Agenda

- Project
- Authentication – Biometrics
- Access Control Models (DAC – Part A)
- Access Control Techniques
- Centralized Remote Access Control Technologies
You and your team are:

- Acting as the CSP (Cloud Service Provider)
- Seeking PA (Preliminary Authorization) for your information system
- Responsible for
  1. Developing the system security architecture for your information system
  2. Developing a System Security Plan (SSP) for your information system
  3. Presenting your SSP to an internal senior management review team
Project Tasks

A. Identify a client organization

B. Identify a mission-based information system to support the organization with one of the 26 government direct services and delivery support lines of business identified in Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories (NIST SP 800-60)

C. Identify the public and organizational groups/roles (along with their geographically distributed wide-area network office locations) that will develop, support/maintain, access and use the information system to effectively conduct the mission

D. Design a security architecture for the information system, which will be hosted in a to be determined (i.e. vendor-neutral) cloud environment, and accessed remotely by individuals working in the groups identified above to conduct the organization’s mission

E. Using NIST resources covered in this course, templates available at https://www.fedramp.gov/resources/templates-2016/ and other resources you find through your research: develop, present and hand in:

1. A draft system security plan for the information system based on the appropriate FedRAMP System Security Plan (SSP) template for the security baseline appropriate for your system, with the following exceptions:
   • Sections 3-6 and attachments - leave names, addresses and phone numbers and email addresses blank as appropriate (fill in titles and organizations)
   • Section 13 – only fill in details for Technical Security Control Class Families (remove all other non-technical security control class families from your SSP document and table of contents)
   • Section 15 - provide all appropriate attachments (At a minimum must have the following SSP Attachments filled in for your system: 3, 4, 5, 9, 10, and 11)

2. Powerpoint presentation covering A-E that will be presented to instructor and class
Project Resources include but are not limited to...

https://www.fedramp.gov/resources/templates-2016/
Project Resources include but are not limited to…
Project resources include...

<table>
<thead>
<tr>
<th>CLASS</th>
<th>FAMILY</th>
<th>IDENTIFIER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>Risk Assessment</td>
<td>RA</td>
</tr>
<tr>
<td>Management</td>
<td>Planning</td>
<td>PL</td>
</tr>
<tr>
<td>Management</td>
<td>System and Services Acquisition</td>
<td>SA</td>
</tr>
<tr>
<td>Management</td>
<td>Certification, Accreditation, and Security Assessments</td>
<td>CA</td>
</tr>
<tr>
<td>Operational</td>
<td>Personnel Security</td>
<td>PS</td>
</tr>
<tr>
<td>Operational</td>
<td>Physical and Environmental Protection</td>
<td>PE</td>
</tr>
<tr>
<td>Operational</td>
<td>Contingency Planning</td>
<td>CP</td>
</tr>
<tr>
<td>Operational</td>
<td>Configuration Management</td>
<td>CM</td>
</tr>
<tr>
<td>Operational</td>
<td>Maintenance</td>
<td>MA</td>
</tr>
<tr>
<td>Operational</td>
<td>System and Information Integrity</td>
<td>SI</td>
</tr>
<tr>
<td>Operational</td>
<td>Media Protection</td>
<td>MP</td>
</tr>
<tr>
<td>Operational</td>
<td>Incident Response</td>
<td>IR</td>
</tr>
<tr>
<td>Operational</td>
<td>Awareness and Training</td>
<td>AT</td>
</tr>
<tr>
<td>Technical</td>
<td>Identification and Authentication</td>
<td>IA</td>
</tr>
<tr>
<td>Technical</td>
<td>Access Control</td>
<td>AC</td>
</tr>
<tr>
<td>Technical</td>
<td>Audit and Accountability</td>
<td>AU</td>
</tr>
<tr>
<td>Technical</td>
<td>System and Communications Protection</td>
<td>SC</td>
</tr>
</tbody>
</table>

Table 2: Security Control Class, Family, and Identifier
Project Resources include but are not limited to...
Authentication – Biometrics

Two different categories of biometric factor authentication:

1. Physiological (“what you are”)
   - Physical attribute unique to a specific individual
   - Less prone to change unless an disfiguring accident
   - Hard to impersonate

2. Behavioral (“what you do”)
   - A characteristic of an individual
   - Can change over time
   - Can be forged
Authentication – Biometrics

During identity verification (i.e. authentication) the biometric system scans personal’s physiological attribute or behavioral trait and compares the captured data to a record created in an earlier enrollment process.

Biometric system
- Must be capable of repeatedly taking accurate measurements of anatomical or behavioral characteristics
- Error types:
  - **False negative** – incorrect rejection of the identity of authorized individual
    - Called a **Type I error**
      - False Rejection Rate (FRR) is a measurement of the likelihood that biometric device will result in Type I errors
  - **False positive** – incorrect match and identity acceptance of unauthorized individual (“imposter”)
    - Called a **Type II error**
      - False Acceptance Rate (FAR) is a measurement of the likelihood that biometric device will result in Type II errors

Organizations have their own security requirements which will dictate how many Type I and Type II errors are acceptable:
- Organizations prioritizing confidentiality would accept a certain rate of Type I errors to achieve no Type II errors
- *Calibration of biometric systems would enable lowering Type II error rate by adjusting system sensitivity which will increase Type I error rate*
Crossover error rate (CER) also called Equal error rate (EER)

- Objective measurement of biometric system accuracy, useful for comparing different biometric system products
- Is a rating, stated as a percentage
- CER is the point at which false rejection rate equals the false acceptance rate: FRR = FAR
- *Most important metric in determining a biometric system’s accuracy!*
Access Control Models

3 Main types (built into the kernel of different operating systems and possibly their supporting applications):

1. Discretionary Access Control (DAC)
2. Mandatory Access Control (MAC)
3. Role-based Access Control (RBAC)

Every operating system has a security kernel based on the access control model embedded in the system.

For each access attempt, before a subject can communicate with an object, the security kernel reviews the rules of the access control model to determine if the request is permitted.
Discretionary Access Control (DAC)

Most operating systems of general purpose computers are based on DAC models and use Access Control List properties on a file or directory to display and control access:

- Windows
- Linux
- OS X
- Unix
Discretionary Access Control (DAC)

The Network Administrator can allow resource owners to control who has access to their files.

If a user creates a file or folder then the user is the owner of the file or folder.

- An identifier is placed in the file header and/or in an access control matrix in the operating system.
  - The identifier can be a user identity or a group membership.
    - For example: Data owner can choose to allow Bill (user identity) and the Accounting group (group membership identity) to access his file.

DAC systems grant or deny access based on the identity of the subject.

- Access is restricted based on the authorization granted to the users.
  - Users can specify what type of access can occur to the objects they own.
- Access control is based on the discretion of the resource owner.
  - Resource owners, for example, can be business unit managers or department managers who “own” the data within their organization.
Discretionary Access Control (DAC)

Most operating systems are based on DAC models and use Access Control List properties on a file or directory to display and control access

- Windows
- Linux
- OS X
- Unix

DACs can apply to both directory tree structure (i.e. folders) and the files it contains.

Access permission:
- No access (-)
- Read (r)
- Write (w)
- Execute (x)
Discretionary Access Control (DAC)

Most operating systems are based on DAC models and use Access Control List properties on a file or directory to display and control access:

- Windows
- Linux
- OS X
- Unix

DACs can apply to both directory tree structure (i.e. folders) and the files it contains.

Access permission:
- No access (-)
- Read (r)
- Write (w)
- Execute (x)
Discretionary Access Control (DAC)

Most operating systems are based on DAC models and use properties of a file or directory to display and control access information.

- Windows
- Linux
- OS X
- Unix
Discretionary Access Control (DAC)

Provides a huge tradeoff:

• On the one hand:
  • Flexibility to user
  • Less administrative overhead to IT

• On the other hand:
  • Achilles’ heel (i.e. weakness) to the operating system
  • Malware can work under the identity (security context) of the user
    • If a user opens an virus infected file, code can install itself in the background without user awareness
    • Code inherits all rights and permissions of the user, can carry out all activities the user can on the system
      • Send copies of itself to all contacts in user’s email client, install a back-door, attck other systems, delete files on hard drive...
      • If the user is a local administrator or has root accounts then once installed malware can do anything
Discretionary Access Control (DAC)

Security administrators can counter the downside of DAC and protect critical assets by removing user control by implementing “nondiscretionary access control” within a DAC Operating System by:

• Setting up workstations with pre-configured and loaded user profiles specifying the level of control the user does and does not have:
  • With permissions on files (including OS command files) and folders set to block discretionary access control to users from:
    • Changing the system’s time
    • Altering system configuration files
    • Accessing a command prompt
    • Installing unapproved applications
    • ...
    • ...