SEGURIDADES EN REDES

Semestre 2014-B

Ing. Fernando Flores C.

OBJETIVOS

- Conocer los elementos constitutivos de Seguridad en una red de Computadores.
- Estudiar las principales Aplicaciones para la impementación de Seguridades en las redes de datos.

Contenido

- Introducción. Definiciones.
- Tipos de Ataques. Mecanismos de Seguridad.
- Criptografía Clásica y Moderna.
- Cifrado Simétrico y Asimétrico.
- Funciones Hash y Firmas Digitales.
- Infraestructura de Manejo de Clave Pública PKI.

Contenido

- Seguridad a nivel de Aplicaciones
- Protocolos Seguros.
- Estudio de Normas de Seguridad.
- Políticas de Seguridad.

Evaluaciones

- **I Bimestre**
  - Prueba Parcial I (35%)
  - Prueba parcial II (35%)
  - Proyecto 1 (30%)
- **II Bimestre**
  - Prueba Parcial III (35%)
  - Prueba Parcial IV (35%)
  - Proyecto Final (30%)

BIBLIOGRAFÍA

- William Stallings, NETWORK SECURITY ESSENTIALS, Aplications and Standards,4a Edición, Prentice Hall, 2010
- JieWang, COMPUTER NETWORK SECURITY, Theory and Practice, Springer 2009.
- CISCO, NETWORK SECURITY TECHNOLOGIES AND SOLUTIONS, Ciscopress 2008.
- Michael Gregg, BUILD YOUR OWN SECURITY LAB A FIELD GUIDE FOR NETWORK TESTING, Wiley 2008.

Antecedentes

- Antiguamente:
  - Objeto físico
    - Datos guardados → Seguridad de almacén { Cerradura, Guarda, Vigilancia electrónica }
    - Datos enviados → Seguridad de comunicación { Cifrado }
  - Datos transmitidos → Seguridad de emisión { Reducción de emisiones electromagnéticas }
- En la actualidad:
  - Datos en computadoras → Seguridad de computadora
  - Computadoras interconectadas → Seguridad de red

Seguridad de la información

Qué es la Seguridad?

- **No hay definición consensuada**
  - Impedir que ocurran cosas malas o, al menos, hacerlas menos probables [Walker, 2004]
  - Conjunto de estrategias y técnicas para hacer frente a infracciones deliberadas de las propiedades deseadas de un sistema (con usuarios que no se portan bien) [Gollman, 2004]
  - Protección de elementos mediante [Stallings, 2005]:
    - **Prevención**: Tomar medidas para impedir que los elementos sean vistos, dañados o robados
    - **Detección**: Tomar medidas para detectar cuándo, cómo y quién ha dañado un elemento
    - **Reacción**: Tomar medidas para recuperar los elementos o recuperarse del daño

¿Qué vamos a tratar?

- Necesidad de seguridad (ataques)
- Servicios de seguridad
- Mecanismos de seguridad

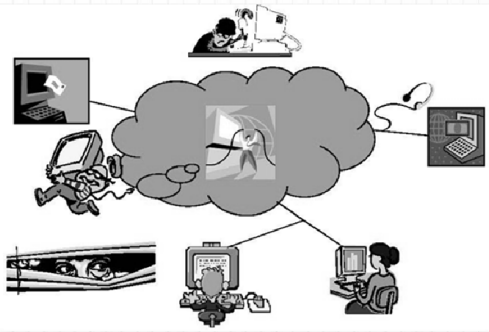
Para datos almacenados en computadoras y transmitidos por redes de computadoras

No veremos cómo delinquir

Necesidad de seguridad

- Pensar en:
  - Posibles situaciones no deseadas a las que enfrentarse
  - Quiénes las pueden provocar

Situaciones no deseadas



Atacantes

- Personas llevadas por desafío intelectual o por aburrimiento (Ex)Empleados vengativos
- Personas (empleados, clientes, delincuentes) que buscan Beneficio económico
- Delincuencia organizada que quiere ocultar actividades ilegales
- Espías de compañías o países rivales con fines económicos, políticos o militares
- Terroristas o naciones que intentan influir en la política de un estado
- Usuario que mete la pata
- Fenómeno de la naturaleza (huracán, terremoto, …) que causa catástrofes
- Y muchos otros …….

Terminología

- **Vulnerabilidad**
  - Debilidad que se puede aprovechar
- **Amenaza**
  - Posibilidad de aprovechar una debilidad
- **Ataque**
  - Realización de una amenaza
- **Riesgo**
  - Medida del costo de una vulnerabilidad (teniendo en cuenta la probabilidad de un ataque exitoso)
- **Seguridad**
  - Identificar vulnerabilidades, proteger frente amenazas reducir impacto de ataques y reflexionar sobre riesgos [Ryan, 2004]

Terminología

- Una amenaza *(threat,* en inglés) es cualquier violación potencial de la seguridad. La información que circula, se procesa y se almacena en una red está sometida a varios tipos de amenazas que pueden ser clasificadas, principalmente, en cuatro grupos:
  - **Destrucción** de la información u otros recursos, quedando estos inutilizados o desaparecida la información en ellos contenida.
  - **Modificación** de la información, produciendo añadidos, sustracciones o permutas entre sus distintas partes.
  - **Robo de información** o publicación indebida de esta de forma que personas diferentes a las legítimamente implicadas tengan conocimiento de ella.
  - **Interrupción del servicio**, consistente en que un determinado usuario deja de tener acceso a un recurso o servicio de la red.

Terminología

Por otra parte, las amenazas pueden ser ***accidentales*** o ***intencionales***.

- Amenazas accidentales son aquellas que aparecen de forma no premeditada: mal funcionamiento en los sistemas, fallos de software, operaciones indebidas por parte de algún usuario inexperto, etc.
- El método para su tratamiento y prevención en el ámbito de las redes debe ser similar a los procedimientos que se siguen en el caso de sistemas informáticos aislados u otros sistemas: revisión peri6dica de equipos, prueba del correcto funcionamiento de los programas informáticos, mantenimiento de las instalaciones, formación adecuada del personal para evitar errores humanos, etc. Deberán ser tomadas en cuenta en un *Análisis de Riesgos* global, pero su incidencia en los protocolos específicos de seguridad es secundaria

Terminología

- Otra cosa son las ***amenazas intencionales*** que presuponen la participación maliciosa de un sujeto o entidad que pretende hacer un uso indebido de la red.
- Una amenaza intencional se denomina un ataque *(attack,* en ingles).
- Los ataques pueden ser clasificados en ***ataques activos*** y ***ataques pasivos***.
- Los primeros son aquellos que alteran el comportamiento normal del recurso o servicio telemático que esta siendo atacado: una información desaparece, o es cambiada, o un sistema envía los datos hacia direcciones no previstas, etc.

Terminología

- Los ataques pasivos, en cambio, no provocan ninguna modificación en el funcionamiento del sistema salvo el uso indebido de sus prestaciones.
- Es decir, si se produce, por ejemplo, un robo de información a causa de un pinchazo en la red, esta seguirá fluyendo de forma normal sin variaciones en su contenido y seguirá siendo utilizada por los usuarios legitimados (además del ladrón, claro esta).
- Desde un punto de vista subjetivo los ataques pasivos ofrecen una imagen más preocupante.
- No obstante, no puede afirmarse a priori que los ataques pasivos sean más peligrosos que los ataques activos.
- Ello dependerá de cada caso concreto y de la naturaleza del valor que sea vulnerado.

Terminología

- Entre los tipos de ataques más significativos que pueden presentarse en los entornos telemáticos, cabe destacar los siguientes:
- **Suplantación de personalidad *(Masquerade)***
  - Se produce cuando una persona o entidad suplanta la personalidad de otra, se enmascara como tal, con fines ilícitos.
  - Alguien se hace pasar por quien no es para realizar una funci6n en la red para la que no esta autorizado.
  - Este es quizás uno de los ataques mas fáciles de imaginar y que con mas frecuencia pretende ser perpetrado.
  - Para facilitar al lector el posterior acceso a documentaci6n en ingles se ha incluido aquí y en las restantes definiciones, junto al nombre en español, la correspondiente versión inglesa del término.
  - Algunos autores traducen *masquerade* por *mascarada,* decisión que aquí no se ha seguido por entender que en español ese termino tiene mas resonancia carnavalesca y índica que de fraude malicioso de suplantación de la verdadera identidad.
  - En la Figura 1 se representa esquemáticamente este ataque reflejando la actuación de un *usuario malicioso* M que interfiere la comunicación entre la usuaria A y el usuario B.

Terminología

- **Divulgación o repetición del contenido *(Replay)***
- Ocurre cuando una entidad repite un mensaje, o parte de el, para dirigirlo a un destinatario no autorizado.
  - Se trata también de un ataque de muy posible aparición, del cual un ejemplo fácil de imaginar puede ser el caso de alguien que accede indebidamente a un nodo de la red y obtiene parte de la información que por allí circula para su provecho o para el de un tercero. El típico «pinchazo» de una línea de comunicación para obtener información de forma fraudulenta es también un ataque de divulgación indebida del contenido.

Terminología

Modificación de mensajes *(Modification)*

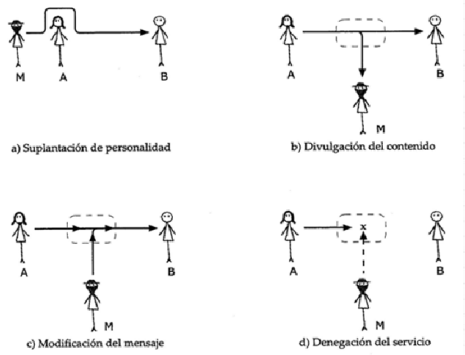
- Consiste en la alteración del contenido de un mensaje (evitando que esta alteración sea detectada) con la finalidad de que su destinatario adopte una decisión o tenga una percepción de la realidad distinta de aquella que se produciría caso de haber recibido el mensaje tal y como fue emitido.
- El término *mensaje* debe ser entendido aquí (y en las sucesivas ocasiones que de aquí en adelante sea usado) en un sentido amplio, considerado como una pieza de información que circula por la red o se encuentra almacenada en uno de sus sistemas.
- La modificación del mensaje puede consistir en la sustracción o adición de partes de un documento, o en la introducción de variaciones en su contenido. Si alguien accede a una base de datos donde está reflejada su nómina y es capaz de modificar su contenido puede regalarse con una subida de sueldo tan sustancial como su prudencia le dicte.

Terminología

Denegación del servicio *(Denial of Service)*

- Se produce cuando se consigue, con fines fraudulentos, que una entidad no cumpla deliberadamente su cometido, o se impide que otras entidades cumplan con las funcionalidades que tienen encomendadas.
- Un ejemplo de competencia ilícita puede consistir en que un atacante, con el fin de evitar que determinado usuario reciba una posible oferta, modifique ciertas tablas de enrutamiento de la red con objeto de conseguir que ese usuario no reciba correo electrónico durante cierto tiempo o no reciba el procedente de un origen concreto, pudiendo producir con ello un grave quebranto económico o una grave distorsión en su normal desempeño.

Tipos de ataques



PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Los cuatro tipos de ataques descritos anteriormente resumen las actuaciones malintencionadas más significativas que pueden presentarse en las redes, frente a las que deberán establecerse, por tanto, las medidas de protección.
- Existen, además, algunos otros términos que hacen referencia a otros tipos de ataques, calificados en cuanto *al modo* de ser llevados a cabo, cuyos efectos o perjuicios puede considerarse que caen dentro de las cuatro categorías antes descritas.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Así, se suele distinguir entre Ataques Externos *(Outsiders Attacks)* y Ataques Internos *(Insiders Attacks)* para discernir si el atacante pertenece o es ajeno a la organización en cuestión.
- Naturalmente, el tema de los *insiders* es particularmente peligroso y difícil de corregir: en todas las organizaciones resulta necesario confiar a determinadas personas la custodia de los recursos.
- Si los propios gestores de la seguridad se corrompen, la cosa se pone difícil.
- Cuando se organicen entornos de seguridad habrá que procurar que una misma persona no ostente demasiadas responsabilidades, y que responsabilidades criticas sean compartidas por mas de una persona.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Se dice que existe una *trapdoor* (llamada en español *trampilla, puerta trasera* o *puerta falsa)* cuando una entidad *o* sistema es alterado para permitir a un atacante concreto un uso no autorizado del recurso.
- Tiene relación con el diseño deliberadamente doloso de determinados sistemas, que funcionando de forma adecuada y protegida para todos los usuarios, permiten, sin embargo, a uno en concreto (perteneciente al entorno del diseñador del producto) «colarse por la trampilla» que fue instalada de forma deliberada e ilícita.
- También recibe este nombre la propiedad que presentan algunos programas por la que consiguen anular las limitaciones que tienen impuestas siguiendo alguna pauta secreta conocida por el propio programador.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Otro tipo posible de ataque es el Caballo de Troya *(Trojan Horse),* denominado así en recuerdo del regalito que Ulises le hizo a los troyanos por aquel asunto de Helena, que tanto dio que hablar.
- Cuando se introduce un Caballo de Troya en un sistema, éste adquiere funcionalidades y privilegios no autorizados, además de ejercer sus funciones legítimas.
- Está también relacionado con vicios de diseño introducidos maliciosamente en el proceso de fabricación de un producto, o con defectos de funcionamiento de los sistemas que permiten que un usuario habilidoso que se haya conectado de forma lícita pueda «prosperar» desde dentro en cuanto a la adquisición de privilegios que excedan a los que, en base a su identidad, el sistema le había concedido inicialmente.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Esto último tiene mucho que ver con las «malas compañías», es decir, con usuarios o sistemas que residen en una misma red u organización y que no cuidan debidamente sus protecciones.
- Alguna gente que quiere atacar redes intenta «colarse» en una red legal entrando a través de un elemento que no este bien protegido y una vez dentro convertirse en usuario «normal» de esa red, desde cuya situación procura hacer uso indebido de los recursos de esa red o atacar a otra red ante la cual los usuarios de la anterior tengan ciertos privilegios.
- Puede ir, así, «escalando» y adquiriendo nuevos privilegios que aumentan la peligrosidad del ataque. Esto es lo que suelen hacer los *hackers,* que son personas habilidosas capaces de entrar en sistemas cuyo acceso es restringido.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Los *hackers* y los *crackers* son gente que, de alguna manera, se dedica a perturbar el normal desenvolvimiento de las redes.
- La diferencia entre ambos es algo sutil, ya que a los primeros se les presume una cierta intención Indicada o respaldada por un convencimiento moral de que «las redes son para los que las trabajan».
- Los *crackers,* en cambia, ofrecen una imagen mas perversa y rompedora: son, directamente, los malos de la película.
- Desde el punto de vista de los intereses comerciales, suele calificarse a los hackers como *piratas informáticos,* por aquello de la navegación a través de las redes.
- En contrapartida con esa acepci6n peyorativa, los partidarios del software libre y de la necesidad de que los códigos fuente sean de publico conocimiento y uso se autodenominan como «hackers».

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Con frecuencia, los *piratas informáticos* suelen ser gente muy joven que tienen además una leyenda gloriosa alimentada por algunas noticias de prensa, mas o menos verosímiles, que descubren cómo un adolescente, desde su casa, ha conseguido acceder a redes desde las que se controlan importantes resortes armamentísticos.
- Estas noticias, de ser ciertas, tendrían mas que ver con la incompetencia de ciertos adultos (en que manos, o en que dedos, estamos?) que con las habilidades de esos jóvenes.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Los virus son programas bien conocidos que, una vez instalados, destruyen parte de la información almacenada o de los recursos del sistema.
- En un principio solo se transmitían a través de disquetes, pero, con el auge de la transferencia de ficheros y de documentos a través de las redes (principalmente vía correo electrónico), representan una amenaza que es necesario conjurar.
- Pueden crear copias de sí mismos, replicar mensajes de correo y, en general, dañar los datos y los recursos del sistema atacado.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Gusanos *(worms)* se da esta definición a programas auto replicables que se transmiten por las redes y provocan la saturación de los sistemas (negación del servicio).
- Es famoso el denominado *gusano de Internet,* que en 1988 produjo un ataque masivo que afectó a múltiples ordenadores y a consecuencia del cual su autor fue condenado a pagar una fuerte multa.
- A veces se llama bacterias a programas de efectos similares a los de los gusanos, pero diseñados no para transmitirse a través de las redes sino para atacar a ordenadores aislados.
- Por otra parte, suele llamarse bomba lógica a un programa cuyo código ejecuta una determinada perturbación cuando se produce una determinada condición, por ejemplo una fecha.

PIRATAS, CABALLOS DE TROYA, GUSANOS Y OTRAS ESPECIES

- Como puede apreciarse, toda esta terminología es muy poco rigurosa y raramente volverá a utilizarse en los capítulos que siguen.
- Para continuar analizando los principales conceptos de seguridad conviene fijar nuestra atención en los posibles ataques que se pueden presentar en las redes telemáticas tal y como los catalogamos en el anterior apartado.
- Lo realmente sustantivo es el tipo de vulneración que representan, no la forma de llevarla a cabo.

SERVICIOS, MECANISMOS Y PROTOCOLOS DE SEGURIDAD

- Un Servicio de Seguridad protege las comunicaciones de los usuarios ante determinados ataques.
- Por eso, reflexionar sobre cuales son los distintos ataques de que pueden ser objeto las redes telemáticas equivale a pensar en cuales son los servicios de seguridad que han de establecer las correspondientes protecciones.
- Un Servicio de Seguridad no difiere, desde un punto de vista conceptual, de cualquier otro servicio telemático, tal y como se definen en las arquitecturas de redes jerarquizadas según niveles o capas.
- Así, se dice que si un determinado *servicio de seguridad* es proporcionado por un *nivel N,* se garantiza a las entidades (N+1) usuarias una determinada protección contra ciertos ataques.

SERVICIOS, MECANISMOS Y PROTOCOLOS DE SEGURIDAD

- Otro tanto ocurre con el concepto de Protocolo de Seguridad. De forma análoga a cualquier otro protocolo telemático, un *protocolo de seguridad* consiste en un conjunto de reglas y formatos que determinan el intercambio de piezas de información, en el que intervienen dos o mas entidades (N), y esta diseñado para conseguir que sean prestadas a las entidades (N+1) usuarias determinados *servicios de seguridad.*
- Como puede apreciarse, esta misma definición seria aplicable, en general, a cualquier protocolo telemático a excepción del término «de seguridad» que aparece al final.
- Además, cabe resaltar que, como en cualquier otro, la especificaci6n del protocolo ha de ser completa y no ambigua.

SERVICIOS, MECANISMOS Y PROTOCOLOS DE SEGURIDAD

- Por ejemplo, el Correo Electrónico X.400 sirve para el envío y recepción de mensajes bajo determinadas circunstancias. En realidad, el protocolo Pl, el conjunto de MTAs y la estructura de la UA permanecen transparentes para el usuario, quien lo único que *ve* es el *servicio* que se le presta (las facilidades) y *como* se le presta (la mayor o menor comodidad en el uso de la Interfaz de Usuario).
- Si añadimos un determinado Servicio de Seguridad al ya existente de Correo Electrónico, el usuario percibirá que la recepción y entrega de mensajes se realiza garantizándole, además, una protección contra ciertos ataques.
- Los Mecanismos de Seguridad son utilizados para implementar un determinado *servicio de seguridad* o una combinación de ellos. Podríamos decir que los *Mecanismos de Seguridad* son las piezas lógicas, los «ladrillos», con los que se construyen los *protocolos de seguridad,* los cuales son los encargados de proporcionar los *servicios de seguridad.*

SERVICIOS, MECANISMOS Y PROTOCOLOS DE SEGURIDAD

- Por lo general, los *mecanismos de seguridad* se apoyan en técnicas criptográficas, es decir, en la actualidad, la mayoría de los *mecanismos de seguridad* que han sido desarrollados son *mecanismos criptográficos.*
- Esta permanente presencia de la Criptografía y la indudable importancia que el comportamiento de los criptosistemas tienen en el resultado final, no puede oscurecer la idea de que *la Seguridad en Redes es mucho más que Criptografía.*
- Salvando las distancias, se puede presentar como ejemplo la realización y comportamiento de una base de datos y su relación con la estructura y funcionamiento de la CPU, con sus instrucciones-maquina y sus registros.
- La presencia de la CPU y la repercusión que su mejor o peor comportamiento tiene en el funcionamiento global de la base de datos. Es mas que conveniente que un diseñador de bases de datos sepa como esta constituido y cómo funciona un ordenador, pero un conocimiento preciso de ello no le releva de la dificultad de acometer la complejidad del diseño de la base de datos.

MECANISMOS PARA PROVISIÓN DE SERVICIOS DE SEGURIDAD

Es importante percatarse de que los *servicios de seguridad* son un caso particular de los *servicios telemáticos* y representan, en la mayoría de los casos, un valor añadido. Por eso, casi nunca aparecen de forma aislada, sino mejorando la funcionalidad de otro servicio telemático mas convencional. *Así,* por ejemplo, puede decirse que el PGP (Pretty Good Privacy) es un protocolo que proporciona un servicio de correo electrónico que, además, ofrece los servicios de autenticación del origen de los datos, integridad y confidencialidad.

PRINCIPALES SERVICIOS DE SEGURIDAD

- Para hacer frente a los *ataques* que puedan presentarse, en la norma ISO/IEC 7498, Part 2, *Security Architecture,* que en 1988 puso los cimientos de la nueva conceptualización de la Seguridad en Redes, se definen cinco servicios básicos de seguridad:
- *Autenticación, Confidencialidad, Integridad, Control de Acceso* y *No Repudio.*
- Hay quienes consideran un sexto servicio básico: *Disponibilidad (Availability).*
- La misma que hace referencia a la protección que es necesario introducir para que las distintas partes del sistema que componen la red estén disponibles para ser utilizadas por quienes dispongan de autorización para ello. Podríamos considerar que esto no constituye realmente un servicio telemático (provisto por un protocolo), sino mas bien un conjunto de facilidades y medidas de seguridad que sirven para contrarrestar, en parte, los ataques de denegación de servicio.

SERVICIO DE AUTENTICACIÓN

- El *Servicio de Autenticación* (*Authentication)* sirve para garantizar que una entidad comunicante (una persona o una máquina) *es quien dice ser.*
- En la literatura puede encontrarse también bajo la denominación de «servicio de autentificación», ya que ambos términos son perfectamente válidos en español, aunque «autenticación» es de origen mas antiguo y mas auténtico (y mas breve).
- Este servicio protege contra un ataque muy facilmente perpetrable en las redes: la *suplantación de personalidad (masquerade)* mediante el cual una entidad remota se hace pasar por quien no es.
- Puede tratarse de *Autenticación de entidad simple,* en cuyo caso solo uno de los participantes en la comunicación (puede ser tanto la entidad origen de los datos como la entidad destino) esta obligado a demostrar su identidad.
- Un ejemplo de ello puede ser el acceso a un servidor remoto que contenga una base de datos que almacene información por cuyo consumo el cliente debe pagar.
- Previo a autorizarle el acceso y anotarle el correspondiente cargo, si el protocolo de acceso tiene implementado el Servicio de Autenticación, se garantiza a los gestores del Servidor que el usuario que esta tratando de acceder a la base de datos es la persona o entidad que proclama ser.

SERVICIO DE AUTENTICACIÓN

- En este mismo ejemplo puede darse el caso de que también el cliente quiera estar seguro de que el servidor al que se ha conectado es el autentico y no una suplantación maliciosa.
- Por ejemplo pensemos que la información que reciba el cliente puede provocar en el una decisión importante que a alguien, con animo fraudulento, le interese orientar.
- En este caso se requeriría un servicio de *Autenticación mutua* mediante el cual la operación de aseguramiento de la identidad de las entidades se realiza en ambos sentidos de la comunicación.

SERVICIO DE AUTENTICACIÓN

- Podrían distinguirse en este servicio dos calidades, una de las cuales es la *Autenticación débil* y está apoyada en el uso mas o menos sofisticado de palabras de paso *(passwords)* o de identificadores, mientras que cuando el resultado es mas eficaz la denominamos Autenticación Fuerte *(Strong Authentication),* que requiere del intercambio de mensajes cifrados y, posiblemente, del concurso de una Tercera Parte de Confianza, TTP *(Trusted Third Party).*
- Las TTPs son agentes especializados que intervienen en las comunicaciones seguras, cuya constitución y comportamiento. Las *tarjetas inteligentes (smartcards)* representan un componente de seguridad importantísimo de cara a la implantación tanto del *Servicio de Autenticación* como de otros servicios de seguridad
- En otros casos se emplean mecanismos criptográficos robustos que aportan la necesaria seguridad en la protección del acceso.

SERVICIO DE CONFIDENCIALIDAD DE DATOS

- Este servicio *(Data Confidentiality*) proporciona protección para evitar que los datos sean revelados, accidental o deliberadamente, a un usuario no autorizado.
- Es decir, garantiza que los datos tan sólo van a ser *entendibles* por el destinatario o destinatarios del mensaje, para ello, el mensaje se alterará de tal manera que aquellas personas que no sean los destinatarios autorizados, aunque lo capturen, no podrán ser capaces de entender su significado.
- Cuando es proporcionado, protege a los usuarios de las redes contra un ataque, muy apreciado por ciertos organismos que en teoría están para proteger al ciudadano, consistente en el «pinchazo» *(wiretapping)* de una comunicación para tener acceso, de forma indebida, a la información que por allí circula.

SERVICIO DE CONFIDENCIALIDAD DE DATOS

- Para llevar a cabo estos pinchazos, en la actualidad no es necesario recurrir a escaleras y alicates, ya que se puede acceder indebidamente a un nodo de la red y obtener parte de la información que por allí circula.
- Este tipo de ataques se encuadrará bajo lo que antes hemos denominado *ataques de divulgación o repetición del contenido (replay).*
- Desde siempre (pensemos, por ejemplo, en el correo postal) se ha considerado como un derecho cívico imprescindible que los poderes públicos garanticen la confidencialidad en las comunicaciones convencionales mediante papel.
- La verdad es que este derecho ha sido violado de manera reiterada a lo largo de la Historia tomando como justificación una pretendida y mas que dudosa defensa de los intereses colectivos.

SERVICIO DE CONFIDENCIALIDAD DE DATOS

- Con la ayuda de un *servicio de confidencialidad* robusto podemos conseguir que la información que circule por las redes, o se almacene en ellas, sólo esté disponible para sus legítimos destinatarios, manteniéndola a salvo de miradas curiosas y malintencionadas.
- Con frecuencia, principalmente en la literatura técnica tiende a considerarse *confidencialidad* como casi sinónimo de *privacidad.* En cuanto a lo que aquí entendemos por el significado de este término, cabe decir que en algunos sitios se traduce la palabra inglesa *privacy* por *intimidad.* La idea de intimidad esta mas relacionada con la «zona espiritual intima y reservada de una persona o grupo», como la define el diccionario de la Real Academia. Se ha optado por traducir *«privacy»* por el neologismo *privacidad* (no recogido en el diccionario de la Academia), resaltando su caracter de derecho ciudadano a mantener protegido aquello que afecta a comportamientos sociales que sólo incumben a una persona o un grupo reducido de ellas. Podríamos, por tanto, considerar que la privacidad es la extensión de la intimidad a aspectos mas formales y públicos relacionados con las sociedades modernas y sus dinámicas de mercantilización.

SERVICIO DE CONFIDENCIALIDAD DE DATOS

- Si bien es cierto que en multitud de casos la existencia de un *servicio de confidencialidad* fiable y robusto es fundamental e imprescindible para la obtención de la *privacidad,* no deben confundirse ambos conceptos, ya que, como tratará de justificarse mas adelante, el uso coordinado de los servicios y políticas de seguridad es el que proporciona, en su conjunto y dependiendo de cada caso, la necesaria *privacidad* en las operaciones que realizan los ciudadanos a través de las redes.
- En muchos casos es necesaria la inclusión del Servicio de Anonimato.

SERVICIO DE INTEGRIDAD DE DATOS

- El *Servicio de Integridad de los datos* (*Data Integrity) g*arantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los enviados por el emisor de los mismos, de tal forma que puede tener garantías de que a la información original no le ha sido añadida, ni modificada, ni sustraída alguna de sus partes.
- Es decir, el receptor de la información (o el proveedor del servicio) detectará si se ha producido o no un ataque de *modificación del mensaje,* lo que le permitirá rechazar o dar por buenos los datos recibidos.

SERVICIO DE INTEGRIDAD DE DATOS

- En los procedimientos ordinarios de intercambio de información mediante papel u otros soportes convencionales no ha resultado muy difícil para los falsificadores alterar mediante sustituciones el contenido de un mensaje.
- Pero se requiere bastante habilidad para llevarlo a cabo sin que se note el fraude.
- Además, las posibilidades de sustitución que tiene el falsificador están muy limitadas por el formato del documento: puede sustituir una palabra o una frase por otra de similar tamaño, pero no puede insertar párrafos demasiado grandes sin alterar sustancialmente la estructura del documento.
- Estas dificultades hacen que los usuarios ante, por ejemplo, un papel firmado no teman en exceso este tipo de ataques. No obstante, cuando se trata de mensajes o datos en soporte electrónico, las posibilidades de hacer modificaciones sin dejar huella están al alcance de cualquiera.

SERVICIO DE INTEGRIDAD DE DATOS

- Pensemos por ejemplo, en que alguien quiera presentar ante un organismo cualquiera, como elemento probatorio, un mensaje de correo impreso en el que se respalde cualquier circunstancia favorable a quien lo presenta.
- Resulta evidente que si no presenta una prueba robusta (por lo general será una prueba criptografica) de la integridad del mensaje, nadie en su sano juicio va a aceptar ese mensaje como una prueba válida (cualquiera puede redactar e imprimir lo que le parezca oportuno y darle el formato que tendría un mensaje de correo).
- Por todo ello, resulta absolutamente imprescindible la provisión del servicio de integridad cuando se trata de intercambiar mensajes, con cierta garantía, a través de redes telemáticas.

SERVICIO DE INTEGRIDAD DE DATOS

- La mayor simplicidad de estos procedimientos deriva del hecho de que pueden implementarse bajo el paradigma de *extremo a extremo (end to end),* es decir, participando solamente la entidad emisora y la entidad receptora, sin el concurso de una TIP que haga de intermediaria en la transferencia del mensaje.
- No obstante, con frecuencia se confunde la *autenticación de origen de los datos* con el *no repudio de envío* que, como mas adelante se justifica, requiere de mayores salvaguardas.
- La mayoría de protocolos de correo seguro, entre ellos el conocido PGP proporcionan a sus usuarios estos tres servicios.

SERVICIO DE NO REPUDIO

- En una primera aproximación relacionaremos este servicio con el intercambio de mensajes a través de redes telemáticas para dar garantías respecto a su emisión y recepción.
- Como su nombre sugiere, sirve para evitar que alguno de los participantes en la comunicación niegue (repudie) haber formado parte de ella.
- El nombre elegido para este servicio *(Non-repudiation)* no es excesivamente afortunado por cuanto está cargado de connotaciones que nos remiten a un pasado (todavía presente en algunos lugares) poco favorable para los derechos de la mujer.
- No obstante, este término esta ya suficientemente extendido y aceptado, por lo que seguiremos utilizándolo haciendo caso omiso de esas connotaciones. Podríamos distinguir tres situaciones:

NO REPUDIO CON PRUEBA DE ORIGEN

- En este caso, el receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos.
- En muchos casos pueden bastar las garantías que el emisor introduce en el mensaje cuando aplica los mecanismos que aseguran la autenticación del origen de los datos.
- En otros casos pueden requerirse evidencias acerca la relación existente entre el autor de un determinado mensaje y la entidad que procede a enviarlo a través de la red.
- Pensemos por ejemplo, en que alguien escriba y firme una carta insultante hacia otra persona pero que no se atreve a enviársela por correo postal.
- Si un tercero localiza ese escrito y lo pone en el correo, el receptor tendrá pruebas demostrables de quien es el autor de la carta, pero no de que además de escribirla ha sido el quien ha tornado la decisión ofensiva de enviársela.

NO REPUDIO CON PRUEBA DE ENVÍO

- El receptor o el emisor del mensaje adquieren una prueba, demostrable ante terceros, de la fecha y hora en que el mensaje fue enviado.
- Este servicio trata de emular al que frecuentemente presta el Servicio Postal cuando al entregar una carta certificada en la estafeta se solicita que una copia del documento que se quiere enviar sea sellada con una marca de tiempo precisa, de tal manera que pueda servir posteriormente como prueba ante determinados actos administrativos que requieren que, por ejemplo, una solicitud sea entregada antes de una fecha concreta bien en el registro de entrada de la oficina de destino o bien en una dependencia de Correos. (Dependiendo de que entidad reciba la prueba, se puede desdoblar en dos este servicio.)

NO REPUDIO CON PRUEBA DE ENTREGA

- El emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado. Continuando con el ejemplo del correo, este servicio equivaldría al envío de cartas con acuse de recibo, en cuyo caso el Servicio de Correos devuelve, convenientemente cumplimentada, una cartulina que sirve de evidencia y justificación de que la carta ha llegado a su destinatario.
- En estos dos últimos ejemplos, Correos se comporta como una entidad intermediaria entre el enviante y el receptor, lo que traducido al mundo de las redes significa que para implantar ese servicio es necesaria alguna entidad que actúe como Tercera Parte de Confianza (TIP).
- Esto equivale a decir que para que este servicio pueda ser provisto es necesario que exista, en alguna medida, una *infraestructura de seguridad* que haga de garante y proporcione las evidencias exigidas.

NO REPUDIO CON PRUEBA DE ENTREGA

- Esta es la causa por la que el *servicio de No Repudio* es mas difícil de implantar que la tema *Autenticación-Confidencialidad-Integridad* que pueden implementarse (en su versión más simplista) solamente en la entidad emisora y en la entidad receptora sin el concurso de ninguna TIP intermediaria.
- No obstante esta mayor dificultad, no es necesario poner mucho énfasis para trasladar la convicción de lo imprescindible que resulta la implantación de servicios de *No Repudio* si lo que se pretende es que dentro de la Sociedad de la Información, la mayoría de las comunicaciones que convencionalmente han venido dando mediante el intercambio de documentos en papel se vean sustituidas por transferencias de documentos digitales a través de redes telemáticas. No es concebible la implantación de operaciones con las Administraciones Públicas a través de la red sin que este tipo de servicios este operativo.

SERVICIO DE CONTROL DE ACCESO

- Este servicio *(Access Control*) sirve para evitar el uso no autorizado de los recursos de la red. Puede servir para permitir que sólo quien este autorizado para ello pueda conectarse a una determinada máquina, y para que, una vez conectado, cada usuario sólo pueda tener acceso a aquellas facilidades para las que ha adquirido permisos. De forma resumida, podríamos decir que este servicio permite especificar *quien puede hacer que*, es decir, que usuarios pueden hacer determinadas operaciones.
- En realidad, este servicio no es privativo de las redes telemáticas, sino que ya estaba implantado en los accesos a ordenadores aislados instalados en los centros de cálculo, en los que en función del *«login»* se permitía acceder a determinados procesadores o programas. Por ejemplo, el compilador de C podría ser un recurso compartido por todos, pero no así el resultado de la compilación de un programa concreto. Es decir, aparece siempre que se presente un escenario en el que distintos usuarios con distintos privilegios accedan concurrentemente a un mismo recurso.

SERVICIO DE CONTROL DE ACCESO

- En las redes telemáticas se puede presentar la necesidad de disponer de un servicio de *control de acceso* en dos situaciones distintas. Estas son:
  - El acceso remoto a servidores de todo tipo como bases de datos, impresoras, servidores de correo, etc. El usuario accede regularmente bajo una arquitectura cliente-servidor y, tras identificarse, los mecanismos en que se apoya el servicio determinan a que partes del servicio se les concede acceso.
  - El acceso a los terminales desde los que el usuario se conecta a la red. Ellos pueden incluir desde ordenadores protegidos a tarjetas inteligentes. Con frecuencia son estos puntos externos de las redes los que necesitan ser protegidos de forma mas estricta, mientras que en otros casos se permite el acceso desde cualquier terminal y los controles se centran solamente en el servidor accedido.

SERVICIO DE CONTROL DE ACCESO

- En la mayoría de los casos este servicio se implementa íntimamente ligado a la provisión previa de un servicio de autenticación. Una vez que el usuario ha demostrado que es quien dice ser se le aplican las restricciones o permisos correspondientes.
- No obstante, se dan otras circunstancias en las que el control de acceso se lleva a cabo mediante *credenciales,* esto es, piezas de información que representan una serie de privilegios a quien las porte, independientemente de su identidad.
- Un ejemplo en el mundo real puede ser un boleto de entrada para acceder a una butaca concreta de una sala de cine: el privilegio se adquiere al comprarla y su aplicación efectiva no depende de la identidad del portador.

SERVICIO DE CONTROL DE ACCESO

- En cuanto al grado de implantación de este servicio, cabe decir que, desafortunadamente, con demasiada frecuencia el control se limita a decir *si* o no al intento de acceso al recurso, sin mayores detalles posteriores. Cuando se trata, por ejemplo, del acceso a una base de datos plural y compleja, una adecuada implementación debería ofrecer un acceso muy pormenorizado, regulando categorías de usuarios y categorías de actuaciones (no puede ser lo mismo tener derecho a leer la información que tener derecho a insertar o modificar datos).

SERVICIO DE CONTROL DE ACCESO

- También con demasiada frecuencia el control de acceso se aplica a través de mecanismos de autenticación muy débiles, como puede ser una palabra de paso *(password)* o PIN (número de identificación personal).
- En otros casos se emplean mecanismos criptográficos robustos que aportan la necesaria seguridad en la protección del acceso. Las *tarjetas inteligentes,* representan un componente de seguridad importantísimo de cara a la implantación tanto del servicio de *Control de Acceso* como de los restantes servicios de seguridad.

SERVICIO DE ANONIMATO

- Se trata de conseguir que la identidad de la persona que realiza una determinada operación telemática permanezca oculta ante algunos de los actores presentes en esa operación.
- Se trata de emular en la Red situaciones de la vida real, en las cuales es conveniente mantener cierto anonimato. Si dentro del correo postal es posible enviar cartas de forma anónima, también el correo electrónico debe permitir esa posibilidad.
- Veamos también otros casos en los que este tipo de requisitos se presentan. En primer lugar supongamos por ejemplo, un buzón de sugerencias de quejas dispuesto para que estas sean depositadas en él de forma anónima.

Algunas vulnerabilidades

- Software (con fallos)
- Contenido activo (malicioso): macros, scripts, etc.
- Puertos abiertos: telnet, correo, etc.
- Configuración de recursos (incorrecta): permisos, etc.
- Puertas traseras (agujeros de seguridad deliberados)
- Comunicación (sin cifrado)
- Contraseñas (mal elegidas)
- Mecanismo de cifrado (con fallos)
- Localización física (no segura)
- Administradores y usuarios (mal adiestrados)
- Muchas otras …….
- Suposiciones:
  - Nadie extraño puede acceder al hardware, el código del programa no se puede modificar durante su ejecución , etc.

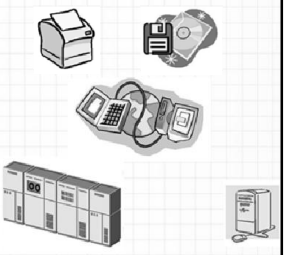
Seguridad total
=
Seguridad de componente más vulnerable

De qué sirve tener una cerradura de US $ 1000 si la ventana está abierta?

Ataques (a la seguridad)

Lugares

- Información en papel
- Información en disco duro
- Información en dispositivo de almacenamiento externo
- Información en servidor
- Información en tránsito

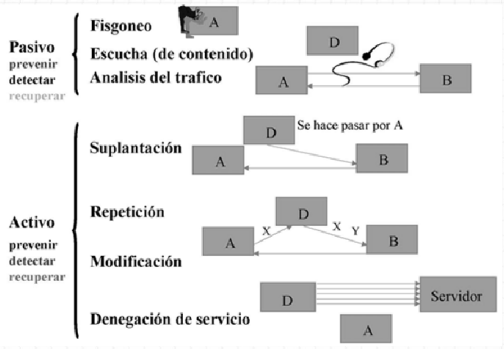


Tipos

Según acción { Pasivo / Activo

Según voluntad { Deliberado / Accidental

Tipos de ataques



Servicios de Seguridad

- Para hacer frente a ataques
- Para mejorar Seguridad
- Qué Servicios?
  - Estudio de consecuencias negativas de ataques
- Agrupación en tipos:

Algunas categorías:
- Autenticación
- Control de acceso
- Confidencialidad
- Integridad
- No repudio
- Disponibilidad
- Responsabilidad

Clasificación que usaremos:
- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación

Servicios

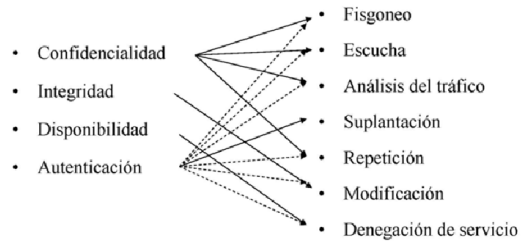
- **Confidencialidad**
  - Impedir que entidad no autorizada conozca la existencia de datos, los examine o revele, o analice su flujo.
  - Términos relacionados: secreto, privacidad
- **Integridad**
  - Asegurar que los datos son correctos
    - Los almacenados no han sido expuestos a alteración no autorizada
    - Los recibidos son exactamente los enviados
  - Muy importante: recuperación de original
- **Disponibilidad**
  - Evitar que entidad no pueda acceder cuando desea a un recurso/servicio para el que está autorizado

Servicios

- **Autenticación**
  - Asegurar que **entidad** es quien dice ser
  - Identificar **entidad**

  Para:
  - Asegurar que la **transmisión** se produce entre **entidades legítimas**
    - Mutua
    - De origen de datos únicamente
  - Asegurar que **se asignan acciones a entidad correcta**
    - Evitar que se desmienta una transmisión
      - De origen: Probar que el mensaje fue enviado por el emisor
      - De destino: Probar que el mensaje fue recibido por el receptor
- Imprescindible para confidencialidad, integridad y disponibilidad

Servicios y Ataques

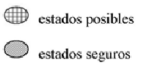


Mecanismos de Seguridad

- Posibilitan la realización de los servicios
- No hay uno que valga para todos

Perspectiva: Mecanismos en anillos de protección concéntricos:
- Centro: mecanismos hardware, fuera: mecanismos de aplicación
- Hacia el centro: más genéricos
- Hacia fuera: más cercano a requisitos de usuario

Tipos según cobertura:



Tipos según fin:

De prevención | De detección | De recuperación | De análisis forense

Mecanismos de Seguridad

- Con **base criptográfica**
  - Uso de algoritmos matemáticos que transforman datos en otros no inteligibles por cualquiera
  - Fundamental: creación y gestión de claves
  - La mayoría
- Dispositivos **hardware**
  - Tarjetas inteligentes
  - Biometría: lector de huellas digitales, reconocimiento de voz, escáner de retina, etc.
  - Componentes seguros de red física: cortafuegos para elegir una ruta segura, y muchos otros

Mecanismos de Seguridad

- Control del **software**
  - Mediante SO: permisos para archivos, detección de acciones, bitácora, etc.
  - Durante el desarrollo: diseño, pruebas, etc.
  - Cortafuegos, antivirus, etc.
- **Tráfico de relleno**
  - Transmisión de basura para impedir análisis de tráfico
- Tareas **administrativas**
  - Política de institución
  - Leyes, normativas, etc.
- Controles **físicos**
  - Cerraduras, copias de seguridad, detector de intrusos, etc.

Mecanismos para cada servicio

- Confidencialidad:
  - cifrado (y descifrado), control de acceso, ...
- Integridad:
  - resumen de mensaje, intercambio de autenticación, control de acceso, firma digital, ...
- Disponibilidad:
  - cortafuegos, antivirus, copias de seguridad, ...
- Autenticación:
  - contraseñas, biometría, certificados, firma digital, intercambio de autenticación, ...