ACS-2821-001

Information Security in Business

Access Control Systems and Methodology

ACS-2821-001 – Slides Used In The Course

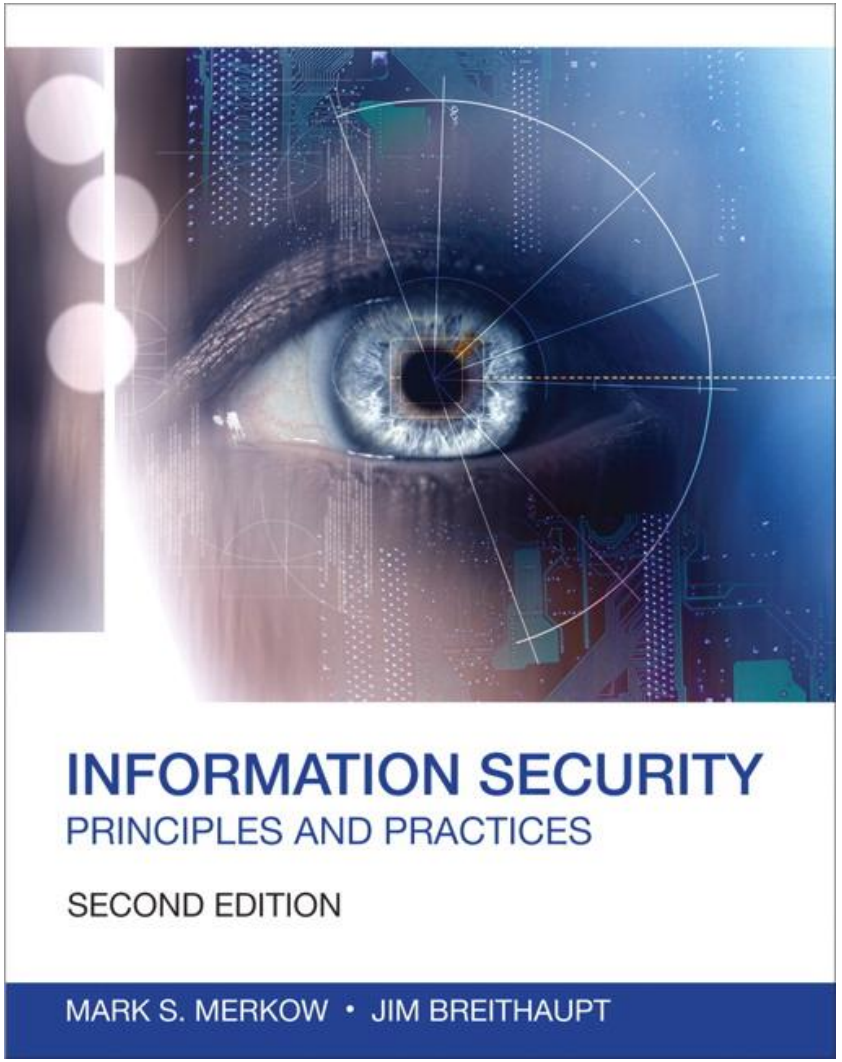
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Apply access control techniques to meet confidentiality and integrity goals
- Understand and implement the major terms and concepts related to access control and tie them to system security
- Apply discretionary access controls (DAC) and mandatory access controls (MAC) techniques as appropriate
- Choose effective passwords and avoid password limitations
- Implement password alternatives, including smart cards, password tokens, and other multifactor techniques
- Apply the goals of single sign-on concepts to business and common users
- Use the techniques described to control remote user access

Overview

- Access controls are a collection of mechanisms that work together to create security architecture to protect the assets of an information system
- One of the goals of access control is personal accountability, which is the mechanism that proves someone performed a computer activity at a specific point in time

Terms and Concepts

- Access control is the heart of an information technology (IT) security system and is needed to meet the major objectives of InfoSec: confidentiality and integrity
- Terms
  - Identification
  - Authentication
  - Least privilege
  - Information owner
  - Discretionary access control
  - Mandatory access control
  - Role-based access control
  - Access control lists
  - User provisioning

Terms and Concepts

- **Identification**
  - Identification credentials uniquely identify the users of an information system
  - Examples: name, initials, email address, or a meaningless string of characters, Social Security number, IDs, and others
- **Authentication**
  - Authentication credentials permit the system to verify one's identification credential
  - Password
- **Least Privilege (Need-to-Know)**
  - The predominant strategy to ensure confidentiality
  - The objective is to give people the least amount of access to a system that is needed to perform the job they're doing

Terms and Concepts

- **Information Owner**
  - Maintains overall responsibility for the information within an information system
  - The information owner must be the one to make the decisions about who uses the system and how to recover the system in the event of a disaster
- **Discretionary Access Control**
  - The principle of discretionary access control (DAC) dictates that the information owner is the one who decides who gets to access the system(s)
  - Most of the common operating systems on the market today (Windows, Macintosh, UNIX, Novell's Netware, and so forth) rely on DAC principles for access and operation

Terms and Concepts

- **Mandatory Access Control**
  - Also called nondiscretionary access control: The system decides who gains access to information based on the concepts of subjects, objects, and labels
  - Often used in military and government systems
  - **Subjects**: The people or other systems that are granted a clearance to access an object within the information system
  - **Objects**: The elements within the information system that are being protected from use or access
  - **Labels**: The mechanism that binds objects to subjects. A subject's clearance permits access to an object based on the labeled security protection assigned to that object

Terms and Concepts

- **Role-Based Access Control**
  - Involves assigning users to a group and then assigning rights to the group for access control purposes
  - RBAC methods are most appropriate where there is high turnover of employees and/or frequent movements between job roles

Terms and Concepts

- **Access Control Lists (ACL)**
  - A list or a file of users who are given the privilege of access to a system or resource (a database, for example)
  - Within the file is a user ID and an associated privilege or set of privileges for that user and that resource
  - Privileges typically include Read, Write, Update, Execute, Delete, or Rename
- **User Provisioning**
  - Granting access to new employees
  - Include checking management approvals for grating access

Principles of Authentication

- The idea of authentication is that only the legitimate user possesses the secret information needed to prove to a system that she has the right to use a specific user ID
- Authentication factors includes:
  - Something you know e.g. password
  - Something you have e.g. smart card or token
  - Something you are or do e.g. biometric – face or voice
- These secrets are commonly passwords, but history has shown that passwords are problematic:
  - Passwords can be insecure
  - Passwords are easily broken
  - Passwords are inconvenient
  - Passwords are reputable

Principles of Authentication

- Single factor authentication
  - Using passwords only for authentication
- Multifactor Authentication
  - Using more than one authentication mechanism
  - With two or three factors (multifactor authentication) to authenticate, an information owner can have confidence that users who access their systems are indeed authorized
  - This is accomplished by adding more controls and/or devices to the password authentication process

Principles of Authentication

- Two-Factor Authentication
  - With a two-factor authentication system, a user has a physical device (a card, a token, a smart card, and so forth) that contains his credentials, protected by a personal identification number (PIN) or a password that the user keeps secret
- Three-Factor Authentication
  - In a three-factor system, unique information related to the user is added to the two-factor authentication process
  - This unique information may be a biometric (fingerprint, retinal scan, and so forth) needed for authentication

Biometrics

- Biometric-based identification works by measuring unique human characteristics as a way to confirm identity
- Biometrics can be further broken down into static and dynamic
- Some common biometric techniques include
  - Fingerprint recognition (static)
  - Signature (dynamic)
  - Iris scanning (static)
  - Retina scanning (static)
  - Voice prints(dynamic)
  - Face recognition (static)
- The most common biometric in use is fingerprint recognition
- Accuracy of a biometric is measured in terms of matching errors, i.e. false acceptance rate (FAR) and false rejection rate (FRR)

Biometrics

- False Rejection Rate (FRR)
  - Measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user
- False Acceptance Rate (FAR)
  - Measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user
- No one type is more accurate then the other, and none is foolproof

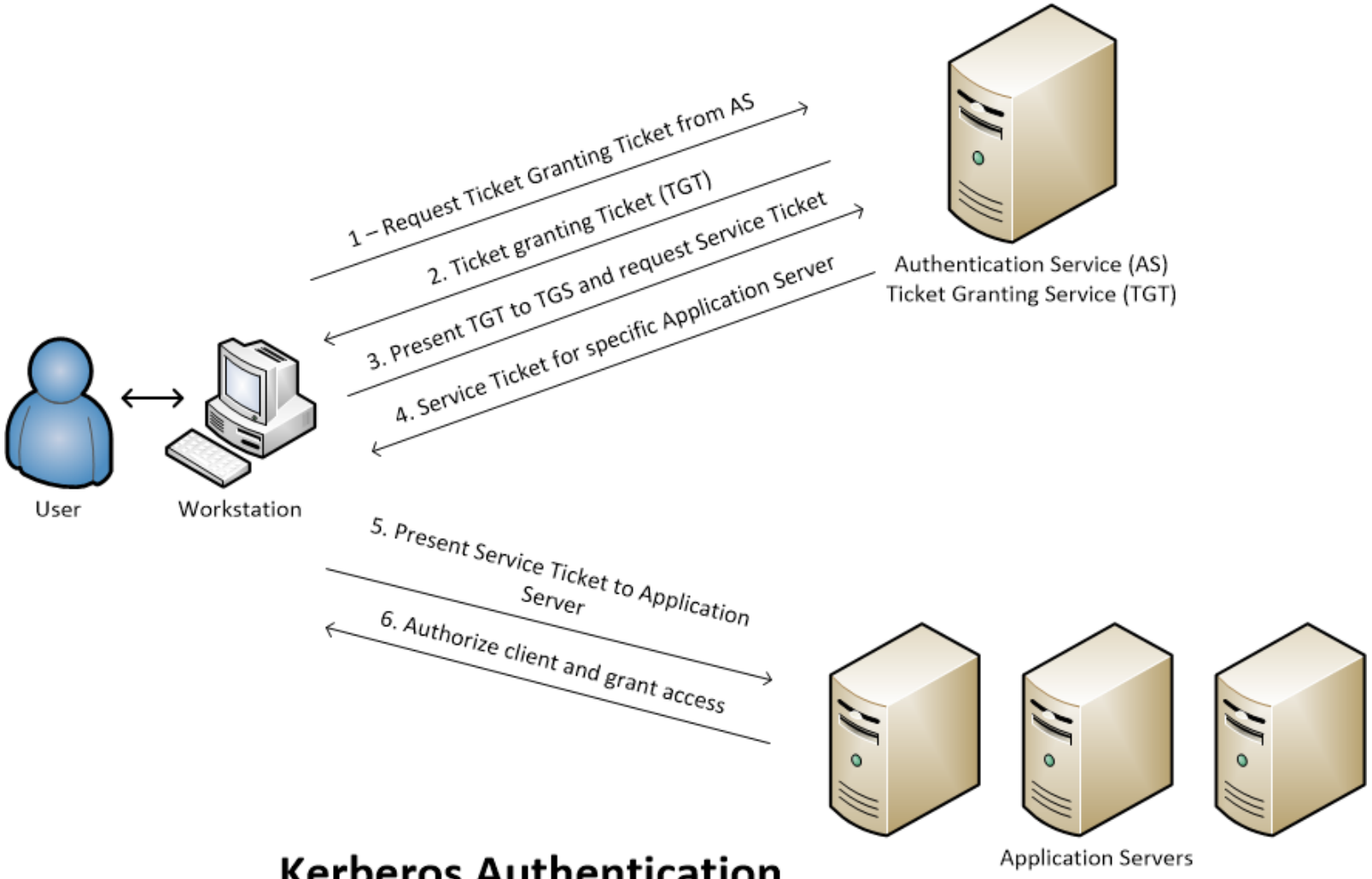
Single Sign-On

- In an SSO system, users have one password for all corporate and back-office systems and applications they need to perform their jobs
  - One consistent password can be remembered and used, thus increasing the security of the overall system of access controls
  - Single Sign-On mechanisms include
    - Password Safe
    - Kerberos
    - Proprietary and custom developed solutions

Single Sign-On

- Kerberos
  - Kerberos is designed to provide authentication for client/server applications by using symmetric-key cryptography
  - A free implementation available from MIT
  - Works by assigning a unique key, called a ticket, to each user
  - User logs in once and then can access all resources based on the permission level associated with the ticket

Single Sign-On



Single Sign-On

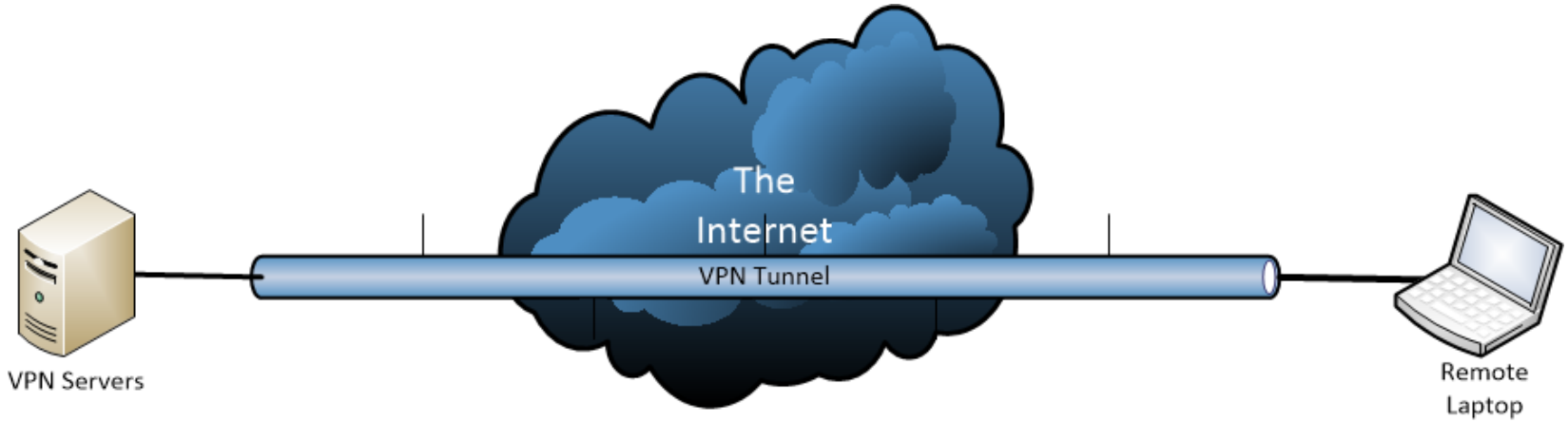
- Federated Identities
  - Facebook
    - Sites have an arrangement with Facebook so users can log in with their Facebook credentials and don't have to create a new unique user name and password
  - Google
  - LinkedIn

Remote User Access and Authentication

- Additional access control mechanisms are required because of the use of insecure networks to create a connection to the corporate local area network
  - Remote Access Dial-In User Service (RADIUS)
    - RADIUS is a client/server protocol and software that enables remote access users to communicate with a central server to authorize their access to the requested system or service
    - Authenticating to a RADIUS server might require a user ID and password or token or smart card

Remote User Access and Authentication

- Virtual Private Networks
  - With a VPN, a user connects to the Internet via his or her ISP and initiates a connection to the protected network, creating a private tunnel between the end points that prevents eavesdropping or data modification
  - Uses cryptography to both authenticate sender and receiver and to encrypt the traffic



Summary

- Access control is needed to meet the goals of confidentiality, integrity, and user accountability—essential for trust in an information system
- Access control is done using discretionary means, mandatory means, and role-based means
- Identification and authentication techniques sometimes use biometric information to add further confidence that users are legitimate
- Single sign-on and associated technologies and protocols aim to reduce the proliferation of IDs and passwords to better control the security of access control mechanisms
- Remote access control technology, such as RADIUS and VPN, permit remote users to access corporate networks without the need for expensive dial-up connections or additional hardware costs

ACS-2821-001 – Questions?