

Sistemas Operativos II



Clase 6

Seguridad

Universidad Arturo Jauretche
Ingeniería Informática

Docentes:

Coordinador: Ing. Jorge Osio

Profesores: Ing. Eduardo Kunysz
Ing. Daniel Alonso

EL ENTORNO DE SEGURIDAD

Seguridad:

Seguridad

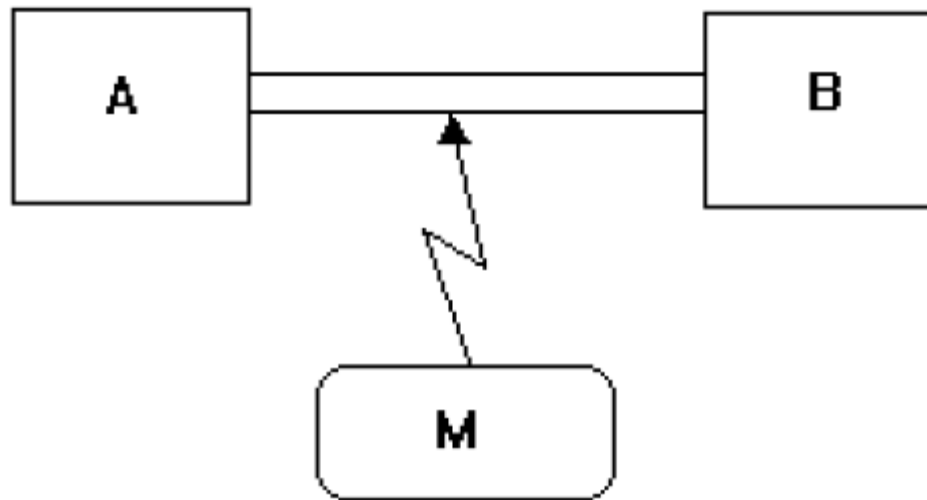
Protección

Medida de cómo se preserva la integridad de un sistema y sus datos

La **seguridad** no solo requiere de un buen sistema de protección sino que además considera el entorno externo dentro del cual opera el sistema.

Los problemas de seguridad son esencialmente problemas de administración y no de sistema

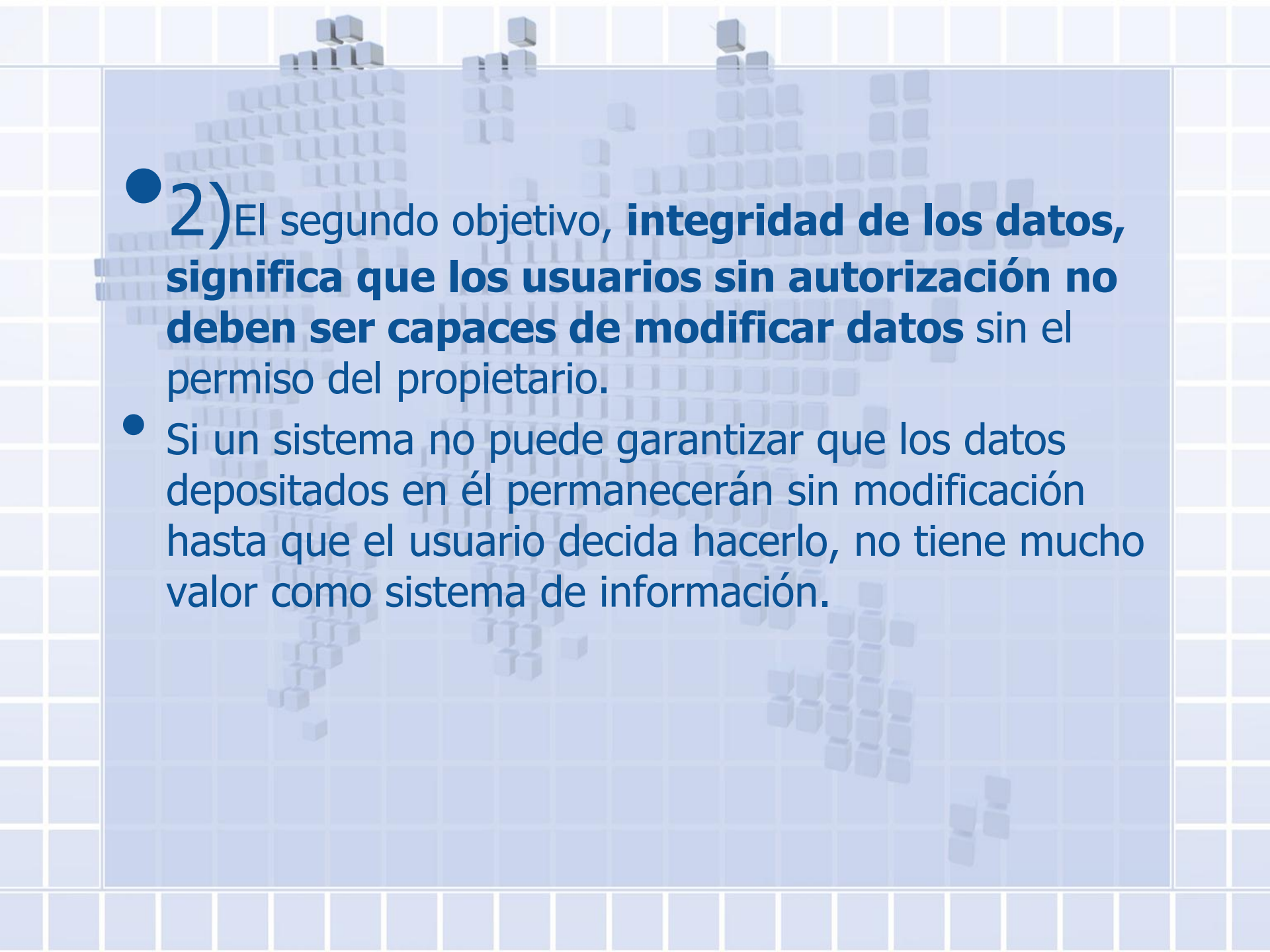
seguridad

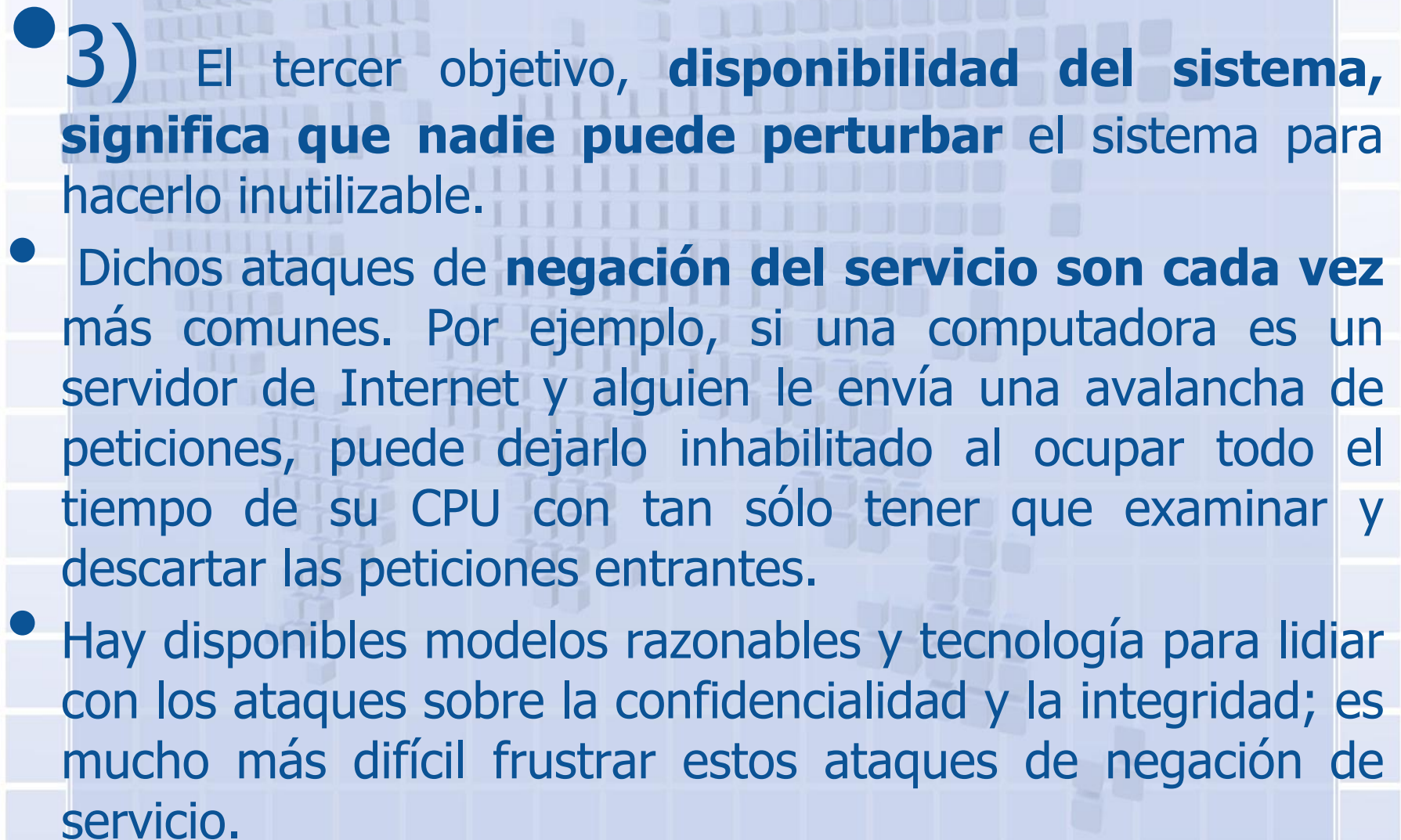


**Escucha, genera o
modifica datos.**

Amenazas

- Se tienen **cuatro objetivos** generales con sus correspondientes amenazas.
- **1)** El primer objetivo, la **confidencialidad de los datos, que implica hacer que los datos secretos permanezcan** así.
- Por ejemplo, si el propietario de ciertos datos ha decidido que éstos pueden estar disponibles sólo para ciertas personas, el sistema debe garantizar que las personas no autorizadas nunca tengan acceso a esos datos.

- 
- 2) El segundo objetivo, **integridad de los datos**, significa que los usuarios sin autorización no deben ser capaces de modificar datos sin el permiso del propietario.
 - Si un sistema no puede garantizar que los datos depositados en él permanecerán sin modificación hasta que el usuario decida hacerlo, no tiene mucho valor como sistema de información.

- 
- 3) El tercer objetivo, **disponibilidad del sistema**, **significa que nadie puede perturbar** el sistema para hacerlo inutilizable.
 - Dichos ataques de **negación del servicio son cada vez** más comunes. Por ejemplo, si una computadora es un servidor de Internet y alguien le envía una avalancha de peticiones, puede dejarlo inhabilitado al ocupar todo el tiempo de su CPU con tan sólo tener que examinar y descartar las peticiones entrantes.
 - Hay disponibles modelos razonables y tecnología para lidiar con los ataques sobre la confidencialidad y la integridad; es mucho más difícil frustrar estos ataques de negación de servicio.

- 4) Surgió una nueva amenaza. Algunas veces los usuarios externos pueden tomar el control de las computadoras (mediante el uso de virus y otros medios) y convertirlas en **zombies, dispuestas a cumplir los deseos del usuario exterior** con sólo dar las órdenes.
- Otro aspecto del problema de seguridad es la **privacidad: proteger a los individuos contra el mal uso de la información sobre ellos**. Esto está generando muchos problemas legales y morales.

Objetivo	Amenaza
Confidencialidad de los datos	Exposición de los datos
Integridad de los datos	Alteración de los datos
Disponibilidad del sistema	Negación del servicio
Exclusión de los usuarios externos	Los virus se apropian del sistema

- ¿Debe el gobierno compilar expedientes de todas las personas para poder atrapar a los que engañan a X , donde X es "*asistencia social*" o "*impuestos*",
- ¿Debe ser capaz la policía de buscar cualquier información sobre cualquier persona para poder detener al crimen organizado?
- ¿Los patrones y las compañías de seguros tienen derechos? ¿Qué ocurre cuando estos derechos entran en conflicto con los derechos individuales?

Intrusos

- Las personas que husmean en lugares en donde no tienen por qué hacerlo se conocen como **intrusos**, o algunas veces como **adversarios**.
- **Los intrusos actúan en dos formas distintas:**
 - **Los** intrusos pasivos sólo quieren leer archivos para los cuales no tienen autorización.
 - Los intrusos activos son más maliciosos; desean realizar modificaciones no autorizadas a los datos.

Algunas categorías de intrusos son:

1. Usuarios **no técnicos** que se entrometen en forma casual. Muchas personas tienen computadoras conectadas a un servidor de archivos compartidos y dichas personas son capaces de leer el correo electrónico y demás archivos de otras.
2. Intrusos que husmean. **Los estudiantes, programadores** de sistemas, operadores consideran como un reto personal la acción de irrumpir en la seguridad de un sistema computacional local.
3. Intentos determinados por obtener dinero. Algunos programadores de bancos han tratado de **robar el banco** en el que trabajan. Desde cambiar el software para truncar en vez de redondear el interés, quedarse con la fracción de un centavo, hasta llegar al chantaje ("Si no me pagan, destruiré todos los registros del banco").

4. Espionaje comercial o militar. El espionaje se refiere a un intento serio y bien fundamentado por parte de un competidor u otro país de robar programas, secretos comerciales, ideas patentables, planes de negocios, etcétera.

5. El virus es otra categoría de plaga de seguridad. es una pieza de código que se duplica a sí mismo y (por lo general) realiza cierto daño. En cierto modo, el escritor de un virus es también un intruso, a menudo con habilidades técnicas elevadas.

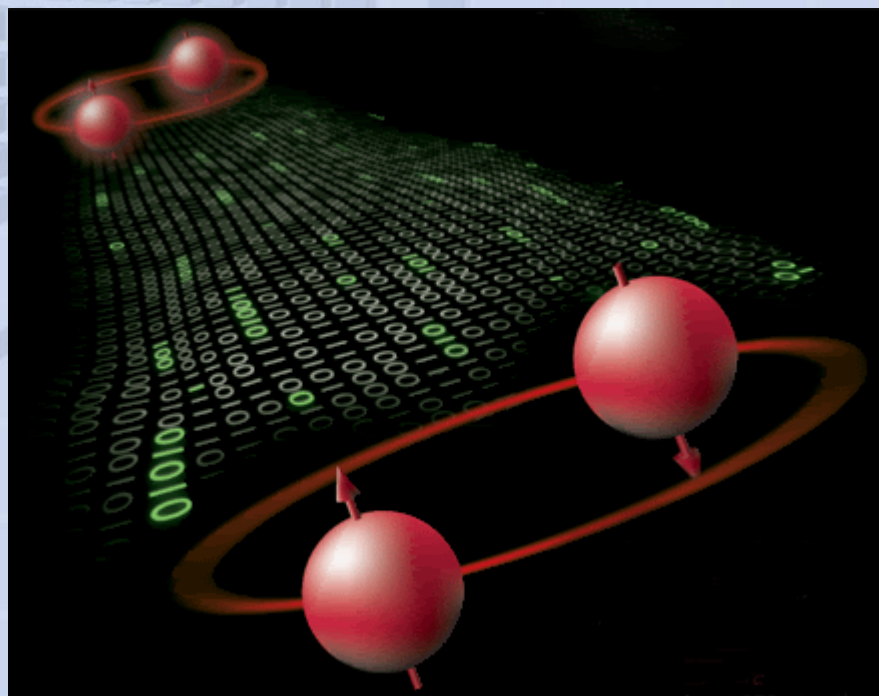
Pérdida accidental de datos

Por accidente se pueden perder datos valiosos. Algunas de las causas comunes de pérdida accidental de datos son:

1. **Accidentes y desastres naturales:** incendios, inundaciones, terremotos, guerras, disturbios, etc.
2. **Errores de hardware o software:** fallas en la CPU, discos, de telecomunicaciones, errores en los programas.
3. **Errores humanos:** error al introducir los datos, al montar un CD-ROM de manera incorrecta; ejecutar el programa incorrecto, perder un disco, etc.

La mayoría de estas causas se pueden prevenir mediante respaldos adecuados. Es probable que haya más daños ocasionados por las pérdidas accidentales que por intrusos.

Criptografía



Criptografía



Criptografía (un poco de historia)

La **escitala** utilizada por los espartanos para enviar **mensajes** consistía de una tira de papel o tela en la cual se escribía el mensaje que solo podía ser comprendido para aquellos que contaban con la escitala (vara o bastón) del diámetro correcto.



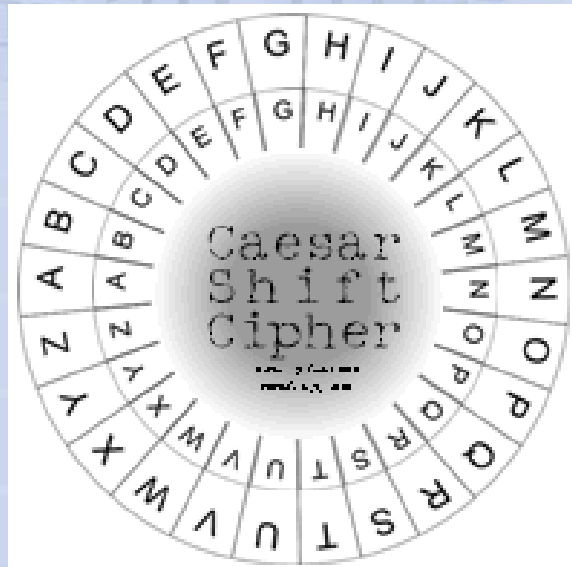
Criptografía (un poco de historia)

CESAR (SUSTITUCIÓN), Atribuido al emperador Julio Cesar.

Se suma un número entero fijo a las letras del alfabeto, por ejemplo + 3

Mensaje: SUPERSECRETO

Mensaje cifrado: VXSHUVHFUHW



Criptografía de clave publica

SUSTITUCIÓN CON PALABRA CLAVE

Se escriben las letras del alfabeto mezcladas con una palabra clave, por ejemplo:

Clave: SIMON BOLIVAR.

Sin letras repetidas: SIMON BLVAR.

Alfabeto:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alf. Transformado:

S I M O N B L V A R C D E F G H J K P Q T U W X Y Z

El texto llano **CESAR** cifrará como MNPSK.

Criptografía

ONE TIME PAD (Bloque de uso único)

Es un método totalmente seguro. Trabaja como el método de Cesar, pero el entero a sumar varía para cada caracter del texto en forma aleatoria.

El criptograma "**SECRETO**" podría provenir de:

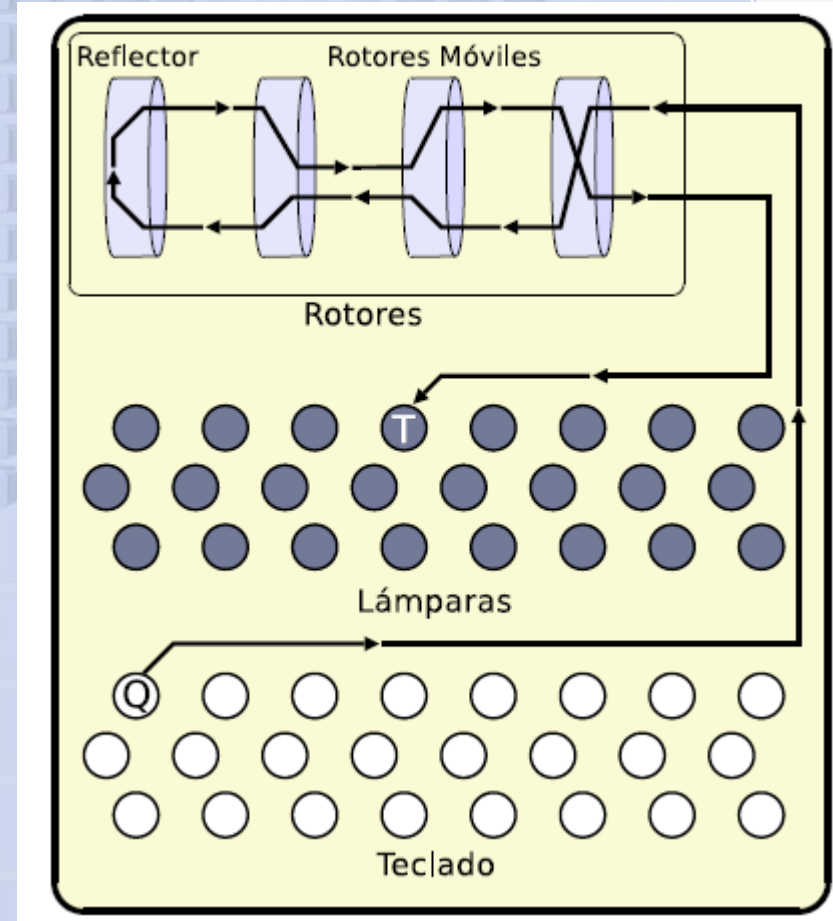
- **MENTIRA** con la clave 6 0 15 2 22 23 12, o de:
- **REALEZA** con la clave 1 0 2 6 0 6 12.

El problema es que la clave debe ser tan larga como el mensaje, y nunca debe ser reutilizada!!!

Criptografía

Maquina ENIGMA (cifrado de Lorenz)

- Quiebre entre criptografía **clásica y moderna**.
- Utilizada por Alemanes en la II Guerra Mundial.
- Cada vez que se pulsa una tecla el primer rotor avanza una posición; el segundo avanza cuando el anterior ha dado una vuelta completa y así sucesivamente.
- El reflector (mas moderno) se utilizaba para invertir sentido y descifrar.



Generalidades de Algoritmos

- **confusión —sustituciones**
- **difusión —transposiciones**

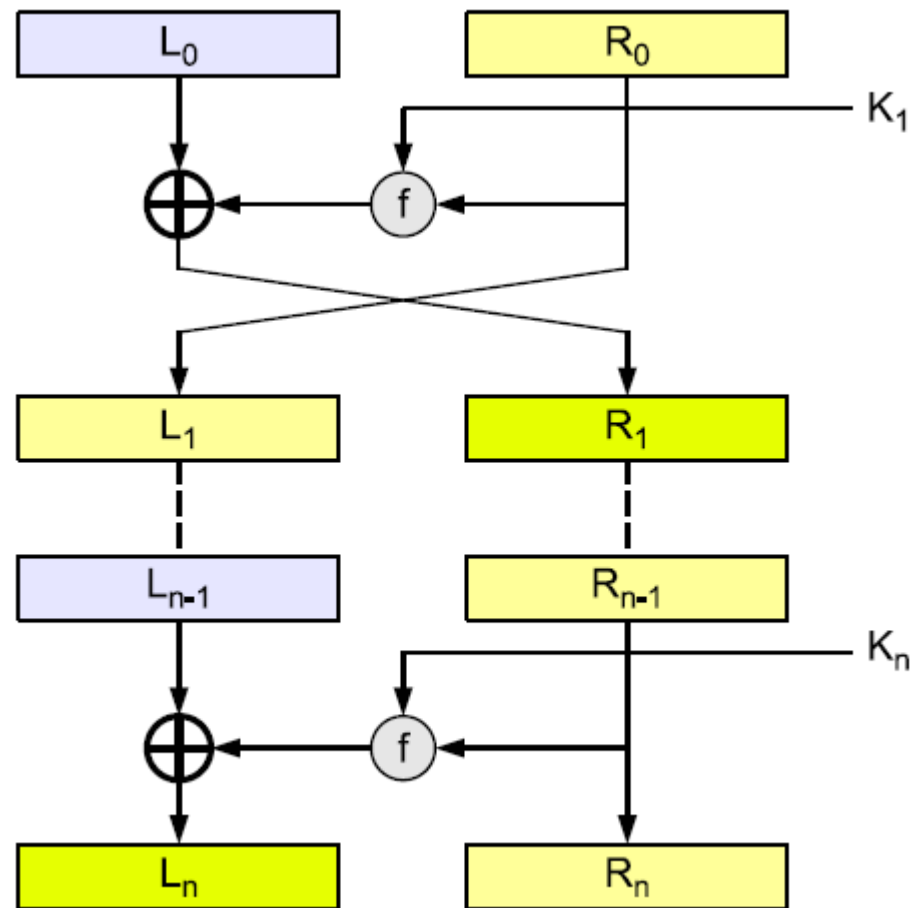
- La confusión consiste en tratar de ocultar la relación que existe entre el texto claro, el texto cifrado y la clave. Un buen mecanismo de confusión hará demasiado complicado extraer relaciones estadísticas entre las tres cosas.
- Por su parte la difusión trata de repartir la influencia de cada bit del mensaje original lo más posible entre el mensaje cifrado.

Redes de Feistel

Dividen un bloque de longitud n en dos mitades, L y R .

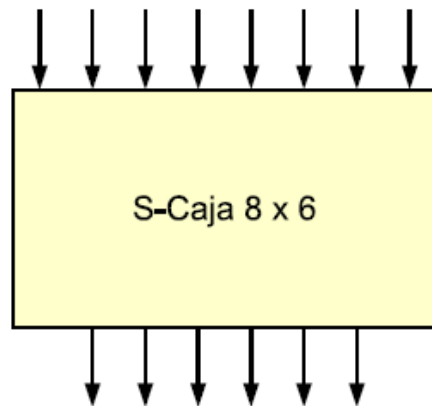
$$\left. \begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned} \right\} \quad \text{si } i < n.$$

$$\begin{aligned} L_n &= L_{n-1} \oplus f(R_{n-1}, K_n) \\ R_n &= R_{n-1} \end{aligned}$$

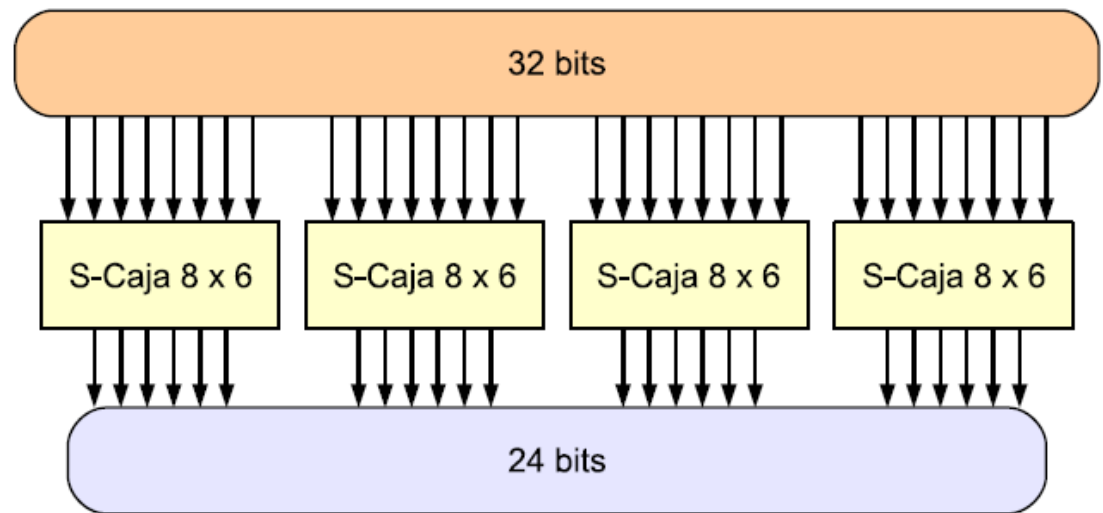


S-BOX o S-CAJA

- Una S-Caja de $m \times n$ bits es una tabla de sustitución que toma como entrada cadenas de m bits y da como salida cadenas de n bits.



A



B

Figura 10.2: **A:** S-Caja individual. **B:** combinación de cuatro S-Cajas.

Criptografía

DES (Data Encryption Standard - 1977)

Divide el texto llano en bloques de 64 bits, utiliza una clave de 56 bits y los 8 bits restantes se utilizan para paridad.

Realiza **16 pasos con funciones intermedias de sustitución (S-boxes) y transposición**, pero su núcleo es la XOR.

XOR

0 1 1

1 0 1

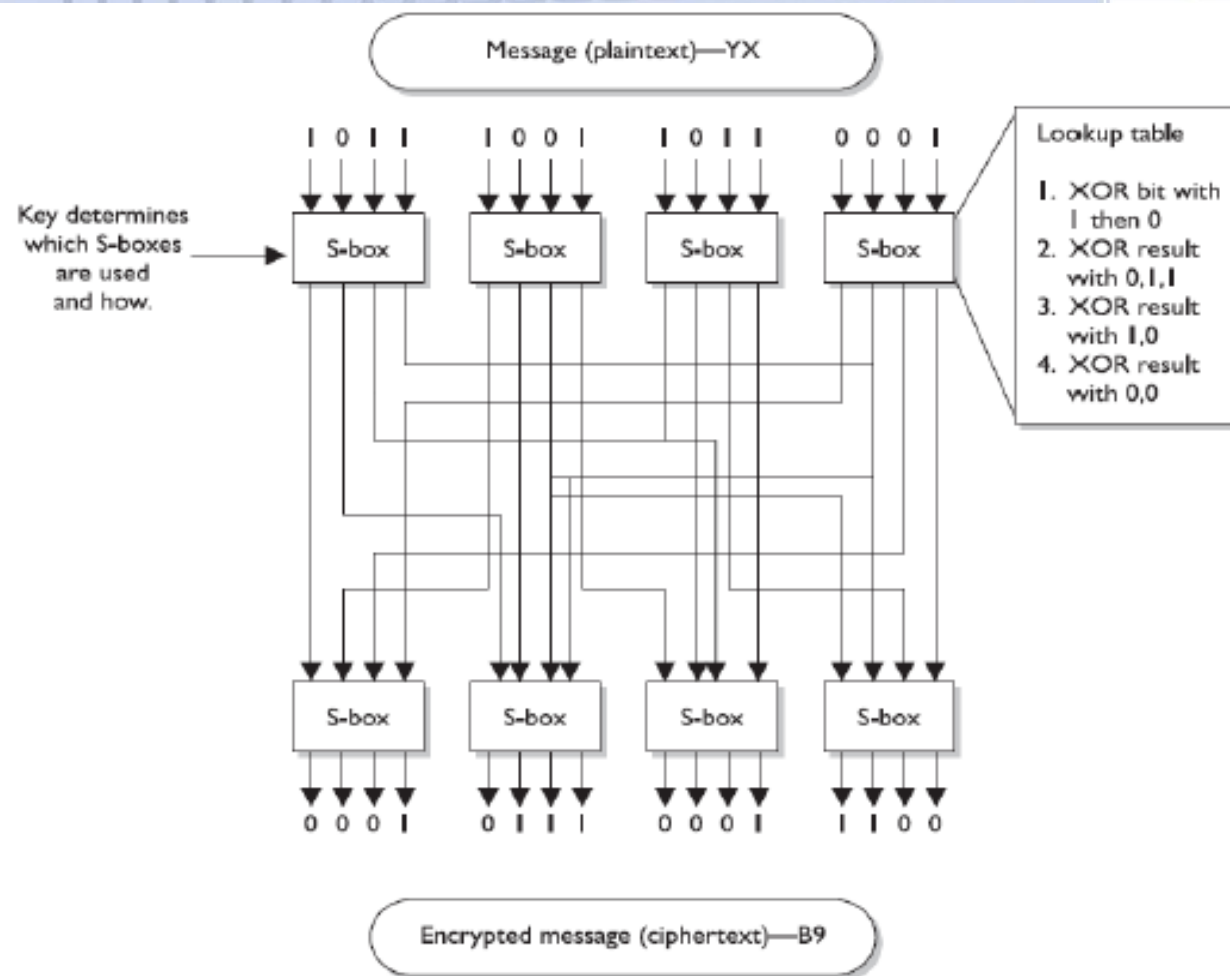
0 0 0

1 1 0

Criptografía

Ejemplo de funciones de sustitución y transposición:

Cada **S-box** tiene una **tabla asociada** que es utilizada por el algoritmo para indicar **cómo deber cifrar los bits**.



Criptografía

DISTRIBUCION DE CLAVES

- Los métodos criptográficos (DES y One-time Pad) tienen el problema de la distribución de las claves.
- Todos los que participan deben conocerlas y por ende existe más de un punto posible de divulgación por parte de un atacante.
- Son **simétricos**

Criptografía

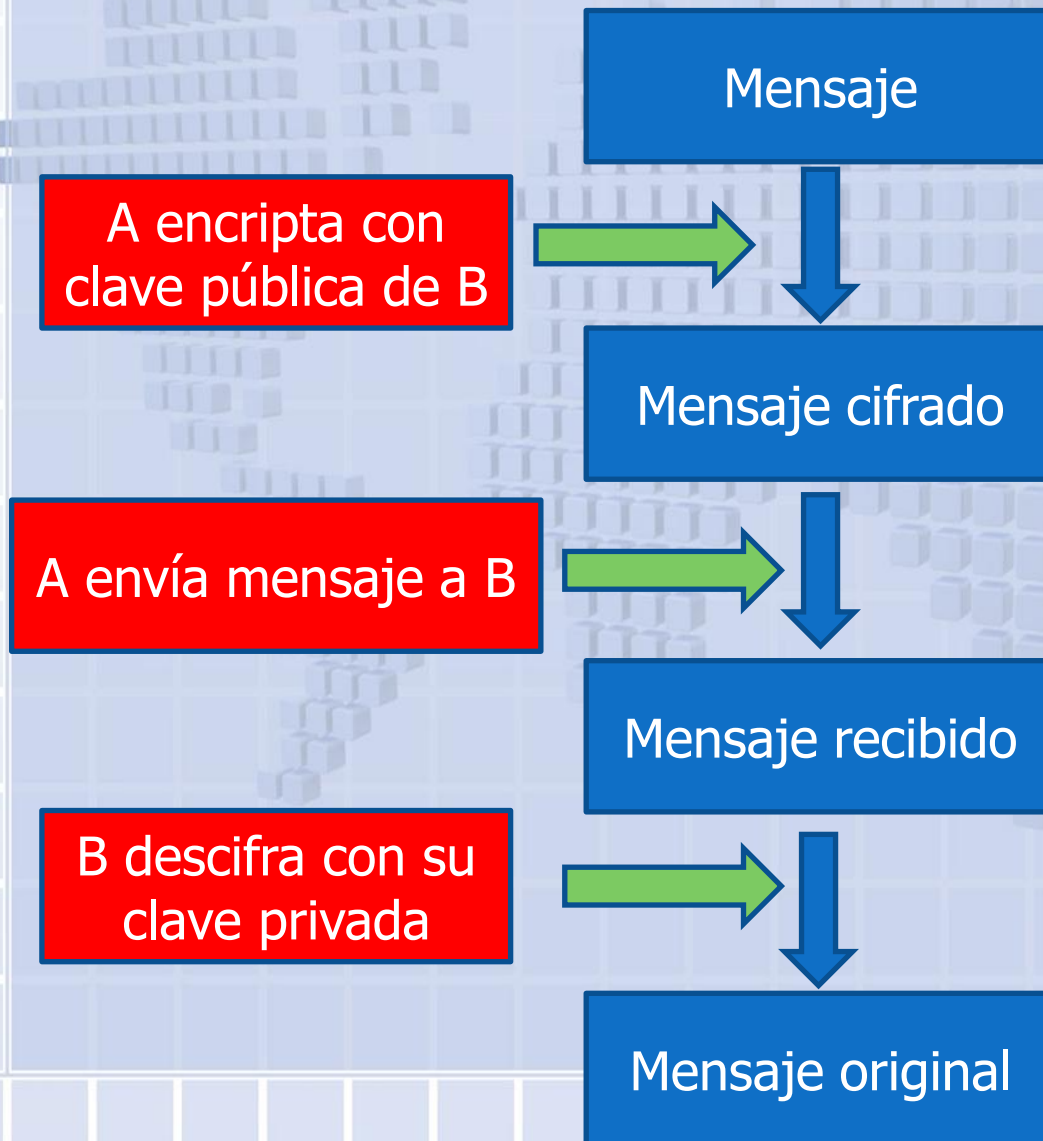
Métodos Asimétricos

Se basan en la existencia de pares de claves: Claves Públicas y Privadas

- A y B publican sus **claves de encriptado E_a y E_b** , y mantiene en secreto sus **claves de desencriptado D_a y D_b** . Con esto, el problema de distribución de claves casi desaparece .
- Existe aún el problema de **un atacante** en el medio de comunicación que **intercepte el intercambio de claves** y suplante la persona de uno de los emisores (man-in-the middle). **El atacante Z se hace pasar por B.**

Criptografía

Métodos Asimétricos



Conceptos Matemático (modulo)

La aritmética modular es una parte de las Matemáticas extremadamente útil en Criptografía

Mucha gente la conoce como la aritmética del reloj, debido a su parecido con la forma que tenemos de contar el tiempo. Por ejemplo, si son las 19:13:59 y pasa un segundo, decimos que son las 19:14:00, y no las 19:13:60

Exponencial Modular: calcula el residuo cuando un número entero positivo b (la base) se eleva a la e -ésima potencia (el exponente), b^e , y es dividido por el entero positivo m , llamado módulo.

$$b^e \bmod(m) \Rightarrow \text{resto de } b^e / m = [(b^e/m) - \text{IP}(b^e/m)] * m$$

$$\text{Ej: } 5^3 \bmod(13) = \text{resto } (125/13) = (9,615-9) * 13$$

Criptografía

Métodos Asimétricos: RSA (Rivest-Shamir-Adleman)

Se buscan dos N° primos grandes p y q , y se obtiene $n = p \cdot q$

Se buscan dos números e y d que contemplen la siguiente propiedad:

$$- e \cdot d \bmod [(p-1) \cdot (q-1)] = 1$$

Se representa el texto llano por medio de un M tal que $0 \leq M \leq n-1$

de forma tal que el encriptado resulta:

$$C = M \cdot e \bmod(n)$$

y el desencriptado es:

$$M = C \cdot d \bmod(n)$$

La clave pública es el par (e, n) y la privada el par (d, n) .

Conocer e y n no da suficiente información como para hallar d (p y q son secretos).

Criptografía

Métodos Asimétricos: RSA (Rivest-Shamir-Adleman)

Ejemplo:

Veamos un ejemplo con números pequeños:

$$p=3; q=5; n=15$$

Se elige $e = 3$ y $d = 11$ tal que $3 \cdot 11 \bmod [2 \cdot 4] = 33 \bmod(8) = 1$

Si suponemos un mensaje $M = 8$, resulta:

$$\text{cifrado } c = 8^3 \bmod(15) = 512 \bmod(15) = 2$$

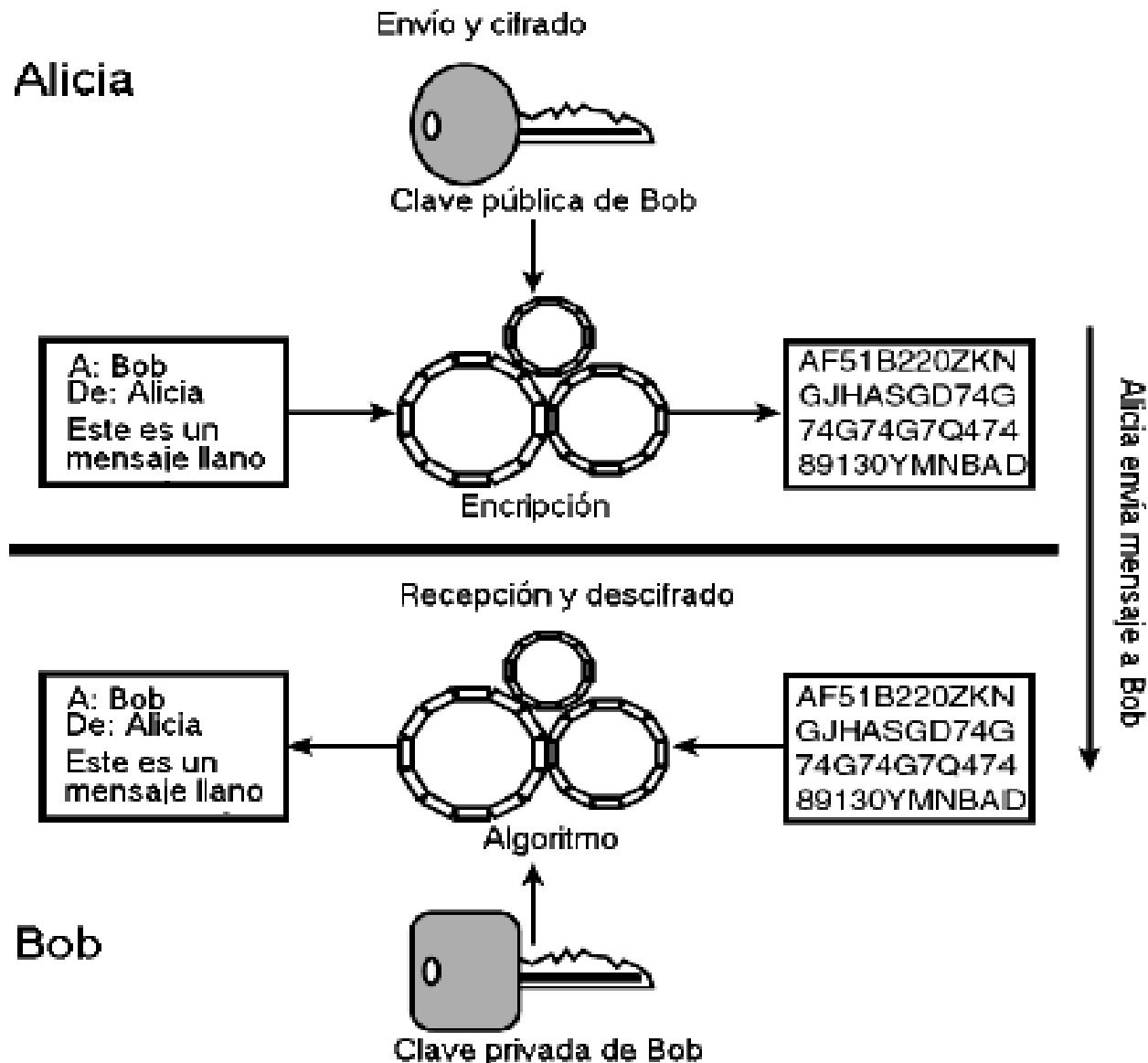
siendo $c = 2$, el mensaje cifrado que viaja por el medio de comunicación.

En el lugar de destino, se hace:

$$M = 2^{11} \bmod(15) = 2048 \bmod(15) = 8$$

donde $M=8$ es el mensaje original descriptado.

Criptografía



Criptografía

AUTENTICIDAD (FIRMA)

- Si pensamos el RSA al revés, por ejemplo, si encriptamos con una clave D secreta, se puede desencriptar con una clave E pública, y nadie podría falsificar el mensaje, ni siquiera el receptor.
- Esto podría usarse como "firma" de documentación electrónica.
- Pero **cifrar un mensaje por RSA es muy costoso** en tiempos de cómputo luego.....
- Para un mensaje dado **se calcula un "digesto"**. El digesto es un valor de tamaño fijo que surge de la aplicación de una función de tipo **HASH (ej: MD5, SHA-1)**.
- Estas funciones son rápido cálculo y son no se puede obtener el input original a partir del resultado hash.
- Ese *digesto se cifra utilizando la clave privada* del emisor y cualquier receptor *conociendo la clave pública* del receptor puede *verificar la autenticidad* del mensaje.

Criptografía

FIRMA DIGITAL

- Ejemplo de mensaje firmado usando PGP

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Aquí termina criptografía

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

iQA/AwUBSB0CSQaP1MLVR6eeEQJIVACfUGF1mORDtJF3hZEfTYF
xiRU3eCwAn3d/vNKStFEJu4YoDyb4zS9Ao/jA=Ib/Z

-----END PGP SIGNATURE-----

*** PGP SIGNATURE VERIFICATION ***

*** Status: Good Signature

*** Signed: 03/05/2008 09:24:41 p.m.

*** Verified: 03/05/2008 09:26:33 p.m.

*** BEGIN PGP VERIFIED MESSAGE ***

*** END PGP VERIFIED MESSAGE ***

Módulo de plataforma confiable



- Si se comprometen las claves, también se compromete toda la seguridad que se basa en ellas. Por lo tanto, es esencial almacenar las claves de una forma segura.
- La industria ha propuesto utilizar un chip llamado **TPM** (***Trusted Platform Modules, Módulos*** de plataforma confiables), un **criptoprocesador** que contiene almacenamiento no volátil para guardar las claves.
- El TPM **puede realizar operaciones criptográficas** como **cifrar bloques de texto** simple o **descifrar bloques de texto** cifrado en la memoria principal.

Módulo de plataforma confiable

- También puede verificar firmas digitales. Al realizar estas operaciones en un hardware especializado, se pueden realizar con más velocidad.
- El TPM es controversial, hay distintas partes que tienen ideas diferentes acerca de **quién va a controlar el TPM** y de quién se va a proteger.
- **Microsoft es defensor de ese concepto** y ha desarrollado Palladium, NGSCB y BitLocker para utilizarlo.
- En su punto de vista, el **sistema operativo controla el TPM** para evitar que se ejecute el software no autorizado.
- El “software no autorizado” podría ser software pirata (es decir, copias ilegales)
- Si el TPM está involucrado en el proceso de arranque, podría iniciar sólo los sistemas operativos firmados por el fabricante

Módulo de plataforma confiable

- Las industrias de la música y las películas también tienen mucho interés en el TPM, ya que se podría utilizar para evitar que pirateen su contenido.
- También podría abrir nuevos modelos de negocios, como rentar canciones o películas durante cierto periodo.
- TPM no ayuda a que las computadoras sean más seguras contra los ataques externos. En realidad se enfoca en el uso de la criptografía para evitar que los usuarios hagan algo que no esté aprobado de manera directa o indirecta por la entidad que controle el TPM.

Autenticación



AUTENTICACIÓN

- Las primeras minicomputadoras (por ejemplo, PDP-1 y PDP-8) no tenían un procedimiento de inicio de sesión, pero **con el esparcimiento de UNIX** en la minicomputadora PDP-11, era necesario tener uno.
- Los sistemas operativos de computadora personal más sofisticados como Linux y Windows Vista sí lo tienen.
- Las máquinas en las LANs corporativas casi siempre tienen configurado un procedimiento de inicio de sesión, de manera que los usuarios no lo puedan evitar.
- Por último, muchas personas hoy en día inician sesión (de manera indirecta) en computadoras remotas para realizar operaciones bancarias por Internet, compras electrónicas, descargar música y otras actividades comerciales.

AUTENTICACIÓN

Los métodos para autenticar usuarios cuando tratan de iniciar sesión se basan en uno de tres principios generales:

1. Algo que el usuario conoce. (password)
2. Algo que el usuario tiene. (magnetics key)
3. Algo que el usuario es. (biometrical)

Algunas veces se requieren dos de estos principios para una seguridad adicional.

Estos principios producen distintos esquemas de autenticación con distintas complejidades y propiedades de seguridad.

AUTENTICACIÓN

- En el mundo de las computadoras la palabra “hacker” es un término honorario que se reserva para los grandes programadores.
- Se utilizará el término en el sentido original y a las personas que tratan de irrumpir en los sistemas computacionales a los que no pertenecen les llamaremos **crackers**.

Autenticación mediante el uso de contraseñas

- La forma más utilizada de autenticación es requerir que el usuario escriba un nombre de inicio de sesión y una contraseña.
- La implementación más simple sólo mantiene una lista central de pares (nombre-inicio sesión, contraseña).
- El nombre de inicio de sesión que se introduce se busca en la lista y la contraseña introducida se compara con la contraseña almacenada. Si coinciden, se permite al usuario que inicie sesión; en caso contrario, se rechaza.
- **UNIX -> No muestra nada**
- **Window -> Asteriscos**

Autenticación mediante el uso de contraseñas

- En la tabla siguiente se muestra un inicio de sesión exitoso, con la salida del sistema en mayúsculas y la entrada del usuario en minúsculas.
- En la segunda columna se muestra un intento fallido de un cracker por iniciar sesión en el Sistema *A*. *Esto* permite al **cracker seguir probando** nombres de inicio de sesión hasta que encuentra uno válido.
- *En la tercer columna se muestra* un intento fallido de un cracker por iniciar sesión en el Sistema *B*. al cracker **siempre se le pide una contraseña** y no recibe ninguna pista sobre si el nombre de inicio de sesión es válido o no.

USUARIO: mitch
CONTRASEÑA: FooBar!-7
INICIO DE SESION
EXITOSO

USUARIO: carol
NOMBRE DE USUARIO
INVALIDO
USUARIO:

USUARIO: carol
CONTRASEÑA: yonose
INICIO DE SESION
INVALIDO
USUARIO:

Autenticación mediante el uso de contraseñas

- La mayoría de las computadoras **notebook** se configuran para requerir un nombre de usuario y una contraseña, de manera que su contenido esté protegido.
- Aunque eso es mejor que nada, la notebook puede iniciarse y de inmediato ir al programa de configuración del BIOS, oprimiendo SUPR, antes de que se inicie el sistema operativo.
- Una vez ahí, puede modificar la secuencia de arranque e insertar una memoria USB que contenga un sistema operativo completo para arrancar la computadora desde ahí.
- El disco duro se puede montar (en UNIX) o utilizar como la unidad *D:* (*Windows*).
- La mayoría de los BIOS permiten que el usuario proteja el programa de configuración con contraseña.

Autenticación mediante el uso de contraseñas

Cómo entran a la fuerza los crackers:

- Para entrar a la fuerza, la mayoría de los crackers se conectan a la computadora destino (por ejemplo, **a través de Internet**) y **prueban muchas combinaciones** (nombre de usuario, contraseña) hasta que encuentran una que funciona.
- **Usuarios suelen ser nombres simples.**
- Con uno de esos libros titulado ***4096 nombres para su bebé más una agenda telefónica llena de apellidos***, un cracker puede compilar con facilidad una lista computarizada de nombres de inicio potenciales apropiados para el país que va a atacar.

Autenticación mediante el uso de contraseñas

- **Hay que adivinar la contraseña -> FACIL!!.**
- Morris y Thompson (1979) realizaron un trabajo clásico sobre la seguridad de las contraseñas en sistemas UNIX.
- **Compilaron una lista de contraseñas probables:** nombres y apellidos, nombres de calles, nombres de ciudades, palabras de un diccionario de tamaño moderado, números de placas de automóviles y cadenas cortas de caracteres aleatorios.
- **Compararon su lista con el archivo de contraseñas** del sistema para ver si había coincidencias. Cerca de 86% de las contraseñas aparecieron en su lista. Klein (1990) obtuvo un resultado similar.

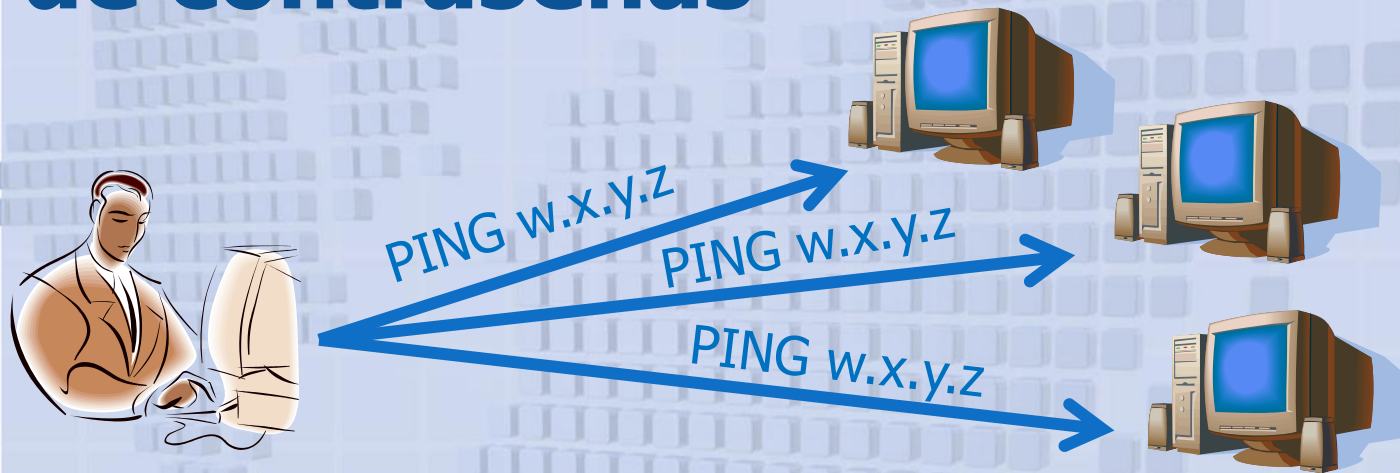
Autenticación mediante el uso de contraseñas

- Se usan **muchas contraseñas para todo => Fáciles.**
- ¿Realmente importa si las contraseñas son fáciles de adivinar? Definitivamente. En 1998, *un residente de Berkeley llamado Peter Shipley* había configurado varias computadoras sin uso, como **"war dialers", que marcaban los 10,000 números** telefónicos que pertenecían a una central telefónica.
- Después de **realizar 2.6 millones de llamadas, localizó 20,000** computadoras en el área de la bahía, 200 de las cuales no tenían ningún tipo de seguridad.
- Peter estimó que un cracker determinado podría irrumpir en casi 75% de las otras computadoras (Denning, 1999).

Autenticación mediante el uso de contraseñas

- Un cracker australiano trató de hacer lo mismo e irrumpió en una computadora de Citibank en Arabia Saudita, que le permitió obtener números de tarjetas de crédito y límites de crédito (en un caso, \$5 millones).
- Uno de sus crackers colegas también irrumpió en el banco y recolectó 4000 números de tarjetas de crédito (Denning, 1999).
- Si se utilizara dicha información con malicia, **el banco sin duda negaría con énfasis y vigor** que pudiera tener una falla, y afirmaría que el cliente debió haber divulgado la información.
- El “war dialing” ahora funciona de la siguiente manera. Cada computadora en Internet tiene una **dirección IP (de 32 bits)** que se utiliza para identificarla.

Autenticación mediante el uso de contraseñas



- *Luego el cracker puede tratar de entrar mediante el comando: **telnet w.x.y.z***
- *Si se acepta el intento de conexión el cracker puede empezar a probar nombres de inicio de sesión y contraseñas de sus listas.*
- *El cracker puede irrumpir y capturar el archivo de contraseñas, que se ubica en **/etc/passwd** en UNIX.*

Autenticación mediante el uso de contraseñas

- Un cracker se puede enfocar en una **empresa, universidad u organización gubernamental específica.**
- Por ejemplo, la Universidad de Foobar en *foobar.edu*. Para averiguar qué direcciones IP utiliza, todo lo que tiene que hacer es escribir **dnsquery foobar.edu**
- Conociendo los primeros 2 bytes de sus direcciones IP *es muy sencillo hacer ping en las 65,536 direcciones para ver cuáles aceptan conexiones telnet.*
- Por último se debe adivinar nombres de inicio de sesión y contraseñas
- Con igual probabilidad estadística es un proceso que se presta muy bien a la automatización

Autenticación mediante el uso de contraseñas

- **PUERTOS ABIERTOS**
- Muchas computadoras tienen una variedad de servicios disponibles por Internet.
- Cada uno de estos servicios está conectado a uno de los 65,536 **puertos asociados con** cada dirección IP.
- Cuando un cracker encuentra una dirección IP activa, con frecuencia ejecuta una **exploración de puertos para ver qué hay disponible.**
- **Algunos de los puertos pueden producir opciones adicionales para irrumpir en el sistema.**

Autenticación mediante el uso de contraseñas

- **Cliff Stoll**, un astrónomo en Berkeley, **detectó el inicio de sesión**, escrita por un cracker que ya había irrumpido en una máquina en el Lawrence Berkeley Laboratory (LBL).
- La cuenta uucp se utiliza para el tráfico de red entre máquinas y tiene poder de superusuario, el cracker se encontraba ahora en una máquina del Departamento de Energía de los EE.UU.

```
LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL
```

Autenticación mediante el uso de contraseñas

- Hay una **solución en UNIX**, para proteger contraseñas.
- El programa de inicio de sesión pide al usuario que escriba su nombre y su contraseña.
- **La contraseña se "cifra"** de inmediato al utilizarla como una clave para cifrar un bloque fijo de datos.
- En efecto, se ejecuta una función de una vía, con la contraseña como entrada y una función de la contraseña como salida.
- Después, el programa de inicio de sesión lee el archivo de contraseñas, que es sólo una serie de líneas ASCII, una por cada usuario, hasta que encuentra la línea que contiene el nombre de inicio de sesión del usuario.

Autenticación mediante el uso de contraseñas

- La ventaja de este esquema es que nadie, **ni siquiera el superusuario**, puede ver las contraseñas de los usuarios debido a que no se almacenan en formato descifrado en ninguna parte del sistema.
- **Ataque -> con diccionario de palabras**
- Lo hicieron Morris y Thompson. Estas contraseñas se cifran mediante el algoritmo conocido, a gusto del cracker.
- Ahora que está armado con una lista de pares (contraseña, contraseña cifrada), el cracker ataca.
- Lee el archivo de contraseñas (que tiene acceso público) y extrae todas las contraseñas cifradas. Luego las compara con las contraseñas cifradas de su lista.

Autenticación mediante el uso de contraseñas

- Morris y Thompson describieron una técnica que inutiliza el ataque casi por completo.
- Su idea es asociar a cada contraseña un número aleatorio de *n bits*, conocido como **salt**.
- ***El número aleatorio se modifica cada vez que se cambia la contraseña.***
- En el archivo de contraseñas, primero se concatenan la contraseña y el número aleatorio y después se cifran juntos. En el ejemplo se usa la función de cifrado, *e*.

Bobbie, 4238, e(Perro, 4238)
Tony, 2918, e(6%%TaeFF, 2918)
Laura, 6902, e(Shakespeare, 6902)
Mark, 1694, e(XaB#Bwcz, 1694)
Deborah, 1092, e(LordByron, 1092)

Autenticación mediante el uso de contraseñas

- Ahora considere las implicaciones para un cracker que desea crear una lista de contraseñas probables, cifrarlas y guardar los resultados *de manera que se pueda buscar* con facilidad cualquier contraseña cifrada.
- Si un intruso sospecha que *Perro* podría ser una contraseña, ahora tiene *que cifrar 2^n cadenas, como Perro0000, Perro0001, Perro0002 y así en lo sucesivo, e introducirlas todas en f . Esta técnica incrementa el tamaño de f por 2^n .*

Autenticación mediante el uso de contraseñas

Contraseñas **de un solo uso**

- La mayoría de los superusuarios exhortan a sus usuarios mortales para que cambien sus contraseñas una vez al mes.
- Lo más extremo es cambiar la contraseña en cada inicio de sesión; a estas contraseñas se les conoce como **contraseñas de un solo uso**.
- **Cuando se utilizan contraseñas de una sola vez, el usuario recibe un libro que contiene una** lista de contraseñas. En cada inicio de sesión se utiliza la siguiente contraseña en la lista.
- Si un intruso llega a descubrir una contraseña no le servirá de nada, ya que la próxima vez se debe utilizar una contraseña distinta.

Autenticación mediante el uso de contraseñas

- En la actualidad no se necesita un libro debido a un elegante esquema ideado por Leslie Lamport
- Este **permite a un usuario iniciar sesión en forma segura a través de una red insegura, mediante contraseñas de un solo uso.**
- A este método se le conoce algunas veces como **cadena de hash de una vía.**
- **El algoritmo se basa en una función $y = f(x)$ que tiene la propiedad de que dada x es fácil encontrar y , pero dada y es imposible calcular el valor de x .**
- El usuario selecciona una contraseña secreta y selecciona un entero n , el cual representa cuántas contraseñas de un solo uso puede generar el algoritmo.

Autenticación mediante el uso de contraseñas

- Como ejemplo, considere que $n = 4$.
- Si la contraseña secreta es s , la primera contraseña se obtiene al ejecutar la función de una vía n veces:
- Para la tercera contraseña se ejecuta f dos veces, y para la cuarta se ejecuta una vez.
- En general, $P_{i_1} = f(P_i)$. La clave a observar aquí es que dada cualquier contraseña en la secuencia, es fácil calcular la anterior en la secuencia numérica (tarea del servidor), pero imposible calcular la siguiente.
- Este método se usa para acceso remoto

$$P_1 = f(f(f(f(s))))$$

La segunda contraseña se obtiene al ejecutar la función de una vía $n - 1$ veces:

$$P_2 = f(f(f(s)))$$

Autenticación mediante el uso de contraseñas

Autenticación de reto-respuesta

- Hace que cada nuevo usuario proporcione una **larga lista de preguntas y respuestas** que posteriormente se almacenan en el servidor en forma segura.
- Las preguntas se deben elegir de tal forma que el usuario no tenga que anotarlas. Las preguntas posibles son:
 1. ¿Quién es la hermana de Eduardo?
 2. ¿En qué calle se encontraba su escuela primaria?
 3. ¿Qué enseñaba la Sra. Samponi?
- Al momento de iniciar sesión, el servidor hace una de estas preguntas al azar y comprueba la respuesta.
- No obstante, para que este esquema sea práctico se necesitan muchos pares de pregunta-respuesta.

Autenticación mediante el uso de contraseñas

Otra variación de **reto-respuesta** :

- **Cuando se utiliza, el usuario elige un algoritmo** al registrarse como usuario, como x^2 *por ejemplo*.
- *Cuando el usuario inicia sesión, el servidor le envía un argumento; por ejemplo, un 7, en cuyo caso el usuario escribe 49.*
- El algoritmo puede ser distinto en la mañana y en la tarde, en distintos días de la semana, y así en lo sucesivo.

Autenticación mediante el uso de contraseñas

Autenticación mediante el uso de un objeto físico

- El segundo método para autenticar a los usuarios es comprobar algún objeto físico que tengan, para este fin se han utilizado las llaves de puertas metálicas durante siglos.
- Hoy en día, el objeto físico es una tarjeta de plástico que se inserta en un lector asociado con la computadora. Por lo general, el usuario no sólo debe insertar la tarjeta, sino que también debe escribir una contraseña para evitar que alguien utilice una tarjeta perdida o robada.

Autenticación mediante el uso de contraseñas

Autenticación mediante biométrica

- El tercer método de autenticación mide las características físicas del usuario que son difíciles de falsificar.
- A estas características se les conoce como **biométricas**.
- Por ejemplo, un lector de huellas digitales o de voz conectado a la computadora podría verificar la identidad del usuario.
- Un sistema biométrico común consta de dos partes:
 1. inscripción
 2. identificación.

The background of the slide is a light blue grid. Overlaid on this grid is a world map where the landmasses are represented by a dense arrangement of small, light blue 3D cubes. The cubes are slightly offset from the grid lines, giving them a three-dimensional appearance. The text "Ataque desde el interior" is centered over the map.

Ataque desde el interior

ATAQUES DESDE EL INTERIOR

- Los “trabajos internos” podrían ser una categoría completamente distinta de problemas de seguridad.
- Los programadores y otros empleados de la empresa que operan la computadora que se debe proteger, o que crean software crítico, son los que ejecutan estos tipos de trabajos.
- Estos ataques son distintos de los externos, debido a que los usuarios internos tienen conocimiento y acceso especializados que los externos no tienen.

ATAQUES DESDE EL INTERIOR

Bombas lógicas

- En estos tiempos de externalización masiva, los programadores se preocupan comúnmente por sus trabajos.
- Para aquellos que se inclinan a favor del chantaje, una estrategia es crear una **bomba lógica**.
- **Este dispositivo es una pieza de código escrita por uno de los programadores de** una empresa (que en ese momento son empleados), y se inserta de manera secreta en el sistema de producción.
- Mientras que el programador le proporcione su contraseña diaria, no hará nada.
- No obstante, si el programador es despedido, el siguiente día (o la siguiente semana) la bomba lógica se activará.

ATAQUES DESDE EL INTERIOR

- En un caso famoso, la bomba lógica comprobaba la nómina; si el número personal del programador no aparecía en ella durante dos periodos de nómina consecutivos, se activaba.
- Al activarse la bomba tal vez se empiece a borrar el contenido del disco, eliminando archivos al azar, realizando cuidadosamente cambios difíciles de detectar en los programas clave o cifrando archivos esenciales.
- La empresa tiene elegir entre llamar a la o ceder al chantaje y volver a contratar al programador como “consultor” por una suma astronómica para que corrija el problema (y esperar que no plante nuevas bombas lógicas mientras lo hace).

ATAQUES DESDE EL INTERIOR

Trampas

- **Este problema se crea** mediante el código que inserta un programador de sistemas para evitar cierto chequeo de rutina.
- Por ejemplo, un programador podría agregar código al programa de inicio de sesión para permitir que cualquiera pueda iniciar sesión con el nombre "**zzzzz**", sin importar qué haya en el archivo de contraseñas.
- El código normal en el programa de inicio de sesión podría ser como el de la figura (a) siguiente. La trampa sería el cambio en la figura (b).
- Lo que hace la llamada a *strcmp* es *comprobar* si el nombre de inicio de sesión es "zzzzz". De ser así el inicio de sesión tiene éxito, sin importar qué contraseña se utilice.
- Si este código de trampa lo insertara un programador que trabaja para un fabricante de computadoras.....

ATAQUES DESDE EL INTERIOR

```
while (TRUE) {  
    printf("usuario: ");  
    obtener_cadena(nombre);  
    deshabilitar_eco();  
    printf("contrasenia: ");  
    obtener_cadena(contrasenia);  
    habilitar_eco();  
    v = comprobar_validez(nombre, contrasenia);  
    if (v) break;  
}  
ejecutar_shell(nombre);  
(a)
```

```
while (TRUE) {  
    printf("usuario: ");  
    obtener_cadena(nombre);  
    deshabilitar_eco();  
    printf("contrasenia: ");  
    obtener_cadena(contrasenia);  
    habilitar_eco();  
    v = comprobar_validez(nombre, contrasenia);  
    if (v || strcmp(nombre, "zzzzz") == 0) break;  
}  
ejecutar_shell(nombre);  
(b)
```

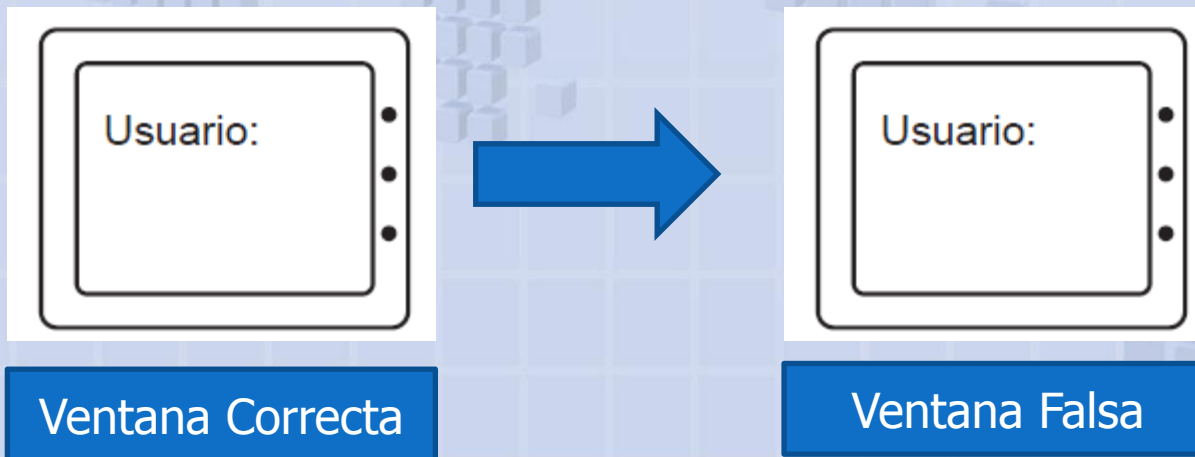

ATAQUES DESDE EL INTERIOR

- Una manera en que las empresas pueden evitar las trampas es hacer **revisiones de código** como una práctica estándar.
- Con esta técnica, una vez que un programador termina de escribir y probar un módulo, éste se comprueba en una base de datos de código.
- Cada cierto tiempo se reúnen los programadores en un equipo, y cada uno de ellos se para frente al grupo para explicar lo que hace su código, línea por línea.

ATAQUES DESDE EL INTERIOR

Suplantación de identidad en el inicio de sesión (Phishing)

- En este ataque interno, el perpetrador es un usuario legítimo que trata de recolectar las contraseñas de otras personas por medio de una técnica conocida como **suplantación de identidad en el inicio de sesión**.
- **Por lo general se emplea en empresas con muchas computadoras públicas en una LAN** utilizada por muchos usuarios.



ATAQUES DESDE EL INTERIOR

- La única manera real de evitar esto es hacer que la secuencia de inicio de sesión empiece con una combinación de teclas que los usuarios de programas no puedan detectar.
- Windows utiliza CTRL-ALT-SUPR para este fin.
- Si un usuario se sienta en una computadora y escribe primero CTRL-ALT-SUPR, el usuario actual se desconecta y se inicia el programa de inicio de sesión del sistema.
- No hay forma de evadir este mecanismo.

Bibliografía extra 1era Parte

- CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES,
MANUEL JOSÉ LUCENA LÓPEZ



**FIN PRIMERA PARTE
SEGURIDAD**