UTN-FRBA-Dto.Sistemas
Redes de Información

Unidad 9
Seguridad en Redes

Fuentes: Stallings, cap. 21 y otras

Versión: 3

1

1-Requisitos de la seguridad

- **Confidencialidad**: garantiza que la información es accesible sólo a aquellas personas autorizadas
- **Integridad**: garantiza la exactitud y totalidad de la información y los métodos de procesamiento y transmisión
- **Disponibilidad**: garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados cuando lo requieran
- **Autenticación:** garantiza que los datos fueron generados por el usuario correcto

2

Tipos de amenazas

- A la confidencialidad
  - Acceder, revelar
  - Observar o monitorear
  - Copiar, robar
- A la integridad
  - Ingresar, usar o producir datos falsos
  - Modificar, reemplazar o reordenar
  - Generar representaciones falsas
  - Repudiar (rechazar como falso)
  - Usar indebidamente o impedir el uso
- A la disponibilidad
  - Destruir, dañar o contaminar
  - Denegar, prolongar o demorar el uso o el acceso

3

Incidente

- Un incidente de seguridad es un evento adverso que puede afectar a un sistema o red de computadoras.
- Puede ser causado por una falla en algún mecanismo de seguridad, un intento o amenaza (concretada o no) de romper mecanismos de seguridad, etc.

4

Ataques pasivos

- Escuchan el contenido de las transmisiones para obtener información
- Se hace análisis de tráfico aunque esté encriptado
- Es dificil de detectar
- Puede ser prevenido

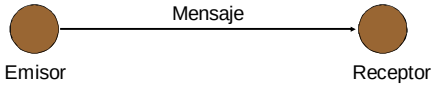
5

Ataques activos

- Enmascaramiento: simular ser otro
- Modificación de mensajes
- Rechazo de servicio
- Son fáciles de detectar
- Son difíciles de prevenir

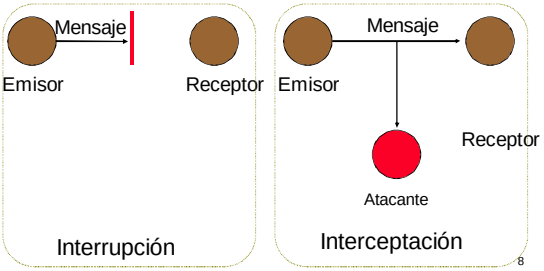
6

Los ataques afectan al proceso básico de la comunicación entre usuario/sistema, cliente/servidor, aplicación/aplicación, host/host.



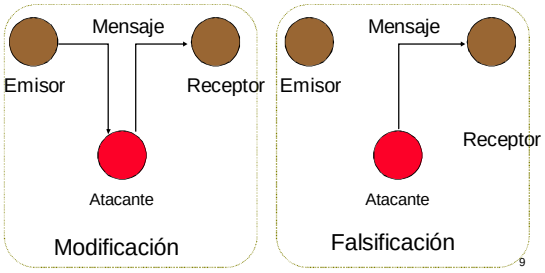
7

Tipos de ataque



8

Tipos de ataques



9

Efectos de los ataques

- La interrupción afecta la **disponibilidad**
  - Por ejemplo, la destrucción de un elemento de hardware, como un disco o una línea.
- La interceptacion afecta la **confidencialidad**
  - Por ejemplo, la interceptacion de una línea o la copia ilícita
- La modificación afecta la **integridad**
  - Por ejemplo, cambiar valores en un archivo de datos o alterar mensajes
- La falsificación afecta la **autenticidad**
  - Por ejemplo, la inserción de mensajes espúreos

10

Código malicioso

- Programa de computadora escrito para producir inconvenientes, destrucción, o violar la política de seguridad.
- Tipos
  - Virus: necesita interacción del usuario
  - Troyanos: doble funcionalidad, conocida y oculta
  - Gusanos: autoreplicación

Ningún antivirus puede detectar todo los programas maliciosos.

11

Ejemplos de cosas que pueden hacer:

- Borrar archivos del disco rígido para que la computadora se vuelva inoperable.
- Infectar una computadora y usarla para atacar a otras.
- Obtener informacion sobre Ud., los sitios web que visita, sus hábitos en la computadora.
- Capturar sus conversaciones activando el microfono
- Ejecutar comandos en la computadora, como si lo hubiera hecho Ud.
- Robar archivos del equipo, por ejemplo aquellos con información personal, financiera, etc.
- Encriptar archivos y pedir recompensa por la clave

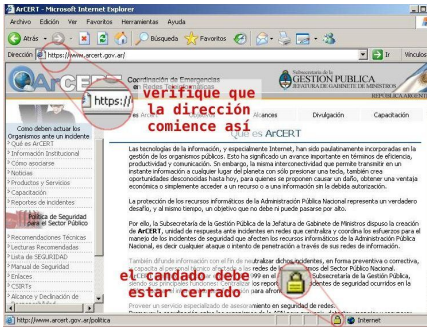
12

2-HTTPS

- Protocolo de red basado en HTTP
- Agrega cifrado de información sensible (usuarios y claves)
- Usa el puerto 443 en TCP
- Descripto en RFC 2818

13

Sitios seguros



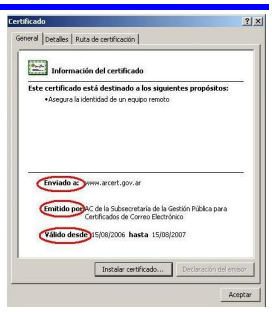
14

Certificado de sitio seguro

Haciendo doble clic sobre el candado, debe mostrarse la información del certificado.

Verifique que:

- El nombre de la entidad coincida con el de la página que usted está visitando
- El certificado se encuentre vigente
- La autoridad emisora sea de su confianza.



15

3-Criptología

- Estudia la codificación de mensajes por medio de algoritmos matemáticos (algebra modular, números primos, etc.) para su trasmisión segura.
- **Criptografía**: Técnica que transforma todo mensaje de claro a ilegible.
- **Criptoanálisis**: Estudio de las técnicas para quebrar mensajes criptográficos.

16

Criptografía

- Generalmente un mecanismo criptográfico utiliza un ***algoritmo*** (función matemática) y un valor secreto conocido como "***Clave***"
- Cuanto más grande es el espacio de claves (rango de posibles valores de la clave) más difícil es obtener la clave por medio de ataques por "*fuerza bruta"*.
- Los ataques por fuerza bruta consisten en aplicar todas las combinaciones posibles hasta encontrar la clave

17

Donde se aplica

No es conveniente aplicar un sistema criptográfico:

- Si el precio para hallar la clave es más caro que el valor de la información.
- Si el tiempo necesario para romperlo es más largo que el tiempo de vida de la información.

18

Longitud de clave	Cantidad de Combinaciones
40	2^{40} = 1.099.511.627.776
56	2^{56} = 7,2057 * 10^{16}
64	2^{64} = 1,8446 * 10^{19}
112	2^{112} = 5,1922 * 10^{33}
128	2^{128} = 3,4028 * 10^{38}

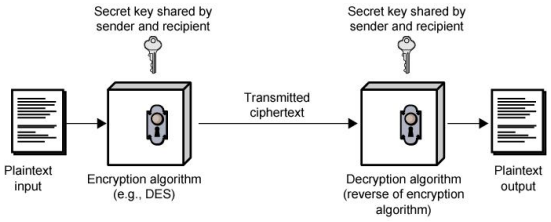
19

Tipos de cifrados

- Simétrico
- Asimétrico
- Hashing

20

Encriptación simétrica



21

Componentes

- Texto plano
- Algoritmo de encriptación
- Una sola clave secreta
- Texto cifrado
- Algoritmo de desencriptación

22

Encriptación asimétrica

- Conocida como encripción de “Encriptación de Clave Pública”
- Los extremos pueden utilizar el mismo algoritmo o uno diferente pero complementario para encriptar y desencriptar la información
- Dos valores de clave diferentes, pero complementarios una clave pública y una clave privada

23

Requisitos para la seguridad

- Fuerte algoritmo de encriptación
- Aunque sea conocido no se puede desencriptar sin la clave
- Las claves secretas se deben distribuir de manera segura
- Conocida la clave toda la comunicación es clara

24

Ataque a la encriptación

- Análisis del encriptado
  - —Requiere conocimientos de la naturaleza del algoritmo y las caracteristicas generales del texto plano
  - —Intenta deducir texto o clave
- Método de “Fuerza Bruta”
  - —Prueba con cada clave posible hasta ver texto claro

25

Algoritmos

- Cifrado en bloque
  - —Procesa el texto plano en bloques de tamaño fijo
  - —Produce bloques de texto crifrado de igual longitud
  - —Algoritmos más usados:
    - DES: Data Encryption Standard
    - TDES: Triple DES
    - AES: Advanced Encryption Standard

26

DES

- Normalizado en Estados Unidos
- Usa bloques de texto plano de 64 bits
- Usa clave de 56 bits
- Fue abierto en 1998 por la *Electronic Frontier Foundation*
  - —Usaron una máquina especial por 3 días
  - —DES ahora no tiene valor

27

TDES (o 3DES)

- Cumple la norma ANSI X9.17 (1985)
- Incorporado en norma DEA en 1999
- Usa 3 claves y 3 ejecuciones del algoritmo DEA
- Claves de 112 or 168 bits
- Es lento
- El tamaño del bloque (64 bit) es muy chico

28

AES

- Creado por el *National Institute of Standards and Technology* (NIST) en 1997
- Normalizado como Federal Information Processing Standard (FIPS 197) en 2001
- Es más seguro y eficiente que 3DES
- En la evaluación hay que ver la seguridad, eficiencia computacional, requisitos de memoria, adaptación al hardware y software, y la flexibilidad

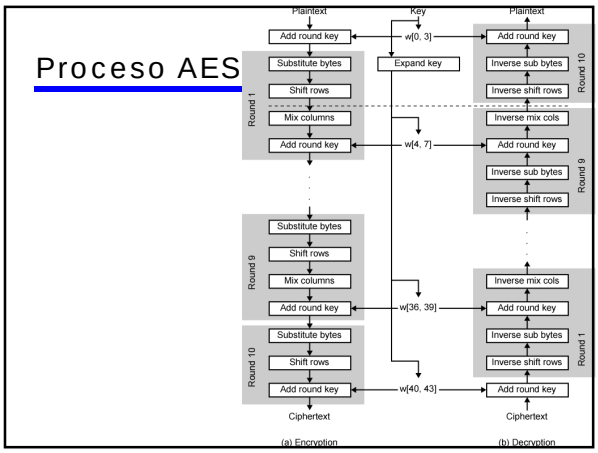
29

Características del AES

- Se usan claves de 128 bits
- La entrada es un bloque simple de 128 bits
  - — Presenta una matriz cuadrada
  - — El bloque se copia en una matriz de estado que se modifica a cada paso
  - — Al terminar la matriz de estado se copia a la matriz de salida
- Las claves se presentan como una matriz cuadrada
  - — Hay 44 palabras de claves de 128-bits
- Bytes ordenados por columna
  - — Primeros 4 bytes de entrada de 128-bit de texto plano ocupan la primera columna de la matriz

30

Proceso AES

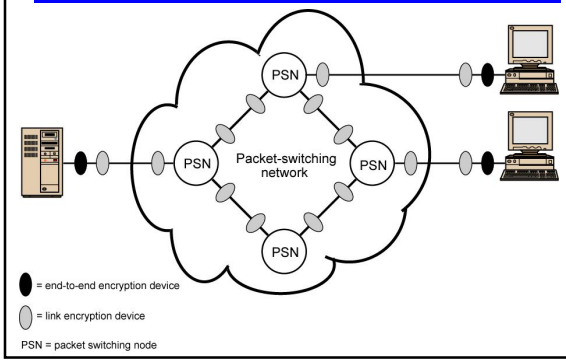


Comentarios sobre AES

- Hay una matriz de claves de 44 palabras de 32 bits
  - En cada vuelta se usan 4 palabras (128 bits)
- Hay cuatro etapas, una permutacion y 3 substituciones
  - Substituye bytes por bloques usando una tabla
  - Permuta filas
  - Mezcla columnas
  - Suma una clave a los bloques
- Es una estructura simple
  - La misma para la encriptación y desencriptación
  - Comienza sumando claves
  - Luego nueve rondas de cuatro etapas
  - Finaliza con una ronda de tres etapas

32

Dispositivos de encriptación



Encriptación de enlaces

- Se hace en cada extremo del enlace
- Todo el tráfico con alto nivel de seguridad
- Requiere muchos dispositivos de encriptación
- Los mensajes deben ser desencriptados en cada switch para leer dirección (circuito virtual)
- La seguridad es vulnerable en los switches
  - Especialmente en redes públicas

34

- Los datos encriptados cruzan la red sin cambios
- Destinos y fuentes comparten la clave
- Sólo se encriptan datos de usuario para que los switches lean encabezamiento y rutas
- El tráfico no es seguro

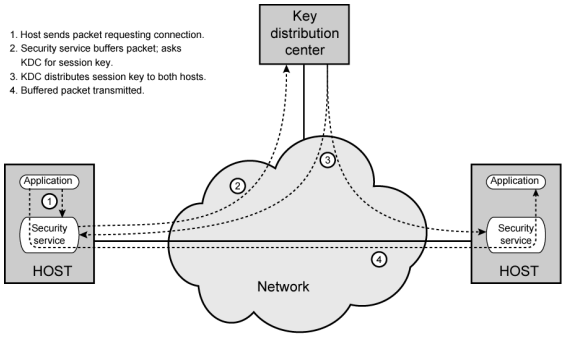
35

Modos de distribución de claves

- Clave seleccionada por A y entregada a B
- Un tercero selecciona clave y la distribuye a ambos
- Usar clave vieja para encriptar y transmitir la nueva de A a B
- Usar clave vieja para transmitir la nueva a ambos

36

Distribución automática



Elementos

- Clave de sesión
  - Usada durante una conexión lógica
  - Se destruye al fin de la sesión
  - Usada para los datos de usuario
- Clave permanente
  - Usada para la distribución de claves
- Centro de distribución de claves
  - Determina cuál sistema puede communicarse
  - Provee una clave de sesión para esa conexión
- Módulo de Servicio de Seguridad (SSM)
  - Realiza encriptación entre extremos
  - Obtiene claves para los host

38

Relleno (padding) de tráfico

- Produce texto cifrado continuamente
- Si no hay texto para codificar, envía datos aleatorios
- Hace imposible el análisis de tráfico

39

Autenticación de mensajes

- Protección contra ataques activos
  - Falsificación de datos
  - Escucha de información
- El mensage es auténtico si es genuino y proviene de una fuente confiable
- Autenticación permite al receptor verificar que el mensaje es auténtico
  - No ha sido alterado
  - Provene de una fuente segura
  - Timeline

40

Autenticación encriptada

- Supone que sólo el trasmisor y el receptor conocen la clave
- Mensaje incluye:
  - Código de detección de error
  - Número de secuencia
  - Estampa de tiempo

41

Autenticación sin encriptación

- Se genera una marca de autenticación y se agrega a cada mensaje
- El mensaje no se encripta
- Es útil para los siguientes casos:
  - Mensajes a destinos múltiples
  - Aliviar la carga de procesamiento (autentica al azar)
  - Programas que se ejecutan sin decodificar

42

Código de autenticación de mensajes

- Se genera a partir de claves compartidas por ambos extremos
- Si solamente el trasmisor y el receptor conocen la clave, y el código coincide, entonces:
  - —El receptor asegura que el mensaje no fue alterado
  - —El receptor asegura que el mensaje proviene del trasmisor correcto
  - —Si el mensaje tiene número de secuencia, el receptor asegura la secuencia correcta

43

Funciones de Hash

Una función de Hash toma una entrada de longitud arbitraria y genera una salida de longitud fija

La salida, de longitud fija, se llama “Digest”

Un algoritmo para ser considerado como una función de Hash, debe cumplir determinados requisitos:

- ***Consistencia***: la misma entrada debe generar siempre la misma salida
- ***Aleatoriedad***: Que impida adivinar el mensaje original
- ***Unicidad***: Debe ser prácticamente imposible encontrar dos mensajes diferentes que generen el mismo Digest
- ***One way***: Para un Digest dado, debe ser muy difícil, sino imposible acertar el mensaje de entrada

44

- Las funciones de Hash garantizan la integridad del mensaje
- Las funciones de Hash más comunes con:
  - o Message Digest 4 (MD4)
  - o Message Digest 5 (MD5)
  - o Secure Hash Algorithm (SHA)

MD5 procesa su entrada en bloques de 512 bits y genera un Digest de 128 bits.

SHA tambien procesa la entrada de a 512 bits y produce un Digest de 160 bits (requiere de mayor poder de procesamiento y corre más lento)

45

Envío de las claves

- Se cifra mediante cifrado simétrico.
- Se envían las claves de cifrado mediante cifrado asimétrico.

Cifrado Simétrico	Cifrado Asimétrico
Confidencialidad	Confidencialidad
Cierto grado de autenticación	Autenticidad
Sin firma digital	Firma digital
Alta velocidad	Baja velocidad

46

Función de Hash unidireccional

- Acepta mensajes de longitud variable y produce tags de longitud fiia (digesto)
- Ofrece autenticación sin las desventajas de la encriptación:
  - —Encriptación es lenta
  - —Encriptación usa hardware caro
  - —El hardware está optimizado para grandes cantidades de datos
  - —Los algoritmos está protegidos por patentes
  - —Los algoritmos están sujetos al control de exportación de Estados Unidos

47

Funciones de Hash seguras

- Propiedades:
  - —Se puede aplicar a cualquier tamaño de datos
  - —Produce salidas de longitud fija
  - —Fácil de procesar
  - —No es posible reversar
  - —No es posible hallar dos mensajes con la misma hash

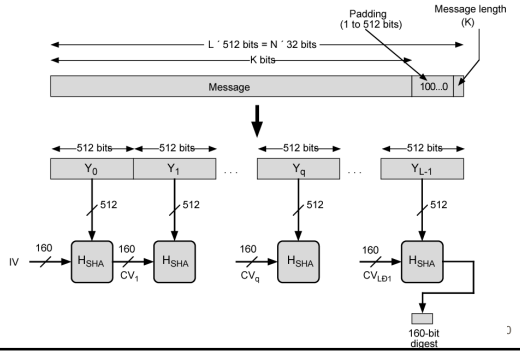
48

SHA-1

- *Secure Hash Algorithm 1*
- Mensaje de entrada de menos de 2^{64} bits
- Procesados en bloques de 512 bits
- La salida es un digesto de 160 bits

49

Generación de digesto con SHA-1

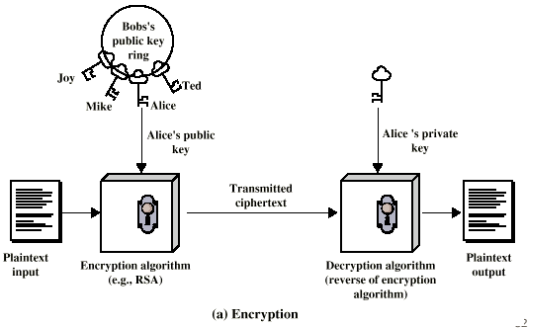


Encriptación de claves públicas

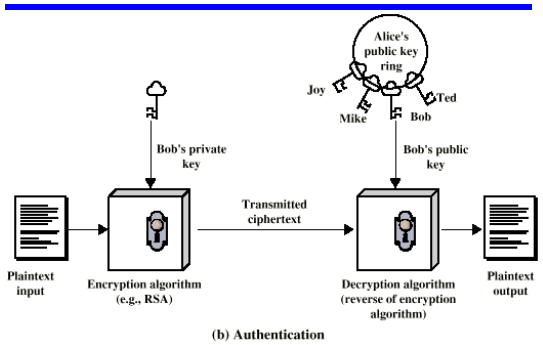
- Basada en algoritmos matemáticos
- Es asimétrica: usa dos claves separadas
- Ingredientes
  - —Texto plano
  - —Algoritmo de encriptación
  - —Claves pública y privada
  - —Texto cifrado
  - —Algoritmo de desencriptación

51

Proceso de encriptación



Proceso de autenticación



Operación

- Una clave que se hace pública se usa para encriptar
- Otra clave que se mantiene privada se usa para desencriptar
- Es imposible determinar la clave de desencriptación aplicando un algoritmo a la clave de encriptación

54

Pasos

- El usuario genera pares de claves
- El usuario publica una clave
- Para enviar un mensaje al usuario, se debe encriptar usando la clave pública
- El usuario desencripta usando la clave privada

55

4-Firma digital

- El trasmisor encripta el mensaje con su clave privada
- El receptor puede desencriptar usando clave pública conocida
- Sirve para autenticar al trasmisor, quien es el único que tiene la clave correcta
- No da privacidad a los datos porque la clave es pública
- Garantiza la integridad del documento

56

Algoritmo RSA

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

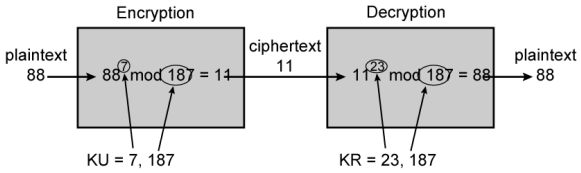
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

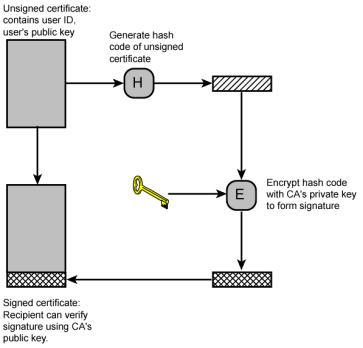
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Ejemplo RSA



58

Certificado digital



59

Firma digital y certificado digital

- Firmar un documento es añadirle un bloque que permite, con una clave pública que corresponde a la firma, verificar que nadie ha modificado el documento.
- Un certificado es una clave pública firmada por una autoridad en la que confiamos, y se usar para verificar firmas digitales.

60

Algoritmos simétricos

- Inconvenientes:
  - Cómo garantizar el intercambio seguro de claves sin disponer de un canal seguro?
  - Además, el manejo de claves es complejo (*n* usuarios = *n* x (*n*-1) / 2 claves)
  - Los mensajes no son irrepudiables.
  - Es necesario ponderar claramente los riesgos antes de implementar.

61

Algoritmos asimétricos

- Se basan en funciones "de una vía con puerta trampa".
- El esfuerzo requerido para quebrarlos equivale a la dificultad de calcular la función inversa.
  - Quebrar una clave con módulo de 512 bits, equivale a factorizar un número de 155 dígitos decimales
  - Implica contar con una potencia de procesamiento mayor a 90,000 MIPS/año.

62

Algoritmos asimétricos

- RSA (Rivest, Shamir, Adleman), basado en el pequeño teorema de Fermat y la generalización de Euler. Implica factorización.
- El Gamal, DSS (Digital Signature Standard). Implica hallar logaritmo discreto módulo *p*.
- Fiat-Shamir, Pohlig-Hellman, Rabin, Ong-Schnorr-Shamir, ...
- De todos, RSA es el más utilizado y ampliamente implementado.

63

Algoritmos asimétricos

- Ventajas:
  - Muy fuertes, dadas las implementaciones correctas.
  - Proporcionan servicios de confidencialidad, integridad, autenticidad (sin restricciones)
  - Los mensajes con firma digital son irrepudiables
  - El manejo de claves es más sencillo (*n* usuarios = *n* pares púbilca/privada) y no requiere un canal seguro para comunicar la clave pública.

64

Inconvenientes de algoritmos asimétricos

- Inconvenientes:
  - Son más lentos en términos de ejecución
  - Son más difíciles de implementar.
  - Es necesario ponderar los riesgos antes de implementar.
- Los esquemas híbridos (simétricos + asimétricos) procuran conseguir "lo mejor de ambos mundos"
- Deseamos preservar todos los atributos, y hacerlo del modo más eficiente

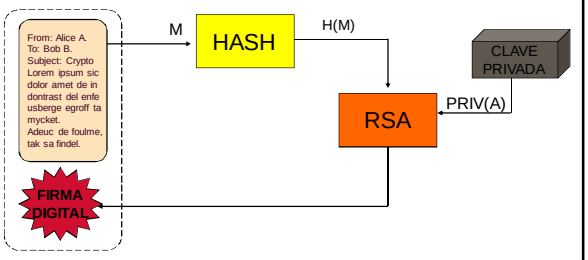
65

Procesamiento de mensajes

- Incluyen la firma para dar autenticidad y codificación adicional para dar integridad.
- Utilizan funciones de Hash y generación de números seudoaleatorios criptográficamente seguros (CSPRNG)

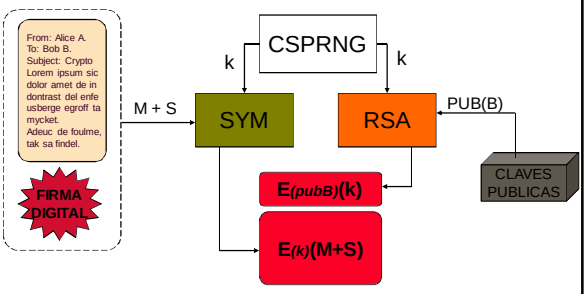
66

Agregado de firma a un mensaje



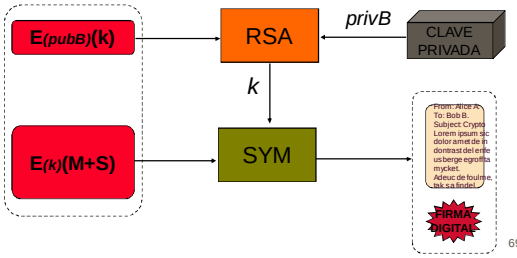
67

Ensobrado adicional



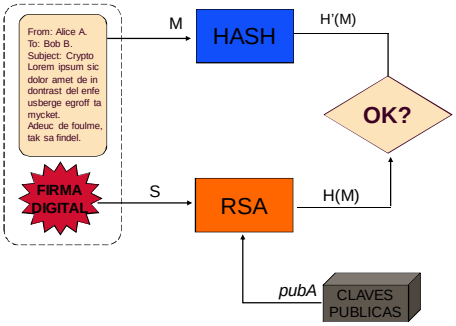
68

Apertura al recibirlo



69

Verificación de la firma

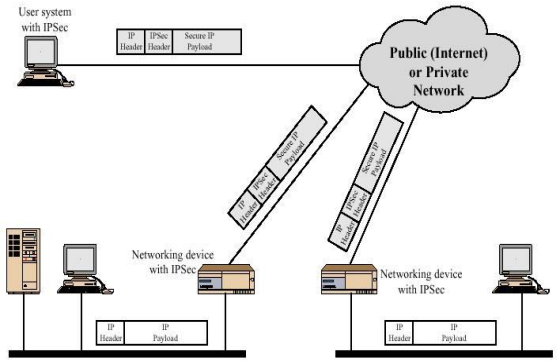


70

5-Seguridad en capa 3

- Se hace por protocolo IPSec
- Permite conexión segura por Internet de una casa central y sus sucursales
- Permite acceso remoto seguro
- Cubre conectividad extranet e intranet
- Mejora la seguridad para el comercio electrónico

71



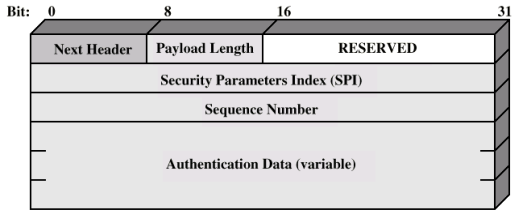
- IPSEc (*IP Security Protocol*)
  - Serie de protocolos desarrollados por el IETF
  - Opera con IP versiones 4 y 6
  - Define un marco pero no especifica los algoritmos
- Tres protocolos básicos
  - IKE *(Internal Key Exchange)*
  - AH *(Authentication Header)*
  - ESP *(Encapsulating Security Patload)*

73

- AH (*IPSEc Authentication Header*)
  - Agregado después del encabezamiento IP
  - No es un campo opcional del IP
  - En el encabezamiento IP se cambia el campo "Protocol"
  - Usa el formato IP versión 6
  - No se envía toda la información de seguridad, sólo pequeños índices preasignados a los parámetros
- ESP (*IPSec Encapsulation Security Payload*)
  - Encripta el contenido de los paquetes
  - Agrega un encabezamiento de 8 octetos y una cola con autenticación

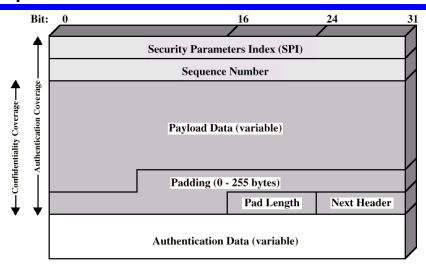
74

Authentication Header



75

Paquete ESP



76

- Seguridad perimetral: en la conexión a Internet se insertan firewalls con políticas coordinadas centralmente
- Firewall:
  - Es un filtro de paquetes que corre en un router
  - Bloquean información según la dirección IP, el protocolo o el port
- Proxy Access: permite el acceso de determinados clientes a determinados servicios y detecta virus
- Stateful firewal:
  - registra pedidos salientes para permitir el ingreso de respuestas entrantes
  - Trabaja bien con TCP pero no con UDP
- Application Proxy: detecta virus en forma integral, ya que firewall sólo ve los datagramas

77

Firewall

- Elemento de hardware o software
- Controla las comunicaciones en base a políticas
- Se ubica en el punto de conexión de la red interna e Internet
- Se pueden conectar a una tercer red (zona desmilitarizada o DMZ) con los servidores
- Operan en distintas capas
- Normalizado en RFC 2979

78

SA

- Security Association
- Relación unidireccional entre trasmisor y receptor
- Para que sea bidireccional hay que hacer dos SA
- Hay 3 parámetros para identificar SA
  - —Indice de seguridad
  - —Dirección IP de destino
  - —Identificador de protocolo de seguridad

79

Parámetros SA

- Contador de número de secuencia
- Contador de desborde de secuencia
- Ventana contra respuesta
- Información AH
- Información ESP
- Tiempo de vida de la asociación
- Modo de protocolo IPSec
  - —Tunel, transporte o wildcard
- MTU de la ruta

80

6-Seguridad en capa 4

- SSL: *Secure Sockets Layer*
- TLS: Capa de Seguridad en el Transporte (está definida en la RFC 2246)
- SSL es un servicio de propósitos generales
- Es una serie de protocolos sobre TCP
- Puede presentarse en dos formas:
  - —Parte de un protocolo transparente a la aplicación
  - —Embebida en un paquete (Netscape, MS Explorer)
- Diferencia menores entre SSLv3 and TLS

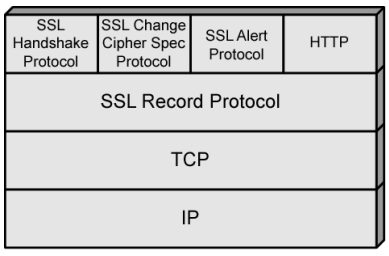
81

Arquitectura SSL

- SSL usa TCP para tener un servicio confiable entre extremos
- SSL comprende dos capas de protocolos
- Protocolo Record: provee servicios básicos a otros protocolos (como HTTP)
- Capa superior
  - —Handshake Protocol
  - —Change Cipher Spec Protocol
  - —Alert Protocol

82

Estructura de protocolos SSL



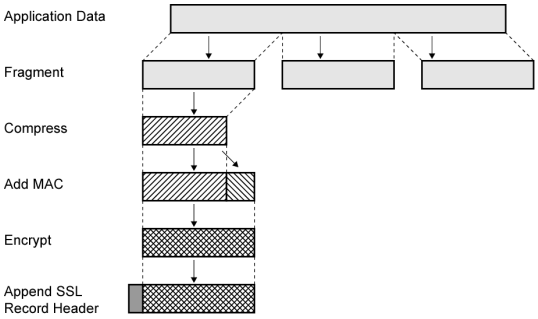
83

Conexión y sesión SSL

- Conexión
  - — Función de Transporte según tipo de servicio
  - — Par a par
  - — Transitorio
  - — Cada conexión asociada con una sesión
- Sesión
  - — Asociación entre cliente y servidor
  - — Creado por Handshake Protocol
  - — Define una serie de parámetros para seguridad criptográfica
  - — Evita negociar parámetros para cada conexión
- Hay múltiples conexiones seguras entre partes
- Podría haber múltiples sesiones seguras entre partes

84

Operación



85

Protocolo Handshake