Seguridad en el acceso

Authentication

Authorization

Accounting

Fundación Proydesa Ing. Fabián Calvete

AAA

Componente clave para comprender la seguridad en el acceso y en las redes

- **A**uthentication
- **A**uthorization
- **A**ccounting

Conjunto de procesos usados para proteger datos, equipos y confidencializar información.
Objetivos:

Confidencialidad: el contenido de los datos no debe ser revelado.
Integridad: el contenido de los datos debe permanecer intacto y no debe sufrir alteraciones.
Disponibilidad: el contenido de los datos debe estar accesible cuando se necesite.

Arquitectura

AAA consiste en tres áreas separadas que trabajan en forma conjunta.

Autenticación

Proceso utilizado para verificar que una máquina o usuario que intenta acceder a un recurso es quien dice ser. Generalmente utiliza nombres de usuario, passwords, identificadores únicos, entidades certificantes, o algunos otros elementos para permitir verificar la identidad contra un dispositivo o software que analice y valide esas credenciales.

Autorización

Puede ser definido como una política, componente de software o hardware que es usado para permitir o denegar el acceso a un recurso. Esto puede ser un componente avanzado como una tarjeta inteligente, un dispositivo biométrico o un dispositivo de acceso a la red como un router, access point wireless o access server. También puede ser: un servidor de archivos o recursos que asigne determinados permisos como los sistemas operativos de red (Windows 2000, Novell, etc)

Auditoría

Es el proceso de registrar eventos, errores, acceso e intentos de autenticaciones en un sistema.

Métodos de autenticación

En su forma más básica, es simplemente el proceso de verificar la identidad de alguien o algo. Todos los procesos de autenticación siguen la misma premisa básica, que necesitamos probar quienes somos o quién es el individuo, el servicio, o el proceso antes de que permitamos que utilicen los recursos.

La autenticación permite que un emisor y receptor de la información se validen como las entidades apropiadas con las cuales desean trabajar. Si las entidades que desean comunicarse no pueden autenticarse correctamente, entonces no se puede confiar en la información provista por cada uno.

Un usuario puede ser identificado principalmente por tres cosas:

- ✓ Algo que el usuario conozca (por ejemplo, una contraseña)
- ✓ Algo que el usuario tenga (una tarjeta magnética)
- ✓ Algo que sea una propiedad intrínseca del usuario (Ej: la huella dactilar, el iris, la retina, la voz)

Username y Password

La combinación de nombres de usuario y contraseñas es el método más común y más utilizados para realizar autenticación. Es importante comprender que la primera línea de defensa de un sistema es la creación y el mantenimiento de una política de contraseñas que se cumpla y tenga la flexibilidad necesaria para hacerla utilizable por los usuarios.

Las políticas para definir las contraseñas de los usuarios pueden obligarlos a incluir:

- ✓ Cantidad mínima de caracteres y diferencias entre estos
- ✓ Caracteres en minúsculas y mayúsculas
- ✓ Números
- ✓ Caracteres especiales
- ✓ Palabras que no figuren en diccionario

One Time passwords

El sistema S/Key utiliza algoritmos de hashing de una vía con el fin de crear un esquema de contraseñas de única vez (o también llamado One time passwords). En este sistema, las contraseñas son enviadas en texto claro a través de la red pero, luego que la password fue utilizada, caduca y no es válida para ser utilizada nuevamente. Una ventaja de S/Key es que protege el intento de acceso de un espía sin necesitar modificaciones del cliente.

El sistema S/Key tiene tres componentes principales:

✓ Cliente: Pide el login del usuario. No realiza almacenamiento de contraseñas.
✓ Host: Procesa la contraseña. Almacena la contraseña de única vez y la secuencia del login en un archivo. También le provee al cliente el valor inicial para calcular el hash.
✓ Un calculador de claves**:** Es la función de hash para la contraseña de única vez.

Token cards

Otro sistema de autenticación de password de única vez que le agrega cierto grado de seguridad adicional es el uso de una token card o "tarjeta inteligente" y un servidor de token. Cada token card es programada para un usuario específico y además de esa tarjeta, cada usuario tiene un código de seguridad que le permite obtener de su tarjeta una clave de única vez.

Pasos para autenticar a un usuario:

✓ Los usuarios generan una clave de única vez con la tarjeta usando un algoritmo de seguridad
✓ El usuario ingresa la contraseña de única vez en la pantalla de autenticación
✓ El cliente remoto envía la contraseña de única vez al servidor de token y al Servidor de Acceso (NAS)
✓ El servidor de token usa el mismo algoritmo para verificar si la password es correcta y autentica al usuario remoto

Token cards (cont.)

Los servidores de token, puede comportarse de tres formas diferentes:
- ✓ Basado en tiempo
- ✓ Por desafío y respuesta
- ✓ Sincronismo de eventos

Basado en tiempo
Las tarjetas y el servidor tienen relojes que miden el tiempo transcurrido desde la inicialización. Cada cierto tiempo el número resultante se encripta y se muestra en la pantalla de la tarjeta; el usuario ingresa su PIN en el servidor junto con el número que se visualiza en su tarjeta. Como el servidor conoce el momento de inicialización de la tarjeta también puede calcular el tiempo transcurrido, dicho valor encriptado deberá coincidir con el introducido por el usuario para que éste sea aceptado.

Token cards (cont.)

Por desafío y respuesta
En este sistema, la token card contiene una llave criptográfica. El servidor de token genera una cadena de dígitos aleatoria (desafío) y la envía al cliente remoto que intenta acceder a la red. El usuario remoto ingresa esa cadena de dígitos más su PIN en la token card, la cual le aplica una función criptográfica (Ej: DES) con una llave almacenada, generando la contraseña (respuesta). El resultado de esa función es enviado nuevamente al servidor de token, quien realiza la misma función y si el resultado es igual, el usuario es autenticado.

Sincronismo de eventos
La tarjeta y el servidor guardan la última contraseña utilizada. El usuario debe ingresar su PIN en la tarjeta; a partir del conjunto formado por el PIN y la última contraseña, se genera una nueva clave aplicando una función criptográfica (Ej: DES) a dicho conjunto, que será enviada al servidor para su verificación.

Identificación biométrica

Los sistemas biométricos se basan en características físicas del usuario a identificar.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica:
✓ Captura o lectura de los datos que el usuario a validar presenta
✓ Extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar)
✓ Comparación de tales características con las guardadas en una base de datos
✓ Finalmente la decisión de si el usuario es válido o no

Dos características básicas de la fiabilidad de todo sistema biométrico:las tasas de rechazo por no poder comprender los datos capturados y de falsa aceptación donde el sistema tomaría como válido a un usuario que no lo es.

Servidores de Acceso a la Red (NAS)

La función de un servidor de acceso de red (NAS) es proveer a los usuarios remotos del acceso a los dispositivos y recursos.

Típicamente el NAS sería un router, ubicado en el perímetro de la red, quien provee dos tipos de accesos:

- ✓ Administración remota o modo de caracteres**:** contiene acceso en modo de caracteres. Esto incluye el acceso por consola, auxiliar, telnet o ssh.
- ✓ Acceso remoto a la red o modo de paquetes**:** puede tomarse desde una línea analógica o digital

Si existiera un NAS brindando el acceso en una red, el administrador deberá almacenar los usuarios y contraseñas en el NAS . Esto indica una autenticación local o base de datos de seguridad local. Las principales características de la seguridad local son:

- ✓ Usado para redes pequeñas
- ✓ Los usuarios y contraseñas son almacenados en el router
- ✓ No se requiere de una base de datos externa

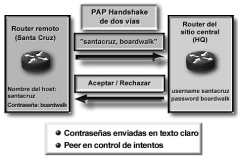
Implementaciones de seguridad en el acceso

Fundación Proydesa **Ing. Fabián Calvete**

PAP

PAP proporciona un método simple para que un nodo remoto establezca su identidad utilizando un handshake de dos vías. PAP se realiza únicamente tras el establecimiento inicial del enlace.
Una vez que la fase de establecimiento del enlace PPP ha sido completada, el nodo remoto envía repetidamente al router un par nombre de usuario/contraseña hasta que se confirma la autenticación, o se termina la conexión.

PAP no es un protocolo de autenticación fuerte. Las contraseñas se envían a través del enlace en texto claro y no existe protección contra la reproducción o contra ataques repetidos de prueba y error. El nodo remoto tiene el control de la frecuencia y temporización de los intentos de acceso.

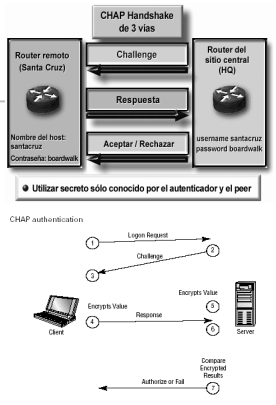


CHAP

CHAP se utiliza al inicio de un enlace, y periódicamente, para verificar la identidad del nodo remoto utilizando un handshake de tres vías. CHAP se efectúa tras el establecimiento inicial del enlace y puede repetirse en cualquier momento una vez que el enlace ha sido establecido.

Una vez que la fase de establecimiento del enlace PPP ha sido completada, el router local envía un mensaje de “challenge” al nodo remoto. El nodo remoto responde con un valor calculado utilizando una función de hash de una vía (generalmente MD5). El router local verifica la respuesta contra su propio cálculo del valor hash esperado. Si los valores coinciden, la autenticación se confirma. De otra manera, la conexión se termina de inmediato.

CHAP proporciona protección contra ataques de reproducción a través del uso de un valor varia - ble de challenge que es único e impredecible. El uso de challenges repetidos tiene como intención limitar el tiempo de exposición a cualquier ataque único. El router local (o un servidor de autenticación de terceras partes tal como TACACS) se halla en control de la frecuencia y temporización de los challenges.

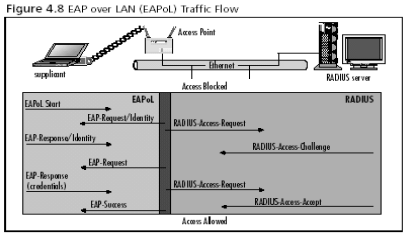


IEEE 802.1x

El estándar IEEE 802.1x - Port Based Network Access Control (Control de acceso a la red basado en puertos) define la forma en que se debe realizar la autenticación y autorización de los usuarios que acceden a una red LAN a través de un puerto con características punto a punto, y prohibir el acceso en caso que falle la autenticación y autorización. Los puertos incluyen los puertos de un switch, puente, o las asociaciones entre estaciones y access points de las redes inalámbricas IEEE 802.11.

La autenticación IEEE 802.1x es una arquitectura cliente servidor provista a través de EAPOL (Extensible Authentication Protocol sobre LAN). . El servidor de autenticación autentica a cada cliente que se conecta a un puerto antes de proveerles acceso a los servicios ofrecidos por la red.

Figure 4.8 EAP over LAN (EAPoL) Traffic Flow



IEEE 802.1x

IEEE 802.1x contiene tres elementos principales :

✓ Autenticador (Authenticator): El dispositivo que permite la autenticación del suplicante. Controla el acceso físico a la red basándose en la autenticación del suplicante. Es un intermediario entre el suplicante y el servidor de autenticación.

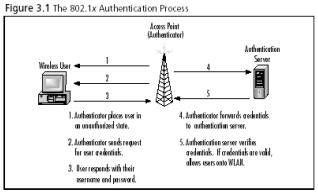
✓ (Supplicant): Cliente que solicita acceso a la red y responde los requerimientos del autenticador.

✓ Servidor de autenticación (Authentication Server): Provee el servicio de autenticación al autenticador. Este servicio determina, dadas las credenciales del Suplicante, si está autorizado o no a acceder a los servicios ofrecidos por el Autenticador

IEEE 802.1x

La comunicación entre el suplicante y el autenticador se realiza mediante EAP sobre LAN. Puede soportar múltiples mecanismos de autenticación, como MD5, one time passwords, Token cards, etc

Figure 3.1 The 802.1x Authentication Process



WEP

El estándar IEEE 802.11 para las redes LAN inalámbricas incluye la definición de WEP (Wired Equivalent Privacy) para proteger a los usuarios autorizados de escuchas casuales. WEP realiza una encripción de cada una de las tramas que se transmiten al aire. Cuando se activa WEP, el cliente y el access point deben tener claves WEP coincidentes. WEP usa el método de cifrado RC4 (Rivest Cipher 4).

La forma en que WEP utiliza el cifrado RC4 tiene muchas vulnerabilidades: una de las vulnerabilidades proviene del Vector de Inicialización. Existen implementaciones que permiten realizar una captura de tramas y realizar el cálculo de la clave WEP, las más difundidas son WEPCrack y Airsnort

La otra, es que WEP está apuntado a realizar autenticación de dispositivos y no de usuarios. Las claves WEP se deben configurar en los dispositivos (Interfaces inalámbricas y Access Points) en lugar de ser ingresadas por un usuario. El robo o acceso indebido a un dispositivo de un usuario malicioso estaría entregando las claves utilizadas en toda la red.

Para solucionar estos problemas se creó el estándar 802.11i, el cual aplica los conceptos vistos en 802.1x, más algunas modificaciones a WEP (TKIP)

IEEE 802.11i

Incluye dos mejoras a la encripción WEP:

✓ TKIP (Temporal Key Integrity Protocol): mejoras por software a la implementación de RC4 utilizada por WEP.

✓ AES: algoritmo de encripción más robusto que RC4.

El problema de WEP es que usa siempre la misma clave. TKIP define una clave temporal de 128 bits que se comparte entre clientes y access points. Esta clave es combinada con la dirección MAC del adaptador, y luego agrega un vector de inicialización de 128 bits (más de 5 veces superior al original) para producir la clave de cifrado . Este procedimiento asegura que cada estación utilizará claves diferentes para realizar el cifrado.

EAP

EAP (Extensible Authentication Protocol - Protocolo de autenticación extensible) es un protocolo de autenticación muy flexible, que generalmente corre sobre otros protocolos, como 802.1x, RADIUS, TACACS+, etc.
EAP permite que el dispositivo autenticador sirva como intermediario entre el servidor de autenticación y el cliente a ser autenticado. Posibilita la distribución dinámica de claves WEP.

Cuando un usuario solicita conexión a un Access Point, comienza la fase de autenticación, que puede ser mutua, del cliente ante el servidor, y viceversa. Una vez que ambos extremos se han autenticado, comienza la fase de definición de claves, donde entre cliente y servidor definen una clave WEP para el tráfico unicast. Esta clave es informada al Access Point, el cual enviará al cliente la clave WEP que utilizará para el envío de broadcasts. Para evitar que un usuario externo escuche esta clave, se encripta con la clave seleccionada para unicast que conocen sólo el Access Point, el cliente y el servidor de autenticación.

EAP, LEAP, PEAP (cont.)

Cuando se utiliza 802.1x en una red inalámbrica, se pueden implementar diferentes variantes de EAP, las más conocidas son:

- LEAP (Lightweight EAP): También llamada EAP-Cisco, es la versión de Cisco de 802.1x EAP. Provee un método de distribución de claves WEP dinámicas, que varían por usuario y por sesión. De esta forma se decrementa la cantidad de tramas con la misma clave WEP, para evitar su cálculo.

- EAP-TLS (EAP-Transport Layer Security): algoritmo de autenticación basado en TLS que implementa autenticación basada en certificados digitales X.509 (se estudiarán mas adelante). Exige que todos los clientes y servidores tengan certificados digitales.

- PEAP (Protected EAP): basado en la autenticación EAP-TLS, PEAP permite utilizar diferentes tipos de autenticación del cliente, como EAP-GTC para one-time passwords y EAP-MD5 autenticación basada en passwords. De esta forma no se requiere que todos los dispositivos tengan certificados digitales.

- EAP-GTC (Generic Token Card EAP): provee autenticación basada en one-time password

- EAP-MD5: provee un método de autenticación basado en username y password.

TACACS+

TACACS+ (Terminal Access Controller Access Control System Plus) es una versión mejorada de TACACS. TACACS+ es un protocolo de Autenticación, Autorización, y Auditoría (AAA) que reside en un servidor centralizado.

Existen al menos tres versiones de TACACS:

- **TACACS:**
TACACS es una especificación estándar de protocolo definido en el RFC 1492 que reenvía el nombre de usuario y contraseña a un servidor centralizado. Este servidor mantiene una base de datos TACACS con los usuarios. De acuerdo a los parámetros pasados, el servidor acepta o rechaza la autenticación, enviando un mensaje.

- **XTACACS:**
XTACACS define extensiones de Cisco al protocolo TACACS para soportar nuevas características. XTACACS es multiprotocolo y puede autorizar conexiones con SLIP, PPP, IPX, ARAP y Telnet. XTACACS soporta múltiples servidores TACACS, y syslog para el envío de información de auditoría. Actualmente, XTACACS se encuentra obsoleto, dados los nuevos requerimientos de AAA

- **TACACS+:**
Es una versión en constante mejora de TACACS que permite al servidor TACACS+ brindar servicios de AAA de manera independiente. Cada servicio puede ser usado con su propia base de datos o puede ser usado en conjunto con los demás servicios.

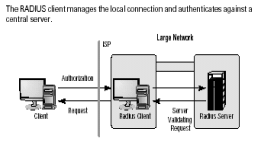
No es compatible con las otras versiones
Se encuentra como una propuesta en la IETF, pero no es un estándar.
Permite encriptar toda la información que se intercambia.

TACACS y sus diferentes versiones utilizan TCP como transporte, y tienen reservado el número de puerto 49.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) es otra alternativa para realizar AAA. Es un sistema de seguridad distribuida que seguriza el acceso remoto a redes y las protege de accesos no autorizados.

Según la definición del protocolo, RADIUS tienen reservados los números de puerto 1812 (para autenticación) y 1813 (para auditoría), pero existen muchas implementaciones que utilizan los puertos 1645 y 1646 respectivamente.



El servidor es ejecutado en una computadora, generalmente dentro del sitio propietario de la red, mientras que el cliente reside en el NAS y puede estar distribuido en toda la red.

Modelo Cliente Servidor
El NAS opera como el cliente, reenviando la información de autenticación de los usuarios al servidor RADIUS configurado, y luego, actuando de acuerdo a la respuesta del servidor. Los servidores RADIUS son los responsables de recibir los requerimientos de los usuarios, autenticarlos, y devolver toda la información necesaria para que el cliente habilite los servicios correspondientes. El servidor RADIUS puede mantener una base de datos de los usuarios de forma local, utilizar la base de datos de Windows, o un directorio LDAP.

Seguridad de la red
Las transacciones entre el cliente y el servidor son autenticadas por un secreto compartido, que no se envía por la red. Las contraseñas son enviadas cifradas.

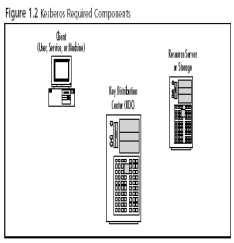
Métodos de autenticación flexibles
El servidor RADIUS soporta diferentes métodos para autenticar un usuario. Soporta PPP, PAP, CHAP, MS-CHAP, Unix login, etc.

TACACS + versus RADIUS

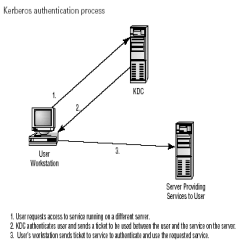
	TACACS +	RADIUS
Protocolo de capa de transporte	TCP	UDP Debe implementar controles. Más complejo
Encripción de datos	Encripción de todo el tráfico entre el cliente y el servidor	Solo encripción de contraseñas
Autenticación y autorización	Utiliza los servicios de manera independiente. Permite autenticar con Kerberos	Combina ambos en el mismo paquete. Se autentica y se pasan sus permisos
Soporte multiprotocolo	Soporte multiprotocolo	No soporta algunos protocolos: AppleTalk Remote Access (ARAP) protocol NetBIOS Frame Protocol Control protocol Novell Asynchronous Services Interface (NASI) X.25 PAD connection
Administrador de Routers	Provee dos métodos: asignar niveles de privilegios a los comandos y especificar en el perfil del usuario o del grupo de usuarios explícitamente el conjunto de comandos que puede ejecutar.	No permite asignar conjuntos de comandos habilitados o deshabilitados a los usuarios, por lo que no es útil para realizar autenticación de administradores de dispositivos

Kerberos

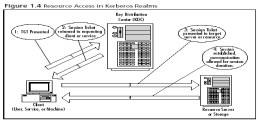
Kerberos fue creado en el Instituto de Tecnología de Massachusetts a comienzo de los 80´. La versión actual de Kerberos es la versión 5, y ha sido publicada por la IETF como el RFC 1510. El sistema operativo Microsoft Windows 2000 utiliza a Kerberos como su técnica de autenticación. Posee tres componentes: un cliente, un servidor y una intermediario de confianza para mediar entre ellos. Este intermediario es el KDC (Key Distribution Center, Centro de Distribución de Claves).



El protocolo Kerberos depende de una técnica de autenticación que incluye secretos compartidos. El concepto básico es bastante simple: si un secreto es conocido solo por dos personas, entonces cualquiera de las dos personas puede verificar la identidad de la otra confirmando que la otra persona conoce el secreto. Kerberos resuelve este problema con criptografía de clave secreta. En vez de compartir una clave de acceso, los extremos de la comunicación comparten una clave criptográfica, y usan el conocimiento de esta clave para verificar la identidad uno del otro.



El KDC es un servicio que corre en un servidor físicamente seguro. Mantiene una base de datos con la información de las cuentas de sistema (usuarios, servidores, estaciones). Para cada cuenta, mantiene una clave conocida sólo por el KDC y la cuenta. Esta clave se usa en intercambios entre la cuenta y el KDC.
Cuando un cliente quiere hablar con un servidor, el cliente envía una solicitud al KDC, y el KDC distribuye una clave de sesión para que utilicen los extremos interesados (el cliente y el servidor) cuando se autentican uno al otro. La copia de la clave de sesión del servidor está encriptada con la clave compartida entre el KDC y el servidor. La copia de la clave de sesión del cliente está encriptada en la clave compartida entre el KDC y el cliente.



FIN

Fundación PROYDESA

Ing. Fabián Calvete