UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

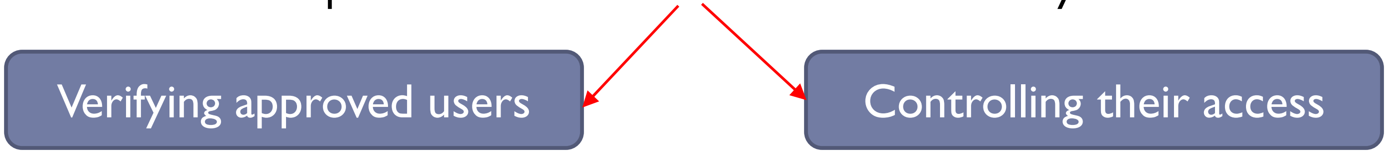
Lecture 10: Access Control Fundamentals

Objectives

- Define access control and list the four access control models
- Describe logical access control methods
- Explain the different types of physical access control
- Define authentication services

Introduction

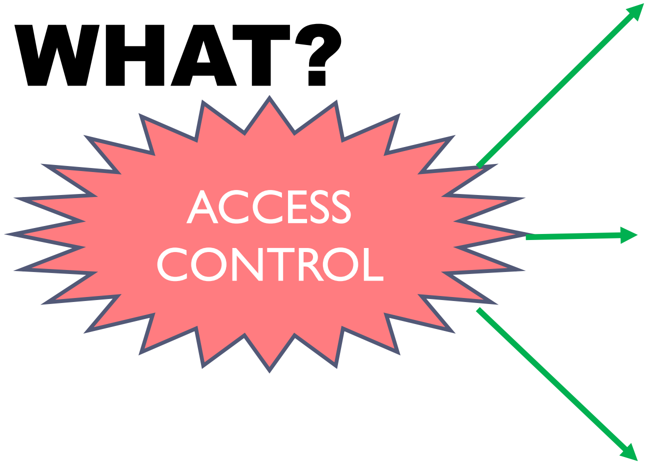
Important foundations in information security



Verifying approved users

Controlling their access

WHAT?



ACCESS CONTROL

Granting or denying approval to use specific resources

Information system's mechanism to allow or restrict access to data or devices

Specific practices used to enforce access control

Access Control Terminology

Identification

Presenting and reviewing credentials
Example: delivery driver presenting employee badge

Authentication

Checking and validating the credentials
Example: examining the delivery driver’s badge

Authorization

Granting permission to take action
Example: allowing delivery driver to pick up package

Object

Specific resource
Example: file or hardware device

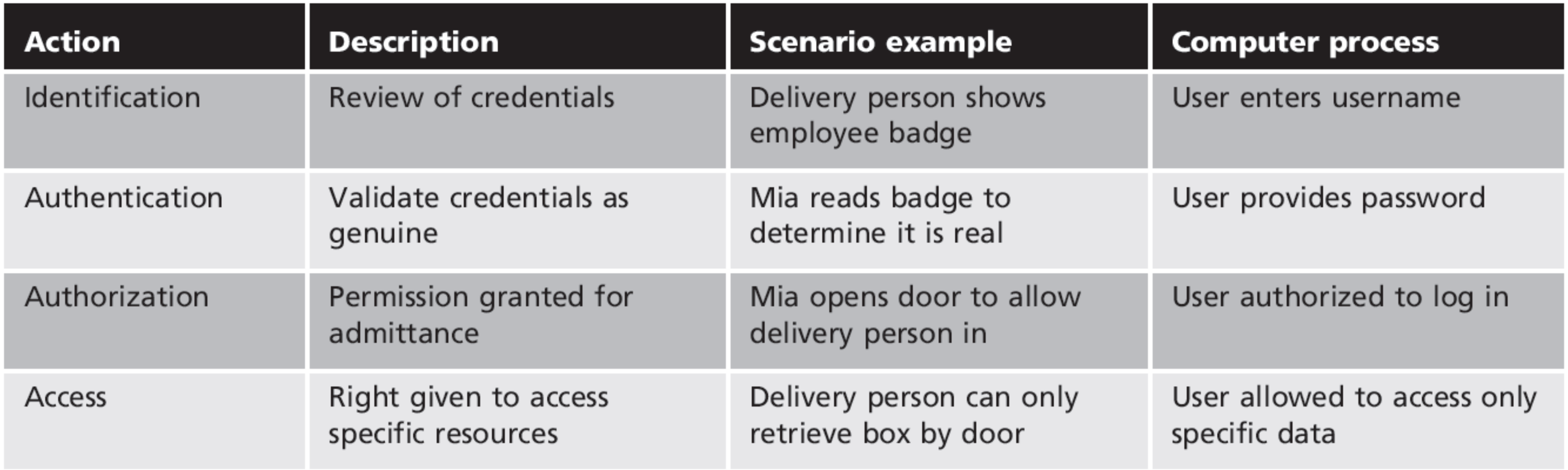
Subject

User or process functioning on behalf of a user
Example: computer user

Operation

Action taken by the subject over an object
Example: deleting a file

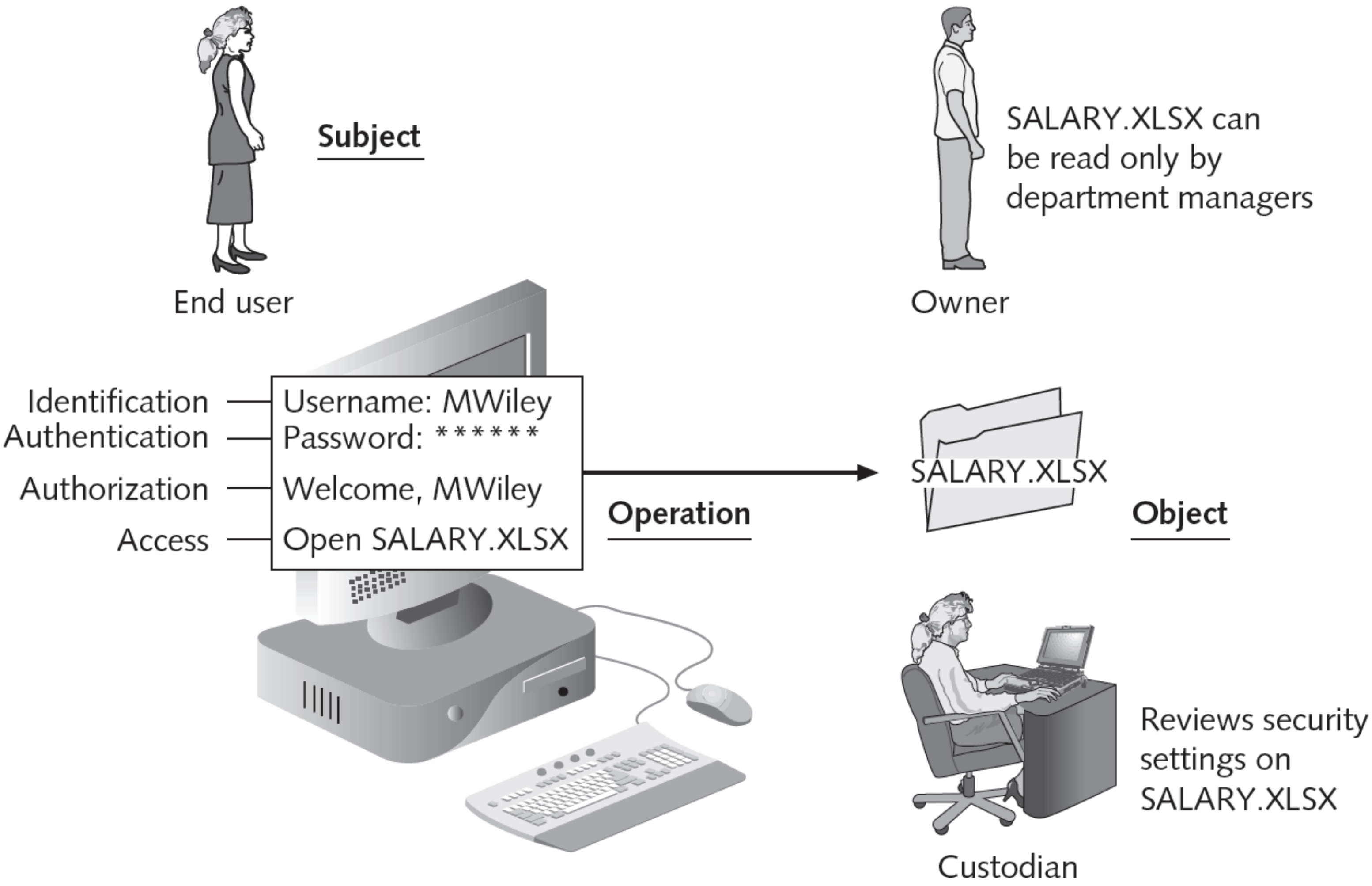
Access Control Terminology



Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Mia reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Mia opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Basic steps in access control

Access Control Terminology



Access control process and terminology

Access Control Models

- Standards that provide a predefined framework for hardware or software developers
- Used to implement access control in a device or application
- Custodians can configure security based on owner's requirements

- Four major access control models

Discretionary Access Control (DAC)

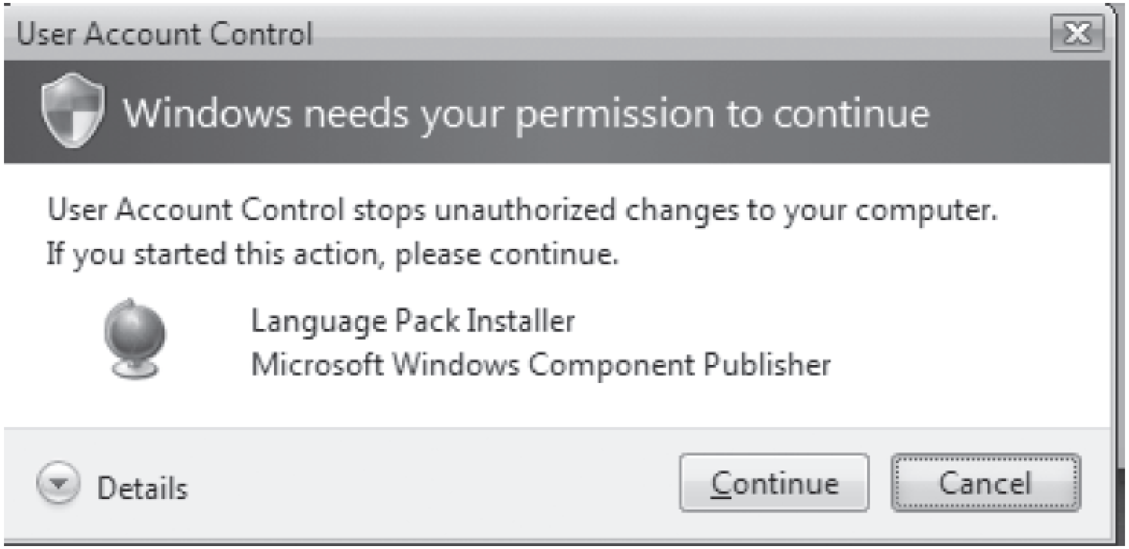
Mandatory Access Control (MAC)

Role Based Access Control (RBAC)

Rule Based Access Control (RBAC)

Access Control Models: Discretionary Access Control (DAC)

- Least restrictive model
- Every object has an owner
- Owners have total control over their objects
- Owners can give permissions to other subjects over their objects



User Account Control

Windows needs your permission to continue

User Account Control stops unauthorized changes to your computer.
If you started this action, please continue.

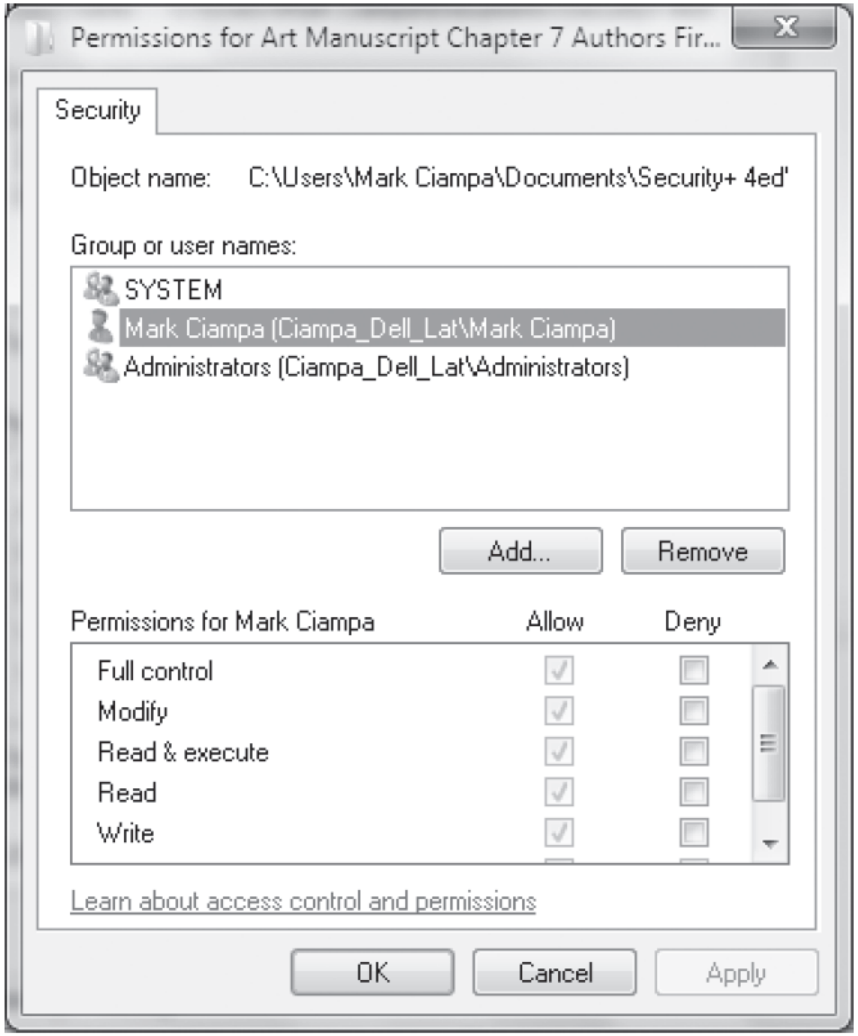
Language Pack Installer
Microsoft Windows Component Publisher

Windows User Account Control (UAC) dialog box

Access Control Models: Discretionary Access Control (DAC)

DAC weaknesses

- Relies on decisions by end user to set proper security level
- Incorrect permissions may be granted
- Subject's permissions will be "inherited" by any programs the subject executes



Permissions for Art Manuscript Chapter 7 Authors Fir...

Security

Object name: C:\Users\Mark Ciampa\Documents\Security+ 4ed'

Group or user names:

- SYSTEM
- Mark Ciampa (Ciampa_Dell_Lat\Mark Ciampa)
- Administrators (Ciampa_Dell_Lat\Administrators)

Permissions for Mark Ciampa	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
Read	☑	□
Write	☑	□

Discretionary Access Control (DAC)

Access Control Models: Mandatory Access Control (MAC)

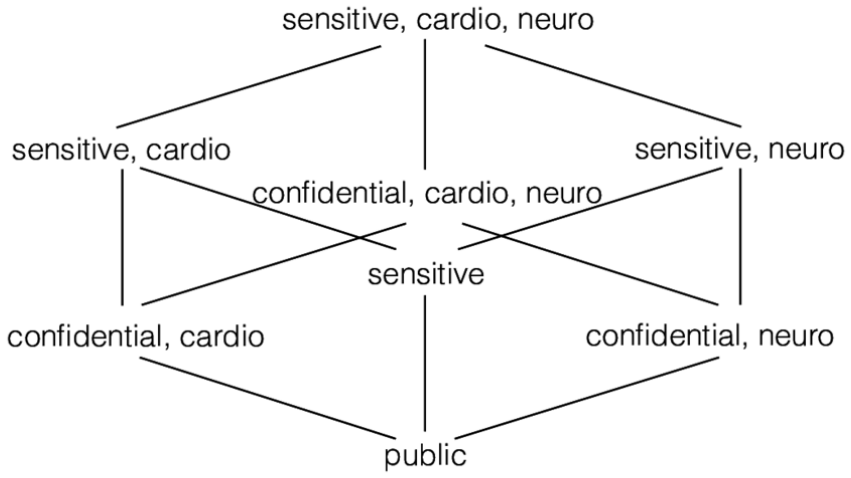
- Most restrictive access control model
- Typically found in military settings
- Two elements
    - Labels
    - Levels
- MAC grants permissions by matching object labels with subject labels
    - Labels indicate level of privilege
- To determine if file may be opened:
    - Compare object and subject labels
    - Subject must have equal or greater level than object to be granted access

Access Control Models: Mandatory Access Control (MAC)

Two major implementations of MAC

Lattice Model

- complex access control model based on the interaction between any combination of objects and subjects
- a lattice is used to define the levels of security that an object may have and that a subject may have access to. The subject is only allowed to access an object if the security level of the subject is greater than or equal to that of the object.
- Multiple lattices can be placed beside each other

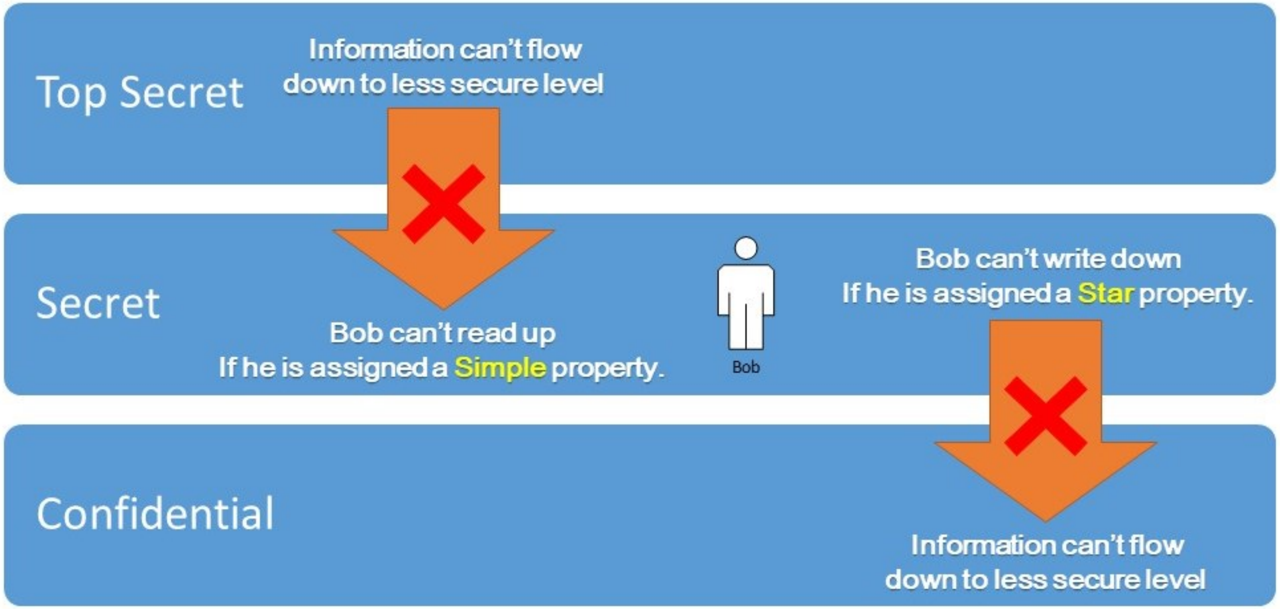


Access Control Models: Mandatory Access Control (MAC)

Two major implementations of MAC

Bell-LaPadula

- Similar to lattice model
- Subjects may not create a new object or perform specific functions on lower level objects


Top Secret
Information can't flow down to less secure level
Secret
Bob can't read up If he is assigned a Simple property.
Bob
Bob can't write down If he is assigned a Star property.
Confidential
Information can't flow down to less secure level

Access Control Models: Role Based Access Control (RBAC)

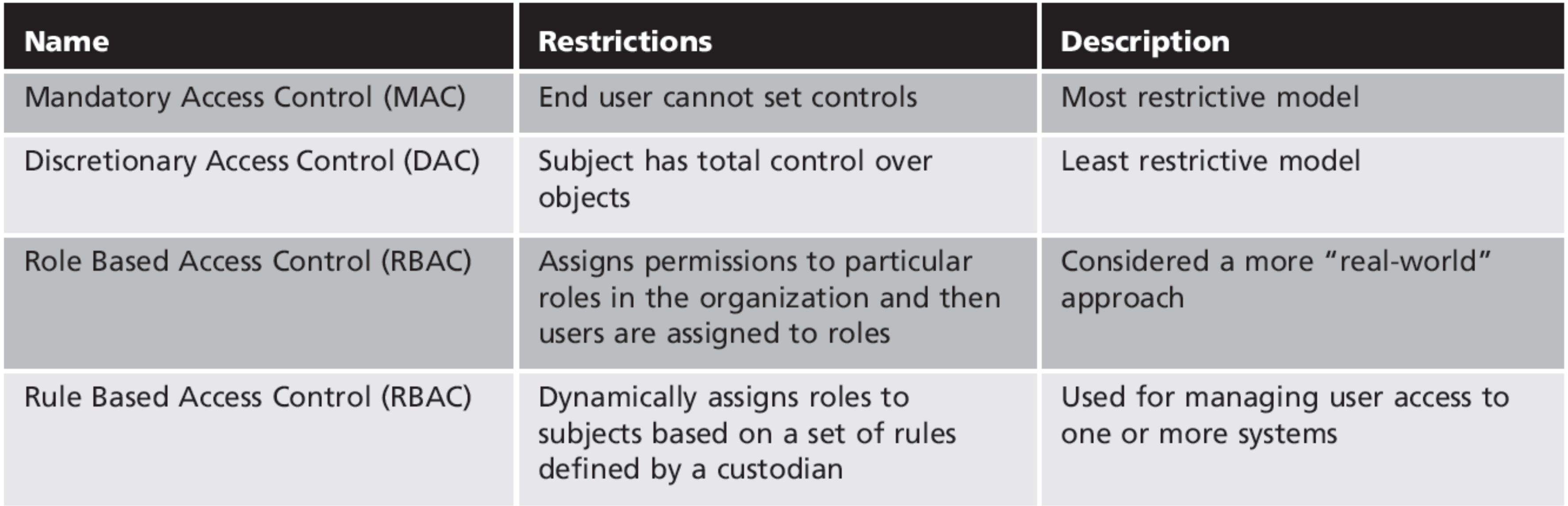
- Also called Non-discretionary Access Control
- Access permissions are based on user's job function
- RBAC assigns permissions to particular roles in an organization
  - –Users are assigned to those roles

Access Control Models: Rule Based Access Control (RBAC)

- Dynamically assigns roles to subjects based on a set of rules defined by a custodian
- Each resource object contains access properties based on the rules
- When user attempts access, system checks object's rules to determine access permission
- Often used for managing user access to one or more systems

  -Business changes may trigger application of the rules specifying access changes

Access Control Models



Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Access control models

Best Practices for Access Control

- Establishing best practices for limiting access can help secure systems and data
- Examples of best practices

- Separation of duties
- Job rotation
- Least privilege
- Implicit deny
- Mandatory vacations

Best Practices for Access Control: Separation of Duties

- Fraud can result from single user being trusted with complete control of a process
- Requiring two or more people responsible for functions related to handling money
- System is not vulnerable to actions of a single person
- requires that if the fraudulent application of a process could potentially result in a breach of security, the process should be divided between two or more individuals.

Best Practices for Access Control: Job Rotation

- Individuals periodically moved between job responsibilities
- Employees can rotate within their department or across departments

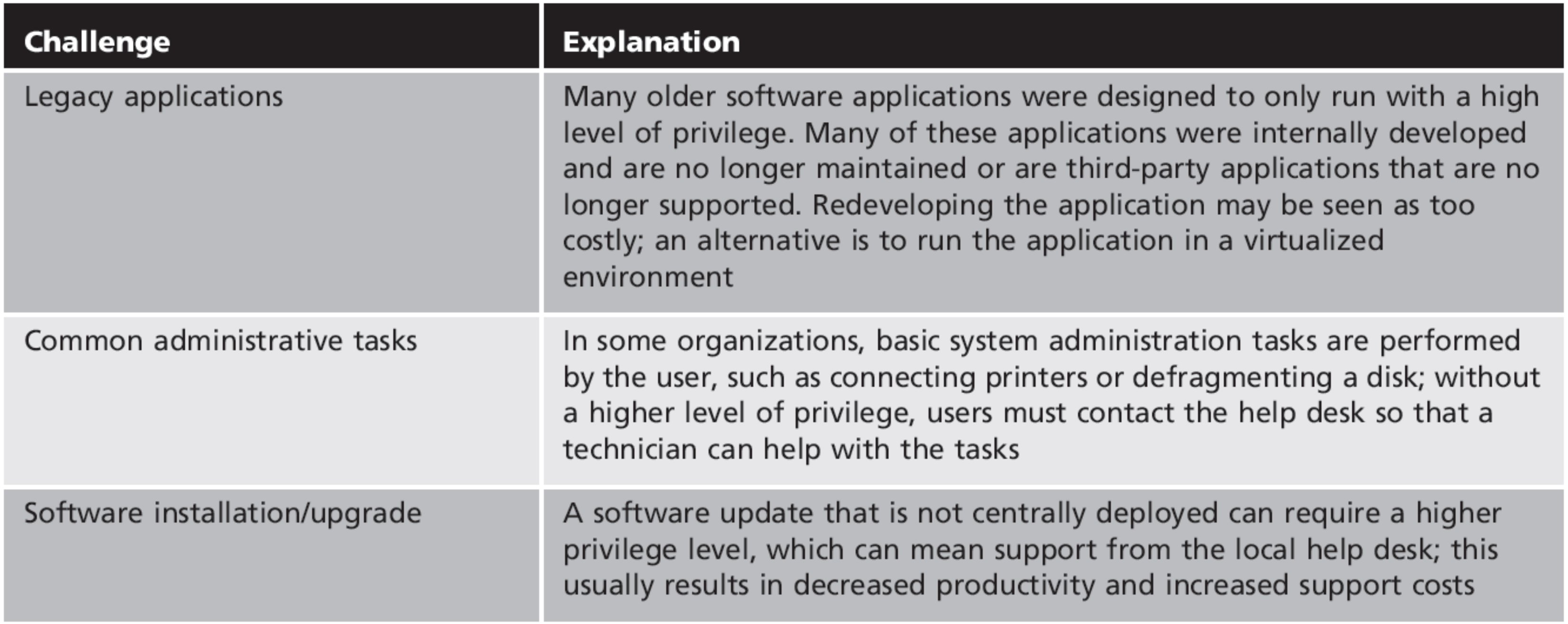
ADVANTAGES

- Limits amount of time individuals are in a position to manipulate security configurations
- Helps expose potential avenues for fraud

  -Individuals have different perspectives and may uncover vulnerabilities
- Reduces employee burnout

Best Practices for Access Control: Least Privilege

- Limiting access to information based on what is needed to perform a job function
- Helps reduce attack surface by eliminating unnecessary privileges
- Should apply to users and processes on the system
- Processes should run at minimum security level needed to correctly function
- Temptation to assign higher levels of privilege is great



Challenge	Explanation
Legacy applications	Many older software applications were designed to only run with a high level of privilege. Many of these applications were internally developed and are no longer maintained or are third-party applications that are no longer supported. Redeveloping the application may be seen as too costly; an alternative is to run the application in a virtualized environment
Common administrative tasks	In some organizations, basic system administration tasks are performed by the user, such as connecting printers or defragmenting a disk; without a higher level of privilege, users must contact the help desk so that a technician can help with the tasks
Software installation/upgrade	A software update that is not centrally deployed can require a higher privilege level, which can mean support from the local help desk; this usually results in decreased productivity and increased support costs

Challenges of least privilege

Best Practices for Access Control: Implicit Deny

- If a condition is not explicitly met, access request is rejected
- Example: network router rejects access to all except conditions matching the rule restrictions

Best Practices for Access Control: Mandatory Vacations

- Limits fraud, because perpetrator must be present daily to hide fraudulent actions
- Audit of employee's activities usually scheduled during vacation for sensitive positions

Access Control Lists (ACL)

- Set of permissions attached to an object
- Specifies which subjects may access the object and what operations they can perform
- When subject requests to perform an operation:

  -System checks ACL for an approved entry

Group Policies

- Microsoft Windows feature
  - –Provides centralized management and configuration of computers and remote users using Active Directory (AD)
  - –Usually used in enterprise environments
  - –Settings stored in Group Policy Objects (GPOs)

- Local Group Policy
  - –Fewer options than a Group Policy
  - –Used to configure settings for systems not part of AD

Account Restrictions

- Time of day restrictions
  - –Limits the time of day a user may log onto a system
  - –Time blocks for permitted access are chosen
  - –Can be set on individual systems
- Account expiration
  - –Orphaned accounts: accounts that remain active after an employee has left the organization
  - –Dormant accounts: not accessed for a lengthy period of time
  - –Both can be security risks

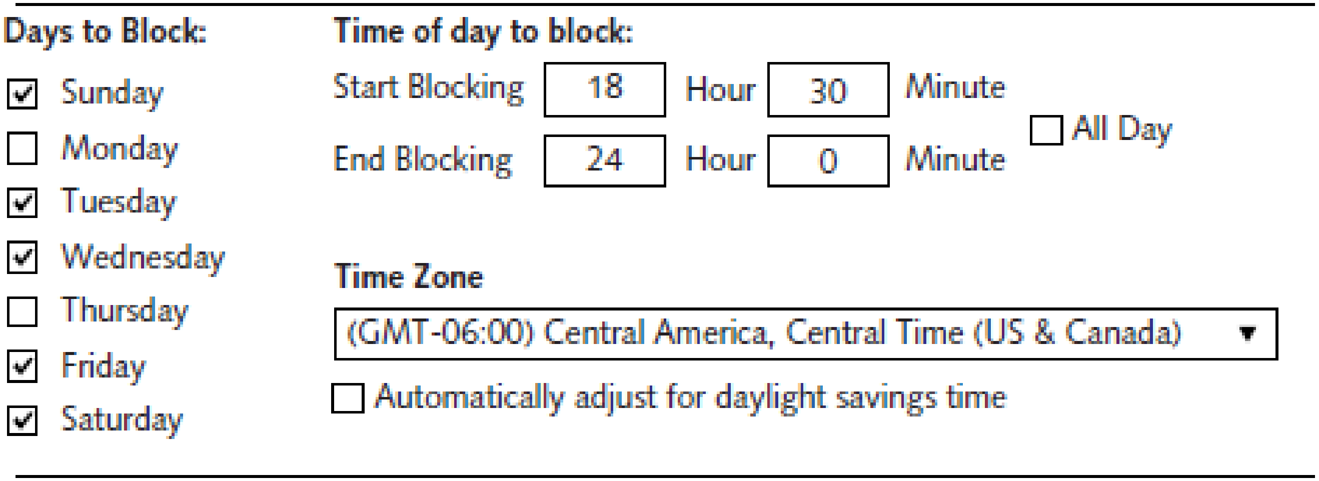
Recommendations for dealing with orphaned or dormant accounts

– Establish a formal process
– Terminate access immediately
– Monitor logs

Account expiration

– Sets a user's account to expire
– Password expiration sets a time when user must create a new password
–Different from account expiration
– Account expiration can be a set date, or a number of days of inactivity

Account Restrictions



Days to Block:

- ☑ Sunday
- □ Monday
- ☑ Tuesday
- ☑ Wednesday
- □ Thursday
- ☑ Friday
- ☑ Saturday

Time of day to block:

Start Blocking 18 Hour 30 Minute

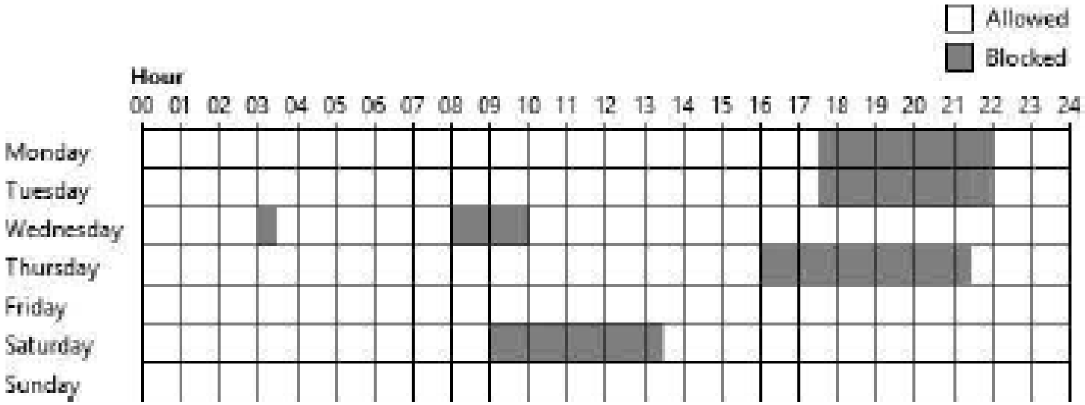
End Blocking 24 Hour 0 Minute

□ All Day

Time Zone

(GMT-06:00) Central America, Central Time (US & Canada) ▼

□ Automatically adjust for daylight savings time



Authentication Services

- Process of verifying credentials
- Authentication services provided on a network
  - –Dedicated authentication server
    - •Or AAA server if it also performs authorization and accounting
- Common types of authentication and AAA servers

Kerberos

RADIUS

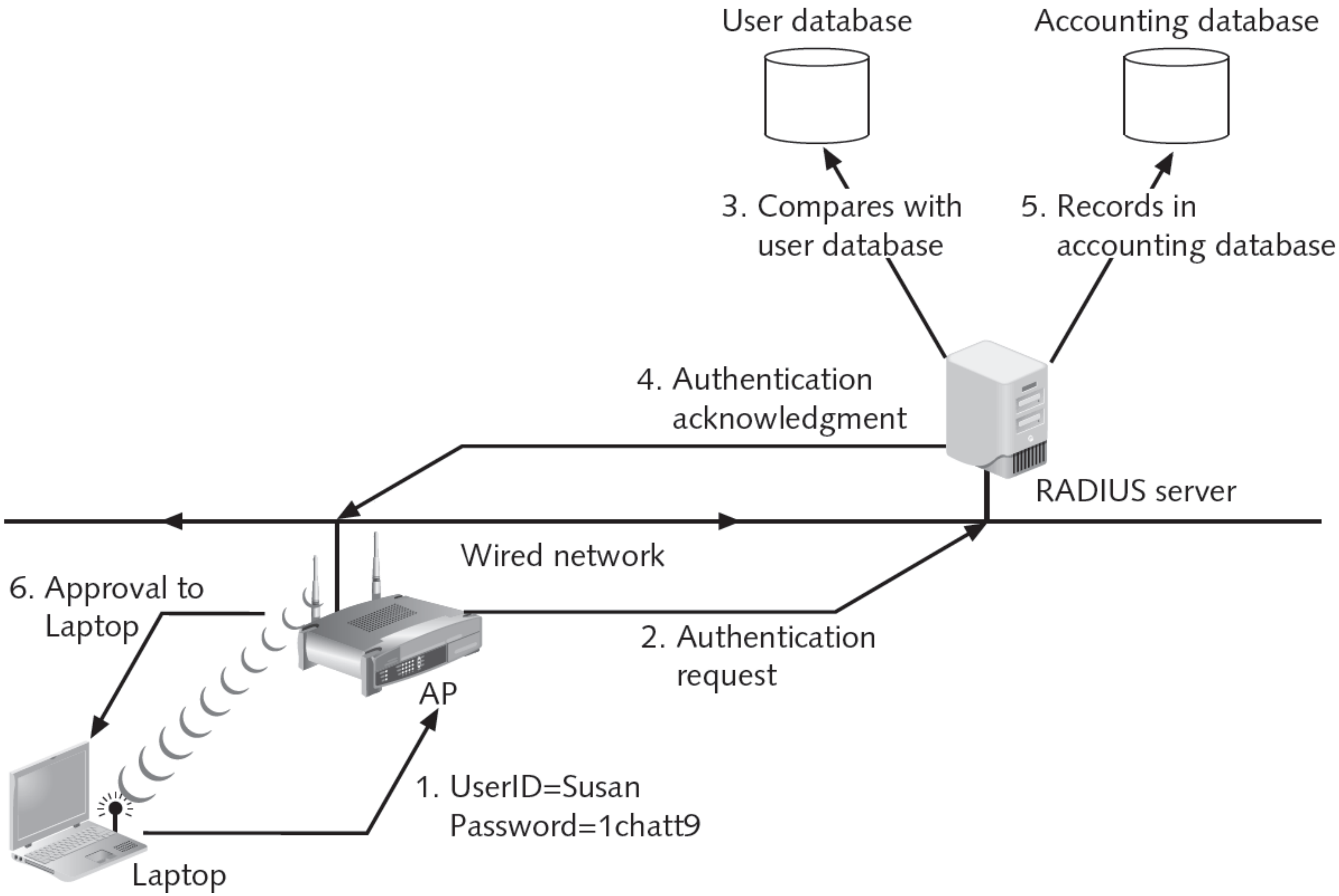
TACACS

LDAP

Authentication Services: RADIUS

- Remote Authentication Dial In User Service
  - –Developed in 1992
  - –Became industry standard
  - –Suitable for high volume service control applications
    - •Such as dial-in access to corporate network
- RADIUS client
  - –Typically a device such as a wireless AP
    - •Responsible for sending user credentials and connection parameters to the RADIUS server
- Advantages of a central service
  - –Increases security due to a single administered network point
  - –Easier to track usage for billing and keeping network statistics

Authentication Services: RADIUS


User database
Accounting database
3. Compares with user database
5. Records in accounting database
4. Authentication acknowledgment
RADIUS server
Wired network
6. Approval to Laptop
2. Authentication request
AP
1. UserID=Susan Password=1chatt9
Laptop

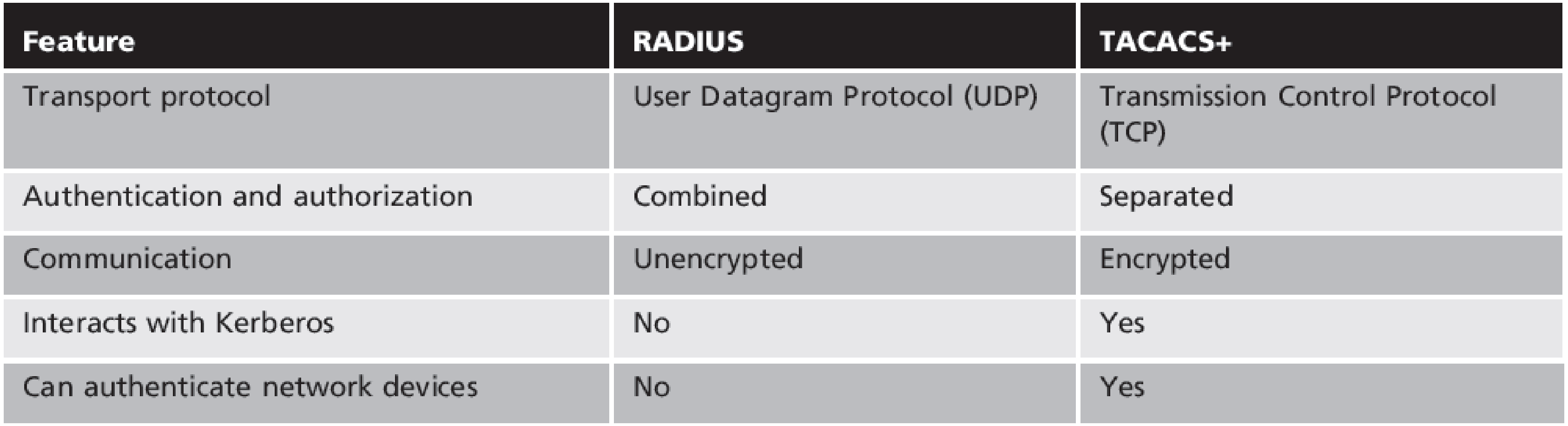
Authentication Services: Kerberos

- Authentication system developed at MIT
  - –Uses encryption and authentication for security
- Most often used in educational and government settings
- A network user requests access to services, Kerberos issues an identifying **ticket**, and the ticket is examined by the entity that grants access to the service.
- Kerberos ticket
  - –Contains information linking it to the user
  - –User presents ticket to network for a service
  - –Difficult to copy
  - –Expires after a few hours or a day

Authentication Services: TACACS

- Terminal Access Control Access Control System (TACACS)
  - Authentication service similar to RADIUS
  - Developed by Cisco Systems
  - It performs authentication, authorization, and accounting functions, and is meant to support a large number of connections.
  - The current version is TACACS+.

Authentication Services: RADIUS vs TACACS



Feature	RADIUS	TACACS+
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
Authentication and authorization	Combined	Separated
Communication	Unencrypted	Encrypted
Interacts with Kerberos	No	Yes
Can authenticate network devices	No	Yes

Comparison of RADIUS and TACACS+

Authentication Services: LDAP

- Directory service
  - –Database stored on a network
  - –Contains information about users and network devices
  - –Keeps track of network resources and user's privileges to those resources
  - –Grants or denies access based on its information
- Standard for directory services
  - –X.500 - defines protocol for client application to access the DAP
- LDAP
  - –A simpler subset of DAP
  - –Designed to run over TCP/IP
  - –Has simpler functions
  - –Encodes protocol elements in simpler way than X.500

WEAKNESS

- Can be subject to LDAP injection attacks
  - -Similar to SQL injection attacks
  - -Occurs when user input is not properly filtered

Summary

- Access control is the process by which resources or services are denied or granted
- Four major access control models exist
- Best practices for implementing access control
    - –Separation of duties
    - –Job rotation
    - –Least privilege
    - –Mandatory vacations
- Access control lists define which subjects are allowed to access which objects
    - –Specify which operations they may perform
- Group Policy is a Windows feature that provides centralized management and configuration
- Authentication services can be provided on a network by a dedicated AAA or authentication server
    - –RADIUS is the industry standard