INFO 6010 Lesson 9
Identity and Access Management
Domain 5

Revision 2

Information Security Management and Network Security and Architecture

FANSHAWE

Discussion Topics

- Identification methods and technologies
- Authentication methods, models, and technologies
- Discretionary, mandatory, and nondiscretionary models
- Accountability, monitoring, and auditing practices
- Registration and proof of identity
- Identity as a service
- Threats to access control practices and technologies

Access Controls

- Access Controls protect systems and assets from unauthorized use
- Access Controls dictate level of access granted to each individual
- Access
  - Flow of information between a subject and object
- Subject
  - Entity requesting access to an object resource or information
- Object
  - Passive entity which contains information

Security Principles – CIA or AIC…

- **Confidentiality:**
  - Assurance information is not disclosed to an unauthorized entity or process
    - Encryption, logical & physical access, database views
- **Integrity:**
  - Assurance information is not modified by unauthorized entity or process
    - Information must remain accurate, complete and protected from tampering or destruction
- **Availability:**
  - Systems must be accessible to all staff in timely manner
  - Productivity cannot be disrupted through availability issues

Access Controls

- **Step1 – Identification**
  - Subject is given a username or account number as identity
  - Identity credentials may be public information and should have the following aspects
  - Must be unique
    - No one else may have same ID
  - Must be non-descriptive
    - ID must not disclose purpose
    - Do not use name Administrator or CEO
  - Must have issuance
    - Issued by an authority

Access Controls

- **Step 2 – Authentication**
  - User provides some private information
  - Password, pass phrase, cryptographic key or token
  - Biometric attribute
  - Strong authentication is 2 factor authentication
  - Includes 2 of the following
    - Something you ARE
    - Something you HAVE
    - Something you KNOW

Access Controls

- **Step 3 – Authorization**
  - Determine level of access to objects
  - Access control matrix
  - List of subject and permissions to objects

- **Step 4 – Accountability**
  - Subject is accountable for actions taken on an object
  - Log or audit trails track who modified data

Access Controls

- Access controls are software components
  - Terms logical and technical access controls are used in CISSP exam
  - Embedded in operating system
  - Application or program
  - Database management
  - Add on 3rd party security package
- Entering public information is the identification step
- Entering private information is authentication step

Race Condition

- Flaw in software were actions can be preformed out of sequence
  - Authentication and authorization are 2 different steps
  - Authentication is required before authorization
- When two processes access the same resource a race condition could force the authorization to be completed before authentication for one of the processes

Identity and Authentication

- A person has been identified through the user ID or a similar value, and then authenticated, which means proving they are who they say they are.
- Three general factors can be used for authentication:
  - *Something a person knows*
  - *Something a person has*
  - *Something a person is*
- These factors are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic.

Identity Management

- Many products can be used to automate user identity, authentication and authorization
- Goal is to streamline management of
  - Identity
  - Authentication
  - Authorization
  - Auditing

Identity Management

- ***Identity management (IdM)*** encompasses the use of different products to identify, authenticate, and authorize users through automated means.
- It includes user account management, access control, credential management, single sign-on (SSO) functionality, managing rights and permissions for user accounts, and auditing and monitoring all of these items.
- IdM requires management of uniquely identified entities, their attributes, credentials, and entitlements.
- IdM allows organizations to create and manage digital identities' life cycles (create, maintain, terminate) in a timely and automated fashion.
- The enterprise IdM must meet business needs and scale from internally facing systems to externally facing systems.

Identity Management Implementation

- What should each user have access to?
- Who approves and allows access?
- How do the access decisions map to policies?
- Do former employees still have access?
- How do we keep up with our dynamic and ever-changing environment?
- What is the process of revoking access?
- How is access controlled and monitored centrally?
- Why do employees have eight passwords to remember?
- We have five different operating platforms. How do we centralize access when each platform (and application) requires its own type of credential set?
- How do we control access for our employees, customers, and partners?
- How do we make sure we are compliant with the necessary regulations?

Identity Management

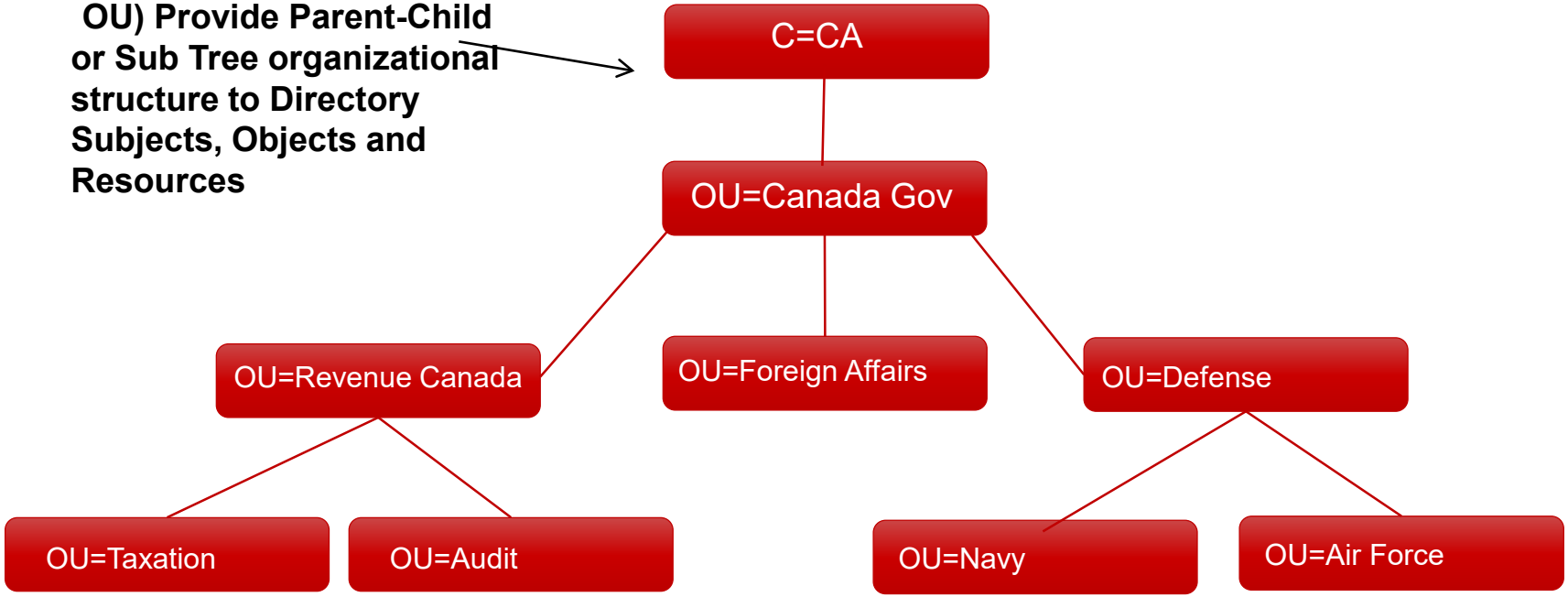
- Management technologies include
  - Directories
  - Web access management
  - Password management
  - Single sign-on
  - Account management
  - Profile updates

Identity Management

- **Directories**
  - Hierarchical database
  - X.500 standard
  - Lightweight Directory Access Protocol -LDAP
  - A directory service manages the database
    - Windows Active Directory
  - Namespace used to label Objects in the directory
  - Distinguished name (DN) assigned to each object
    - The DN represents a collection of attributes for an object
  - The DN is made up of a common name and domain component
    - ism.ity.fanshawec.ca

Identity Management

- Objects are organized into Organizational Unit (OU)



Identity Management

- Directory is single database for user attributes
  - Identity & passwords
  - Authorization profiles
  - Roles and groups
  - Security control policy
- Meta directory stores attributes from many sources in one location
  - Identity store
  - Identity info from different servers on network
  - Synchronizes changes
- Virtual directory just points to location of data

Web Access Management

- Plug-in for a web server
- Front end process for web server
  - WAM console used to configure authentication requirement, access levels, accounting
- Issues cookie to manage session
  - Allows access with all web servers on the web site
  - Single sign on
  - Cookie contains user personal account information

Authentication Methods

- Various methods that are commonly used to verify that users are who they claim to be. This is commonly done through the use of passwords, personal identification numbers (PINs), biometrics (e.g., fingerprint scans), and access tokens.

Credential Management Systems

- Credential management deals with creating user accounts on all systems, assigning and modifying the account details and privileges when necessary, and decommissioning the accounts when they are no longer needed.
- The IT department creates accounts manually on the different systems, users are given excessive rights and permissions, and when an employee leaves the company, many or all of the accounts stay active. This typically occurs because a centralized credential management technology has not been put into place.
- Credential management products allow management of user accounts across multiple systems.
- The automated workflow reduces the potential errors, it also logs and tracks each step (including account approval).
- Enables accountability, provides documentation. Ensures only the necessary amount of access is provided to the account and that there are no “orphaned” accounts still active when employees leave the company.

Password Management

- User may be required to have a password on many different systems
- Goal is to reduces help desk request for forgotten passwords
- Methods to handle user passwords
  - Password Managers
  - Password Synchronization
  - Self-Service Password Reset
  - Assisted Password Reset

Password Management

- **Password Managers or *password vaults***, come in two flavors: as a stand-alone application, or as a feature within another application (such as a web browser).
  - The application stores user identifiers and passwords in a password-encrypted data store. The user need only remember this master password and the application maintains all others.

- Most modern web browsers provide features that remember the user identifiers and passwords for specific websites.
- An obvious problem with using password vaults is that they provide one-stop-shopping for malicious persons.

Password Management

- **Password Synchronization**
- One password used across multiple system
- System updates all system passwords
  - Easier for user to remember just one password
- Requires strong password
  - 12 characters, upper & lower case, numbers & symbols
  - Changed regularly
  - If guessed hacker has access to multiple systems

Password Management

- **Self-Service Password Reset**
  - Users change own password
- Must confirm identity before change allowed
- System prompts user for question that only user should know
  - Set up with account
  - Favourite colour, teacher
  - Should not contain any information that may be publically available
- Password change sent in email
- Or e-mail links to web site to change password

Password Management

- **Assisted Password Reset**
- Help desk will ask user questions to confirm user identity
- Help desk resets password
- User logs in will be prompted to enter a new password
- Help desk should not know user password

Legacy Single Sign-On

- An SSO technology allows a user to authenticate one time and then access resources in the environment without needing to re-authenticate.
- The application sends a request for credentials, but the SSO software responds. So in SSO environments, the SSO software intercepts the login prompts from network systems and applications and fills in the necessary identification and authentication information (that is, the username and password) for the user.
- With password synchronization, a product takes the user's password and updates each user account on each different system and application with that one password.

Biometrics

- Analyzes a personal unique attribute or behaviour during authentication process
  - Hard to impersonate user
  - Sophisticated but expensive and complex to implement
- Two types of biometric authentication
  - Physiological
    - What you are
    - Fingerprint, iris scan etc.
  - Behavioural
    - What you do
    - Signature analysis, typing pattern

Biometrics

- System must perform accurate and repeatable measurements
  - Compare scan to stored values
  - Should take 5-10 seconds
  - Susceptible to margin of error
  - Scanner creates hash or encrypts biometric data
  - Sends to backend authentication database for comparison to sample provided by user

Biometrics

- Type 1 Error - False Rejection Rate
  - Biometric device REJECTS authorized person
- Type 2 Error - False Acceptance Rate
  - Biometric device ACCEPTS unauthorized person
- Crossover Error Rate - CER
  - Common biometric evaluation metric
  - Represented as a percentage
  - Represents point at which Type 1 Error equals Type 2 Error rate
  - Goal of accurate biometric device is to minimize both errors

Biometrics

- **Palm Scan**
  - Palm has creases, ridges and grooves
  - Fingerprints scanned along with palm
- **Hand Geometry**
  - Shape, length and width of a persons hand and fingers
- **Retina Scan**
  - Blood Vessel patterns on the back of the eyeball
- **Iris Scan**
  - Coloured portion of eye around the pupil
  - Unique patterns made up of rings, rifts, patterns, coronas, and furrows
  - Most accurate of all biometric types
    - Iris remains identical throughout adulthood

Biometrics

- **Facial Scan**
  - Bone structure, eye width, nose and chin shape
  - Head size
- **Voice Print**
  - User repeats several previously recorded words
  - Measure sound and patterns of speech
- **Hand Topology**
  - Used in conjunction with hand geometry
  - Camera gets side view of hand for different data from hand geometry

Biometrics

- Biometrics can authenticate a user by the specific way they perform a task
  - User perform task in same way every time
- Signature Dynamics
  - Measure how quickly a signature is completed
  - Amount of pressure exerted by pen
  - Motion of pen

Biometrics

- **Keystroke Dynamics**
  - Each individual has a distinct typing pattern and style
  - Measure timing of keystrokes when password entered
  - More accurate then a password
    - Much harder to impersonate a persons typing style then typing persons password.

Passwords

- Most frequently used method
- Weakest authentication method
  - User allowed to create easily guessed password
  - Write passwords down
- Password generators need to create uncomplicated pronounceable non dictionary words
  - Or user will write down passwords that are hard to remember

Password Cracking

- **Electronic Monitoring**
  - Listening to network traffic
  - Replay attack
- **Access Password File**
  - Reading stored passwords from system file on the authentication server
  - SAM or /etc/shadow
- **Brute Force Attack**
  - Automated tool which cycles through different password combinations

Password Cracking

- **Social Engineering**
  - Attacker tricks target user into giving their password
- **Rainbow Tables**
  - Pre computed tables containing all possible passwords in hash format

Password Security

- **Password Checkers**
  - Password cracker used by IT Professionals to detect weak passwords
  - Same tool as used by hacker
- **Password Hashing and Encryption**
  - Mathematical process changes the password into a unrecognizable value when stored on system
- **Password Aging**
  - Setting a password expiry date
- **Limit Logon Attempts**
  - Set threshold allowing bad password attempts
  - Typically accounts are locked

Password Security

- **Cognitive Password**
  - Uses fact or opinion method to generate a password
  - Store answers to several life experience questions unique to user
  - Used to identify user to help desk
    - Not used for every day authentication

Password Security

- **One Time Password**
  - Becomes invalid after first use.
- **Token Device**
  - Handheld device, synchronized with authentication server
  - Generating a password value
  - Same value generated by authentication server at time of login
- **Synchronous Tokens**
  - Tokens generated using a time-based or counter technique

Password Security

- **Asynchronous Tokens**
  - Challenge/Response method when generating token
  - Server presents Challenge value to client
  - Client enters value into token device and responds with computed response value based on entered value
- Both token methods can fall pray to masquerading attacks
  - Hacker has username or user id

Password Security

Cryptographic Keys

- Digital signature could be used in place of password
- Requires a Public Key Infrastructure
  - Private Key
  - Public Key
- Used for higher security requirements

Password Security

- **Password Phrase**
  - More secure than passwords because it is longer
  - Easier for user to remember than a complex password
- **Memory Cards**
  - Holds but does not process information
  - Holds user authentication info
  - User presents card and enters PIN
  - If data matches user is authenticated
  - 2 factor authentication
  - Credit Cards and Debit Cards use this technology with magnetic stripes

Password Security

- **Smart Cards** have an embedded CPU
  - Can process stored data
- Provides 2 Factor Authentication
  - Something you have & something you know
- User enters a PIN to unlock Smart Card
- Two Types of Smart Cards
  - **Contact** – must be inserted into a reader
    - Gold seal on chip
  - **Contactless** – antenna in proximity of electromagnetic field generates enough power to activate card

Smart Card Attack

- Fault generation, attackers introduce computational errors into smart cards to uncover the encryption keys used and stored on the cards by manipulating environmental component of the card (changing input voltage, clock rate, temperature fluctuations).
- Analysis of the results may allow an attacker to reverse-engineer the encryption process, with the hope of uncovering the encryption key.
- Side-channel attacks are nonintrusive and are used to uncover sensitive information about how a component works, without trying to compromise any type of flaw or weakness.
- A non-invasive attack is one in which the attacker watches how something works and how it reacts in different situations instead of trying to “invade” it.
  - E.g. differential power analysis (examining the power emissions released during processing), electromagnetic analysis (examining the frequencies emitted), and timing (how long a specific process takes to complete).

Authorization

- Next step after authentication
- Confirm level of access
- Core component of an operating system
  - Can be part of application or 3rd party security add on package
- Default to no access
  - Enter permissions based on user profile
  - Read write delete etc
- Follow Principle of Least Privilege

Access Criteria

- Roles
  - Access based on users tasks or job assignment
- Groups
  - Access based on users group membership
- Physical or Logical Location
  - Physical restrictions may require a user to be at console keyboard
  - Logical restriction may restrict certain network segments (subnets) or specific hosts

Access Criteria

- Time of Day
  - Access based on business hours
- Transaction Type
  - Restrict users to specific operational tasks

Default to No Access

- Access control mechanisms should default to no access.
- What is not explicitly allowed should be implicitly denied.
- Access controls should be based on the concept of zero access.
- Add privileges based on need to know.

Single Sign-On

- Single sign-on (SSO) enables users to securely authenticate with multiple applications and websites by logging in only once—with just one set of credentials (username and password).
- With SSO, the application or website that the user is trying to access relies on a trusted third party to verify that users are who they say they are.
- There are many different SSO technologies each with different advantages and disadvantages.

Kerberos

- Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

- The protocol was named after the character Kerberos (or Cerberus) from Greek mythology, the ferocious three-headed guard dog of Hades.

- Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

- Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.

Security Domains

- A domain is a set of resources available to a subject.
- A subject can be a user, process, or application.
- Within an operating system, a process has a domain, which is the set of system resources available to the process to carry out its tasks.
- These resources can be memory segments, hard drive space, operating system services, and other processes.
- In a network environment, a domain is a set of physical and logical resources that is available, which can include routers, file servers, FTP service, web servers.

Directory Services

- A network service is a mechanism that identifies resources (printers, file servers, domain controllers, and peripheral devices) on a network.
- A network directory service contains information about different resources and the subjects that need to access them and carries out access control activities.
- If based on X.500 standard, it works in a hierarchical schema that outlines the resources' attributes, such as name, logical and physical location, subjects that can access them, and the operations that can be carried out on them.
- In an X500 database access requests made from users and other systems using the LDAP protocol provides a hierarchical structure of objects (subjects and resources).
- The directory service develops unique distinguished names for each object and appends the corresponding attribute to each object as needed.
- The directory service enforces a security policy to control how subjects and objects interact.

Thin Clients

- A thin client is a computer that runs from resources stored on a central server instead of a localized hard drive.
- Thin clients work by connecting remotely to a server-based computing environment where most applications, sensitive data, and memory, are stored.
- There are several advantages such as cost savings, ease of administration by having the software in one place and it is easier to control malware infections.

Accountability

- Once a user has been authenticated and granted authorized access accounting ensure policies are followed and users are accountable for their actions.
  - Accountability and auditing ensures bad deeds are tracked to source and stopped
  - Auditing mechanisms allow
    - Intrusion detection
    - Event monitoring & event reconstruction
    - System monitoring

Accountability

- Provide legal recourse (documented evidence)
- Provide reports, logs files and documentation
- Event monitoring can aid in detecting system performance problems or operational errors

Accountability

- System-level events:
  - System performance
  - Logon attempts (successful and unsuccessful)
  - Logon ID
  - Date and time of each logon attempt
  - Lockouts of users and terminals
  - Use of administration utilities
  - Devices used
  - Functions performed
  - Requests to alter configuration files

Auditing

- Enable appropriate level of auditing to ensure all required events are tracked
- Audit logs can become very large and unmanageable quickly
  - Log management tools required to administer log information
- Audit logs must be reviewed by a human to be valuable
- Audit logs are protected and only Administrators have access
  - Hacker tampering, User accidental or deliberate deletion
- Audit log retention policies provide adequate protection
  - Security logs overwriting daily may not be ideal

Auditing & Logging

- **Keystroke Monitoring**
  - Active user key logging
    - Stores every key pressed by user
  - Usually done in special circumstances
  - Can be used by hackers to gain passwords
  - Privacy and legal considerations if done without authorization

Auditing & Logging

- Protecting Audit Data and Log Files
  - Only Administrators should have access to audit data
  - Should protect against accidental corruption, deletion or alteration
  - Should implement appropriate retention policy
    - Backup and store Audit and Log information for period of time
  - Confidentiality and Integrity of log files is priority
    - May be used in court of law

FANSHAWE

Session Management

- A session is an agreement between two parties to communicate interactively.
- Session management is the process of establishing, controlling, and terminating sessions. The session establishment usually entails authentication and authorization of one or both endpoints.
- Controlling the session can involve logging the start and end and anything in between. It could also keep track of time, activity, and even indicia of malicious activity. These are three of the most common triggers for session termination.

  - **Timeout**: When sessions are established, the endpoints typically agree on how long they will last.

  - **Inactivity**: Some sessions could go on for very long periods, if the user is active.

  - **Anomaly:** Usually, anomaly detection is an additional control added to a session that is triggered by timeouts or inactivity (or both). This control looks for suspicious behaviors in the session, such as requests for data that are much larger than usual or communication with unusual or forbidden destinations. These can be indicators of session hijacking.

Digital Identity

- A user's identity can be a collection of their **attributes** (*department, role in company, shift time, clearance*, and others); their **entitlements** *(resources available to them, authoritative rights in the company*, and so on); and their **traits** (*biometric information, height, sex*, and so forth).
  - If a user requests access to a database that contains sensitive employee information, the IdM solution would need to pull together the necessary identity information and their supplied credentials before they are authorized access.
- The directory (or meta-directory) of the IdM system has all of this identity information centralized, which is why it is so important.

Access Control Markup Language

- HTML – HyperText Markup Language
  - Used for static web pages
  - Based on GML & SGML
    - Generalized Markup Language
    - Standard Generalized Markup Language
- XML – Extensible Markup Language
  - Specification used to create other XML standards for different industries

Access Control Markup Language

- SPML – Service Provisioning Markup Language
  - Based on XML specifications
  - Allows a user authenticated on one system to pass credentials to another system
  - *Producer of assertions* is sending company
  - *Consumer of assertions* is receiver of credentials
- XACML – eXtensible Access Control Markup Language
  - Use to share security policy rules between companies

OpenID

- *OpenID* is an open standard for user authentication by third parties.
- By relying on specialized identity providers (IdPs) such as Amazon, Google, or Steam, developers of Internet services (e.g., websites) do not need to develop their own authentication systems.
- Instead, they are free to use any IdP or group of IdPs that conforms to the standard. All that is required is that all parties use the same standard and that everyone trusts the IdP(s).

- OpenID, currently in version 1.0, defines three roles:
  - **End user** The user who wants to be authenticated in order to use a resource.
  - **Relying party** The server that owns the resource that the end user is trying to access
  - **OpenID provider** The IdP (e.g., Google) in which the end user already has an account and which will authenticate the user to the relying party

OAuth

- OAuth is an open standard for **authorization** to third parties. The general idea is that this lets you authorize a website to use something that you control at a different website.
  - E.g. LinkedIn asks you to let it have access to your Google contacts in order to find your friends who already have accounts in LinkedIn.
  - If you agree, you will next see a pop-up from Google asking whether you want to authorize LinkedIn to manage your contacts. If you agree to this, LinkedIn gains access to all your contacts until you rescind this authorization.
- OAuth solves a different but complementary problem than OpenID: instead of a third party allowing a user to access a website, a user allows a website to access a third party.

OpenID Connect

- OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User.
- OIDC supports three flows:
  - **Authorization code flow** The relying party is provided an authorization code (or token) and must use it to directly request the ID token containing user information from the IdP.
  - **Implicit flow** The relying party receives the ID token containing user information with the redirect response from the IdP after user authentication and consent. The token is passed through the user's browser, potentially exposing it to tampering.
  - **Hybrid flow** Essentially a combination of the previous two flows.

Integrating Identity as a Service

- Identity as a Service **(IDaaS)** is a type of Software as a Service **(SaaS)** offering that is normally configured to provide single sign on **(SSO),** federated IdM, and password management services. Most IDaaS vendor's focus on cloud and web-centric systems, it is possible to use their products for IdM on legacy platforms within the enterprise network.
- There are two basic approaches to architecting identity services: **in-house** or **outsourced**. The first approach, in-house, is simple because all the systems and data are located within the enterprise. In an outsourced model, on the other hand, an external party will host most or all of the systems or data.

Integrating Identity as a Service - IDaaS

- **On-premise**
- An on premise IdM system have all needed resources under your physical control. This usually means that you purchase or lease the necessary hardware, software, and licenses and then use your own team to build, integrate, and maintain the system.
  - Some research companies and government organizations have networks that are air-gapped for security.
- **Cloud**
- Some regulated industries may not be able to use IDaaS and remain compliant. This is because a critical function (i.e., IdM) is being outsourced and the service provider may not be able to comply with all the regulatory requirements.
  - Concerns that: the most critical data in the enterprise is exposed once it moves out of the enterprise.
  - Some legacy applications may not be supported.

Integrating Identity as a Service - IDaaS

- **Integration Issues**
- Integration of any set of different technologies or products is a complex and risky phases of deployment. To mitigate both the complexities and risks, it is necessary to carefully characterize each product or technology as well as the systems and networks into which they will be incorporated.
  - Plan how to address connectivity, trust, testing, and federation issues.
- **Establishing Connectivity**
- A critical requirement is that we need to ensure the components are able to communicate with one another in a secure manner.
  - In-house chokepoints are all internal to the organization's network.
  - Outsourced chokepoints are in the public Internet. Clearing a path for this traffic mean creating new rules for firewalls and IDS/IPS and must be restrictive enough to allow the IdM traffic, but nothing else, to flow between the various nodes.

Integrating Identity as a Service - IDaaS

- **Establishing Trust**
  - All traffic between nodes engaged in identity services must be encrypted e.g. PKI.
- **Incremental Testing**
  - When dealing with complex systems, assume that some important issue will not be covered in the plan.
  - This is why it is important to incrementally test the integration of identity services instead of rolling out the entire system at once.
- **Integrating Federated Systems**
  - Organizations have a remarkable amount of connectivity with other organizations and individuals. E.g. A contractor require access to some information systems but belongs to a different company's IdM architecture.
  - Suppliers or other partners systems communicate directly with yours in some limited capacity. The degree to which your systems are intertwined with others is not always realized.
  - Examine every external dependency and ensure that the proposed solution is compatible and correct parameters are known and tested.

Access Control Mechanisms

FANSHAWE

Access Control Models

- There are 5 access control models
  - Discretionary
  - Mandatory
  - Role based
  - Rule based
  - Attribute based

- Each model type uses different methods to control how subjects access objects, and each has its own merits and limitations

Discretionary Access Control

- When a user creates a file they are the owner of the file
- Owners may at their discretion grant access to other users
- System Administrator can allow resource owners to specify level of access to objects they own
- Most well known operating systems utilize discretionary access model
  - Windows, MAC, Linux, Unix

Mandatory Access Control

- Data owners or users do not control level of access to files they own
- Based on a security label system
  - Security labels assigned to subjects & objects
- Typically used by military or organizations where data secrecy and confidentiality is most important
  - Dedicated versions of Unix utilize (MAC) Access Model
- SE Linux
  - Security Enhanced Linux - Developed by NSA
- Trusted Solaris

Role-Based Access Control

- **RBAC**
  - Nondiscretionary access control
    - Permission on a role are predetermined
  - User is assigned access granted to the role
  - Easier administration
  - Best for organizations with very high turn over

Role-Based Access Control

- Two types of RBAC Access Models
- **Core RBAC**
  - User can be a member of many roles
  - Inherits permissions of all roles
  - Can include controls for time of day, etc.
- **Hierarchical RBAC**
  - Access maps to hierarchical employee structure of company
  - Access limitations are defined based on authority and responsibility

Role-Based Access Control

- **Static Separation of Duties (SSD)**
  - User can not be a member of 2 roles with conflicts
  - Cashier & auditor
- **Dynamic Separation of Duties (DSD)**
  - User member of both roles
  - Can not login to both roles at same time

Access Control Techniques

- **Rule-Based Access Control**
  - Rules apply to all regaurdless of identity
  - Typically used in MAC based systems as an enforcement mechanism
  - Uses If-Then logic to define access conditions
    - Time of day, security clearance
  - Developer friendly
    - Easier to define access scenarios

Attribute-Based Access Control

- *Attribute-based access control (ABAC)* uses attributes of any part of a system to define allowable access. These attributes can belong to belong to **subjects, objects, actions, or contexts**. Here are some possible attributes to describe ABAC policies:
  - **Subjects** Clearance, position title, department, years with the company, training certification on a specific platform, member of a project team, location.
  - **Objects** Classification, files pertaining to a particular project, HR records, location, security system component.
  - **Actions** Review, approve, comment, archive, configure, restart.
  - **Context** Time of day, project status (open/closed), fiscal year, ongoing audit.

Access Control Techniques

- **Constrained User Interface**
  - Users denied access to data or functionality
  - Database views
    - Database view may limit returned data
  - Menu or shell
    - Command options in menu or shell are limited for the user
  - Interface
    - Limit keys on keypad

Central Access Control

- **RADIUS**
  - Remote Access Dial-in User Service
  - Used by most ISP
  - Client connect to ISP access server with ppp protocol
    - Sends password via CHAP, PAP or EAP
  - ISP access server sends authentication request to authentication server via RADIUS protocol
  - Used in Dial-in, VPN or wireless connection
  - Only password field encrypted
  - UDP transport
  - Maximum 256 AVP (2^8)
    - Attribute Value Pairs – AAA settings

Access Control Techniques

- **TACACS**
  - Terminal Access Control Access Control System
  - TACACS+ newest version
  - Allows 2 factor authentication
  - One-time passwords
  - Complete data packet encrypted
  - TCP transport
  - More attributes than some free versions of RADIUS

Access Control Techniques

- **Diameter**
  - Protocol name play on RADIUS
    - Diameter is twice the RADIUS
  - Newest AAA protocol
  - Base protocol allows for extensions for different protocols such as VoIP, wireless and others
  - TCP transport
  - Maximum 4 billion AVP (2^{32})
  - Peer to peer connection with NAC devices
    - Can request NAC to get more info from login client
    - RADIUS & TACACS+ are client server

Mobile IP

- **Mobile IP**
- This technology allows a user to move from one network to another and still use the same IP address.
- It is an improvement upon the IP protocol because it allows a user to have a *home IP address*, associated with his home network, and a *care-of address*.
- The care-of address changes as he moves from one network to the other. All traffic that is addressed to his home IP address is forwarded to his care-of address.

Access Control Matrix

- **Access Control Matrix**
  - Table listing objects and subjects
  - Usually used by DACL
  - Specifies level of access between an object and subject
    - File2 – Diane can Read, Write, Execute
    - File2 – Katie can Read, Execute
    - File2 – John has no access

User	File1	File2	File3
Diane	Read and execute	Read, write, and execute	No access
Katie	Read and execute	Read	No access
Chrissy	Read, write, and execute	Read and execute	Read
John	Read and execute	No access	Read and write

Table 5-2 Example of an Access Control Matrix

Access Control Matrix

- Capability Table
  - Specifies access granted to a subject
  - Property of the subject
  - The row in the access control matrix show the permissions (capability) for subject Curly to the objects File1-4

Access Control Matrix

	Subject	File 1	File 2	File 3	File 4
	Larry	Read	Read, write	Read	Read, write
Capability	Curly	Full control	No access	Full control	Read
	Mo	Read, write	No access	Read	Full control
	Bob	Full control	Full control	Full control	No access
				ACL	

Capability = row in matrix
ACL = column in matrix

Figure 5-23 A capability table is bound to a subject, whereas an ACL is bound to an object.

Access Control Techniques

- **Access Control List**
  - Property of an object
  - List permissions granted to which subjects
  - Maps values from access control matrix to the object
  - Column in the matrix
  - The ACL for File1 is the permissions in the column under File1

User	File1
Diane	Read and execute
Katie	Read and execute
Chrissy	Read, write, and execute
John	Read and execute

Table 5-3 The ACL for File1

Access Control Techniques

- **Content-Dependent Access Control**
  - Content within object dictates access
  - Spam Filtering (keyword)
    - Match = no access
    - No Match = access
    - Content filtering
- Context-Dependent Access Control
  - Access is based on the data in the context of a packet flow not just a key word
  - Stateful firewall is example
    - State of TCP connection

Managing the Identity & Access Provisioning Life Cycle

- Usually part of regulatory requirement
- Work flow process for
  - Creation of new accounts
  - Removal of accounts no longer required
    - Terminated employees, contract employees
- Provisioning
  - Data for new account pulled from Human Resource data
    - Authoritative source
  - All user identity attributes stored in an *identity repository*
    - *Meta-directory or virtual directory*

User Access Review

- The list of conditions under which an account is disabled or de-provisioned will vary by organization.
- User access reviews ensure that all active accounts are actually needed.
- User accounts should be disabled or de-provisioned when an employee is terminated, other situations require a deliberate review by the individual's supervisor and/or the IT department:
  - Extended vacation or sabbatical
  - Hospitalization
  - Long-term disability (with an expected future return)
  - Investigation for possible wrong-doing
  - Unexpected disappearance

System Account Access Review

- **System Account Access Review**
- Conduct system account access reviews both periodically and when certain conditions are met.
  - A systematic approach to system account access review is the best way to avoid ending up with unneeded, potentially privileged accounts.
- **De-provisioning**
- Sooner or later every account gets de-provisioned.
- For system accounts, this could happen because a system or configuration change rendered an account unnecessary.
- A potential challenge with de-provisioning accounts is that it could leave orphaned resources.
  - When de-provisioning accounts, therefore, it is important to transfer ownership of its resources to someone else.

FANSHAWE

Controlling Physical and Logical Access

- **Access Control Layers**
- Access control consists of three broad categories: **administrative, technical, and physical**. Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.
- Each category of access control has several components that fall within it:
  - **Administrative controls:**
  - Policy and procedures
  - Personnel controls
  - Supervisory structure
  - Security-awareness training
  - Testing

Physical Control

- **Physical controls** supplement administrative and technical controls
  - Network segregation is done through physical or logical means
  - Perimeter security
  - Computer controls
  - Work area separation dictates certain employees have access to specific areas
  - Data backups
  - Cabling
  - Control zones – public lobby, executive office, production

Technical Control

- Software tools found in operating systems, applications and add-on security packages
  - **System Access**
    - (MAC, DAC)
  - **Network architecture** utilizes logical means of segregating network resources
    - Public Network, DMZ (Demilitarized Zone), Internal Network
  - **Network Access** utilizes each systems logical controls to authenticate and authorize access to various resources
    - Firewall ACL rules
    - Router rules
    - Proxy Server rules

Technical Control

- **Encryption and protocols** ensure data integrity confidentiality remains in tact
- **Auditing** utilizes inherent system or application controls to track user activity
  - Track security breach

Access Control Practices

The following is a list of tasks that must be done on a regular basis to ensure security stays at a satisfactory level:

- Deny access to systems to undefined users or anonymous accounts.
- Limit and monitor the usage of administrator and other powerful accounts.
- Suspend or delay access capability after a specific number of unsuccessful logon attempts.
- Remove obsolete user accounts as soon as the user leaves the company.
- Suspend inactive accounts after 30 to 60 days.
- Enforce strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unneeded system features, services, and ports.
- Replace default password settings on accounts.
- Limit and monitor global access rules.
- Remove redundant resource rules from accounts and group memberships.
- Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
- Enforce password rotation.
- Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
- Audit system and user events and actions, and review reports periodically.
- Protect audit logs.

Unauthorized Disclosure of Information

- To disclose information to an individual who is not authorized to receive it.
- An event involving the exposure of information to entities not authorized access to the information.
- A communication or physical transfer of classified national intelligence an to unauthorized recipient.
- **Object reuse:**
- Protects confidentiality of objects that are reassigned after initial use. E.g. a deleted file still exists on storage media;
- Residual data may be restored, which describes the problem of *data remanence.* Object-reuse requirements define procedures for actually erasing the data.

Emanation Security (EMSEC)

- (**EM**anations **SEC**urity/**EM**issions **SEC**urity)
- The protection against frequencies emanating from chips, bus pathways and communication lines. Sabotage is accomplished by covert receivers that detect the frequencies and software that isolates the data and looks for account numbers, passwords or other private information.

Tempest

- An umbrella term for external electromagnetic radiation from data processing equipment and the security measures used to prevent them.
- Almost all electronic equipment, including chips, bus pathways and metal communications lines, emanates signals into free space or surrounding conductive objects such as metal cabinets, wires and pipes.
- Equipment and cables that meet TEMPEST requirements have extra shielding in order to keep data signals from escaping and being picked up by unauthorized eavesdropping.
- It is also possible to use TEMPEST software that generates sufficient electronic noise to mask meaningful radio-frequency emissions.

Access Control Monitoring

- **Intrusion Detection System - IDS**
  - Process specifically designed to detect unauthorized access, use or attack vector against a network resource
- Looks for unusual patterns or activity
- Alerts on non-normal behaviour
- Two types of Intrusion Detection Systems
  - NIDS - Network Intrusion Detection System
  - HIDS - Host Intrusion Detection System

NIDS

- Uses sensors connected to various points on network
  - Individual computers or dedicated devices
  - Monitors network traffic
  - Sniffer on network
  - Send alerts to a central management system
  - NIDS software places network adapter card into promiscuous mode
    - Process all network traffic not just packets destined for network adapter on NIDS

Host Based IDSs

- **Host Intrusion Detection System**
  - Installed on individual PC's (Workstations/Servers)
  - HIDS monitors computer processes and behaviour
  - Changes to critical system files, configuration files, Windows registry locations, file integrity, system statistics
  - Alerts on any changes to above items
  - Typically installed on critical Servers

HIDS

- **Signature-based:**
  - Pattern matching
  - Stateful matching
- **Anomaly-based:**
  - Statistical anomaly–based
  - Protocol anomaly–based
  - Traffic anomaly–based
  - Rule- or heuristic-based

Intrusion Detection

- **Signature-based** IDS examines for a specific attack
- Each attack has a known signature or bit pattern
  - **Pattern matching**
    - XMAS attack (all flags in TCP header set to value 1)
  - Most used method
  - Requires frequent updates

Intrusion Detection

- Anomaly based IDS look for changes in the normal activities or behaviour on a system
  - **Statistical anomaly**
    - User log on at 3am
  - **Protocol anomaly**
    - Outside normal expected operation
    - Covert channel – HTTP call back
  - **Traffic anomaly**
    - DoS – SYN flood

Intrusion Detection

- **Heuristic analysis** is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods

- **Rule-based IDS**
  - Used on expert systems
  - Inference engine gathers data from sensor or log and processes to determine attack

Intrusion Prevention System

- IPS will stop traffic identified as attack
- Inline device like a firewall
- IPS is proactive
  - Will drop packets
  - Send reset for TCP connection back to source address
  - Rate limit interface to reduce packets entering network
- IDS is detective
  - Send alert or log attack
  - Can not stop or prevent

Honeypots

- **Honeypots** are decoy systems or servers deployed alongside production systems within your network.
- When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target.

- **A network sniffer** (also known as network analyzer or packet analyzer) is a software or hardware that can intercept and log traffic on a network. The sniffer captures each packet that flows across the network and analyzes its content.

Threats to Access Control

- There is more risk and a higher probability of an attacker causing mayhem from within an organization than from outside it.
- Most of the security **threats** and **risks** to an organization are the result of inadequate and improper **access control**.
- Poor **access control** can expose the organization to unauthorized **access** of data and programs, fraud, or the shutdown of computer services.

Dictionary Attack

- A **dictionary attack** is a method of breaking into a password-protected computer or server by systematically entering every word in a **dictionary** as a password.
- **Countermeasures**
  - To properly protect an environment against dictionary and other password attacks, the following practices should be followed:
  - Do not allow passwords to be sent in clear text.
  - Encrypt the passwords with encryption algorithms or hashing functions.
  - Employ one-time password tokens.
  - Use hard-to-guess passwords.
  - Rotate passwords frequently.
  - Employ an IDS to detect suspicious behavior.
  - Use dictionary-cracking tools to find weak passwords chosen by users.
  - Use special characters, numbers, and upper- and lowercase letters within the password.
  - Protect password files.

Brute–Force Attacks

- A **brute force attack** is an attempt to crack a password or username or find a hidden web page, or find the key used to encrypt a message, using a trial and error approach and hoping, eventually, to guess correctly.
- **Countermeasures**
- For phone brute-force attacks, auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate a war-dialing attack:
  - Perform brute-force attacks to find weaknesses and hanging modems.
  - Make sure only necessary phone numbers are made public.
  - Provide stringent access control methods that would make brute-force attacks less successful.
  - Monitor and audit for such activity.
  - Employ an IDS to watch for suspicious activity.
  - Set lockout thresholds.

Phishing and Pharming

- ***Phishing*** is a type of social engineering with the goal of obtaining personal information, credentials, credit card number, or financial data. The attackers lure, or fish, for sensitive data through various different methods.
- ***Pharming***, which redirects a victim to a seemingly legitimate, yet fake, website. In this type of attack, the attacker carries out something called *DNS poisoning*, in which a DNS server resolves a hostname into an incorrect IP address.
- When a phishing attack is crafted to trick a specific target and not a large generic group of people, this is referred to as a ***Spear-Phishing*** *attack*.

Summary

- Access controls are the first line of defense in asset protection.
- They are used to dictate how subjects access objects, and their main goal is to protect the objects from unauthorized access.
- These controls can be administrative, physical, or technical in nature and should be applied in a layered approach, ensuring that an intruder would have to compromise more than one countermeasure to access critical assets.
- Access control defines how users should be identified, authenticated, and authorized.
- Access control needs to be integrated into the core of operating systems through the use of DAC, MAC, RBAC, RB-RBAC, and ABAC models. It needs to be embedded into applications, network devices, and protocols and enforced in the physical world through the use of security zones, network segmentation, locked doors, and security guards.
- Security is all about keeping the bad guys out, and unfortunately there are many different types of “doorways” they can exploit to get access to our most critical assets.

Homework

- Read the relevant chapter in the set book 'All In One CISSP Exam Guide' – by Shon Harris.

- Depending on which edition you have the relevant sections will be in different places – so use the index.

- Then identify and do the practice m/c questions relating to this subject.

Questions

- ?