Control de Acceso (AC) e implementaciones

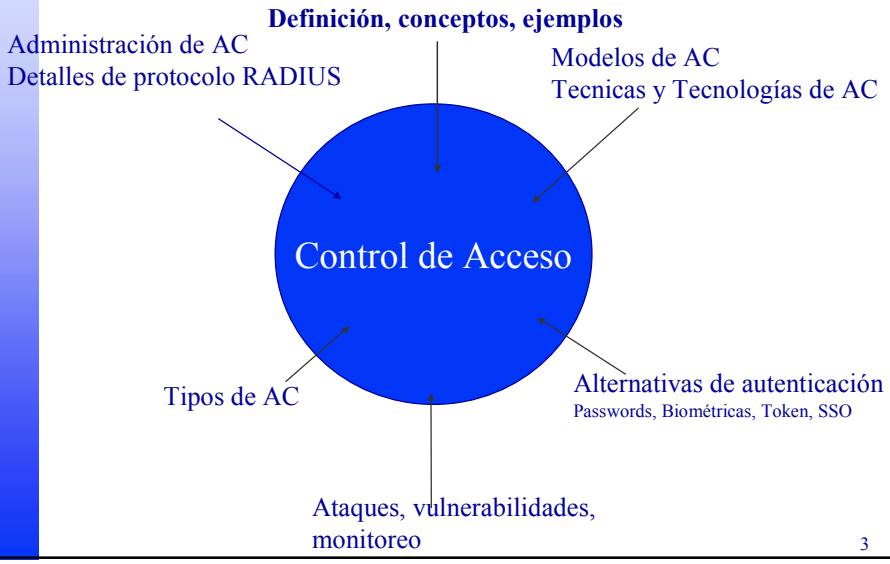
Segunda semana:

- Clase expositiva
- Demo de Radius

Temario

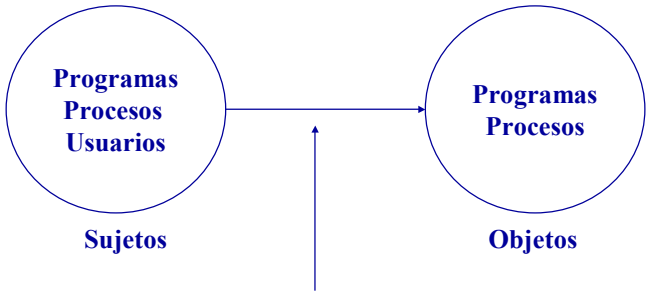
- Introducción:
  - Definición
  - Ejemplo
  - Conceptos
- Implementación de un control de acceso (AC)
- Tipos de control de acceso
- MAC-DAC-RBAC
- Tecnologías y Técnicas de CA
- Autenticación
- Uso de passwords (credenciales)
- Técnicas Biométricas
- Tokens/SSO
- Kerberos
- Ataques/Vulnerabilidades/ Monitoreo
- TEMPEST
- Administración del control de acceso
- Protocolos de AAA: Radius/TACACS
- Ejemplo uso de protocolo Radius
- PAP-CHAP-EAP
- Ejemplo de PAP y CHAP

Pauta



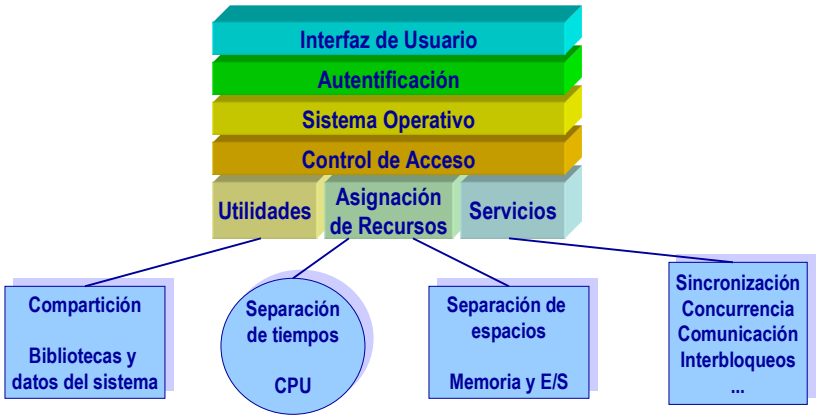
Qué es el control de acceso (AC)?

- Se dice que es la piedra angular de la seguridad
- Definición:



•El acceso es el flujo que se da desde los Sujetos a los Objetos
•El control de acceso regula el flujo desde los sujetos a los objetos

Ejemplo de uso: Sistemas operativos



Qué se espera proteger con AC?

- Un control de acceso tiene por objetivo mantener la confidencialidad, integridad y disponibilidad de la información
  - Confidencialidad:
    - se refiere a prevenir accesos no autorizados a información sensible o crítica
  - Integridad:
    - proteger la información (almacenada o en tránsito) de modificaciones de usuarios no autorizados
    - de prevenir cambios no autorizados por usuarios autorizados
    - los datos almacenados reflejan la realidad.
  - Disponibilidad:
    - Se refiere a prevenir interrupciones en el servicio o la producción

Volveremos sobre estos conceptos en módulo 8, clase 13

Conceptos básicos

1. Identificación

El sujeto "dice" quien es.
Ejemplo: uso de username, uso de un número identificador, etc..

2. Autenticación

El sujeto debe mostrar o entregar un elemento adicional que demuestre quién es. Ejemplo: password, llave criptográfica, etc.

3. Autorización

Si el sujeto es autenticado OK, recibe las credenciales o permisos para acceder a los objetos que le corresponden

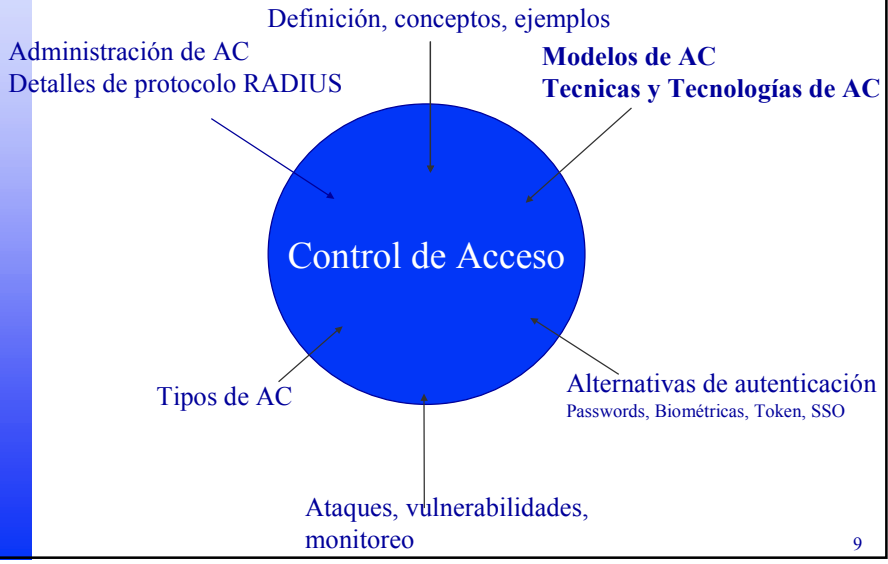
4. Accounting

Se debe mantener un registros de las acciones y actividades asociadas a los sujetos

Cómo se puede implementar AC?

– Un AC se puede implementar en tres distintos niveles:
  - Administrativo: Políticas y procedimientos, controles sobre el personal, estructura de supervisión, entrenamiento, tests
  - Físico: Segregación de red, seguridad perimetral, controles computacionales, separación de áreas de trabajo, respaldo de datos, cableado
  - Técnico o lógico: Acceso a los sistemas, arquitectura de red, acceso a la red, encriptación y protocolos, zonas de control, auditorías.

Pauta



Modelos de control de acceso

- Los modelos son pautas que determinan como los sujetos acceden a los objetos:
  - Discrecional (DAC)
  - Mandatorio (MAC)
  - Basado en roles (RBAC)

Definiciones: DAC- MAC - RBAC

- DAC:
  - Los dueños de la información o datos deciden quien accede a los recursos
- MAC:
  - El sistema decide como la información será compartida, en función de los niveles de seguridad asignado a los objetos
- RBAC:
  - Las decisiones de acceso son tomadas en función del rol del sujeto

Problemas con los modelos formales

- Basados en infraestructura estática
- Requieren definición de políticas
- No funcionan adecuadamente en sistemas muy cambiantes y extremadamente dinámicos
- Estos modelos no consideran algunas amenazas a la seguridad:
  - Virus/active content
  - Trojan horses
- Documentación limitada, ¿Cómo se construyen estos sistemas?

Modelo de AC MAC (1)

- Asignación de niveles de sensibilidad
- Cada objeto posee un label de sensibilidad y es accesible sólo por usuarios que tienen un nivel particular
- Sólo los administradores pueden cambiar a los objetos de nivel, no sus propios dueños
- Generalmente más seguro que DAC
- De difícil programación, configuración y implementación

13

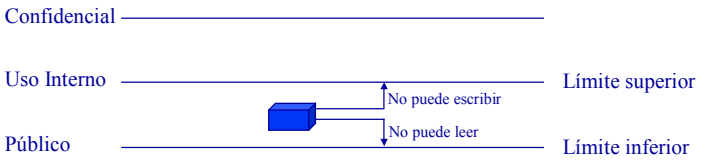
Modelo de AC MAC (2)

- Bajo performance
- Confía en el sistema para el AC
- Ejemplo: Si un archivo es clasificado como confidencial, un sistema MAC debería prevenir que esta se escriba como información secreta o top secret
- Todas las salidas como trabajos de impresión, discos, CDs, etc, deberían ser etiquetados con su nivel de sensibilidad

14

Modelo de AC MAC (3)

- Ejemplos de modelos mandatorios: Bell-LaPadula, Biba
- Modelo BIBA:
  - Fue creado después que el modelo Bell LaPadula
  - Está orientado a la integridad de la información
  - Se usa en instituciones comerciales



- Tarea: ¿En qué consiste el modelo Bell LaPadula?, ¿Cómo se compara con BiBa?

Modelo de AC DAC

- Los accesos de usuarios son restringidos según autorización dada a los usuarios
- Separación de uso de información, protección de usuarios de información no autorizada
- Usado por Unix, NT/Win2000/XP, NetWare, Linux, Vines, etc.
- Descansa en que cada dueño de un objeto controla el acceso a este

Modelo de AC Basado en roles

- También se define como control de acceso no discrecional
- Usa un set de controles centralizados para determinar qué sujetos acceden a qué objetos
- Ejemplo:
  - Un usuario "Jhon Doe" que llega como administrador de respaldos recibe los atributos de acceso asociados a su rol, no a Jhon Doe directamente.

Técnicas y tecnologías de AC

- Control de acceso basado en roles (RBAC). Este tipo de acceso no es sólo un modelo, también es una técnica de AC que puede aplicarse a los modelos MAC y DAC:
  - Ejemplo de aplicación en DAC: se definen roles, y los dueños de los sistemas deciden que rol aplicar a cada sujeto
  - Ejemplo de aplicación en MAC: se definen roles asociados al acceso de los objetos de acuerdo a su nivel de sensibilidad.
- Control de acceso basado en reglas: es un tipo de control de mandatorio, en el que se definen reglas para que los objetos puedan ser accesados.
  - Ejemplo: la definición de reglas que hace un administrador de red para que los paquetes IP sean enrutados
- Interfaces restringidas:
  - Son interfaces que restringen los accesos de los usuarios a funciones, información o recursos
  - Ejemplos:
    - menús que sólo permiten ejecutar algunos comandos,
    - vistas de bases de datos que muestran la información de acuerdo a su fucnión
    - restricción física que requiere la intervención física de los usuarios

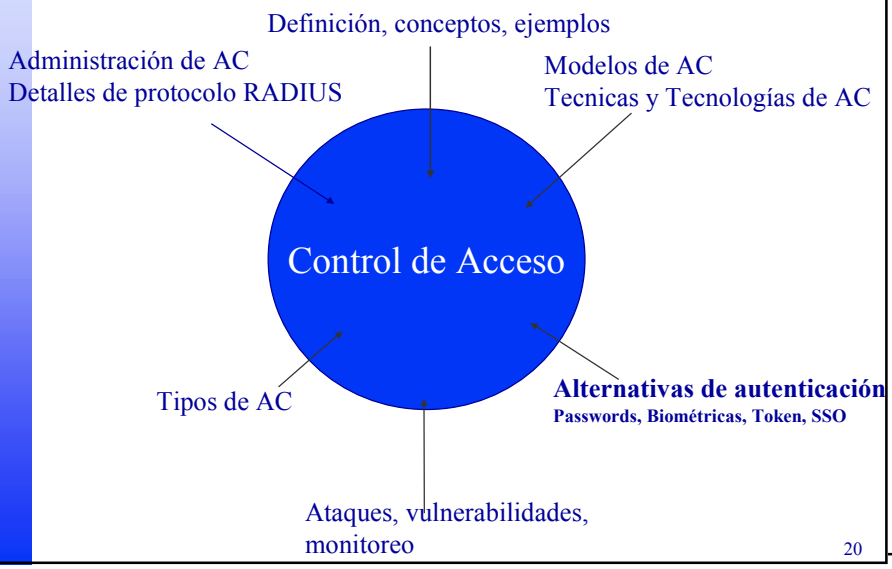
Técnicas y tecnologías de AC

- Matriz de control de acceso: especifica las acciones que pueden realizar los usuarios sobre los recursos específicos. Se usa como base para especificar los controles de un sistema operativo.

Usuarios	Archivo 1	Archivo 2	Archivo 3
German	Leer y ejecutar	Leer	Sin acceso
Jorge	Sin acceso	Escribir	Escribir
Mauricio	Sin acceso	Leer y ejecutar	Leer

- Las listas de acceso se obtienen de las columnas de la matriz de acceso

Pauta



Autenticación

3 tipos de autenticación :

- What you have: Se requiere contar con un elemento que permita identificar al usuario. Ejemplos: ATM card, smart card, token, key, identificaciones, pasaporte
- What you know: Típicamente corresponde a información de usuario y password que habilita un perfil correspondiente al usuario ingresado. Ejemplos: Password, PIN
- What you are: corresponden a sistemas que se basan en la información física de la persona para determinar su identidad. Ejemplos: Huella digital, voice scan, iris scan, retina scan, DNA

21

Passwords (1): ejemplo típico de autenticación "what you know"

- Inseguras: dadas las opciones, las personas eligen passwords de fácil recordación, que son fáciles de "adivinar".
- Fáciles de quebrar: programas como crack, SmartPass, PWDUMP, NTCrack y l0phtcrack desencriptan fácilmente passwords de sistemas Unix, Windows, etc.
  - Ataques de diccionario, tienen más éxito precisamente porque los usuarios eligen passwords fáciles de adivinar
- Inconvenientes: en un intento para mejorar la seguridad, las organizaciones a menudo generan passwords, que son imposibles de recordar
- Repudio: como en el papel, con una firma, cuando una transacción es firmada con un password, esto no puede considerarse como una prueba real de la identidad de la persona realizando la operación

22

Passwords (2): reglas clásicas

- Las mejores passwords son las que son fáciles de recordar y difíciles de quebrar usando diccionarios.
- El mejor camino para crear passwords con estas deseables características, es usar , por ejemplo, dos pequeñas palabras o fonemas, idealmente con un carácter especial.
- No usar:
  - Nombres comunes, identificaciones, números de telefóno (o parte de ellos), etc.
  - Palabras que encontramos en los diccionarios
  - Password como password
  - Las passwords defaults de los sistemas

Passwords (3): recomendaciones

- Configurar los sistemas para usar strings
- Setear el tiempo de vigencia de las claves
- Limitar el número de logins fallidos
- Limitar las conexiones simúltaneas
- Habilitar las auditorías
- Políticas para el revocamiento y cambio de passwords
- Colocar la fecha en banners, del último login

Password (4): ataques

- Fuerza bruta
  - Ejemplo aplicación: l0phtcrack
- Diccionarios
  - Ejemplo aplicación: Crack
  - Ejemplo aplicación: John the Ripper
- Caballo de troya: programa de login

25

Biométrica (1): ejemplo “what you are”

- Autentificación vía características humanas
- Uso de medidas físicas características de una persona para proveer su identificación:
  - Huella digital
  - Iris
  - Retina
  - Voz
  - Rostro
  - DNA, sangre

26

Biométrica (2)

- Efectividad de las técnicas biométricas:
  - Un sistema biometrico puede cometer un error tipo I: rechazar un usuario autorizado
  - También puede darse un error tipo II: aceptar un suuario no autorizado
  - CER o Cross Error Rate es la tasa en la que los errores tipo I son iguales a los errores tipo II.
  - Mientras más efectivo un sistema biométrico, menor CER
- Ranking de efectividad (año 2002):
  - Scan de la palma de la mano, geometría de la mano, Scan del iris, patrón de retina, huella digital, verificación de voz, reconocimiento de cara, dinámica de la firma, dinámica al tipear
- Ranking de aceptación (año 2002):
  - Scan de iris, dinámica al tipear, dinámica de la firma, verificación de voz, reconocimiento de cara, huella digital, Scan de la palma de la mano, geometría de la mano, patrón de retina

Biométrica (3): ventajas y desventajas

- Ventajas:
  - La clave no puede ser prestada ni olvidada
  - En algunos casos presenta un buen equilibrio entre facilidad de uso, costo y precisión.
  - En general son de muy larga duración
  - En general son de fácil uso
- Desventajas:
  - Relativamente cara por usuario
  - Requiere mayor desarrollo en algunos temas
  - No es muy estándar
  - Existe cierta resistencia a aceptar este tipo de autenticación

Biométrica (4): privacidad ?

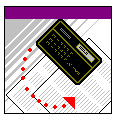
- Es muy fácil hacer búsquedas y vigilar a las personas
- Comienza a desaparecer el concepto de anonimato
- Se pueden hacer perfiles de los comportamientos de las personas

Biométrica (6): aplicaciones

- Control de acceso a la red
- Seguimiento del comportamiento del personal
- Autorizar transacciones bancarias
- Muy beneficiosa para información servicios gubernamentales
- Se puede usar en conjunto con tarjeta de crédito
- Control de acceso físico
- Proteger contra secuestros
- Voto/pasaporte/visa e immigracion

Autenticación Multi-factor

- 2-factor autentificación. Para incrementar el nivel de seguridad generalmente un usuario debe proporcionar 2 de los 3 tipos de autentificación.
  - ATM card + PIN
  - Tarjeta de crédito + firma
  - PIN + huella digital
  - Username + Password (NetWare, Unix, NT default)



- 3-factor autentificación – alta seguridad
  - Username + Password + huella digital
  - Username + Passcode + SecurID token

Tokens (1)

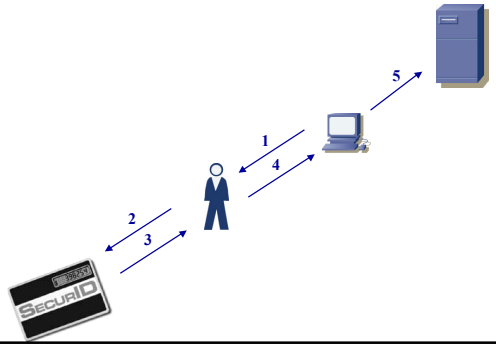
- Un token es un dispositivo generador de passwords
- Son usados para facilitar el uso de one-time passwords (passwords que duran una sola vez)

- Existen Tokens Síncronos y Asíncronos
  - Tokens síncronos: se sincronizan con el servidor de acceso usando alguna variable en común. Ejemplo: tokens basados en tiempo.
  - Funcionamiento de token basado en tiempo:
    - El usuario ingresa al servicio y accede al servidor de acceso
    - La tarjeta Token y el servidor de acceso están sincronizados a la misma hora. La tarjeta Token le muestra al usuario la hora encriptada.
    - El usuario ingresa su login y el valor mostrado por el token al sistema.
    - El servidor de acceso desencripta el valor ingresado y lo compara con el valor interno esperado. Si existe coincidencia el usuario queda OK. Si no, se rechaza

Tokens (2)

- Tokens Asíncronos

1. El servidor le envía al usuario un desafío
2. El usuario ingresa el desafío al token junto con su PIN
3. El token muestra un valor de respuesta
4. El usuario ingresa el valor mostrado en el sistema
5. El servidor de acceso valida que la respuesta al desafío esté OK



33

Single Sign-On (SSO)

- Un usuario accede a todos los sistemas usando un acceso único.
- El acceso único está limitado por un usuario y una password.
- Así no es necesario recordar múltiples passwords y se puede usar una password robusta.
- Es más fácil administrar el acceso a los sistemas de esta forma
- Estos sistemas son difíciles de implementar
- Ejemplos de sistemas:
  - Scripting, SESAME y Kerberos

34

Kerberos (1): introducción

- Fue parte del proyecto Athena, desarrollado por el MIT a mediados de los años 80
- Kerberos era un perro de tres cabezas de la mitología griega, que protegía el acceso al Hades.
- Kerberos ha evolucionado y se encuentra en la versión 5
- Kerberos is the three-headed dog that guards the entrance to Hades (this won't be on the test)

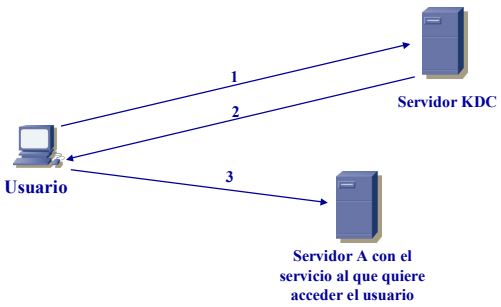
35

Kerberos (2): elementos

- Kerberos se basa en un servidor central de distribución de llaves (*KDC; Key Distribution System*)
- El KDC le entrega tickets a los *"principales"* (usuarios, aplicaciones o servicios) para que se comuniquen.
- El set de principales a los cuales el KDC les entrega seguridad de acceso, conforman un dominio

36

Kerberos (3): funcionamiento



1. El usuario requiere al KDC para acceder a un servicio dado por otro servidor A
2. El KDC autentica al usuario y le envía un ticket para que se comunique con el servidor A. El usuario debe ingresar su password para hacer uso del ticket.
3. El PC del usuario envía el ticket al servidor A, quien al reconocer el ticket como válido, provee el servicio solicitado

Kerberos (4): desventajas

- Todos los elementos de la red deben conocer el protocolo
- Requiere sincronización de la información que comparten los dispositivos. Cuando un usuario cambia su calve, todo debe actualizarse.
- Se basa en protocolo UDP, que en general es bloqueado en el acceso en las redes.
- El servidor que distribuye los tickets se transforma en un solo punto de falla.
- El tráfico en la red no es protegifo por Kerberos

Pauta

Ataques (1): conceptos

- Pasivos: monitorear tráfico para averiguar passwords o para luego generar un ataque del tipo replay
  - Son difíciles de detectar
- Activos: un usuario trata de acceder al sistema tomando acciones directamente sobre él
  - Explotar vulnerabilidades de los sistemas
  - Hacerse pasar por otro usuario
  - Ataques sobre información encriptada
- Denegación de servicio: no se trata de ganar acceso en forma directa, si no de evitar que el sistema opere:
  - Smurf, SYN Flood, Ping of death
  - Mail bombs

Ataques (2): ejemplos

Ataque	Descripción
Smurf	This attack is carried out by sending an ICMP ECHO REQUEST (PING) packet with a forged source address matching that of the target system. This packet is sent to "amplifier" networks — networks that allow sending packets to the broadcast address — so that every machine on the amplifier network will respond to what they think is a legitimate request from the target. As a result, the target system is flooded with ICMP ECHO REPLY messages, causing a denial of service attack.
SYN Flood	This attack can be used to completely disable your network services by flooding them with connection requests. This will fill the queue which maintains a list of unestablished incoming connections, forcing it to be unable to accept additional connections.
Ping of death	With this attack, a remote user can cause your system to reboot or panic by sending it an oversized PING packet. This is done by sending a fragmented packet larger than 65536 bytes in length, causing the remote system to incorrectly process the packet. The result is that the remote system will reboot or panic during processing.
Fraggle	This attack is a UDP variant of the Smurf attack. By sending a forged UDP packet to a particular port on a broadcast address, systems on the "amplifier" network will respond to the target machine with either a UDP response or an ICMP UNREACHABLE packet. This flood of incoming packets results in a denial of service attack against the target machine.
Jolt	A remote denial of service attack using specially crafted ICMP packet fragments. May cause slowdowns or crashes on target systems.

Vulnerabilidades

- Física
- Naturales
  - Inundaciones, terremotos, tormentas
- Hardware/Software
- Medios
  - Respaldos corruptos
- Emanaciones
- Comunicaciones
- Humanos
  - Ingeniería social

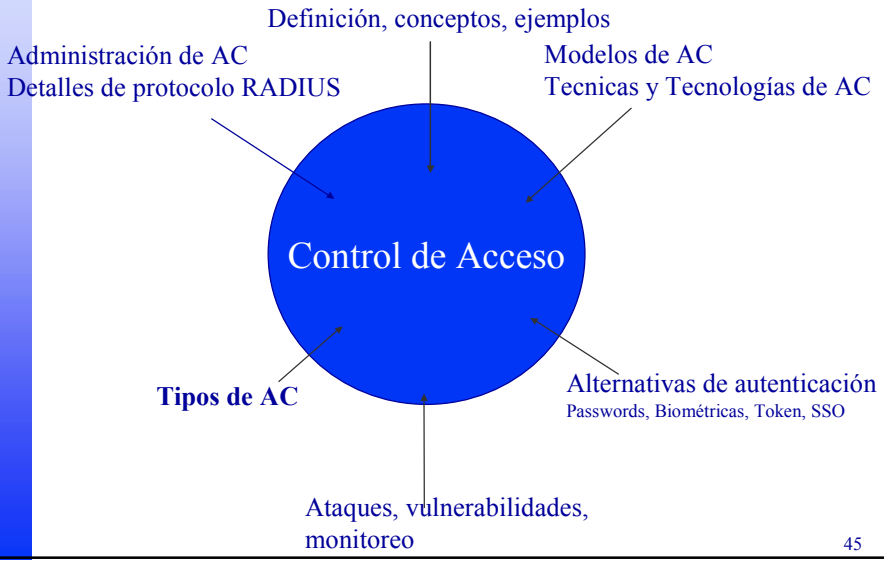
Monitoreo lógico

- Revisión de registros logs
- Auditorias
- Herramientas de red: sniffer
- Uso de IDS de red y de servidor

TEMPEST

- Es un estándar que regula las emanaciones electromagnéticas de los dispositivios electrónicos: PCs, routers, cables, pantallas, impresoras, etc.
- Se supone que contando con el equipo adecuado se pueden utilizar esas emanaciones para descubrir la información que está siendo ingresada o se encuentra en tránsito.
- El HW certificado TEMPEST es muy caro.
- Las dependencias donde se encuentran los equipos también deben certificarse.
- Los estandares TEMPEST NACSEM 5100A y NACSI 5004 son documentos clasificados

Pauta



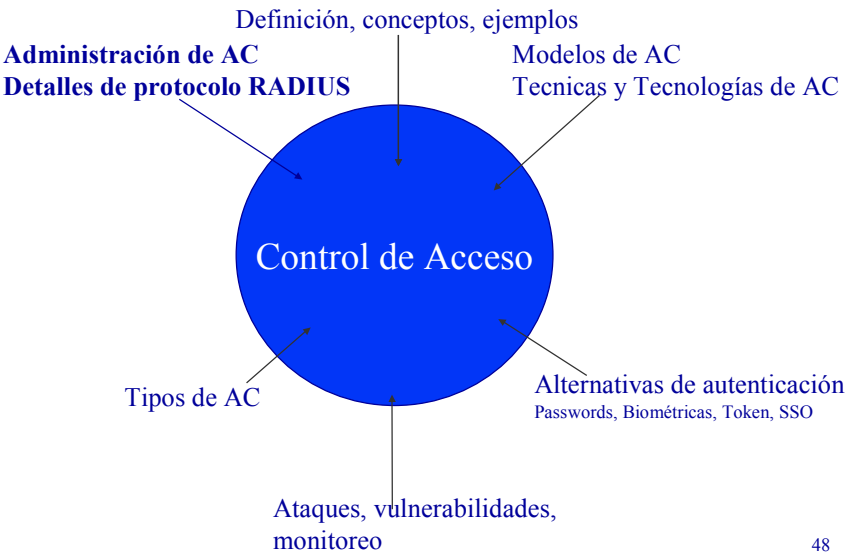
Tipos de control de acceso (1)

- Los controles de acceso se pueden clasificar en:
  - Preventivo: se evita que eventos indeseables se produzcan
  - Detectivo: se identifican situaciones de violación a los accesos
  - Correctivo: se corrigen las consecuencias de un acceso indeseado
  - Inhibitorias: se desanima a quien que quiera quebrantar los controles
  - De recuperación: se activan al momento de volver a su estado normal los recursos.
  - De compensación: se usan como medios alternativos a otros controles

Tipos de control de acceso (2)

- Actividad de clasificación de controles de acceso

Pauta

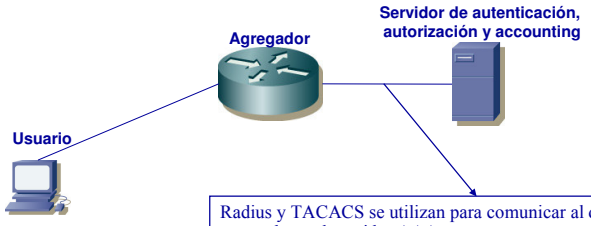


Administración del control de acceso (1)

- **Distribuido: muchas entidades controlan el acceso a los recursos. Ejemplo de implementación:**
  - **Dominios de seguridad**
- **Centralizado: una sola entidad se encarga de autorizar los accesos. Ejemplos de implementación:**
  - **Uso de protocolo TACACS/TACACS+** (Terminal Access Controller Access Control System)
  - **Uso de protocolo RADIUS**: Remote Acces Dial-In User Servicefigura + base de funcionamiento
- **Híbrido: algunas entidades dan acceso en forma distribuida a algunos objetos (por ejemplo archivos de usuarios), y otras concentran el acceso a elementos más sensibles (bases de datos, info. confidencial, etc.)**

Administración del control de acceso (2)

- **Arquitectura sistemas centralizados**



Radius y TACACS se utilizan para comunicar al dispositivo agregador y el servidor AAA.
Con estos protocolos se autoriza el acceso de los usuarios a los recursos de red.

Administración del control de acceso (3)

- **Radius y TACACS:**
  - **RADIUS es un protocolo estándar (RFC 2865- RFC 2866- RFC 2869). TACACS es propietario de Cisco**
  - **RADIUS utiliza UDP para establecer las comunicaciones. TACACS utiliza TCP**
- **Ejemplo de uso del protocolo RADIUS**

Ejemplo uso de protocolo Radius

- *Aún no está confirmada la realización de esta actividad*