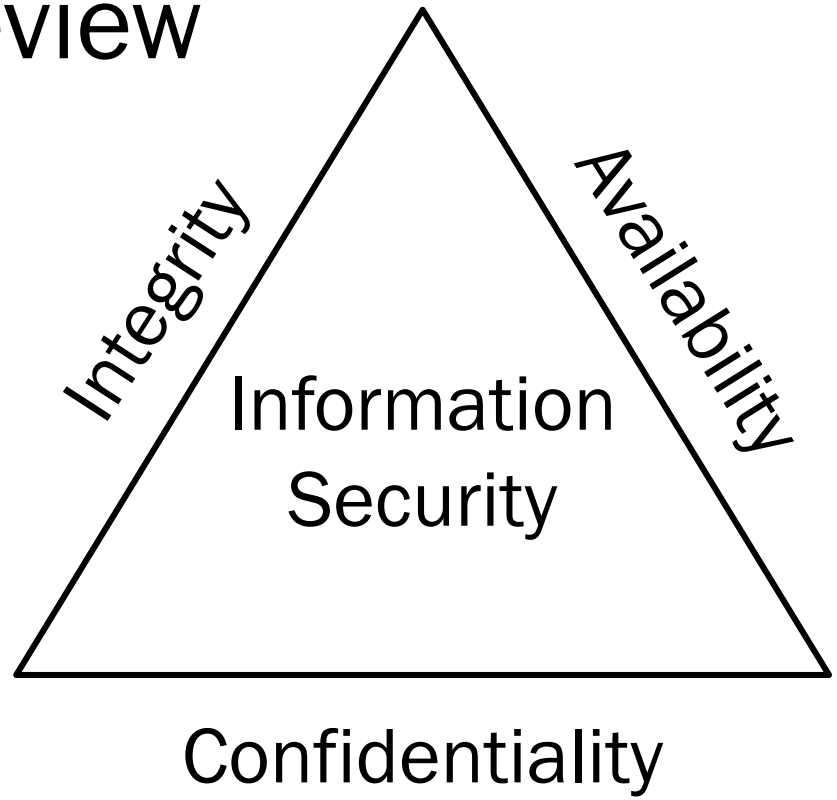
Unit 2 Review



Quantitative Analysis

A quantitative impact analysis assigns a dollar value to the impact

Qualitative Analysis

A qualitative impact analysis assesses impact in relative terms such as high impact, medium impact, and low impact without assigning a dollar value to the impact

Quantitative vs. Qualitative

- **Quantitative**
- Focuses on factual and measurable data

- **Qualitative**
- Focuses on perceptions about the probability of a risk occurring

10. What is the main advantage of using a quantitative impact analysis over a qualitative impact analysis?

A. A qualitative impact analysis identifies areas that require immediate improvement
B. A qualitative impact analysis provides a rationale for determining the effect of security controls
C. A quantitative impact analysis makes a cost benefit analysis simple
D. A quantitative impact analysis provides specific measurements of attack impacts

Answer: A

14. A business asset is best described by which of the following?

A. An asset loss that could cause a financial or operational impact to the organization
B. Controls put in place that reduce the efforts of threats
C. Competitive advantage, capability, credibility, or goodwill
D. Personnel, compensation, and retirement programs

Answer: C

Which option most accurately reflects the goals of risk migration?

A. Determining the effects of a denial of service and preparing the company's response
B. The removal of all exposure and threats to the organization
C. Defining the acceptable level of risk and assigning the responsibility of loss or disruption to a third-party, such as an insurance carrier
D. Defining the acceptable level of risk the organization can tolerate and reducing risk to that level

Answer: D

Risk Registers

Authentication

Authorization

Accounting

ACCESS CONTROLS


GRANT ME the SERENITY to ACCEPT THAT MY PASSWORD WILL BE HACKED, THE COURAGE to FREQUENTLY CHANGE IT, AND the WISDOM to COME UP WITH A BETTER ONE.
12 - STEP VERIFICATION
klossner

Identity (Who Is the Subject?)

Identification

- Asserts a unique user or process identity
- Typically in the form of an assigned user name
- Could be public information whether intentional or not

Registration of New Users

- **Manual user registration:**
  - Greatest granularity
  - Too high of an administrative burden

- **Automated provisioning solutions:**
  - Provide a framework for managing access control policies

Periodic Review of Access Levels

The periodic review of user access levels is incorporated into regulations, including Sarbanes–Oxley

Clearance

Critical where access controls are based on security labels

Trusted user directory

Certificates

Authentication (Proof of Identity)

Verification that the identity presented belongs to the party that has presented it.

Password Reset

Consume a large volume of time in most IT support departments

Provide an effective entry vector for social engineering attacks

Password Reset Made Easy

https://www.darkreading.com/endpoint/self-service-password-reset-and-social-engineering-a-match-made-in-hell/a/d-id/1325891

https://specopssoft.com/blog/social-engineering-warning-watch-out-for-that-password-reset-call/

https://www.csoonline.com/article/3203386/security/even-weak-hackers-can-pull-off-a-password-reset-mitm-attack-via-account-registration.html

Mass Lockouts

Effective denial-of-service attack

Example: eBay Account Lockout Attack

Ownership

Something the user has in their possession

- Smart cards: Contact, contactless
- Dynamic passwords
- Tokens: Synchronous, asynchronous
- Radio Frequency Identification (RFID)

Characteristic

physical - Thumb print

Characteristic

- A physical trait of the user
- Allows for the confirmation of an individual's identity

Biometrics

- **Two steps:**
  - Enrollment process
  - Verification process

- **Two main classifications:**
  - Behavioral
  - Physiological

Behavioral Biometrics

Signature analysis

Voice pattern recognition

Keystroke dynamics

Physiological Biometrics

- Fingerprint verification technology
- Hand geometry technology
- Eye features/retina scan
- Eye features/iris scan
- Facial recognition

Biometric Accuracy

Important terms

False Rejection Rate (FRR)

Rejects when valid

False Acceptance Rate (FAR)

Accepts when invalid

Physical Use as Identification

- Biometrics takes advantage of the unique physical traits of each user
- Arguably is the most effective methodology of identifying a user

99% confidence level

Tokens

Proves identity electronically

Used in addition to or in place of a password

Smart Card Applications

- Secure identity applications
- Healthcare applications
- Payment applications
- Telecommunications applications

Multifactor Authentication

Implement at least two of the three common techniques for authentication

- Knowledge based
- Token based
- Characteristic based

Two-Factor vs. Three-Factor Authentication

- In two-factor authentication, typically the mechanism provides for:
  - Something the user has
  - Something the user knows

- This can be significantly improved upon by incorporating a third factor

https://www.youtube.com/watch?v=0dFAyT4K0a4

Dual Control

No one person should have access to information that would allow the person to determine the encryption key quickly than a brute force attack

Time Outs

If the user leaves the proximity of the device authenticated after a specific time period, he or she is automatically logged off and the authentication process starts over

Reverse Authentication

Today, it is necessary to authenticate the website/page to the user as part of the authentication process

Certificate-Based Authentication

Relies on the machine that the user authenticates having a digital certificate installed that is used along with the encrypted user's password to authenticate the user and device

Authorization

A reference monitor typically grants access based on an ACL within the reference monitor

Access control list

Once access is granted, what the subject can then do is controlled by the authorization matrix or table

what Actor/subject can do!

Access to Systems vs. Data, Networks

Defining ACLs that only address access to systems can facilitate unintended user access

Including access controls to specific data within a given system increases overall security

Access Control Lists/Matrix

- **Authorization table**
  - A matrix of access control objects, access control subjects, and their respective rights

- **Access control matrix**
  - Provide simple user interface to implement an ACL
  - Determines the access

Directories

Lightweight Directory Access Protocol (LDAP)

X.500

Microsoft Active Directory Directory Service

Single Sign-On (SSO)

An authentication mechanism that allows a single identity to be shared across multiple applications

Allows the user to authenticate once and gain access to multiple resources

The primary purpose of SSO is for the convenience of the user

SSO Implementation: Kerberos

- Designed to provide strong authentication using secret-key cryptography
- An operational implementation of key distribution technology

Kerberos Process

1. Request a ticket to the Kerberos TGS from the Kerberos AS
2. AS looks up the access control subject and generates a session key
3. Access control subject decrypts the first message and recovers the session key
4. Access control subject sends a request to the TGS for a ticket to a particular target server

Kerberos Process

5. TGS decrypts the TGT and uses the session key to decrypt the authenticator
6. TGS creates a new session key
7. Access control subject decrypts the message and extracts the session key
8. Target access control object server decrypts and checks the ticket and the authenticator
9. Server sends the access control subject a message

Kerberos Considerations

- Overall security depends on careful implementation
- Requires trusted and synchronized clocks across the enterprise network
- Enforce limited lifetimes for authentication based on time stamps
- The Key Distribution Server must be physically secured
- Isolate the Key Distribution Server on the network
- The AS can be a critical single point of failure

Comparing Internetwork Architectures

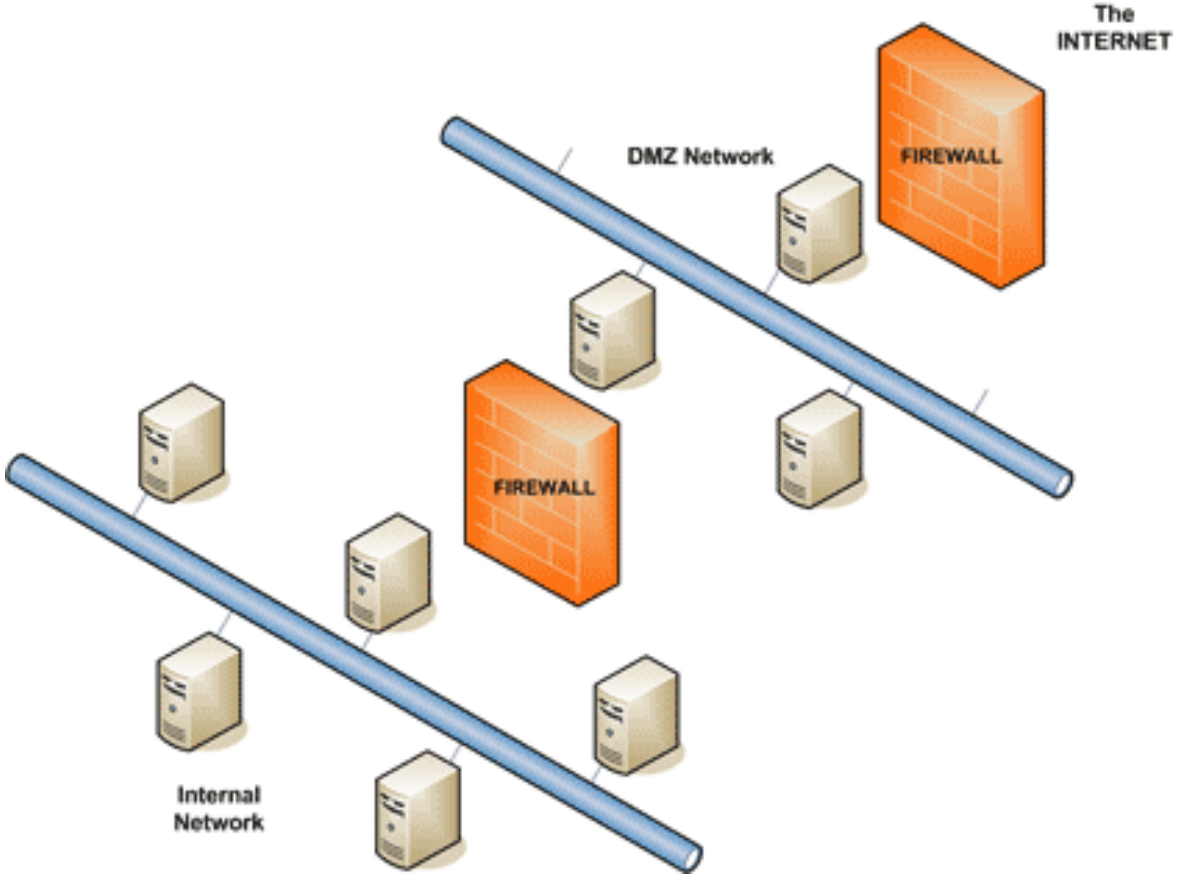
Internet

Intranet

Extranet

Demilitarized Zone (DMZ)

Typical DMZ Design



One-Way Trust

- A unidirectional authentication path that is created between two domains
- Some one-way trusts can be either a non-transitive trust or a transitive trust

Two-Way Trust

In a two-way trust, Domain A trusts Domain B, and Domain B trusts Domain A

Authentication requests can be passed between the two domains in both directions

Some two-way relationships can be either non-transitive or transitive

Transitive Trust

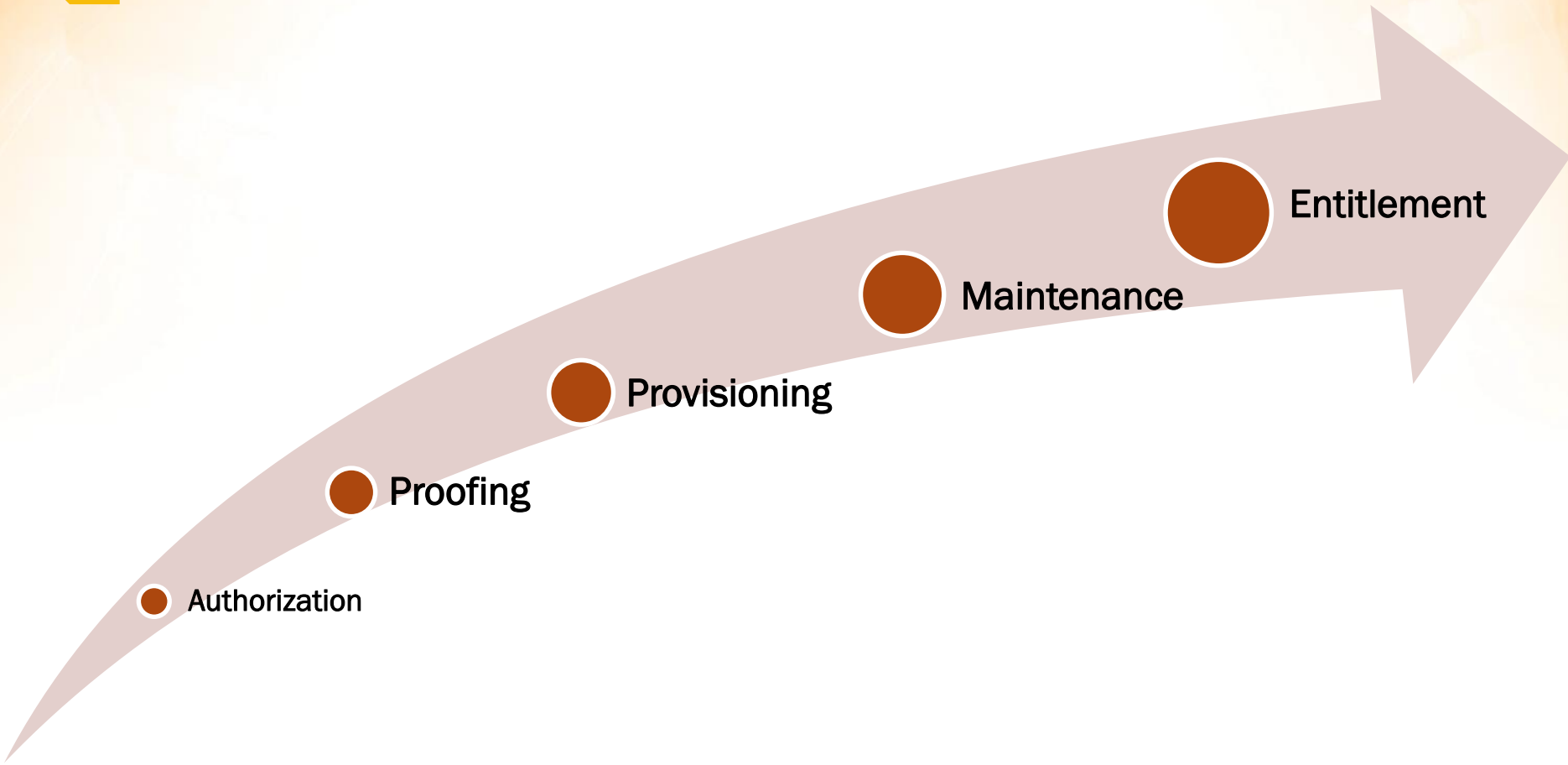
- Transitivity determines whether a trust can be extended outside the two domains between which the trust was formed
- You can use a transitive trust to extend trust relationships with other domains
- You can use a non-transitive trust to deny trust relationships with other domains


IST
MIT STUDENTS:
SIGN UP HERE FOR
$(\frac{\pi}{2})*(\sum_{n=0}^{\infty}\frac{(-1)^n}{2n+1})^{-1}$-FACTOR
AUTHENTICATION
@MIT

Identity Management

- Identity management is the task of controlling information about users on computers
- Goal:
  - Improve company-wide productivity and security, while lowering the costs associated with managing users

Identity Management Life Cycle



Authorization

Determines whether a user is permitted to access a particular resource

Performed by checking the resource access request against authorization policies that are stored in an Identity Access Management (IAM) policy store

Provisioning

Creation of the identifier for the identity

Linkage to the authentication providers

Setting and changing attributes and privileges

Decommissioning of the identity

Maintenance

User management

Delegated administration

Self-password reset

Entities

People

Devices

Organizations

Code

Agents

Entitlement Defined

A set of rules, defined by the resource owner, for managing access to a resource and for what purpose

Mandatory Access Control (MAC)

- Eliminates problems of relying on each system owner to properly control access to each object
- The system participates in applying a mandatory access policy
- The system owner applies the “need to know” element

Non-Discretionary Access Control

Non-discretionary policies establish controls that cannot be changed by users but only through administrative action

Discretionary Access Control (DAC)

A DAC policy is a means of assigning access rights based on rules specified by the owner

Rule Set-Based Access Controls (RSBAC)

Discretionary controls giving data owners the discretion to determine the rules necessary to facilitate access

Many security policies can be implemented as a decision module

Role-Based Access Control (RBAC)

Users are granted membership into roles based on their competencies and responsibilities

The operations that a user is permitted to perform are based on the user's role

Simplifies the administration and management of privileges

Role Hierarchies

Natural way of organizing roles to reflect authority, responsibility, and competency

The role in which the user is gaining membership is not mutually exclusive with another role for which the user already possesses membership

Constrained User Interface (CUI)

Methodology that restricts the user's actions to specific functions by not allowing the user to request functions that are outside of his/her respective level of privilege or role

Types of Restricted Interfaces

Menu and Shells

Database views

Physically constraining a user interface

View-Based Access Control (VBAC)

Separates a given access control object into subcomponents and permits or denies access to view or interact with specific subcomponents

Content-Dependent Access Control (CDAC)

Protects databases containing sensitive information

Permits or denies access based on the explicit content within the object

Requires a great deal of labor in defining the respective permissions

Context-Based Access Control (CBAC)

Used in firewall applications to extend the firewall's decision-making process to:

- Decisions based on state
- Application-layer protocol session information

Temporal Isolation (Time-Based)

- Used to enhance or extend the capabilities of RBAC implementations
- Supports periodic role enabling and disabling and temporal dependencies

Attribute-Based Access Control (ABAC)

Subject requests to perform operations on objects are granted or denied based on:

- Assigned attributes of the subject
- Assigned attributes of the object
- Environment conditions
- A set of policies

New Forms of Two-Factor Authentication:
Your password plus ...