Lecture 16 – Access Control and Security Policies

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017
Announcement

• Midterm:
  – Monday, Oct. 16\textsuperscript{th} 7-9pm
  – ECEB 1002 (here)

• Conflict
  – Friday Oct. 13\textsuperscript{th} 4-6pm
  – Siebel Center 4405
  – MUST have an email from you
Security News

- Verizon reveals Yahoo breach was all 3 billion accounts, includes Tumblr and Flickr
- Former DNI Clapper attributes 2012 DDoS to Iran, US decided not to hack back
- US DDoS of N. Korea, new connection through Russia
- Equifax CEO testified before House Energy and Commerce Committee
Access Control

- Access control is a collection of methods and components that support
  - confidentiality
  - integrity
  - accountability

- **Goal**: allow only authorized subjects to access permitted objects

- **E.g., Least privilege philosophy**
  A subject is granted permissions needed to accomplish required tasks and nothing more
Principles

- **Context (entities and functions)**
  - Authentication - verifying credentials of users
  - Authorization - granting rights/permissions to users
  - Accountability - reviewing records and activities

- **Policies**
  - MAC - Mandatory access control
  - DAC - Discretionary access control
  - RBAC - Role-based access control (RBAC)
  - ABAC - Attribute-based access control
  - *ABACAB* - 11th studio album by the British band *Genesis*
Basic elements of access control

- **Subjects** - entities capable of accessing objects (users)
  - Owner - creator of object
  - Group - subjects grouped together
  - World - widest possible group; all valid subjects

- **Objects** - resources with controlled access (files, programs)

- **Access rights** - what subjects are permitted do to objects
  - Read, write, execute, delete, create, search
MAC vs DAC

- MAC - administrator defines all of the access rights
- DAC - owners define access rights
Mandatory Access Control

- It is a restrictive scheme that does not allow users to define permissions on files, regardless of ownership.
- Instead, security decisions are made by a central policy administrator.
- A common implementation is rule-based access control
  - Subject demonstrates need-to-know in addition to proper security clearance
  - Need-to-know indicates that a subject requires access to object to complete a particular task
- Security-Enhanced Linux (SELinux) incorporates mandatory access control.
Discretionary Access Control

- Discretionary access control, or DAC, refers to a scheme where users are given the ability to determine the permissions governing access to their own files.
  - DAC typically features the concept of both users and groups
  - In addition, DAC schemes allow users to grant privileges on resources to other users on the same system.

- Most common design in commercial operating systems
  - Generally less secure than mandatory control
  - Generally easier to implement and more flexible
Discretionary Access Control

- **Access matrix** of users and objects
- If matrix is sparse, can be reduced to an *access control list* (ACL)
- Row of access matrix gives us *capability tickets* for a user

<table>
<thead>
<tr>
<th>OBJECTS</th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
<th>File 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>User A</td>
<td>Own Read Write</td>
<td>Own Read Write</td>
<td>Read Write</td>
<td>Read Write</td>
</tr>
<tr>
<td>User B</td>
<td>Read</td>
<td>Own Read Write</td>
<td>Write</td>
<td>Read</td>
</tr>
<tr>
<td>User C</td>
<td>Read Write</td>
<td>Read</td>
<td>Own Read Write</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 4.2 Example of Access Control Structures](image)

(a) Access matrix

(b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)
DAC Example

- Unix file system
  - 3 octets establishing permissions for each file

```
masked entries
user: :rw-
user:joe:rw-
group::r--
mask::rw-
other:::---
```
Role-Based Access Control

- The role-based access control (RBAC) model can be viewed as an evolution of the notion of group-based permissions in file systems.
- An RBAC system is defined with respect to an organization, such as company, a set of resources, such as documents, print services, and network services, and a set of users, such as employees, suppliers, and customers.
- Uses a subject’s role or task to grant or deny object access.
Role-based access control (RBAC)

- Users are assigned roles
- Roles have permissions

<table>
<thead>
<tr>
<th>R_1</th>
<th>R_2</th>
<th>...</th>
<th>R_n</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U_1</th>
<th>U_2</th>
<th>U_3</th>
<th>U_4</th>
<th>U_5</th>
<th>U_6</th>
<th>...</th>
<th>U_m</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OBJECTS</th>
<th>R_1</th>
<th>R_2</th>
<th>R_n</th>
<th>F_1</th>
<th>F_1</th>
<th>P_1</th>
<th>P_2</th>
<th>D_1</th>
<th>D_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>control</td>
<td>owner</td>
<td>owner control</td>
<td>read *</td>
<td>read owner</td>
<td>wakeup</td>
<td>wakeup</td>
<td>seek</td>
<td>owner</td>
<td></td>
</tr>
<tr>
<td>control</td>
<td>write *</td>
<td>execute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>owner</td>
<td>seek *</td>
<td></td>
</tr>
<tr>
<td>control</td>
<td>write</td>
<td>stop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Diagram showing assignments and permissions.
Role-based access control (RBAC)
Visualizing Role Hierarchy
Attribute-based access control (ABAC)

- Subjects and objects given *attributes*
- Decisions are made based on attributes of both
- Capable of enforcing any DAC, RBAC, or MAC idea
Define a *policy* to decide rules and relationships to govern allowable behavior

**Example rule:**

\[(\text{Age}(u) \geq 17 \land \text{Rating}(m) \in \{R, \text{PG-13, G}\}) \lor \]
\[(\text{Age}(u) \geq 13 \land \text{Age}(u) < 17 \land \]
\hspace{1cm} \text{Rating}(m) \in \{\text{PG-13, G}\}) \lor \]
\[(\text{Age}(u) < 13 \land \text{Rating}(m) \in \{G\})\]
SECURITY POLICIES
Security Policy

- Defining constraints and rules so that a system, asset, or organization is secure
- Designed by assessing risk and identifying potential adversaries
- Implemented by policy, crypto protocols, authentication systems, access control, etc.
Military classifications of access rights for documents based on concepts

- Unclassified
- Confidential
- Secret
- Top secret
E.g., The Orange Book

- Trusted Computer System Evaluation Criteria (TCSEC)
  - Division D: “minimal protection”
  - Division C: “Discretionary protection”
  - Division B: “Mandatory protection”
  - Division A: “Verified protection”
E.g., Cisco Best Practices

- **Preparation**
  - Create Usage Policy Statement
  - Conduct a Risk Analysis
  - Establish a Security Team Structure

- **Prevention**
  - Approving Security Changes
  - Monitoring Security of Your Network

- **Response**
  - Security Violations
  - Restoration
  - Review
Example of Implementing Policy

Filesystem Access Control
Unix Permissions

• Standard for all UNIXes
• Every file is owned by a user and has an associated group
• Permissions often displayed in compact 10-character notation (type, user, group, others)
• To view permissions: ls -l To change: chmod

jk@sphere:~:/test$ ls -l
total 0
-rw-r----- 1 jk ugrad 0 2005-10-13 07:18 file1
-rwxrwxrwx 1 jk ugrad 0 2005-10-13 07:18 file2
## Permissions Examples (Regular Files)

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-rw-r--r--</code></td>
<td>read/write for owner, read-only for everyone else</td>
</tr>
<tr>
<td><code>-rw-r-----</code></td>
<td>read/write for owner, read-only for group, forbidden to others</td>
</tr>
<tr>
<td><code>-rwx------</code></td>
<td>read/write/execute for owner, forbidden to everyone else</td>
</tr>
<tr>
<td><code>-r--r--r--</code></td>
<td>read-only to everyone, including owner</td>
</tr>
<tr>
<td><code>-rwxrwxrwx</code></td>
<td>read/write/execute to everyone</td>
</tr>
</tbody>
</table>
Permissions for Directories

- Permissions bits interpreted differently for directories
- **Read** bit allows listing names of files in directory, but not their properties like size and permissions
- **Write** bit allows creating and deleting files within the directory
- **Execute** bit allows entering the directory and getting properties of files in the directory
- Lines for directories in `ls -l` output begin with `d`, as below:

```
jk@sphere:~/test$ ls -l
Total 4
drwxr-xr-x  2 jk ugrad 4096 2005-10-13 07:37 dir1
-rw-r--r--  1 jk ugrad   0 2005-10-13 07:18 file1
```
## Permissions Examples (Directories)

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxr-xr-x</td>
<td>all can enter and list the directory, only owner can add/delete files</td>
</tr>
<tr>
<td>drwxrwx---</td>
<td>full access to owner and group, forbidden to others</td>
</tr>
<tr>
<td>drwx--x---</td>
<td>full access to owner, group can access known filenames in directory, forbidden to others</td>
</tr>
<tr>
<td>-rwxrwxrwx</td>
<td>full access to everyone</td>
</tr>
</tbody>
</table>
Special Permission Bits

• Three other permission bits exist
  – Set-user-ID ("suid" or "setuid") bit
  – Set-group-ID ("sgid" or "setgid") bit
  – Sticky bit
Set-user-ID

- Set-user-ID ("suid" or "setuid") bit
  - On executable files, causes the program to run as file owner regardless of who runs it
  - Ignored for everything else
  - In 10-character display, replaces the 4^{th} character (x or -) with s (or S if not also executable)

- rwsr-xr-x: setuid, executable by all
- rwxr-xr-x: executable by all, but not setuid
- rwSr--r--: setuid, but not executable (not useful)
Root

• “root” account is a super-user account, like Administrator on Windows

• Multiple roots possible

• File permissions do not restrict root

• This is *dangerous*, but necessary, and OK with good practices
Becoming Root

- **su**
  - Changes home directory, PATH, and shell to that of root, but doesn’t touch most of environment and doesn’t run login scripts

- **su -**
  - Logs in as root just as if root had done so normally

- **sudo <command>**
  - Run just one command as root

- **su [-] <user>**
  - Become another non-root user
  - Root does not require to enter password
Changing Permissions

• Permissions are changed with `chmod` or through a GUI like Konqueror
• Only the file owner or root can change permissions
• If a user owns a file, the user can use `chgrp` to set its group to any group of which the user is a member
• root can change file ownership with `chown` (and can optionally change group in the same command)
• `chown`, `chmod`, and `chgrp` can take the `-R` option to recur through subdirectories
## Examples of Changing Permissions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>chown -R root dir1</code></td>
<td>Changes ownership of <code>dir1</code> and everything within it to root</td>
</tr>
<tr>
<td><code>chmod g+w,o-rwx file1 file2</code></td>
<td>Adds group write permission to file1 and file2, denying all access to others</td>
</tr>
<tr>
<td><code>chmod -R g=rwX dir1</code></td>
<td>Adds group read/write permission to dir1 and everything within it, and group execute permission on files or directories where someone has execute permission</td>
</tr>
<tr>
<td><code>chgrp testgrp file1</code></td>
<td>Sets file1’s group to testgrp, if the user is a member of that group</td>
</tr>
<tr>
<td><code>chmod u+s file1</code></td>
<td>Sets the setuid bit on file1. (Doesn’t change execute bit.)</td>
</tr>
</tbody>
</table>
Example Threat and Policy

Lost Devices
## Council confidential data loss causes ICO concern

By Arwyn Jones
BBC News Wales

Welsh councils are not doing enough to protect people’s confidential data from falling into the wrong hands, according to the UK information watchdog.

<table>
<thead>
<tr>
<th>Department</th>
<th>Number of records lost</th>
<th>Narrative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department for Work and Pensions</td>
<td>n/a</td>
<td>USB memory stick, apparently encrypted and containing passwords for an old version of the Government Gateway, a website giving access to millions of records of personal data.</td>
</tr>
<tr>
<td>Ministry of Defence</td>
<td>1,700,000</td>
<td>Hard drive being held by contractor EDS is found to be missing.</td>
</tr>
<tr>
<td>Service Personnel and Veterans Agency</td>
<td>50,500</td>
<td>Three USB portable hard drives with details of staff are allegedly stolen from a high security facility at RAF Innsworth. The Agency holds records on 900,000 current and former personnel. Stolen records included sensitive information about the private lives of senior staff.</td>
</tr>
<tr>
<td>Insolvency Service</td>
<td>400</td>
<td>Names, addresses and bank details of up to 400 directors of 122 firms were lost when four laptops were stolen from a Manchester premises.</td>
</tr>
<tr>
<td>Tees, Esk and Wear Valleys NHS Trust</td>
<td>200</td>
<td>Memory stick with details of patients found in a public park.</td>
</tr>
<tr>
<td>Home Office</td>
<td>84,000</td>
<td>PA Consulting lost an unencrypted memory stick containing details high-risk, prolific and other offenders.</td>
</tr>
<tr>
<td>Colchester Hospital University NHS Foundation Trust</td>
<td>21,000</td>
<td>A manager’s unencrypted laptop holding patient addresses and treatment details is stolen from his car whilst on holiday in Edinburgh.</td>
</tr>
<tr>
<td>Department for Work and Pensions</td>
<td>45,000</td>
<td>West Yorkshire benefit claimants’ data lost.</td>
</tr>
<tr>
<td>Department for Work and Pensions</td>
<td>000s</td>
<td>CDs with personal data found at the home of a former contractor.</td>
</tr>
<tr>
<td>City and Hackney Teaching Primary Care Trust</td>
<td>180,000</td>
<td>&quot;Heavily encrypted&quot; disks containing details of children are lost by couriers. The loss prompted the agency to implement hard drive and USB memory stick encryption systems across all PCs.</td>
</tr>
<tr>
<td>Foreign and Commonwealth Office</td>
<td>50,000</td>
<td>Details of visa applicants were made available on an FCO website.</td>
</tr>
<tr>
<td>HM Revenue and Customs</td>
<td>25,000,000</td>
<td>Two CDs containing details of the families of child benefits claimants went missing in the post. HMRC’s handling of data was described as &quot;woefully inadequate&quot; and staff were described as &quot;muddling through&quot; in a June 2008 Independent Police Complaints Commission report.</td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td>5,000</td>
<td>Hard disk with details of HM Prison Service staff is lost on the premises of EDS.</td>
</tr>
<tr>
<td>Driving Standards Agency</td>
<td>3,000,000</td>
<td>Hard disk with details of candidates for the driving theory test was lost in a premises in Iowes by subcontractors.</td>
</tr>
<tr>
<td>Foreign and Commonwealth Office</td>
<td>50</td>
<td>Details of individuals made public after &quot;unauthorised disclosure by a contractor&quot;</td>
</tr>
</tbody>
</table>
Glue it?

1. Remove cap

2. Insert glue nozzle into USB port and apply liberally

3. Kick back and relax, your endpoint security problems are over!
£120,000 fine for lost USB stick

The ICO has fined Greater Manchester Police £120,000 after a memory stick containing sensitive personal data was stolen from an officer's home.

According to the ICO the device had no encryption or password protection, and contained details of more than a thousand people with links to serious crime investigations.

The ICO found that some officers across the force regularly used unencrypted memory sticks, which may also have been used to copy data from police computers to access away from the office. Despite a similar security breach in September 2010, the force had not put restrictions on downloading information, and staff were not sufficiently trained in data protection.

David Smith, ICO Director of Data Protection, said: "This is a substantial monetary penalty, reflecting the significant failings the force demonstrated. We hope it will discourage others from making the same data protection mistakes."

"It is easy to protect against such risks" says Jon Stanton from PEM IT Services. "The organisation could have installed security software such as DriveLock to control what USB devices can access their PCs. DriveLock would also have enabled them to encrypted their memory sticks, and given them an audit trail of what files had been transferred. This, combined with staff training, would have minimised the risks of any data loss."
Lost Laptops

• Lost and stolen laptops are a common occurrence
  – Estimated occurrences in US airports every week: 12,000

• Average cost of a lost laptop for a corporation is $50K
  – Costs include data breach, intellectual property loss, forensics, lost productivity, legal and regulatory expenses
  – Data breach much more serious than hardware loss

• Data breach cost estimated at $200 per customer record
  – Direct costs include discovery, notification and response
  – Indirect costs include customer turnover (higher loss and lower acquisition)

• Data can also be copied while laptop is unattended

From Device to Data – Encryption

• In a perfect world, we would not store sensitive data on portable devices
  – All sensitive data should be held on secure servers.
  – Unfortunately, this approach is not always practical.
• Keep the benefit of using portable devices
• Reduce the risk of data leakage by encryption
Encryption of File Systems

• Disk encryption
  – Block-level encryption
  – Encryption of physical or logical drive
  – BitLocker in Windows Vista and 7
  – TrueCrypt open source software

• File system encryption
  – File-level encryption
  – Encrypting File System (EFS) in Windows
Example Threat and Policy

Passwords
Warning to the Users

- Do not use shared credentials
- Strength your password
  - 2,295: “123456” or a sequential list of number
  - 780: “password”
  - 437: “welcome”
Compromised UofM Accounts

- **613 incidents** related to unauthorized use of university accounts during 2010 and first 6 months of 2011 at UofM

Some people steal university accounts to access the library.
Compromised UofM Accounts

- What did they do with the compromised accounts?
  - Netflow data analysis
    - Library website repeatedly visited
    - 8.2% of HTTP flows visited consist of 10 websites blocked in China
    - Login to accounts at 7 universities

- Market place for the compromised university accounts
  - 500 RMB ~ less than 100 USD = access to multiple databases for a year
  - $20 = UofM account with VPN and Library access

New motivation of attackers who steal university credentials:

Free and unfettered access to information
Weak Password Scanning

- UofM scan weak password accounts twice a year using a commercial password cracker
- 2,284 weak password are detected in June, 2011
- Whether accounts with weak passwords are a problem?

<table>
<thead>
<tr>
<th></th>
<th># of total</th>
<th># of compromised</th>
<th>Pr (compromise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak Password</td>
<td>2,284</td>
<td>12</td>
<td>0.525%</td>
</tr>
<tr>
<td>Total Population</td>
<td>550,000</td>
<td>380</td>
<td>0.069%</td>
</tr>
</tbody>
</table>

*Test statistics of deviance of 28.09 and a p-value of 1.16^{-16}
Educating the Users

- From ‘what tools to use’ to ‘who uses the tool’

Yearly Security Quiz at UofM

<table>
<thead>
<tr>
<th></th>
<th># of total</th>
<th># of compromised</th>
<th>Pr (compromise)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passed Quiz</td>
<td>9.227</td>
<td>9</td>
<td>0.1%</td>
</tr>
<tr>
<td>NOT passed</td>
<td>41,924</td>
<td>105</td>
<td>0.25%</td>
</tr>
</tbody>
</table>

Test statistics of deviance of 13.52 and a p-value of $2.36^{-4}$