Agenda

- Access Controls
- Tools Demo - Paros Proxy
Access Control

- "The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner."
- Central element of computer security.
Four-Part Access Control

- **Identification** - Who is asking to access the asset?
- **Authentication** - Can the requestor’s identity be verified?
- **Authorization** - What, exactly, can the requestor access? And what can they do?
- **Accountability** - How can actions be traced to an individual? We need to ensure that a person who accesses or makes changes to data or systems can be identified. This process of associating actions with users for later reporting and research is known as accountability.
Subjects and Objects

- Subject - user. An active entity that requests access to an object or the data in an object.
- Object - resource. A passive entity that contains information.
- Access - the flow of information between subject and object.
Two Types of Access Controls

- **Physical access controls** - control access to physical resources. They could include buildings, parking lots, and protected areas? e.g., you probably have a key to the door of your office. This key controls the physical access to your office.

- **Logical access controls** - control access to a computer system or network. Your company probably requires that you enter a unique username and password to log on to your company computer.
Terms

- **Access Control List (ACL)** - a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Alice: read, write; Bob: read), this would give Alice permission to read and write the file and Bob to only read it. - wikipedia

- **Privilege Escalation** - Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. - wikipedia
## Access Control List Example

<table>
<thead>
<tr>
<th>#</th>
<th>Page/Namespace</th>
<th>User/Group</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>*</td>
<td>@ALL</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#2</td>
<td>*</td>
<td>bigboss</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#3</td>
<td>devel:*</td>
<td>@ALL</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#4</td>
<td>devel:*</td>
<td>@devel</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#5</td>
<td>devel:*</td>
<td>bigboss</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#6</td>
<td>devel:*</td>
<td>@marketing</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#7</td>
<td>devel:funstuff</td>
<td>bigboss</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#8</td>
<td>devel:marketing</td>
<td>@marketing</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#9</td>
<td>marketing:*</td>
<td>@marketing</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
<tr>
<td>#10</td>
<td>start</td>
<td>@ALL</td>
<td>None  ○  Read ○  Edit ○  Create ○  Upload ○  Delete</td>
</tr>
</tbody>
</table>

image source: https://www.dokuwiki.org/_media/aclexample.png
Formal Models of Access Control

- **Discretionary access control (DAC)** - with DAC, the owner of the resource decides who gets in and changes permissions as needed. You, as the owner, decide how you want to protect and share data.

- **Mandatory access control (MAC)** - with MAC, permission to access a system or any resource is determined by the sensitivity of the resource and the security level of the subject. The system decides how the data will be shared. This model is used in highly classified and confidential environments, such as military or government. Example: The law allows a court to access driving records without the owner’s permission.
Discretionary Access Control

In discretionary access control (DAC), owner of a resource decides how it can be shared.

- Owner can choose to give read or write access to other users.

Image source:
https://www.youtube.com/watch?v=UNRnSaXajC4
Mandatory Access Control (MAC) Models

- User works in a company and the company decides how data should be shared
- Hospital owns patient records and limits their sharing
- Regulatory requirements may limit sharing

image source:
https://www.youtube.com/watch?v=UNRnSaXajC4
Role-based Access Control (RBAC)

- Role based access control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
- An RBAC policy bases access control approvals on the jobs the user is assigned.
- Best system for an organization that has high turnover.
Threats to Access Controls

Access controls can be compromised in several ways.

- Gaining physical access
- Eavesdropping by observation
- Reusing or discarding media
- Electronic eavesdropping
- Intercepting communication
- Accessing networks
- Exploiting applications
Gaining Physical Access

- If an intruder has physical access to a device, logical access control is basically worthless.
- Data can be copied or stolen outright.
- Someone with physical access can install hardware or software keystroke loggers or can damage equipment.
Eavesdropping by Observation

- Sometimes security staff misses the most obvious breach, allowing information to be seen.
- Data on papers on an authorized user’s desk or screen are open to a spy.
Reusing or Discarding Media

- Attackers can recover erased information from discarded or reused media.
- It is safer and cheaper to shred documents and physically destroy media than to simply throw them out.
Electronic Eavesdropping

- Attackers can eavesdrop by wiretapping network cables.
- Users who connect their devices to insecure access points are easy targets for attackers.
Intercepting Communication

- Physical interception of data communication.
- Another variation of eavesdropping. This is called **sniffing**.
- With sniffing, attackers capture network traffic as it passes by.
- Sniffing is often used in a **man-in-the-middle (MITM)** attack.
Networks often include unprotected connections.

Many organizations build their networks with more drops than they needed. This allows an organization to add more users in the event of future growth. These unused connection points are often active connections.

Intruders can use these connections to gain network access.

Network access risks increase as organizations add wireless access points.
Permission Groups: In Linux, each file and directory has three user based permission groups

- owner
- group
- other users
Permission Types: in Linux, each file or directory has three basic permission types.

- **read**: The read permission refers to a user’s capability to read the contents of the file.
- **write**: The write permission refers to a user’s capability to write or modify a file or a directory.
- **execute**: The execute permission affects a user’s capability to execute a file or view the contents of a directory.
Hands-on - Understand Linux File System Permissions

- On onyx, use `id` command to figure out what group are you in.
- Use `touch abc`, to create a file abc. Use `ls -l` to see its permissions.
- Change its permissions, `chmod g+rw`, see if the person next to you can access this file.
- Change its permissions, `chmod g-rw`, see if the person next to you can access this file.
- Ideally, you can only access your own home directory, but not other people’s home directory. However, this is not the truth on onyx. Find out whose home directory on onyx is accessible.
A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G. Solomon