SEGURIDAD EN REDES Y SISTEMAS INFORMÁTICOS

Ana González (Kao)

UNIDAD 7. Seguridad en sistemas operativos

Ana González (Kao)

ÍNDICE UNIDAD 7

UNIDAD 7. SEGURIDAD EN SISTEMAS OPERATIVOS.

Ana González (Kao)

1 Introducción

El Sistema operativo es normalmente solo una porción del total de software que corre en un sistema particular. Pero el Sistema Operativo controla el acceso a los recursos del sistema.

La seguridad de los Sistemas Operativos es solo una pequeña parte del problema total de la seguridad en los sistemas de computación, pero éste viene incrementándose en gran medida. Hay muchas razones para que la seguridad de los Sistemas Operativos reciba especial atención hoy en día.

La evolución de los sistemas de computación, ha sido en las últimas décadas de una magnitud asombrosa. Las computadoras se han tornado más accesibles, también se tiene un aumento en los riesgos vinculados con la seguridad. Pero hay una cosa que se ha mantenido constante a través de todo este tiempo, y es que los sistemas digitales se han vuelto cada vez más complejos. Los microprocesadores se han vuelto más complejos. Los sistemas operativos se han vuelto más complejos. Los ordenadores se han vuelto más complejos. Las redes se han vuelto más complejas. Las redes individuales se han combinado y han aumentado todavía más su complejidad.

Ejemplo claro de ello es Internet, la gran red de computadoras, a medida que aumenta su complejidad va tornándose más insegura.

Si tenemos en cuenta que todo software no está libre fallos, entonces un software complejo es probable que falle y un porcentaje de estos fallos afecte a la seguridad.

También es importante mencionar que los sistemas complejos son necesariamente modulares, ya que de otra manera no se podría manejar su complejidad. Pero el aumento de la modularidad significa que la seguridad disminuye porque falla a menudo donde dos módulos se comunican.

La única manera razonable de probar la seguridad de un sistema es realizar evaluaciones de seguridad en él. Sin embargo, cuanto más complejo es el sistema, más dura se vuelve la evaluación de su seguridad.

Ana González (Kao)

Un sistema más complejo tendrá más errores relacionados con la seguridad en su análisis, diseño y programación. Y desgraciadamente, el número de errores y la dificultad de evaluación no crece de acuerdo con la complejidad, crece mucho más rápido.

Cuanto más complejo es un sistema, más difícil es de entender. Hay toda clase de puntos de vulnerabilidad -interface entre usuario y máquina, interacciones del sistema- esto crece exponencialmente cuando no se puede mantener el sistema completo en la cabeza.

Cuanto más complejo es un sistema, más duro es hacer este tipo de análisis. Todo es más complicado: su análisis, su diseño, su programación y su uso.
Los sistemas operativos no escapan a esta realidad y se tornan cada vez más complejos.

Un ejemplo es Microsoft Windows, que cuando se publicó en 1992 (Versión 3.1) tenía alrededor de 3 millones de líneas de código; Windows 95 alcanzó a los 15 millones y Windows 98 tiene 18 millones; Windows NT lanzado en 1992 tenía 4 millones de líneas de código; Windows NT 4.0 tiene 16.5 millones; Windows 2000 tiene entre 35 y 80 millones de líneas.

Como punto de comparación tenemos a Solaris que mantuvo su código fuente en aproximadamente 7 a 8 millones de líneas y Linux (Incluso con la suma del entorno gráfico X Windows y de Apache) que todavía se mantiene por debajo de los 5 millones de líneas.

En el pasado la seguridad física fue suficiente para resguardar un computadora contra ataques de intrusos, actualmente controles sofisticados deben instrumentarse para prevenir intentos de login desde terminales remotas y sobre otras redes de comunicación.
Por último, cabe destacar que el nivel de seguridad apropiado para un sistema en particular depende del valor de los recursos que se aseguran.

Ana González (Kao)

2. Seguridad en sistemas operativos

Seguridad Externa y Seguridad Operacional

Seguridad Externa

La *seguridad externa* consiste en:

- Seguridad física.
- Seguridad operacional.

La *seguridad física* incluye:

- Protección contra desastres.
- Protección contra intrusos.

En la seguridad física son importantes los *mecanismos de detección*, algunos ejemplos son:

- Detectores de humo.
- Sensores de calor.
- Detectores de movimiento.

La *protección contra desastres* puede ser costosa y frecuentemente no se analiza en detalle; depende en gran medida de las consecuencias de la pérdida.

La *seguridad física* trata especialmente de impedir la entrada de intrusos:

- Se utilizan sistemas de *identificación física:*
  - Tarjetas de identificación.
  - Sistemas de huellas digitales.
  - Identificación por medio de la voz.

Seguridad Operacional

Ana González (Kao)

Consiste en las *diferentes políticas y procedimientos* implementados por la administración de la instalación computacional.

La *autorización* determina qué acceso se permite y a quién.

La *clasificación* divide el problema en subproblemas:

- Los datos del sistema y los usuarios se dividen en *clases:*
    - A las clases se conceden diferentes *derechos de acceso.*

Un aspecto *crítico* es la *selección y asignación de personal:*

- La pregunta es si se puede *confiar en la gente.*
- El tratamiento que generalmente se da al problema es la *división de responsabilidades:*
    - Se otorgan distintos conjuntos de responsabilidades.
    - No es necesario que se conozca la totalidad del sistema para cumplir con esas responsabilidades.
    - Para poder comprometer al sistema puede ser necesaria la cooperación entre muchas personas:
        - Se reduce la probabilidad de violar la seguridad.
    - Debe instrumentarse un gran número de verificaciones y balances en el sistema para ayudar a la detección de brechas en la seguridad.
    - El personal debe estar al tanto de que el sistema dispone de controles, pero:
        - Debe desconocer cuáles son esos controles:
            - Se reduce la probabilidad de poder evitarlos.
        - Debe producirse un efecto disuasivo respecto de posibles intentos de violar la seguridad.

Para diseñar *medidas efectivas de seguridad* se debe primero:

- Enumerar y comprender las amenazas potenciales.
- Definir qué grado de seguridad se desea (y cuánto se está dispuesto a gastar en seguridad).
- Analizar las contramedidas disponibles.

Vigilancia, Verificación de Amenazas y Amplificación

Ana González (Kao)

Vigilancia

La vigilancia *tiene que ver con:*

- La verificación y la auditoría del sistema.
- La autentificación de los usuarios.

Los sistemas sofisticados de *autentificación de usuarios* resultan muy difíciles de evitar por parte de los intrusos.

Un problema existente es la posibilidad de que el sistema *rechace* a usuarios legítimos:

- Un sistema de reconocimiento de voz podría rechazar a un usuario legítimo resfriado.
- Un sistema de huellas digitales podría rechazar a un usuario legítimo que tenga una cortadura o una quemadura.

Verificación de Amenazas

Es una técnica según la cual los usuarios *no pueden tener acceso directo a un recurso*:

- Solo lo tienen las rutinas del S. O. llamadas *programas de vigilancia.*
- El usuario solicita el acceso al S. O.
- El S. O. niega o permite el acceso.
- El acceso lo hace un programa de vigilancia que luego pasa los resultados al programa del usuario.
- Permite:
    - Detectar los intentos de penetración en el momento en que se producen.
    - Advertir en consecuencia.

Amplificación

La *amplificación* se produce cuando:

- Un *programa de vigilancia* necesita para cumplir su cometido mayores derechos de acceso de los que disponen los usuarios:
    - Ej.: se requiere calcular un promedio para lo cual es necesario leer un conjunto de registros a los que el usuario no tiene acceso individualmente.

Ana González (Kao)

Protección por Contraseña

Las clases de elementos de *autentificación* para establecer la *identidad de una persona* son:

- Algo *sobre la persona:*
  - Ej.: huellas digitales, registro de la voz, fotografía, firma, etc.
- Algo *poseído por la persona:*
  - Ej.: insignias especiales, tarjetas de identificación, llaves, etc.
- Algo *conocido por la persona:*
  - Ej.: contraseñas, combinaciones de cerraduras, etc.

El esquema más común de autentificación es la *protección por contraseña:*

- El usuario elige una *palabra clave*, la memoriza, la teclea para ser admitido en el sistema computarizado:
  - La clave no debe desplegarse en pantalla ni aparecer impresa.

La protección por contraseñas tiene ciertas *desventajas* si no se utilizan criterios adecuados para:

- Elegir las contraseñas.
- Comunicarlas fehacientemente en caso de que sea necesario.
- Destruir las contraseñas luego de que han sido comunicadas.
- Modificarlas luego de algún tiempo.

Los *usuarios* tienden a elegir contraseñas *fáciles de recordar:*

- Nombre de un amigo, pariente, perro, gato, etc.
- Número de documento, domicilio, patente del auto, etc.

Estos datos *podrían ser conocidos* por quien intente una violación a la seguridad mediante intentos repetidos, por lo tanto debe *limitarse la cantidad de intentos fallidos* de acierto para el ingreso de la contraseña.

La contraseña no debe ser muy corta para no facilitar la probabilidad de acierto.

Tampoco debe ser muy larga para que no se dificulte su memorización, ya que los usuarios la anotarían por miedo a no recordarla y ello incrementaría los riesgos de que trascienda.

Ana González (Kao)

Auditoría y Controles de Acceso

Auditoría

La auditoría suele realizarse *a posteriori* en *sistemas manuales*, es decir que se examinan las recientes transacciones de una organización para determinar si hubo ilícitos.

La auditoría en un *sistema informático* puede implicar un *procesamiento inmediato*, pues se verifican las transacciones que se acaban de producir.

Un *registro de auditoría* es un registro permanente de acontecimientos importantes acaecidos en el sistema informático:

- Se realiza automáticamente cada vez que ocurre tal evento.
- Se almacena en un área altamente protegida del sistema.
- Es un mecanismo importante de detección.

El registro de auditoría debe ser *revisado* cuidadosamente y con frecuencia:

- Las revisiones deben hacerse:
  - Periódicamente:
    - Se presta atención regularmente a los problemas de seguridad.
  - Al azar:
    - Se intenta atrapar a los intrusos desprevenidos.

Controles de Acceso

Lo fundamental para la *seguridad interna* es *controlar el acceso a los datos almacenados.*

Los *derechos de acceso* definen *qué acceso* tienen varios sujetos o varios objetos.

Los sujetos acceden a los objetos.

Los *objetos* son entidades que contienen *información.*

Los *objetos* pueden ser:

- Concretos:
  - Ej.: discos, cintas, procesadores, almacenamiento, etc.
- Abstractos:
  - Ej.: estructuras de datos, de procesos, etc.

Ana González (Kao)

Los objetos están *protegidos* contra los sujetos.

Las *autorizaciones* a un sistema se conceden *a los sujetos.*

Los *sujetos* pueden ser varios tipos de entidades:

- Ej.: usuarios, procesos, programas, otras entidades, etc.

Los *derechos de acceso* más comunes son:

- Acceso de lectura.
- Acceso de escritura.
- Acceso de ejecución.

Una forma de *implementación* es mediante una *matriz de control de acceso* con:

- Filas para los sujetos.
- Columnas para los objetos.
- Celdas de la matriz para los derechos de acceso que un usuario tiene a un objeto.

Una matriz de control de acceso debe ser muy celosamente protegida por el S. O.

Núcleos de Seguridad y Seguridad por Hardware

Núcleos de Seguridad

Es mucho más fácil hacer un sistema más seguro si la seguridad se ha incorporado desde el principio al diseño del sistema.

Las *medidas de seguridad* deben ser implementadas en *todo el sistema informático.*

Un sistema de alta seguridad requiere que el *núcleo del S. O.* sea seguro.

Las medidas de seguridad más decisivas se implementan en el *núcleo*, que se mantiene intencionalmente lo más pequeño posible.

Generalmente se da que aislando las funciones que deben ser aseguradas en un S. O. de propósito general a gran escala, se crea un núcleo grande.

La *seguridad del sistema* depende especialmente de *asegurar las funciones que realizan:*

- El control de acceso.
- La entrada al sistema.
- La verificación.
- La administración del almacenamiento real, del almacenamiento virtual y del sistema de archivos.

Seguridad por Hardware

Existe una tendencia a *incorporar al hardware funciones del S. O:*

- Las *funciones* incorporadas al hardware:
  - Resultan mucho *más seguras* que cuando son asequibles como instrucciones de software que pueden ser modificadas.
  - Pueden operar mucho *más rápido* que en el software:
    - Mejorando la performance.
    - Permitiendo controles más frecuentes.

Sistemas Supervivientes

El diseño de *sistemas de alta seguridad* debe asegurar:

- Su operación de manera continua y confiable.
- Su disponibilidad.

Un *sistema de computación superviviente* es aquel que *continúa operando aún después de que uno o más de sus componentes falla:*

- Es una cuestión cada vez más importante, especialmente para *sistemas en línea.*

Generalmente continúan operando con una *degradación suave* en los niveles de prestación.

Los componentes fallidos deben poder *reemplazarse sin interrumpir* el funcionamiento del sistema.

Una clave para la capacidad de supervivencia es la *redundancia:*

- Si un componente falla, otro equivalente toma su puesto.
- Se puede implementar como:
  - Un conjunto de recursos idénticos que funcionan en paralelo.

Ana González (Kao)

- Un conjunto separado de recursos redundantes que se activan cuando se produce un fallo.

Algunas *características de supervivencia* son:

- La incorporación de *mecanismos contra fallos en el hardware* en vez de en el software.
- El uso de *multiprocesamiento transparente* para permitir mejorar el rendimiento sin modificar el software.
- El uso de *subsistemas múltiples* de entrada / salida.
- La incorporación de *mecanismos de detección de fallos* en el hardware y en el software.

Principales Fallos Genéricos Funcionales de los Sistemas

Los principales fallos genéricos funcionales de los sistemas son los siguientes:

Autentificación:

- Los usuarios no pueden determinar si el hardware y el software con que funcionan son los que deben ser.
- Un intruso podría reemplazar un programa sin conocimiento del usuario.
- Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

Cifrado:

- No se almacena cifrada la lista maestra de contraseñas.

Implementación:

- Implementación improcedente de un buen diseño de seguridad.

Confianza implícita:

- Una rutina supone que otra está funcionando correctamente cuando, de hecho, debería examinar los parámetros suministrados por la otra rutina.

Compartimiento implícito:

- El S. O. deposita inadvertidamente información importante del sistema en un espacio de direcciones del usuario.

Ana González (Kao)

Comunicación entre procesos:

- Usos inadecuados de los mecanismos de send / receive que pueden ser aprovechados por los intrusos.

Verificación de la legalidad:

- Validación insuficiente de los parámetros del usuario.

Desconexión de línea:

- Ante una desconexión de línea el S. O. debería:
  - Dar de baja al usuario (o los usuarios) de la línea.
  - Colocarlos en un estado tal que requieran la re - autorización para obtener nuevamente el control.

Descuido del operador:

- Un intruso podría engañar a un operador y hacer que le habilite determinados recursos.

Paso de parámetros por referencia en función de su valor:

- Es más seguro pasar los parámetros directamente en registros que tener los registros apuntando a las áreas que contienen los parámetros.
- El paso por referencia puede permitir que los parámetros, estando aún en el área del usuario, puedan ser modificados antes de ser usados por el sistema.

Contraseñas:

- No deben ser fácilmente deducibles u obtenibles mediante ensayos repetidos.

Entrampamiento al intruso:

- Los S. O. deben tener mecanismos de entrampamiento para atraer al intruso inexperto.

Privilegio:

- Cuando hay demasiados programas con demasiados privilegios se viola el *principio del menor privilegio.*

Confinamiento del programa:

Ana González (Kao)

- Un programa *"prestado"* de otro usuario puede actuar como un *"Caballo de Troya".*

Prohibiciones:

- Se advierte a los usuarios que no utilicen ciertas opciones porque los resultados podrían ser *"indeterminados"*, pero no se bloquea su uso, con lo que puede robar o alterar datos.

Residuos:

- Un intruso podría encontrar una lista de contraseñas con solo buscar en lugares tales como una *"papelera":*
  - Del sistema o física.
  - La información delicada debe ser sobrescrita o destruida antes de liberar o descartar el medio que ocupa.

Blindaje:

- Los intrusos pueden conectarse a una línea de transmisión sin hacer contacto físico:
  - Utilizan el campo inducido por la circulación de corriente en un cable.
  - Se previene con un adecuado blindaje eléctrico.

Valores de umbral:

- Si no se dispone de valores umbral, no habrá:
  - Límites al número de intentos fallidos de ingreso.
  - Bloqueos a nuevos intentos.
  - Comunicaciones al supervisor o administrador del sistema.

Ataques Genéricos a Sistemas Operativos

Los principales ataques genéricos a los S. O. son los siguientes:

Asincronismo:

- Se tienen procesos múltiples que progresan asincrónicamente.
- Un proceso podría modificar los parámetros ya validados por otro proceso pero aún no utilizados.
- Un proceso podría pasar valores malos a otro aún cuando el segundo realice una verificación extensa.

Ana González (Kao)

Rastreo:

- Un usuario revisa el sistema intentando localizar información privilegiada.

Entre líneas:

- Se utiliza una línea de comunicaciones mantenida por un usuario habilitado que está inactivo.

Código clandestino:

- Se modifica el S. O. bajo una presunta depuración pero se incorpora código que permite ingresos no autorizados.

Prohibición de acceso:

- Un usuario escribe un programa que bloquea el acceso o servicio a los usuarios legítimos mediante:
  - Caídas del sistema, ciclos infinitos, monopolio de recursos, etc.

Procesos sincronizados interactivos:

- Se utilizan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

Desconexión de línea:

- El intruso intenta acceder al trabajo de un usuario desconectado:
  - Luego de una desconexión de línea.
  - Antes de que el sistema reconozca la desconexión.

Disfraz:

- El intruso asume la identidad de un usuario legítimo luego de haber obtenido la identificación apropiada por medios clandestinos.

Ataque "nak":

- Si el S. O. permite a un usuario:
  - Interrumpir un proceso en ejecución mediante una *"tecla"* de *"reconocimiento negativo".*
  - Realizar otra operación.
  - Reanudar el proceso interrumpido.

Ana González (Kao)

- Un intruso podría *"encontrar"* al sistema en un estado no protegido y hacerse con el control.

Engaño al operador:

- Con un engaño se hace realizar al operador una acción que comprometa la seguridad del sistema.

Parásito:

- Mediante equipamiento especial el intruso:
  - Intercepta los mensajes entre un usuario habilitado y el procesador.
  - Los modifica o reemplaza totalmente.

Caballo de Troya:

- El intruso coloca un código dentro del sistema que luego le permita accesos no autorizados.
- Puede permanecer en el sistema.
- Puede borrar todo rastro de sí mismo luego de la penetración.

Parámetros inesperados:

- El intruso suministra valores inesperados a una llamada al núcleo.
- Intenta aprovechar una debilidad de los mecanismos de verificación de la legalidad del S. O.

3. Métodos de autenticación clásica

Ya sabemos que unos requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismo de seguridad adecuados a la información que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos

activos del sistema, generalmente usuarios) que intentan acceder a los objetos (elementos pasivos, como ficheros o capacidad de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones retinales.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser identificar a una persona, sino autenticar que esa persona es quien dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para un ordenador existe una gran diferencia entre ellos: imaginemos un potencial sistema de identificación estrictamente hablando, por ejemplo uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector, y el sistema sería capaz de decidir si es un usuario válido, y en ese caso decir de quién se trata; esto es identificación. Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario...) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, sino autenticarlo: comprobar los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser: estamos reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido, el grupo de usuarios del sistema que necesita autenticarlos.

Dentro de un sistema de control de acceso con autenticación, este será sin duda el proceso más importante. Si por ejemplo un sitio web tiene información sensible o dirigida sólo a un pequeño grupo de personas, la autenticación asegura que las personas que ven esas páginas estén autorizadas. En el caso de utilizar tarjetas criptográficas como el DNIe la autenticación que estas ofrecen puede permitir controlar al completo cuándo y dónde alguien entra, navega y sale. Entonces, se puede definir la autenticación como el proceso electrónico mediante el cual se verifica la identidad de un usuario.

Existen tres métodos de autenticación:

- basados en algo conocido: contraseñas, frases de paso, etc.
- basados en algo poseído: tarjeta de identidad, tarjeta inteligente (smartcard), dispositivo usb (token), etc.
- basados característica físicas del usuario: verificación de voz, escritura, huellas, patrones oculares, etc.

En función del número de factores en los que se base el sistema de autenticación se puede hablar de:

- Autenticación unimodal: basada en un elemento conocido, algo poseído o alguna característica física (por ejemplo la contraseña asociada a un usuario para entrar en un portal web o un token criptográfico o la utilización de la huella dactilar).

- Autenticación multimodal: es una combinación de varios métodos de autenticación distintos, en la que intervienen un elemento que el usuario sabe y otro que el usuario posee o cualquier combinación posible. Por ejemplo el DNIe es un soporte seguro (que el usuario posee) y además para poder autenticarse en un sistema necesitará un PIN (algo que el usuario conoce).

Dentro de estos grupos los sistemas más utilizados o reconocidos son los siguientes:

- Autentificación biométrica: consiste en la verificación de la identidad de un sujeto, basándose en ciertos elementos morfológicos que le son inherentes y que sólo se dan en ese sujeto. Es decir, rasgos distintivos de una persona (su voz, su huella dactilar, etc.) para más tarde ser capaces de comparar esa muestra con otra original, y poder averiguar si son iguales o no. Puede ser unimodal o multimodal.

- Autenticación basada en tokens: son dispositivos para autenticación de usuarios que permiten la portabilidad de certificados. Se conectan al computador mediante USB, lo cual los hace compatibles con prácticamente cualquier ordenador y sistema operativo. Los certificados van protegidos con clave, lo que para su uso hace imprescindible estar en posesión del token y conocer la contraseña. Multimodal basado en algo que el usuario poseé y conoce.

- Autenticación SSO(del inglés, Single Sign-On): es un procedimiento de autenticación multimodal que habilita al usuario para acceder a varios sistemas con una sola instancia de identificación. Hay cinco tipos principales de SSO:
  - E-SSO (Enterprise SSO) también llamado legacy single sign-on, funciona para una autenticación primaria, interceptando los requerimientos de login presentados por las aplicaciones secundarias para completar los mismos con el usuario y contraseña. Los sistemas E-SSO permiten interactuar con sistemas que pueden deshabilitar la presentación de la pantalla de login.
  - Web-SSO también llamado Web access management (Web-AM) trabaja sólo con aplicaciones y recursos accedidos vía web. Los accesos son interceptados con la ayuda de un servidor proxy o de un componente instalado en el servidor web destino. Los usuarios no autenticados que tratan de acceder son redirigidos a un servidor de autenticación y regresan solo después de haber logrado un acceso exitoso. Se utilizan cookies, para reconocer aquellos usuarios que acceden y su estado de autenticación.
  - Kerberos es un método popular de externalizar la autenticación de los

Ana González (Kao)

usuarios. Los usuarios se registran en el servidor Kerberos y reciben un "ticket", luego las aplicaciones-cliente lo presentan para obtener acceso.

- Identidad federada es una nueva manera de concebir este tema, también para aplicaciones Web. Utiliza protocolos basados en estándares para habilitar que las aplicaciones puedan identificar los clientes sin necesidad de autenticación redundante.
- OpenID es un proceso de SSO distribuido y descentralizado donde la identidad se compila en una url que cualquier aplicación o servidor puede verificar.

- Autenticación LDAP (del inglés,Lightweight Directory Access Protocol): es un protocolo de acceso unificado a un conjunto de información sobre una red.

La autenticación requiere de ciertos algoritmos criptográficos para el desarrollo de las anteriores aplicaciones. Estos algoritmos criptográficos precisan de dos claves (criptografía asimétrica), una clave (criptografía simétrica) o ninguna (funciones hash) para la codificación del mensaje original. El resultado obtenido variará en función de la clave utilizada. En general los algoritmos criptográficos se pueden clasificar en tres grandes familias tal como hemos visto en el tema anterior.

- **Criptografía simétrica o criptografía de clave secreta:** Utiliza una sola clave para cifrar el mensaje original. DES, TDES, RC2, RC4, RC5, IDEA, Blowfish yAES son algunos ejemplos de algoritmos de criptografía simétrica.

- **Criptografía asimétrica o criptografía de clave pública:** Utiliza dos claves diferentes, una para cifrar y otra para descifrar, en función del orden utilizado proporciona unas servicios de seguridad u otros. Diffie-Hellman, RSA,DSA, El Gamal, son algunos de los algoritmos de criptografía asimétrica.

- **Algoritmos hash o de resumen:** No precisa de ninguna clave para realizar el resumen. SHA, MD5, Rabin-Karp, son algunas funciones de resumen.

Los sistemas DSS, PGP, GPG, SSH, SSL y TLS utilizan los algoritmos anteriores para proporcionar diferentes servicios seguros como cifrado avanzado de documentos comunicación segura, etc.

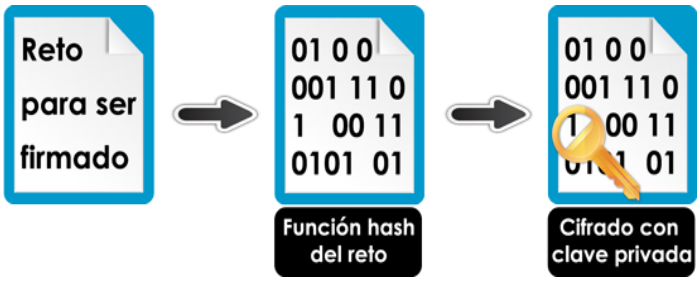
La autenticación con certificado electrónico se basa en el protocolo de reto-respuesta, en inglés, challenge-response, donde una de las partes presenta un reto (challenge) y la otra parte le contesta con una respuesta válida (response) que necesita ser

Ana González (Kao)

autenticada. Más específicamente:

- Participan dos partes en la autenticación: el usuario que necesita ser autenticado y la parte encargada de realizar la autenticación.
- Cada parte implicada tiene un par de claves: una clave pública conocida por las otras partes, y una privada que sólo conoce el propietario de la misma.
- La parte encargada de la autenticación envía un reto al usuario que desea autenticarse.
- El usuario calcula un resumen de los datos, hash, y lo cifra con su clave privada. Le envía estos datos a la parte encargada de la autenticación a modo de respuesta.
- Por último, la parte encargada de la autenticación descifra la respuesta utilizando la clave pública del usuario y verifica que los datos que obtiene, es decir el resumen de los datos calculados por el usuario, es igual al resumen realizado por él, que es el emisor del mensaje original, es decir, el reto.

Autenticación. Esquema vista emisor



Autenticación. Esquema vista autenticador

Es fácil ver ejemplos de cada uno de estos tipos de autenticación: un password (Unix) o passphrase (PGP) es algo que el usuario conoce y el resto de personas no, una tarjeta de identidad es algo que el usuario lleva consigo, la huella dactilar es una característica física del usuario, y un acto involuntario podría considerarse que se produce al firmar (al rubricar la firma no se piensa en el diseño de cada trazo individualmente). Por

Ana González (Kao)

supuesto, un sistema de autenticación puede (y debe, para incrementar su fiabilidad) combinar mecanismos de diferente tipo, como en el caso de una tarjeta de crédito junto al PIN a la hora de utilizar un cajero automático o en el de un dispositivo generador de claves para el uso de One Time Passwords.

Cualquier sistema de identificación (aunque les llamemos así, recordemos que realmente son sistemas de autenticación) ha de poseer unas determinadas características para ser viable; obviamente, ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros), económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto) y ha de soportar con éxito cierto tipo de ataques (por ejemplo, imaginemos que cualquier usuario puede descifrar el password utilizado en el sistema de autenticación de Unix en tiempo polinomial; esto sería inaceptable).

Aparte de estas características tenemos otra, no técnica sino humana, pero quizás la más importante: un sistema de autenticación ha de ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen. Por ejemplo, imaginemos un potencial sistema de identificación para acceder a los recursos de la Universidad, consistente en un dispositivo que fuera capaz de realizar un análisis de sangre a un usuario y así comprobar que es quien dice ser; seguramente sería barato y altamente fiable, pero nadie aceptaría dar un poco de sangre cada vez que desee consultar su correo.

Sistemas basados en algo conocido: contraseñas

El modelo de autenticación más básico consiste en decidir si un usuario es quien dice ser simplemente basándonos en una prueba de conocimiento que a priori sólo ese usuario puede superar, desde Alí Babá y su “Ábrete, Sésamo” hasta los más modernos sistemas Unix, esa prueba de conocimiento no es más que una contraseña que en principio es secreta.

Evidentemente, esta aproximación es la más vulnerable a todo tipo de ataques, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad, como es el caso de los sistemas Unix en redes normales (y en general en todos los sistemas operativos en redes de seguridad media-baja); otros entornos en los que se suele aplicar este modelo de autenticación son las aplicaciones que requieren de alguna identificación de usuarios, como el software de cifrado PGP o el escáner de seguridad NESSUS. También se utiliza como complemento a otros mecanismos de autenticación, por ejemplo en el caso del Número de

Ana González (Kao)

Identificación Personal (PIN) a la hora de utilizar cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común, y si ésta es correcta se otorga el acceso a un recurso. Lo habitual es que existan unos roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior (en el modelo del acceso a sistemas Unix, tenemos al usuario y al sistema que le permite o niega la entrada).

Como hemos dicho, este esquema es muy frágil: basta con que una de las partes no mantenga la contraseña en secreto para que toda la seguridad del modelo se pierda; por ejemplo, si el usuario de una máquina Unix comparte su clave con un tercero, o si ese tercero consigue leerla y rompe su cifrado (por ejemplo, como veremos luego, mediante un ataque de diccionario), automáticamente esa persona puede autenticarse ante el sistema con éxito con la identidad de un usuario que no le corresponde.

Sistemas basados en algo poseído: tarjetas inteligentes

Hace más de veinte años un periodista francés llamado Roland Moreno patentaba la integración de un procesador en una tarjeta de plástico; sin duda, no podía imaginar el abanico de aplicaciones de seguridad que ese nuevo dispositivo, denominado chipcard, estaba abriendo. Desde entonces, cientos de millones de esas tarjetas han sido fabricadas, y son utilizadas a diario para fines que varían desde las tarjetas monedero más sencillas hasta el control de accesos a instalaciones militares y agencias de inteligencia de todo el mundo; cuando a las chipcards se les incorporó un procesador inteligente nacieron las smartcards, una gran revolución en el ámbito de la autenticación de usuarios.

Desde un punto de vista formal, una tarjeta inteligente (o smartcard) es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la adulteración, que ofrece funciones para un almacenamiento seguro de información y también para el procesamiento de la misma en base a tecnología VLSI.

En la práctica, las tarjetas inteligentes poseen un chip empotrado en la propia tarjeta que puede implementar un sistema de ficheros cifrado y funciones criptográficas, y además puede detectar activamente intentos no válidos de acceso a la información

Ana González (Kao)

almacenada. Este chip inteligente es el que las diferencia de las simples tarjetas de crédito, que solamente incorporan una banda magnética donde va almacenada cierta información del propietario de la tarjeta.

Estructura genérica de una smartcard.

En la figura se muestra la estructura más generalista de una tarjeta inteligente. En ella podemos observar que el acceso a las áreas de memoria solamente es posible a través de la unidad de entrada/salida y de una CPU (típicamente de 8 bits), lo que evidentemente aumenta la seguridad del dispositivo. Existe también un sistema operativo empotrado en la tarjeta - generalmente en ROM, aunque también se puede extender con funciones en la EEPROM - cuya función es realizar tareas criptográficas (algoritmos de cifrado como RSA o Triple DES, funciones resumen...); el criptoprocesador apoya estas tareas ofreciendo operaciones RSA con claves de 512 a 1024 bits. Un ejemplo de implementación real de este esquema lo constituye la tarjeta inteligente CERES, de la Fábrica Nacional de Moneda y Timbre española, en ella se incluye además un generador de números aleatorios junto a los mecanismos de protección internos de la tarjeta.

Cuando el usuario poseedor de una smartcard desea autenticarse necesita introducir la tarjeta en un hardware lector; los dos dispositivos se identifican entre sí con un protocolo a dos bandas en el que es necesario que ambos conozcan la misma clave (CK o CCK, Company Key o Chipcard Communication Key), lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía; además esta clave puede utilizarse para asegurar la comunicación entre la tarjeta y el dispositivo lector. Tras identificarse las dos partes, se lee la identificación personal (PID) de la tarjeta, y el usuario teclea su PIN; se inicia entonces un protocolo desafío-respuesta: se envía el PID a la máquina y ésta desafía a la tarjeta, que responde al desafío utilizando una clave personal del usuario (PK, Personal Key). Si la respuesta es correcta, el host ha identificado la tarjeta y el usuario obtiene acceso al recurso pretendido.

Las ventajas de utilizar tarjetas inteligentes como medio para autenticar usuarios son muchas frente a las desventajas. Se trata de un modelo ampliamente aceptado entre los usuarios, rápido, y que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Además, su uso es factible tanto para controles de acceso físico como para controles de acceso lógico a los hosts, y se integra fácilmente con otros mecanismos de autenticación como las contraseñas, y en caso de desear bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuando la introduzca en el lector o marcarla como inválida en una base de datos (por ejemplo, si se equivoca varias veces al teclear su PIN, igual que sucede con una tarjeta

Ana González (Kao)

de crédito normal).

Como principal inconveniente de las smartcards podemos citar el coste adicional que supone para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas; aparte, que un usuario pierda su tarjeta es bastante fácil, y durante el tiempo que no disponga de ella o no puede acceder al sistema, o hemos de establecer reglas especiales que pueden comprometer nuestra seguridad (y por supuesto se ha de marcar como tarjeta inválida en una base de datos central, para que un potencial atacante no pueda utilizarla).

También la distancia lógica entre la smartcard y su poseedor - simplemente nos podemos fijar en que la tarjeta no tiene un interfaz para el usuario - puede ser fuente de varios problemas de seguridad

Aparte de los problemas que puede implicar el uso de smartcards en sí, contra la lógica de una tarjeta inteligente existen diversos métodos de ataque, como realizar ingeniería inversa - destructiva - contra el circuito de silicio (y los contenidos de la ROM), adulterar la información guardada en la tarjeta o determinar por diferentes métodos el contenido de la memoria EEPROM. Sin duda una de las personas que más ha contribuido a incrementar la seguridad de las smartcards gracias a sus estudios y ataques es el experto británico Ross J. Anderson en su página web personal, http://www.cl.cam.ac.uk/users/rja14/, podemos encontrar todos sus artículos sobre este tema, demasiados como para citarlos aquí uno a uno.

Método de Autenticación	Commentarios		
Passwords Estáticas	•Bajo Coste		•Vulnerable
Secretos Compartidos con autorización en el dispositivo	•Bajo Coste •Autenticación Mutua •PC amenaza de virus		•Movilidad Poco amigable •No 2-factor •Escalabilidad Problemas
Autorización basada en Riesgo	•Detection de Anonalías •Usuario amenudo transparente		•Mobile unfriendly •Not 2-factor
Scratch / Tarjetas de Coordenadas	•2-factor •Bajo Coste		•Huella Footprint •Bajo tecnología/ manual
One Time Password (OTP) OTP Tokens	Hard Tokens	•Mas coste total •Incómodo	•Token "collar" •Enterprise applications
	Soft Tokens	**•2-factor •Fácil de usar en movilidad**	**•No hardware extra •Bajo Coste de Implementación**
Tarjetas Inteligentes & PKI	**•Firma de Transacción •Autorización Mutua**		**•Modelos de Confianza •Costoso ciclo de vida •Mas complejas**

Protocolos PPP, PAP, CHAP

¿Qué es el protocolo "PPP"?

El PPP fue desarrollado por el IETF (Internet Engineering Task Force) en 1993 para mejorar estas y algunas otras deficiencias, y crear un estándar internacional, para generar un protocolo de encapsulación de capa 2 que puede ser utilizado tanto en enlaces sincrónicos como asincrónicos.

Características:

- PPP es un protocolo usado para enviar tramas datagramas a través de una conexión serie.
- El protocolo PPP no es propietario.
- Resuelve dificultades del protocolo SLIP.
- Opera en modo sincrónico y asincrónico.
- Puede utilizarse para conectar redes IP, Apple Talk e IPX. A través de conexiones WAN.
- Este protocolo se utiliza para conectar estaciones a Internet vía MODEMS y líneas analógicas.
- Utiliza la compresión Van Jacobson para la cabecera UDP-IP

¿Para qué sirve el protocolo "PPP"?

- El protocolo PPP proporciona un método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos estaciones. Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

- Tiene tres componentes:
  - Un mecanismo de enmarcado para encapsular datagramas multiprotocolo y manejar la detección de errores.
  - Un protocolo de control de enlace (LCP, protocolo de control de enlace) para establecer, configurar y probar la conexión de datos.
  - Una familia de protocolos de control de red (NCPs, Network Control Protocols) para establecer y configurar los distintos

Ana González (Kao)

protocolos de nivel de red.

¿Cuál es el Funcionamiento del protocolo "PPP"?

- ✓ En primera instancia, la PC llama al router del ISP (Internet Service Provider, proveedor del servicio de Internet), a través de una ETCD.
- ✓ Al establecer la conexión física y lógica. La PC manda al router una serie de paquetes LCP en la trama de PPP.
- ✓ Una vez que se han acordado estos parámetros se envían una serie de paquetes NCP para configurar la capa de red.
- ✓ Típicamente, la PC quiere ejecutar una pila de protocolos TCP/IP, por lo que necesita una dirección IP. No hay suficientes direcciones IP para todos, por lo que normalmente cada ISP tiene un bloque de ellas y asigna dinámicamente una a cada PC que se acaba de conectar para que la use durante su sesión. Se utiliza el NCP para asignar la dirección de IP.
- ✓ En este momento la PC ya es un host de Internet y puede enviar y recibir paquetes IP. Cuando el usuario ha terminado se usa NCP para destruir la conexión de la capa de red y liberar la dirección IP.
- ✓ Al culminar la TX, se usa un NCP para destruir la conexión de la capa de red y liberar la IP. Y un LCP para cancelar la capa de enlace de datos.
- ✓ PPP se puede usar en capa física a nivel de SONET o líneas HDLC.

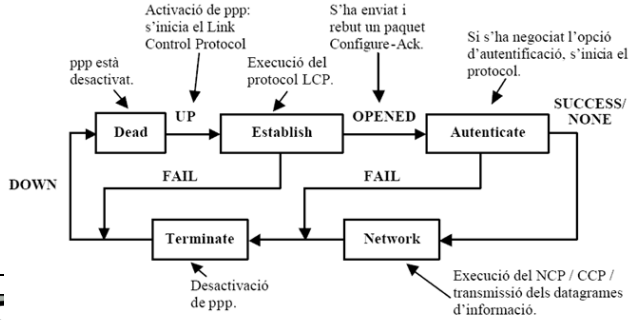
PAP Y CHAP AUTENTIFICACION DE PPP PAP Y CHAP

PPP a diferencia de HDLC soporta autentificación.

PAP (PPP Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol RFC 1334 y RFC 1994.

La autentificación se realiza una vez el nivel de enlace y de red se han realizado mediante NCP. Si la autentificación falla, el enlace se deshabilita.

Tanto PAP como CHAP son métodos de autenticación entre dispositivos, con el fin de establecer conexiones más o menos seguras. Englobando en la palabra dispositivos, tanto ordenadores, servidores, dispositivos móviles, routers, firewalls, etc… La diferencia entre PAP y CHAP es la seguridad y la forma de autenticarse.



PAP (Password Authentication Protocol), Protocolo de autenticación por contraseña:

Cuando dos equipos A y B, necesitan establecer comunicación, uno de los equipos envía al otro equipo la información de usuario y contraseña para establecer la comunicación.

El dispositivo receptor, comprueba el usuario y su contraseña asociada en la base de datos local que posee. Tanto usuario y contraseña han de ser las mismas en las bases de datos locales de ambos dispositivos.

Una vez autenticado el usuario, se establece la conexión. Este método de autenticación se le denomina también método de dos vías.

El principal riesgo de este tipo de autenticación es el envío de usuario y contraseña en texto plano a través de la red, esto es sin encriptar. Lo cual puede ser un riesgo si dicho mensaje es interceptado en una red.

Por otro lado existen motivos por los cuales no se debe usar PAP: incompatibilidad de diferentes implementaciones de fabricantes, requerimientos de aplicaciones, etc..

CHAP (Challenge Handshake Authetication Protocol)- Protocolo de autenticación por intercambio de señales por desafío.

Dos dispositivos necesitan establecer conexión, dispositivo A y B.

El dispositivo A, es el que desea establecer dicha conexión y por tanto el dispositivo B, necesita que A se autentifique.

El dispositivo B manda su nombre de usuario, genera un identificador (ID) y un número aleatorio. Todo ello se denomina cadena de desafío.

El equipo A al recibir la información, comprueba el nombre de usuario recibido y comprueba la contraseña (que es la misma en ambas bases de datos locales) asociada a ese usuario.

Mediante el ID recibido, el numero aleatorio y nombre de usuario recibido, así como con la contraseña que posee asociada a ese usuario, el dispositivo A genera un hash (que es una cadena alfanumérica) y lo envía al dispositivo B. Dicho hash esta encriptado en MD5.

Ejemplo de Hash: DFCD3454

El dispositivo B por su parte ha creado otro hash, con el usuario (que envió al dispositivo A) y la contraseña asociada, el ID que genero y el numero aleatorio (todo lo que envió al dispositivo A en un primer momento).

Cuando el dispositivo B, recibe el hash del dispositivo A, compara el hash recibido con el hash calculado por él, los cuales deben ser iguales.

Ana González (Kao)

Después de esto se establece la comunicación.

Este método es el más "seguro", puesto que en ningún momento se envía la contraseña, tan solo el usuario y números aleatorios, además de ir encriptada la información. El método de autenticación se le denomina **método de tres vías**.

Las bases de datos donde se guardan tanto usuarios como contraseñas para autenticar los accesos se denominan AAA (authentication, Authorization and accounting), también existen otros como TACACS y TACACS +, los cuales además de autenticar y autorizar, definen que puede hacer el usuario (que privilegios tiene) y que hace en todo momento (monitorización).

PAP frente a CHAP

PAP, que es utilizado por muchos proveedores de Internet (ISP), tal como acabamos de ver funciona básicamente de la misma forma que el procedimiento normal de registro.

El cliente se autentifica a sí mismo enviando un nombre de usuario y una contraseña (opcionalmente encriptada) al servidor, la cual es comparada por el servidor con su base de datos de claves o secrets.

Esta técnica es vulnerable a los intrusos que pueden intentar obtener la contraseña escuchando en una línea serie y a otros que hagan sucesivos intentos de ataque por el método de prueba y error.

CHAP no tiene estos defectos. Con CHAP, el autentificador (i.e. el servidor) envía una cadena de "reto" generada aleatoriamente al cliente, junto a su nombre de ordenador. El cliente utiliza el nombre del ordenador para buscar la clave apropiada, la combina con el reto, y encripta la cadena utilizando una función de codificación de un solo sentido. El resultado es devuelto al servidor junto con el nombre del ordenador cliente. El servidor realiza ahora la misma computación, y advierte al cliente si obtiene el mismo resultado.

Otra característica de CHAP es que no solicita autentificación al cliente solamente al comienzo de la sesión, sino que envía retos a intervalos regulares para asegurarse de que el cliente no ha sido reemplazado por un intruso.

RADIUS.

¿Qué es RADIUS?

RADIUS es un protocolo UDP de autenticación y autorización, para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones. Sus principales características son:

1. Cliente / Servidor Modelo A Network Access Server (NAS): Funciona como un cliente de RADIUS. El cliente es responsable de pasar la información del usuario a los servidores RADIUS designados, y luego actuar sobre la respuesta que se devuelve.
Servidores RADIUS. Se encargan de recibir las solicitudes de conexión del usuario, la autenticación del usuario, y luego regresar toda la información de configuración necesarios para el cliente para ofrecer un servicio al usuario. Un servidor RADIUS puede actuar como un cliente proxy para otros servidores RADIUS o de otros tipos de servidores de autenticación.

2.- Red de Seguridad: Las transacciones entre el cliente y el servidor RADIUS se autentican a través de la utilización de un secreto compartido, que nunca se envían a través de la red. Además, todas las contraseñas de usuario se envían cifrados entre el cliente y el servidor RADIUS, para eliminar la posibilidad de que alguien husmeando en una red no segura podría determinar la contraseña de un usuario.

3.- Mecanismos de autenticación flexible: El servidor RADIUS puede apoyar una variedad de métodos para autenticar a un usuario. Cuando se proporciona con el nombre de usuario y la contraseña original dado por el usuario, que puede soportar PPP PAP o CHAP, inicio de sesión UNIX, y otros mecanismos de autenticación.

4.- Protocolo Extensible: Todas las transacciones se compone de atributo de longitud variable Relación longitud-3-tuplas. Nuevos valores de los atributos se pueden añadir sin perturbar las implementaciones existentes del protocolo.

Estas son las 4 características principales de RADIUS, sus funciones principales y características. RADIUS permite una autenticación segura, basada en cliente/servidor, o servidor/servidor, las autenticaciones que realiza son mediante puertos seguros, un claro ejemplo del uso de este protocolo es el conectarse al internet. Los ISP's (Internet Service Provided), usan este protocolo para mediante el ADSL-Modem enviar la información del usuario que quiere conectarse a sus servidores.

Radius fuerza a los usuarios a autenticarse a bajo nivel antes de que el switch abra el puerto.

Ana González (Kao)

RADIUS es un protocolo de autenticación ampliamente utilizado que permite tener la autenticación, la autorización y la contabilidad centralizadas para el acceso de red. Desarrollado inicialmente para acceso remoto dial-up (marcado manual), RADIUS es soportado actualmente por servidores VPN (Virtual Private Network), puntos de acceso inalámbricos, conmutadores de autenticación Ethernet, acceso DSL (Digital Subscriber Line) y otros tipos de redes de acceso.

El protocolo RADIUS se describe en la RFC 2865 (www.ietf.org). Un cliente RADIUS, (normalmente un servidor de acceso) envía las credenciales de usuario y la información de los parámetros de conexión en forma de mensaje RADIUS al servidor RADIUS.

El servidor RADIUS comprueba las credenciales del cliente, indicando mediante un mensaje de respuesta si se autoriza o no la petición del cliente RADIUS. El cliente RADIUS también puede enviar al servidor RADIUS mensajes de contabilidad (Accounting).

Adicionalmente, el estándar RADIUS soporta el uso de servidores proxy RADIUS.

Un proxy RADIUS es un equipo que remite mensajes RADIUS entre clientes RADIUS, servidores RADIUS u otros proxies RADIUS.

Los mensajes RADIUS nunca se envían entre el cliente de acceso y el servidor de acceso.

Los mensajes RADIUS son enviados como mensajes UDP. El puerto UDP 1812 se usa normalmente para los mensajes RADIUS de autenticación y el puerto UDP 1813 para los mensajes RADIUS de contabilidad. Algunos servidores de acceso emplean el puerto UDP 1645 para los mensajes RADIUS de autenticación y el puerto 1646 para los mensajes RADIUS de contabilidad.

Los tipos de mensajes RADIUS son: Access- Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request y Accounting-Response.

Si os interesa ver los servidores radius con más detalle podéis descargaros open radius o free radius y seguir las wikis para su configuración:

http://sites.eadvies.nl/openradius/
http://freeradius.org/

EAP-TTLS, PEAP, EAP-FAS

EAP-TTLS Protocolo desarrollado por Funk Software y Certicom.

Ofrece ciertas ventajas frente otros protocolos de autentificación, por ejemplo, nos ahorra infraestructura frente a EAP-TLS, mucho más sencillo de gestionar al utilizar únicamente certificados de servidor. Ofrece una autentificación mutua fuerte y además permite autenticarse de manera fácil al cliente mediante usuario y contraseña, sin existir peligro de un ataque por diccionario. Corrige las vulnerabilidades y debilidades de EAP-TLS. Por estas razones es una de las mejores opciones para implementarlo en empresas, universidades, Administraciones públicas. Además es compatible con un gran número de bases de almacenamiento de contraseñas como Windows Active Directory, SQL, LDAP.

Es similar a EAP-TLS, con la diferencia de que únicamente se autentifica con certificado el servidor (se establece un túnel TLS mediante el certificado del servidor, se envía la autentificación del cliente, sin utilizar EAP, utilizando otro tipo de autentificación compatible como PAP, CHAP, MSCHAP, MSCHAPv2, Kerberos por lo que se elimina el PKI y el certificado del cliente)

Proceso de autentificación:

1. Los intercambios son similares a EAP-TLS. El cliente autentica el servidor a través de un certificado.
2. el cliente no necesita presentar un certificado, la clave utilizada para cifrar el período de sesiones se puede crear directamente. Al final de esta etapa, el TLS handshake está completo, los intercambios siguientes serán cifrados por la clave de sesión, el establecimiento de un túnel TLS permite cifrar los intercambios, proporcionando así la identificación del cliente (nombre de usuario y contraseña) al servidor utilizando, por ejemplo MS-CHAPv2.
3. Después el proceso continúa igual que en EAP-TLS

VULNERABILIDADES EAP-TTLS:

Las posibles vulnerabilidades vendrían por parte del sistema de autentificación elegido, por ejemplo las debilidades contenidas en MSCHAP v1 y v2 que son vulnerables a ataques de diccionario y existen herramientas que realizan este proceso muy rápidamente o la vunerabilidad MS09-071

PEAP (PROTECTED EAP)

Protocolo creado conjuntamente por Microsoft, Cisco y la RSA Security. Su principal característica es la protección de los mecanismos más débiles utilizados por EAP mediante un túnel TLS. Es un protocolo recomendable ya que cumple perfectamente con su función. Es muy parecido a EAP-TTLS:

- Utiliza TLS para crear un túnel seguro, el servidor requiere de certificados mientras que el cliente no ya que este se autentifica mediante contraseñas.
- Se realiza un proceso de autentificación mutua entre servidor y cliente.
- Se realizan intercambios de claves dinámicas.

PEAP corrige las debilidades contenidas en EAP-TLS :

- Primeramente se crea túnel TLS, protegiendo así los mensajes EAP-Identity, EAP-Success y EAP-Reject de ataques tipo sniffing o snooping.
- Después se realiza la autentificación a través del túnel creado, la autentificación se realiza únicamente con mensajes EAP y es aquí donde reside la principal diferencia entre EAP-TTLS y PEAP ya que EAP-TTLS utiliza el túnel para ejecutar métodos de autentificación no implementados en el EAP.

EAP-FAST (Flexible Authentication via Secure Tunneling)

Protocolo creado por CISCO para sustituir LEAP por su inseguridad. Se encuentra definido en el RFC 4851
Utiliza túneles para proteger el tráfico aunque a diferencia de PEAP y EAP-TTLS no requiere de certificados digitales para la autentificación, aunque de forma opcional se pueden implantar.

Cisco quiso inventar un protocolo que proporcionase la sencillez de LEAP y la seguridad de PEAP, para ello debía de trabajar con túneles seguros pero eliminando la necesidad de certificados digitales.

¿Cómo trabaja EAP-FAST?

EAP-FAST utiliza PAC (credencial de acceso protegido) para autentificar al cliente y al servidor a la hora de establecer el túnel seguro, permitiendo la autentificación mutua. El proceso se podría dividir en dos fases, comportándose de forma similar a como lo hace PEAP

1- se establece un túnel seguro.

Ana González (Kao)

2- se inicia una PAC (credencial de acceso protegido) mediante una sesión MS-CHAPv2 para verificar la autentificación del cliente al servidor.

Como ya hemos dicho anteriormente MS-CHAPv2 es vulnerable contra ataques de diccionario, para solventar esto los túneles cifrados establecidos durante la Fase 1 proporcionan un entorno seguro para la sesión MS-CHAPv2. En la fase 2 EAP-FAST utiliza PAC (Credencial de acceso protegido) que es un secreto compartido para configurar el túnel, de igual forma que PEAP utiliza el certificado digital del servidor para establecer el túnel TLS. Una credencial única para cada usuario generada a partir de una clave maestra por parte del servidor.

Vulnerabilidades

Hay que destacar que Cisco no cumplió con su objetivo al 100% ya que si el administrador se decanta por sencillez deja de ser tan seguro como PEAP y se prefiere seguridad dejará de ser tan sencillo.

Para que fuese tan sencillo como LEAP, Cisco tuvo que recurrir a que la autentificación del servidor fuese del tipo “Diffie-Helliman”, que consiste en el establecimiento de las claves entre las partes que no han tenido contacto previo, utilizando un canal inseguro y que esto sea de forma anónima. Esto significa que no se puede verificar quién está en el otro extremo. Por lo tanto, es susceptible a que un atacante realizando un MITM se haga pasar por el punto de acceso y por el servidor de autentificación y esperar a que un usuario se conecte a él y envié el nombre de usuario en claro y las contraseñas con el algoritmo hash, capturando la sesión MS-CHAP para luego reventarlo con ASLEAP. EAP-FAST utiliza calves simétricas en vez de la asimétricas utilizadas por EAP-TLS, EAP-TTLS, PEAP

Conclusión
Si bien es un protocolo más seguro que su antecesor LEAP no lo es tanto como lo son EAP-TLS, EAP-TTLS, PEAP

OTROS MÉTODOS DE AUTENTIFICACIÓN EAP

EAP-POTP (Protocol One Time Password):
RFC 4793 Se basa en OTP (autentificación de contraseñas de un solo uso) bien usando un hardware o mediante software.

Ana González (Kao)

EAP-GTC (Generic Tolken Card)

RFC 2284 Se basa en el uso de tarjetas token, es comúnmente utilizado para complementar otros protocolos de autentificación especialmente en EAP-TLS/TTLS/PEAP.
Es similar a EAP-POTP

EAP SIM (Subscriber Identity Module)

RFC 4186 Utilizado comúnmente para telecomunicaciones haciendo uso de la tarjeta SIM GSM para realizar la autentificación, realizándose mediante el método desafió/respuesta sin autentificación mutua

EAP-AKA (Authentication and Key Agreement)

RFC 4187 Utilizado comúnmente para los dispositivos de comunicaciones de tercera generación. La autentificación se realiza a través del UMTS (Sistema Móvil Universal de Telecomunicaciones) y el SUSIM (Modulo de Identidad del Suscriptor)

4. Sistemas Biométricos

¿Qué es la biometría?

El concepto de «biometría» se deriva de las palabras griegas bios (de vida) y metron (de medida). Este concepto no se puso en práctica hasta finales del siglo XIX, si bien se sabe que al menos desde el siglo XIV los comerciantes chinos estampaban las impresiones y huellas de la palma de la mano de los niños en papel con tinta para distinguirles.

El concepto clásico de biometría denota la aplicación de técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas. Dentro del contexto tecnológico, la biometría expresa la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características físicas o de comportamiento de las personas con el objetivo de establecer una identidad.

Durante la última década, investigadores del campo de la ciencia cognitiva han perseguido crear sistemas dotados de las habilidades humanas. Quizás la más admirada y estudiada de todas sea la visión, una tarea que resulta extremadamente fácil para nosotros. De hecho, se lleva a cabo de forma automática, y esconde un proceso realmente complejo, que aún hoy no se conoce por completo.

Ana González (Kao)

Un sistema biométrico es todo aquel que realiza labores de biometría de manera automática. En otras palabras, se trata de sistemas basados en medir y analizar las características físicas y del comportamiento humano con propósito de autentificación. En la actualidad, los métodos más aceptados de identificación se basan en la colección de rastros dactilares y, últimamente, en las muestras de ácido desoxirribonucleico (ADN), cuyos grados de confiabilidad resultan casi infalibles.

La mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. Aunque, se comienza a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo, el calor facial, la voz, la mano o la firma.
Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser, posiblemente, el mejor método de identificación humana.

Existen una serie de requisitos para que se pueda definir un sistema como sistema biométrico. Estos requisitos dependen de las características que se utilizan como parámetro de identificación y clasificación. Para poder decir que una característica es biométrica, ésta debería cumplir las siguientes condiciones:

- Universalidad: todos los individuos deben tener la característica.
- Unicidad: dos personas no pueden ser la misma en términos de la característica.
- Permanencia: la característica debe ser invariante con el tiempo.
- Cuantificable: la característica puede ser medida cualitativamente.

En la práctica hay otros requerimientos importantes:

- Realización: referido a si es posible la identificación exacta, los recursos requeridos y los factores del entorno y de trabajo que afectan a la identificación.
- Aceptabilidad: referido a la extensión de población que estaría predispuesta a aceptar el sistema de identificación.
- Engañable: referido a cómo de fácil sería engañar al sistema con técnicas fraudulentas.

¿Por qué usar la biometría?

Ana González (Kao)

Son claras las ventajas que se obtienen al utilizar sistemas biométricos: Es fácil de usar. La utilización de sistemas biométricos libera al usuario del uso de elementos externos auxiliares. De forma resumida:

- *el usuario no tiene nada que recordar,*
- *nada que cambiar,*
- *y nada que perder.*

Proporciona un nivel más alto de seguridad ya que los parámetros utilizados son unívoca "firma" de una característica humana que no puede ser fácilmente adivinada o descifrada.

La biométrica explota el hecho de que ciertas características biológicas son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto las hace más confiables, amigables y seguras que las contraseñas.

Por razones de automatización. En el pasado el procesamiento de biométrico era hecho manualmente por gente que física y mentalmente comparaba huellas dactilares contra tarjetas, rostros contra fotos de pasaportes y voces contra cintas grabadas nada que recordar.

Hoy en día, dispositivos tales como escáneres, videocámaras, y micrófonos pueden, electrónicamente, capturar y entregar estas mismas características biométricas para automatizar procesos y comparaciones.

Cada tecnología biométrica (huella dactilar, rostro, voz, etc.) tiene sus propias características, variedades y certezas.

Los niveles de precisión biométricos pueden variar pero son siempre más confiables que el 100% de falsas aceptaciones experimentadas con las contraseñas prestadas o robadas.

Importancia de la identificación personal. El problema de resolver la identidad de una persona se puede clasificar fundamentalmente en dos tipos distintos de planteamientos: reconocimiento (más popularmente conocido como identificación) y verificación.

El reconocimiento se centra en determinar la identidad del sujeto dentro de un conjunto ya conocido de identidades. La verificación se encamina a confirmar o denegar la identidad aducida por una persona. En muchas situaciones de nuestra vida cotidiana nos vemos requeridos a probar nuestra identidad, como por ejemplo cuando realizamos una compra con una tarjeta de crédito.

Ana González (Kao)

Una verificación certera de la identidad de una persona podría disuadir la delincuencia y el fraude, dinamizar las transacciones comerciales y salvaguardar los recursos críticos.

¿Cómo funcionan los dispositivos biométricos?

La mayoría de los sistemas biométricos funcionan con arreglo a un modelo general que consiste en dos pasos. El primer paso es el registro de la persona en el sistema. Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia.

De acuerdo con la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona.

En el caso de verificación, la persona le informa al sistema cuál es su identidad, ya sea presentando una tarjeta de identificación o introduciendo alguna clave especial. Se captura el rasgo biométrico y se compara con el modelo de referencia de la persona. Si ambos modelos parean, la verificación se realizó con éxito, si no es fallida.

En caso de que sea identificación, la persona no le informa al sistema biométrico cuál es su identidad. El sistema tan sólo captura el rasgo biométrico y lo compara con un conjunto de modelos de referencia para determinar la identidad de la persona.

Existe una gran variedad de tecnologías biométricas, tantas como características biométricas. Muchas de ellas se están aplicando en la vida real y otras están en proceso de estudio. Algunas características biométricas que se utilizan actualmente son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma de la mano, forma de la oreja, forma de andar, forma de escribir en un teclado, firma, ADN y olor. Partiendo de estas características se han desarrollado dispositivos que han tenido mayor o menor éxito en el mercado. En la actualidad, los sistemas comerciales más usados son:

Sistema	*Descripción*
Reconocimiento facial	Estos sistemas extraen los rasgos faciales de los usuarios para su identificación. La fuente para realizar la identificación puede ser tanto imágenes fotográficas como de vídeo. La identificación se puede hacer en

Ana González (Kao)

	2D, 3D o una combinación de ambas. El objetivo de un sistema de reconocimiento facial es, generalmente, el siguiente: dada una imagen de una cara «desconocida», o imagen de test, encontrar una imagen de la misma cara en un conjunto de imágenes «conocidas», o imágenes de entrenamiento. La gran dificultad añadida es la de conseguir que este proceso se pueda realizar en tiempo real.
Lector de impresión digital	Esta tecnología se basa en identificar al individuo por medio de su huella dactilar. Aunque puede utilizarse cualquier dedo de la mano, por una cuestión de dimensión y comodidad, los dedos más utilizados son el índice y el corazón. Su funcionamiento se basa en tomar una imagen de la huella y por medio de algoritmos reducir dicha imagen a una representación matemática de la huella ("plantilla") y compa. Esta plantilla patrón se acumula en la memoria interna del equipo (junto con un número de identificación o PIN si se trata de un verificador, a fin de tener asociada la huella al individuo). Luego, cada vez que la persona necesite identificarse, ya sea para registrar su horario de ingreso o regreso al trabajo o activar una puerta o barrera, debe digitar su PIN (en el caso que sea un verificador) y a continuación colocar su dedo (el mismo que registró originalmente) en el lector.
Reconocimiento de manos	El reconocimiento de la mano se puede hacer en dos y tres dimensiones. Los sistemas de dos dimensiones buscan en la palma de la mano patrones en las líneas, estos patrones son casi tan distintivos como las huellas digitales. El sistema toma entonces las características de la palma, los compara contra el modelo de referencia (reference template), y procede en consecuencia. Los lectores de tres dimensiones, sin embargo funcionan de forma distinta. Estos miden las dimensiones de la mano (largo de los dedos, altura de la mano, etc.). Aunque no es la más segura de las técnicas biométricas, el uso de la palma de la mano como medida de autenticación ha resultado ser una solución ideal para aplicaciones de seguridad media y donde la conveniencia es considerada una opción mucho más importante que la seguridad o la precisión.
Sistema de autentificación biométrica de las venas.	Es sistema que captura la distribución de las venas de la palma de la mano o de los dedos. Esta siendo muy utilizado en la actualidad debido a su fácil implementación y gran aceptabilidad por parte de los usuarios ya que muchos de ellos no requieren de contacto físico.
Sistema de identificación mediante el iris.	La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado, usando una cámara de alta resolución. Generalmente esto se hace mirando a través de la lente de una cámara

Ana González (Kao)

	fija, la persona simplemente se coloca frente a la cámara y el sistema automáticamente localiza los ojos, los enfoca y captura la imagen del iris, ésta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos suficiente para los propósitos de autenticación. El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal, una estructura única por individuo que forma un sistema muy complejo (de hasta 266 grados de libertad) e inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.
Sistema de reconocimiento mediante de la vasculatura retinal.	La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, tan distinto como una impresión digital y aparentemente más fácil de ser leído, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura. En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter-ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento sé escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.
Sistema de reconocimiento de firmas.	La firma es un método de verificación de identidad de uso común. Diariamente las personas utilizan su firma para validar cheques y documentos importantes. Como la firma es una habilidad adquirida, se le considera un rasgo de comportamiento. Además es muy complejo reproducir la habilidad humana de identificar si una firma es o no auténtica. En biometría, el uso de la firma para verificación de identidad se hace de una manera diferente a la tradicional. Dependiendo del sistema, tanto la superficie donde se firma como el

	bolígrafo utilizado pueden contener varios sensores. Estos sensores miden características mucho más allá que simplemente la forma o apariencia de la firma: la presión que se aplica sobre la superficie, el ángulo al cual se sujeta el bolígrafo y hasta la velocidad y el ritmo de cómo la persona ejecuta su firma son características capturadas por el sistema.
Sistema de Reconocimiento de voz:	La voz es otra característica que las personas utilizan comúnmente para identificar a los demás. Es posible detectar patrones en el espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares. Tan solo basta recordar las veces en que se reconoce a alguien conocido por teléfono para comprender la riqueza de esta característica como método de reconocimiento. Los sistemas de verificación mediante la voz "escuchan" mucho más allá del modo de hablar y el tono de voz. Mediante el análisis de los sonidos que se emiten, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la garganta, también crean modelos de la anatomía de la tráquea, cuerdas vocales y cavidades. Muchos de estos sistemas operan independientemente del idioma o el acento de la persona