or procedure that enforces some part of the security policy
  • Access controls (like bits to prevent someone from reading a homework file)
  • Disallowing people from bringing CDs and floppy disks into a computer facility to control what is placed on systems
Question

• Policy disallows cheating
  • Includes copying homework, with or without permission
• CS class has students do homework on computer
• Anne forgets to read-protect her homework file
• Bill copies it
• Who breached security?
  • Anne, Bill, or both?
Answer Part 1

• Bill clearly breached security
  • Policy forbids copying homework assignment
  • Bill did it
  • System entered unauthorized state (Bill having a copy of Anne’s assignment)

• If not explicit in computer security policy, certainly implicit
  • Not credible that a unit of the university allows something that the university as a whole forbids, unless the unit explicitly says so
Answer Part #2

• Anne didn’t protect her homework
  • Not required by security policy

• She didn’t breach security

• If policy said students had to read-protect homework files, then Anne did breach security
  • She didn’t do this
Types of Security Policies

• Military (governmental) security policy
  • Policy primarily protecting confidentiality

• Commercial security policy
  • Policy primarily protecting integrity

• Confidentiality policy
  • Policy protecting only confidentiality

• Integrity policy
  • Policy protecting only integrity
Integrity and Transactions

• Begin in consistent state
  • “Consistent” defined by specification

• Perform series of actions (*transaction*)
  • Actions cannot be interrupted
  • If actions complete, system in consistent state
  • If actions do not complete, system reverts to a consistent state
Trust

Administrator installs patch

1. Trusts patch came from vendor, not tampered with in transit
2. Trusts vendor tested patch thoroughly
3. Trusts vendor’s test environment corresponds to local environment
4. Trusts patch is installed correctly
Trust in Formal Verification

• Gives formal mathematical proof that given input $i$, program $P$ produces output $o$ as specified

• Suppose a security-related program $S$ formally verified to work with operating system $O$

• What are the assumptions?
Trust in Formal Methods

1. Proof has no errors
   - Bugs in automated theorem provers

2. Preconditions hold in environment in which $S$ is to be used

3. $S$ transformed into executable $S'$ whose actions follow source code
   - Compiler bugs, linker/loader/library problems

4. Hardware executes $S'$ as intended
   - Hardware bugs (Pentium $\pm 0.00\pm$ bug, for example)
Types of Access Control

• Discretionary Access Control (DAC, IBAC)
  • Individual user sets access control mechanism to allow or deny access to an object

• Mandatory Access Control (MAC)
  • System mechanism controls access to object, and individual cannot alter that access

• Originator Controlled Access Control (ORCON, ORGCON)
  • Originator (creator) of information controls who can access information
Policy Languages

• Express security policies in a precise way
• High-level languages
  • Policy constraints expressed abstractly
• Low-level languages
  • Policy constraints expressed in terms of program options, input, or specific characteristics of entities on system
High-Level Policy Languages

• Constraints expressed independent of enforcement mechanism
• Constraints restrict entities, actions
• Constraints expressed unambiguously
  • Requires a precise language, usually a mathematical, logical, or programming-like language
Example: Ponder

- Security and management policy specification language
- Handles many types of policies
  - Authorization policies
  - Delegation policies
  - Information filtering policies
  - Obligation policies
  - Refrain policies
Entities

• Organized into hierarchical domains

• Network administrators
  • Domain is /NetAdmins
  • Subdomain for net admin trainees is
  • /NetAdmins/Trainees

• Routers in LAN
  • Domain is /localnet
  • Subdomain that is a testbed for routers is
  • /localnet/testbed/routers
Authorization Policies

• Allowed actions: netadmins can enable, disable, reconfigure, view configuration of routers

\[
\text{inst auth+ switchAdmin} \{
\text{subject } /\text{NetAdmins};
\text{target } /\text{localnetwork/routers};
\text{action enable()}, \text{ disable()}, \text{ reconfig()}, \text{ dumpconfig()};
\}
\]
Authorization Policies

• Disallowed actions: trainees cannot test performance between 8AM and 5PM

```plaintext
inst auth-testOps {
  subject /NetEngineers/trainees;
  target /localnetwork/routers;
  action testperformance();
  when Time.between("0800", "1700");
}
```
Delegation Policies

• Delegated rights: net admins delegate to net engineers the right to enable, disable, reconfigure routers on the router testbed

\[
\text{inst deleg+ (switchAdmin) delegSwitchAdmin}\{\\ 
\text{grantee } /\text{NetEngineers};\\ 
\text{target } /\text{localnetwork/testNetwork/routers};\\ 
\text{action } \text{enable()}, \text{disable()}, \text{reconfig>();\\ 
\text{valid } \text{Time.duration(8);}\\ \}
\]
Information Filtering Policies

• Control information flow: net admins can dump everything from routers between 8PM and 5AM, and config info anytime

```plaintext
inst auth+ switchOpsFilter {
    subject /NetAdmins;
    target /localnetwork/routers;
    action dumpconfig(what)
        { in partial = "config"; }
        if (Time.between("2000", "0500")){
            in partial = "all";
        }
}
```
Refrain Policies

• Like authorization denial policies, but enforced by the *subjects*: net engineers cannot send test results to net developers while testing in progress.

```plaintext
inst refrain testSwitchOps {
    subject  s=/NetEngineers;
    target   /NetDevelopers;
    action   sendTestResults();
    when     s.teststate="in progress"
}
```
Obligation Policies

- Must take actions when events occur: on 3rd login failure, net security admins will disable account and log event

```plaintext
inst oblig loginFailure {
  on     loginfail(userid, 3);
  subject s=/NetAdmins/SecAdmins;
  target t=/NetAdmins/users ^ (userid);
  do     t.disable() -> s.log(userid);
}
```
Example

• Policy: separation of duty requires 2 different members of Accounting approve check

\[
\text{inst auth+ separationOfDuty } \{
\begin{align*}
\text{subject} & \quad s=/\text{Accountants}; \\
\text{target} & \quad t=\text{checks}; \\
\text{action} & \quad \text{approve()}, \text{ issue>();} \\
\text{when} & \quad s.\text{id} <> t.\text{issuerid};
\end{align*}
\}
\]
DTEL

• Basis: access can be constrained by types
• Combines elements of low-level, high-level policy languages
  • Implementation-level constructs express constraints in terms of language types
  • Constructs do not express arguments or inputs to specific system commands
Example

• Goal: users cannot write to system binaries
• Subjects in administrative domain can
  • User must authenticate to enter that domain
• Subjects belong to domains:
  • \texttt{d\_user} ordinary users
  • \texttt{d\_admin} administrative users
  • \texttt{d\_login} for login
  • \texttt{d\_daemon} system daemons
Types

• Object types:
  • *t_sysbin* executable system files
  • *t_readable* readable files
  • *t_writable* writable files
  • *t_dte* data used by enforcement mechanisms
  • *t_generic* data generated from user processes

• For example, treat these as partitions
  • In practice, files can be readable and writable; ignore this for the example
Domain Representation

• Sequence
  • First component is list of programs that start in the domain
  • Other components describe rights subject in domain has over objects of a type

  \[(\text{crwd} - \rightarrow \text{t\_writable})\]

  means subject can create, read, write, and list (search) any object of type \text{t\_writable}
**d_daemon Domain**

domain d_daemon = (/sbin/init),
    (crwd->t_writable),
    (rd->t_generic, t_readable, t_dte),
    (rxd->t_sysbin),
    (auto->d_login);

• Compromising subject in *d_daemon* domain does not enable attacker to alter system files
  • Subjects here have no write access

• When /sbin/init invokes login program, login program transitions into *d_login* domain
**d_admin Domain**

```plaintext
domain d_admin =
  (/usr/bin/sh, /usr/bin/csh, /usr/bin/ksh),
  (crwxd->t_generic),
  (crwxd->t_readable, t_writable, t_dte, t_sysbin),
  (sigtstp->d_daemon);
```

- **sigtstp** allows subjects to suspend processes in *d_daemon* domain
- Admin users use a standard command interpreter
**d_user Domain**

```plaintext
domain d_user =
    (/usr/bin/sh, /usr/bin/csh, /usr/bin/ksh),
    (crwxd->t_generic),
    (rxd->t_sysbin),
    (crwd->t_writable),
    (rd->t_readable, t_dte);
```

- No auto component as no user commands transition out of it
- Users cannot write to system binaries
\texttt{d_login} Domain

\begin{verbatim}
domain d_login =
    (/usr/bin/login),
    (crwd->t_writable),
    (rd->t_readable, t_generic, t_dte),
    setauth,
    (exec->d_user, d_admin);
\end{verbatim}

- Cannot execute anything except the transition
  - Only /usr/bin/login in this domain

- \textit{setauth} enables subject to change UID

- \textit{exec} access to \texttt{d_user, d_admin} domains
Set Up

initial_domain = d_daemon;

• System starts in $d_{\text{daemon}}$ domain

assign \(-r\) t_generic /;
assign \(-r\) t_writable /usr/var, /dev, /tmp;
assign \(-r\) t_readable /etc;
assign \(-r\) \(-s\) dte_t /dte;
assign \(-r\) \(-s\) t_sysbin /sbin, /bin, /usr/bin, /usr/sbin;

• These assign initial types to objects
• \(-r\) recursively assigns type
• \(-s\) binds type to name of object (delete it, recreate it, still of given type)
Add Log Type

• Goal: users can’t modify system logs; only subjects in \textit{d\_admin}, new \textit{d\_log} domains can

\begin{verbatim}
type t_readable, t_writable, t_sysbin,
        t_dte, t_generic, t_log;
\end{verbatim}

• New type \textit{t\_log}

\begin{verbatim}
domain d_log =
    (/usr/sbin/syslogd),
    (crwd->t_log),
    (rwd->t_writable),
    (rd->t_generic, t_readable);
\end{verbatim}

• New domain \textit{d\_log}
domain d_daemon =
    (/sbin/init),
    (crwd->tWritable),
    (rxd->tReadable),
    (rd->tGeneric, t_dte, t_sysbin),
    (auto->d_login, d_log);

• Subject in *d_daemon* can invoke logging process
• Can log, but not execute anything

assign -r t_log /usr/var/log;
assign t_writable /usr/var/log/wtmp, /usr/var/log/utmp;
• Set type of logs
Low-Level Policy Languages

• Set of inputs or arguments to commands
  • Check or set constraints on system

• Low level of abstraction
  • Need details of system, commands
Example: X Window System

• UNIX X11 Windowing System
• Access to X11 display controlled by list
  • List says what hosts allowed, disallowed access
    \[
    \text{xhost } +\text{groucho } -\text{chico}
    \]
• Connections from host groucho allowed
• Connections from host chico not allowed
Example: tripwire

• File scanner that reports changes to file system and file attributes
  • *tw.config* describes what may change
    /usr/mab/tripwire +gimnpsu012345678-a
    • Check everything but time of last access (“–a”)
  • Database holds previous values of attributes
Example Database Record

```
/usr/mab/tripwire/README 0 ..../.. 100600 45763 1 917 10 33242 
.gtPvf .gtPvY .gtPvY 0 .ZD4cc0Wr8i2lZKaI..LUOr3 
.0fwo5:hf4e4.8TAqd0V4ubv ?....... ...9b3 1M4GX01xbGIX0oVuGo1h15z3 
?:Y9jfa04rdzM1q:eqt1APgHk ?.Eb9yo.2zkEh1XKovX1:d0wF0kfAvC 
?1M4GX01xbGIX2947jdyrior38h15z3 0
```

- file name, version, bitmask for attributes, mode, inode number, number of links, UID, GID, size, times of creation, last modification, last access, cryptographic checksums
Comments

• System administrators not expected to edit database to set attributes properly

• Checking for changes with tripwire is easy
  • Just run once to create the database, run again to check

• Checking for conformance to policy is harder
  • Need to either edit database file, or (better) set system up to conform to policy, then run tripwire to construct database
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 of 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
Secure, Precise Mechanisms

• Can one devise a procedure for developing a mechanism that is both secure \textit{and} precise?
  • Consider confidentiality policies only here
  • Integrity policies produce same result

• Program a function with multiple inputs and one output
  • Let $p$ be a function $p: I_1 \times \ldots \times I_n \rightarrow R$. Then $p$ is a program with $n$ inputs $i_k \in I_k$, $1 \leq k \leq n$, and one output $r \rightarrow R$
Programs and Postulates

• Observability Postulate: the output of a function encodes all available information about its inputs
  • Covert channels considered part of the output

• Example: authentication function
  • Inputs name, password; output Good or Bad
  • If name invalid, immediately print Bad; else access database
  • Problem: time output of Bad, can determine if name valid
  • This means timing is part of output
Protection Mechanism

• Let $p$ be a function $p: I_1 \times \ldots \times I_n \rightarrow R$. A protection mechanism $m$ is a function

$$m: I_1 \times \ldots \times I_n \rightarrow R \cup E$$

for which, when $i_k \in I_k$, $1 \leq k \leq n$, either

- $m(i_1, \ldots, i_n) = p(i_1, \ldots, i_n)$ or
- $m(i_1, \ldots, i_n) \in E$.

• $E$ is set of error outputs

  - In above example, $E = \{ \text{“Password Database Missing”}, \text{“Password Database Locked”} \}$
Confidentiality Policy

• Confidentiality policy for program $p$ says which inputs can be revealed
  • Formally, for $p: I_1 \times \ldots \times I_n \rightarrow R$, it is a function $c: I_1 \times \ldots \times I_n \rightarrow A$, where
    \[ A \subseteq I_1 \times \ldots \times I_n \]
  • $A$ is set of inputs available to observer

• Security mechanism is function
  \[ m: I_1 \times \ldots \times I_n \rightarrow R \cup E \]
  • $m$ is secure if and only if $\exists m': A \rightarrow R \cup E$ such that,
    \[ \forall i_k \in I_k, 1 \leq k \leq n, m(i_1, \ldots, i_n) = m'(c(i_1, \ldots, i_n)) \]
  • $m$ returns values consistent with $c$
Examples

• \( c(i_1, \ldots, i_n) = C \), a constant
  • Deny observer any information (output does not vary with inputs)

• \( c(i_1, \ldots, i_n) = (i_1, \ldots, i_n) \), and \( m' = m \)
  • Allow observer full access to information

• \( c(i_1, \ldots, i_n) = i_1 \)
  • Allow observer information about first input but no information about other inputs.
Precision

• Security policy may be over-restrictive
  • Precision measures how over-restrictive

• $m_1$, $m_2$ distinct protection mechanisms for program $p$ under policy $c$
  • $m_1$ as precise as $m_2$ ($m_1 \approx m_2$) if, for all inputs $i_1, ..., i_n$
    $m_2(i_1, ..., i_n) = p(i_1, ..., i_n) \Rightarrow m_1(i_1, ..., i_n) = p(i_1, ..., i_n)$
  • $m_1$ more precise than $m_2$ ($m_1 \sim m_2$) if there is an input $(i'_1, ..., i'_n)$ such that
    $m_1(i'_1, ..., i'_n) = p(i'_1, ..., i'_n)$ and $m_2(i'_1, ..., i'_n) \neq p(i'_1, ..., i'_n)$. 
Combining Mechanisms

- $m_1, m_2$ protection mechanisms
- $m_3 = m_1 \cup m_2$
  - For inputs on which $m_1$ and $m_2$ return same value as $p$, $m_3$ does also; otherwise, $m_3$ returns same value as $m_1$

- Theorem: if $m_1, m_2$ secure, then $m_3$ secure
  - Also, $m_3 \approx m_1$ and $m_3 \approx m_2$
  - Follows from definitions of secure, precise, and $m_3$
Existence Theorem

• For any program $p$ and security policy $c$, there exists a precise, secure mechanism $m^*$ such that, for all secure mechanisms $m$ associated with $p$ and $c$, $m^* \approx m$
  • Maximally precise mechanism
  • Ensures security
  • Minimizes number of denials of legitimate actions
Lack of Effective Procedure

• There is no effective procedure that determines a maximally precise, secure mechanism for any policy and program.
  • Sketch of proof: let policy $c$ be constant function, and $p$ compute function $T(x)$. Assume $T(x) = 0$. Consider program $q$, where

```plaintext
p;
  if z = 0 then y := 1 else y := 2;
  halt;
```
Rest of Sketch

- $m$ associated with $q$, $y$ value of $m$, $z$ output of $p$ corresponding to $T(x)$
- $\forall x[T(x) = 0] \rightarrow m(x) = 1$
- $\exists x' [T(x') \neq 0] \rightarrow m(x) = 2$ or $m(x)$ undefined
- If you can determine $m$, you can determine whether $T(x) = 0$ for all $x$
- Determines some information about input (is it 0?)
- Contradicts constancy of $c$.
- Therefore no such procedure exists
Key Points

• Policies describe *what* is allowed
• Mechanisms control *how* policies are enforced
• Trust underlies everything