Introducción a la Seguridad y la Criptografía

F. J. Martínez Zaldívar

Departamento de Comunicaciones
ETSI Telecomunicación
Universidad Politécnica de Valencia

Comunicación de Datos II

Índice

1. **Introducción**
   - Seguridad
2. **Arquitectura de seguridad**
   - Servicios de seguridad
   - Mecanismos de seguridad
   - Ataques de seguridad
3. **Sistemas criptográficos**
   - Criptografía
   - Seguridad criptográfica
   - Criptosistemas
   - Algunas clasificaciones

Contextos de seguridad

- Evolución:
  1. Seguridad de la Información
  2. Seguridad en equipos informáticos
  3. Seguridad en redes (intranet/internet)
- Seguridad en internet:

  "Medidas para disuadir, prevenir, detectar y corregir violaciones de seguridad que implican la transmisión de información"

Algunas reflexiones

- La seguridad: uso de mecanismos complejos
- Los ataques: observan el problema de manera "*no convencional*"
- Contramedidas: necesidad no siempre obvia
- Mecanismos de seguridad: interlocutores con cierta *"información secreta"*. Cuestión:

  ¿Cómo se crea, distribuye y protege esta "información secreta"?

  (Complicación de los mecanismos de seguridad).
- Comparación con documentos físicos:

	Papel	**Fichero**
Copia	Detectable	Idéntico
Alteración	Rastros	No rastro
Autenticidad	Firma, sello,...	Autocontenida

1 Introducción
- Seguridad

2 Arquitectura de seguridad
- Servicios de seguridad
- Mecanismos de seguridad
- Ataques de seguridad

3 Sistemas criptográficos
- Criptografía
- Seguridad criptográfica
- Criptosistemas
- Algunas clasificaciones

- Define un enfoque sistemático para los requisitos de seguridad.
- La arquitectura de seguridad OSI (ITU-T X.800) se centra en servicios, mecanismos y ataques de seguridad

Definición

"Servicio que mejora la seguridad de los sistemas de proceso de datos y las transferencias de información de una organización"

- **Intención**: contrarrestar los ataques de seguridad
- Perspectivas:
  - **X.800**: servicio proporcionado por una capa de protocolo en relación a transferencias seguras.
  - **RFC 2828**: un servicio de proceso o comunicación que es provisto por un sistema para dar una clase específica de protección para recursos de un sistema.
- Los servicios de seguridad:
  - **Implementan políticas de seguridad**
  - Son **implementados por mecanismos de seguridad**

Relación de servicios

- Autenticación
- Control de acceso
- Confidencialidad
- Integridad de los datos
- No repudio
- Servicio de disponibilidad

Servicio de autenticación

“Se garantiza que la entidad comunicante es quien dice ser”

- **Autenticación de entidad par**: corroboración de la identidad de la entidad par en una asociación
- **Autenticación de origen de datos**: corroboración de la fuente de una unidad de datos (no interacción previa)

Servicio de control de acceso

“Capacidad de limitar y controlar el acceso a sistemas y aplicaciones”

Cada entidad que desee acceder al sistema debe ser identificada y autentificada.

Servicio de confidencialidad de los datos

"Evita la revelación no autorizada de los datos"

- **Confidencialidad con conexión**: en todos los datos de usuario de la conexión
- **Confidencialidad sin conexión**: en todos los datos de usuario en un bloque simple
- **Confidencialidad selectiva por campos** en cualquiera de los casos anteriores
- **Confidencialidad del flujo de tráfico**: protección de la información derivada de la observación del flujo de información

Integridad de los datos

"Se garantiza que los datos recibidos son exactamente como fueron enviados por la entidad autorizada (sin modificación, inserción, borrado o repetición)"

- **Integridad con conexión con recuperación**: integridad de todos los datos de usuario con detección de cualquier modificación, inserción, borrado o repetición, con intento de recuperación
- **Integridad con conexión sin recuperación**: idem que anterior, sin intento de recuperación
- **Integridad con conexión selectiva por campos**: idem que anteriores, pero en campos específicos
- **Integridad sin conexión**
- **Integridad sin conexión selectiva por campos**

No repudio

"Proporciona protección frente a la negación de que alguna de las entidades implicadas en una comunicación haya participado en toda o parte de la comunicación"

- **No repudio de origen**: prueba de que el mensaje fue enviado por el origen
- **No repudio de destinatario**: prueba de que el mensaje fue recibido por el destinatario

Servicio de disponibilidad

"Propiedad de un sistema de ser accesible y utilizable bajo demanda por una entidad autorizada, de acuerdo con las especificaciones de rendimiento del sistema"

(Ciertos ataques se centran en disminuir o anular esta disponibilidad —ataques por denegación de servicio—)

Definición

"Procedimiento diseñado para detectar, prevenir o recuperarse de un ataque de seguridad"

- Nosotros describiremos **técnicas criptográficas** como mecanismos de seguridad

Relación de mecanismos

- Cifrado
- Firma digital
- Control de acceso
- Integridad de datos
- Intercambio de autenticación
- Relleno de tráfico
- Control de *enrutamiento*
- Notarización

Descripciones I

- **Cifrado**: algoritmos matemáticos que transforman información a un formato no inteligible
- **Firma digital**: adición de datos o transformación a una unidad de datos que permite que el receptor verifique el origen y la integridad de dicha unidad de datos
- **Control de acceso**: control de derecho de acceso a recursos
- **Integridad de datos**: variedad de mecanismos que aseguran la integridad de una unidad de datos o un flujo de unidades de datos
- **Intercambio de autenticación**: asegura la identidad de una entidad mediante el intercambio de información

Descripciones II

- **Relleno de tráfico**: inserción de bits en huecos dentro de un flujo de datos para frustar el análisis de tráfico
- **Control de *enrutamiento***: permite la selección de rutas seguras para ciertos datos así como cambios en éstas cuando hay sospechas de brechas de seguridad
- **Notarización**: uso de un tercero confiable para asegurar ciertas propiedades en el intercambio de datos.

Relaciones entre servicios y mecanismos de seguridad

	Mecanismos							
Servicios	Cifrado	Firma digital	Control de acceso	Integridad de datos	Intercambio de autenti-cación	Relleno de tráfico	Control de enruta-miento	Notari-zación
Autenticación de de entidad par	×	×			×			
Autenticación de origen de datos	×	×						
Control de acceso			×					
Confidencialidad	×						×	
Confidencialidad de flujo de trafico	×					×	×	
Integridad de datos	×	×		×				
No repudio		×		×				×
Disponibilidad				×	×			

Ejemplos de uso de mecanismos y servicios de seguridad

- EFT: Electronic Funds Transfer (Banca)
- EDI: Electronic Document Interchange (Empresas)
- EC: Comercio electrónico
- Televisión digital
- Comunicaciones móviles
- Seguridad y protección de software
- Moneda electrónica (pagos anónimos)
- …

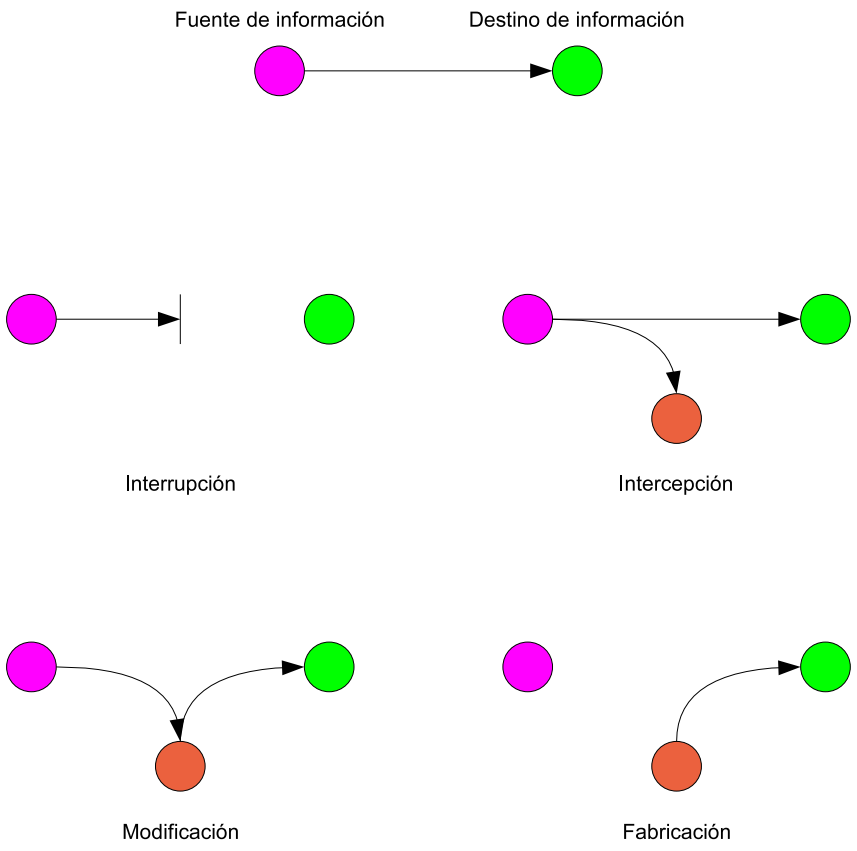
Definición

"Cualquier acción que compromete la seguridad de la información propiedad de cierta organización"

- ***Amenaza***: posible peligro que puede explotar una vulnerabilidad.
- **Ataque de seguridad**:
  - Amenaza hecha realidad
  - Agresión o asalto a un sistema de seguridad derivado de una amenaza inteligente.
  - Acto inteligente e intento deliberado de evadir servicios de seguridad y de violar la política de seguridad de un sistema (RFC 2828).

Categorías de ataques de seguridad

- Interrupción
- Intercepción
- Modificación
- Fabricación



Otra perspectiva: ataques pasivos y activos

- **Ataques pasivos**:
  - Revelación de contenido de mensajes (se puede evitar mediante cifrado)
  - Análisis de tráfico (origen y destinatario, volumen, instantes,...)
- **Ataques activos**: modificación del flujo de datos o creación de un falso flujo
  - Suplantación
  - Repetición o reactuación
  - Modificación
  - Denegación de servicio (degradación fraudulenta del servicio)

Ataques a mecanismos criptográficos

- Ataque a partir de **sólo texto cifrado** (análisis exhaustivo, ataque por fuerza bruta): probar todas las claves.
- Ataque a partir de **texto en claro conocido** : se conocen algunas parejas de texto en claro-texto cifrado.
- Ataque a partir de **texto en claro escogido** : se introduce texto en claro y se analiza el cifrado
- Ataque a partir de **texto cifrado escogido** : se introduce texto cifrado y se analiza el texto en claro descifrado.
- . . .

Ataques a protocolos criptográficos

- Ataque con **clave conocida**: el atacante conoce una clave e intenta conseguir más a partir de este conocimiento
- Ataque por **reutilización de protocolo**: “graba” y “reproduce” una comunicación
- Ataque por **suplantación**de personalidad: asume la identidad de un comunicante
- Ataque por **compilación de diccionario**: prueba con claves “típicas” guardadas en una base de datos
- Ataque por **búsqueda exhaustiva**: generación aleatoria de todas las claves
- Ataque por **intromisión**: introducción entre dos comunicantes
- . . .

1 Introducción
- Seguridad

2 Arquitectura de seguridad
- Servicios de seguridad
- Mecanismos de seguridad
- Ataques de seguridad

3 Sistemas criptográficos
- Criptografía
- Seguridad criptográfica
- Criptosistemas
- Algunas clasificaciones

Definición

Criptografía *es el "arte o técnica de escribir con clave o de un modo enigmático". (RAE)*

- Existencia desde principios de la humanidad.
- Conglomerado de disciplinas:
  - Teoría de la Información
  - Teoría de números
  - Complejidad algorítmica
  - Informática
  - Telecomunicaciones
  - Electrónica
  - ...
- Herramienta a utilizar para crear **mecanismos de seguridad**

Documentos fundamentales

- **1948**: Claude E. Shannon, [1]
- **1949**: Claude E. Shannon, [2]
- **???**
- **1976**: DES (Data Encryption Standard) [3]: cifrador simétrico estándar
- **1976**: Diffie, W., Hellman, M.F., [4]: primeros pasos en criptografía de clave asimétrica
- **1978**: Rivest, R., Shamir, A., Adelman, L., [5]: cifrador asimétrico

Acontecimientos

- Máquina **ENIGMA** (*Chiffriermaschinen Aktiengesellshaft*). Patente alemana de los años 20. Hitler la relega para usos militares.
- Segunda guerra mundial
  - Proyecto **ULTRA** en Bletchley Park (Reino Unido)
  - Criptoanálisis de ENIGMA
  - Bomba de **Turing** (Alan Turing)
  - Empleo del primer ordenador electrónico: **Colosus** (no ENIAC). Secreto hasta 1976.
- Ya en la actualidad:
  - Denuncias de puertas traseras en los sistemas operativos **Windows** a finales de los 90
  - Continuos problemas de seguridad en los navegadores **Netscape** e **Internet Explorer**, lenguajes como **Java**, etc.

Organizaciones

- **Echelon**: organización internacional de varios países para monitorización de comunicaciones electrónicas.
- **Enfopol**: algo parecido a nivel europeo
- Problema ético con estas organizaciones:
  - Intimidad personal
  - Control gubernamental absoluto
  - Solución intermedia: **TTP**(*Trusted Third Party*). Una entidad *TTP* posee todas las claves de las comunicaciones electrónicas secretas, accesibles sólo por vía judicial. Problema: **¿quén vigila al vigilante...?**

Disciplinas *Cripto**

- **Criptografía**: *arte*/técnica de cifrar
- **Criptoanálisis**: *arte*/técnica de romper los sistemas de cifrado
- **Criptología**: unión de **Criptografía**+ **Criptoanálisis**

Clases de seguridad criptográfica

- **Seguridad incondicional**
- **Seguridad teórica**
- **Seguridad computacional**

Seguridad incondicional

- Es imposible *romper* el sistema de cifrado
- Ocurre cuando $\mathrm{I}(L;C) = 0$. Si es así, entonces:

$$\mathrm{H}(K) \geq \mathrm{H}(C) \geq \mathrm{H}(L)$$

  Concepto de clave **OTP** (*One Time Pad*): clave tan larga como texto en claro
- Ejemplo: **cifrador Vernam**

- No son criptosistemas prácticos

Seguridad teórica

- Depende de longitud del texto a cifrar
- El sistema es **teóricamente seguro** si la longitud del texto en claro es inferior a la **longitud de unicidad** n_1:

$$n_1 = \frac{\mathrm{H}(K)}{R}$$

con R la redundancia del lenguaje.

Seguridad teórica: cálculo de la longitud de unicidad

***Ejemplo**: Calcúlese la longitud de unicidad de un sistema de cifrado que cifra mensajes compuestos por letras que pertenecen a un alfabeto de 28 letras, con una información media de 1,9 bit/letra, utilizando claves de 56 bits escogidas al azar.*

$$
\begin{aligned}
H(K) &= 56 \ \textit{bits} \quad \textit{(Hay un total de } 2^{56} \textit{ claves distintas)} \\
\lceil \log_2(m) \rceil &= \lceil \log_2(28) \rceil = \lceil 4{,}8 \rceil = 5 \ \textit{bits/letra} \\
R &= \lceil \log_2(m) \rceil - H(S) = 5 - 1{,}9 = 3{,}1 \ \textit{bits/letra} \\
n_1 &= \frac{H(K)}{R} = \frac{56}{3{,}1} = 18{,}06 \ \textit{letras}
\end{aligned}
$$

*Si el texto en claro tiene una longitud inferior a 18 letras, el mejor criptoanalista con los mejores medios dudaría **entre dos o más claves** con la misma probabilidad. Si el texto tuviera una longitud superior, se decantaría con más probabilidad por una de las claves.*

***Si se comprime el texto en claro,** $R \to 0$**, entonces** $n_1 \to \infty$

Seguridad computacional

Se puede calcular el tiempo necesario en hacer un ataque por texto cifrado (análisis exhaustivo o por fuerza bruta).

Si los recursos (tiempo, memoria, coste monetario, . . .) resultantes son extremadamente grandes:

- Puede disuadir a un criptoanalista de realizar un ataque por fuerza bruta
- Puede que después de transcurrido dicho tiempo, el secreto pierda importancia

y entonces el criptosistema se denomina **computacionalmente seguro**.

Seguridad computacional: cálculo del tiempo de ataque

Ejemplo:

- *Sistema de cifrado **DES** con claves de 56 bits*
- *Sistema de ataque: por búsqueda exhaustiva —ataque por fuerza bruta—. Capaz de descifrar a una velocidad de* 10^6 *descifrados/s*

$$
\begin{aligned}
10^6 \ \textit{descifrados} &\rightarrow 1 \ \textit{segundo} \\
2^{56} \ \textit{descifrados} &\rightarrow x \ \textit{segundos} \\
x &= \frac{2^{56}}{10^6} \ s \\
&= 7,2 \cdot 10^{10} \ s \\
&= 1,2 \cdot 10^{9} \ min \\
&= 20 \cdot 10^{6} \ h \\
&= 834 \cdot 10^{3} \ d \\
&= 2285 \ a
\end{aligned}
$$

En la práctica existen ataques por fuerza bruta mucho más eficientes que el mostrado aquí.

Definiciones

- **Texto en claro** M: texto o mensajes *legibles* a cifrar
- **Texto cifrado** C: texto *no legible* resultado de realizar el cifrado del texto en claro
- **Método de cifrado E**: familia de transformaciones de textos en claro en textos cifrados
- **Método de descifrado** $\mathbf{E}^{-1}$: familia de transformaciones de textos cifrados en textos en claro

Definiciones II

- **Clave** K: información que determina la transformación concreta a aplicar para cifrar (E_K) o para descifrar (E_K^{-1}). Algunos sistemas emplean claves distintas para cifrar y para descifrar.
- **Cifrador/Descifrador**: sistema o algoritmo o método que cifra/descifra
- **Criptosistema**:

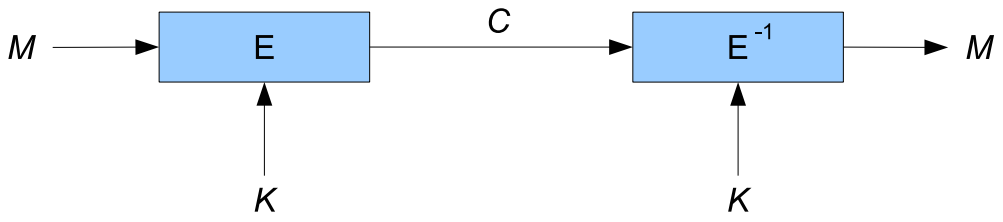
$$\begin{aligned} E_K(M) &= C \\ E_K^{-1}(C) &= E_K^{-1}(E_K(M)) = M, \ \forall M \end{aligned}$$

Criterio: qué es secreto

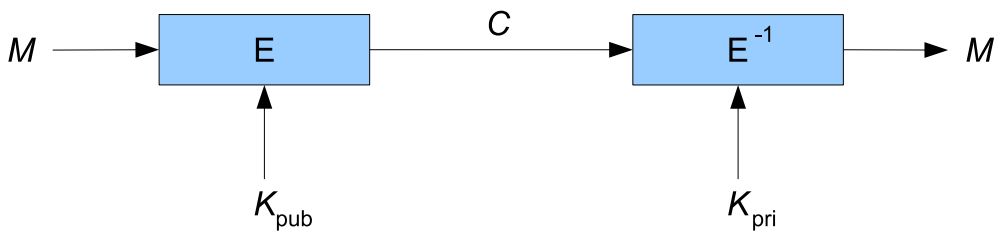
- **Criptografía clásica**: método y clave secretos
- **Criptografía moderna**: método conocido; lo único secreto es la clave

Criterio: claves de cifrado/descifrado

- **Criptografía simétrica (o de clave secreta)**: la misma clave para cifrar que para descifrar. Clave **secreta** K



- **Criptografía asimétrica (o de clave pública)**: claves distintas para cifrar que para descifrar.
  - Clave para cifrar: clave **pública** K_{pub}
  - Clave para descifrar: clave **privada** K_{pri}



Referencias I


Claude E. Shannon.
"A Mathematical Theory of Communication".
The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948


Claude E. Shannon.
"Communication Theory of Secrecy Systems".
The Bell System Technical Journal, Vol. 28-4, pp. 656-715, 1949


Data Encryption Standard (DES)
Federal Information Processing Standard Publicacion (FIPS PUB 46, 46-2, 46-3)
NBS/NIST 1977, 1983, 1988, 1993, 1998.

Referencias II


Diffie, W., Hellman, M.F.
"New Directions in Cryptography".
IEEE Transactions on Information Theory. 1976, IT-22, pp. 644–654.


Rivest, R., Shamir, A., Adelman, L.
"A method for obtaining digital signatures and public-key cryptography".
Communications of the ACM, 21, 1978, pp. 120–126


Stallings, W.
"Cryptography and Network Security. Principles and Practices"
Prentice Hall, 3rd. Edition , 2003