

SEGURIDAD DE LA INFORMACIÓN

TEMA 1

FUNDAMENTOS DE SEGURIDAD

Índice del tema

- Introducción
 - Ciclo de vida de la Seguridad
 - Modelo de escenario de Seguridad
- Servicios y mecanismos de seguridad
- Referencias bibliográficas

INTRODUCCIÓN

- Algunas definiciones de “Seguridad de la Información”

*“Information security is the **protection of information from a wide range of threats** in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities”*

ISO/IEC 17799: Code of practice for information security management

*“The **protection of information assets through the use of technology, processes, and training**”*

Microsoft Security Glossary

*“The ability of a system to **manage, protect, and distribute sensitive information**”*

Software Engineering Institute, Carnegie Mellon University

- Un error en la fase de análisis, diseño, desarrollo o implementación puede producir, a posteriori, un **fallo de seguridad**
 - También llamado **vulnerabilidad**
- Como consecuencia, se viola la **política de seguridad del sistema**, y este queda en peligro
 - En una red como Internet, con las dimensiones, números de hosts y número de usuarios actuales, el efecto devastador es exponencial



Ciclo de vida de la Seguridad

- La política de seguridad es el conjunto de reglas/requisitos que gobiernan el comportamiento del sistema, en lo que a seguridad se refiere
- Ejemplos de requisitos:

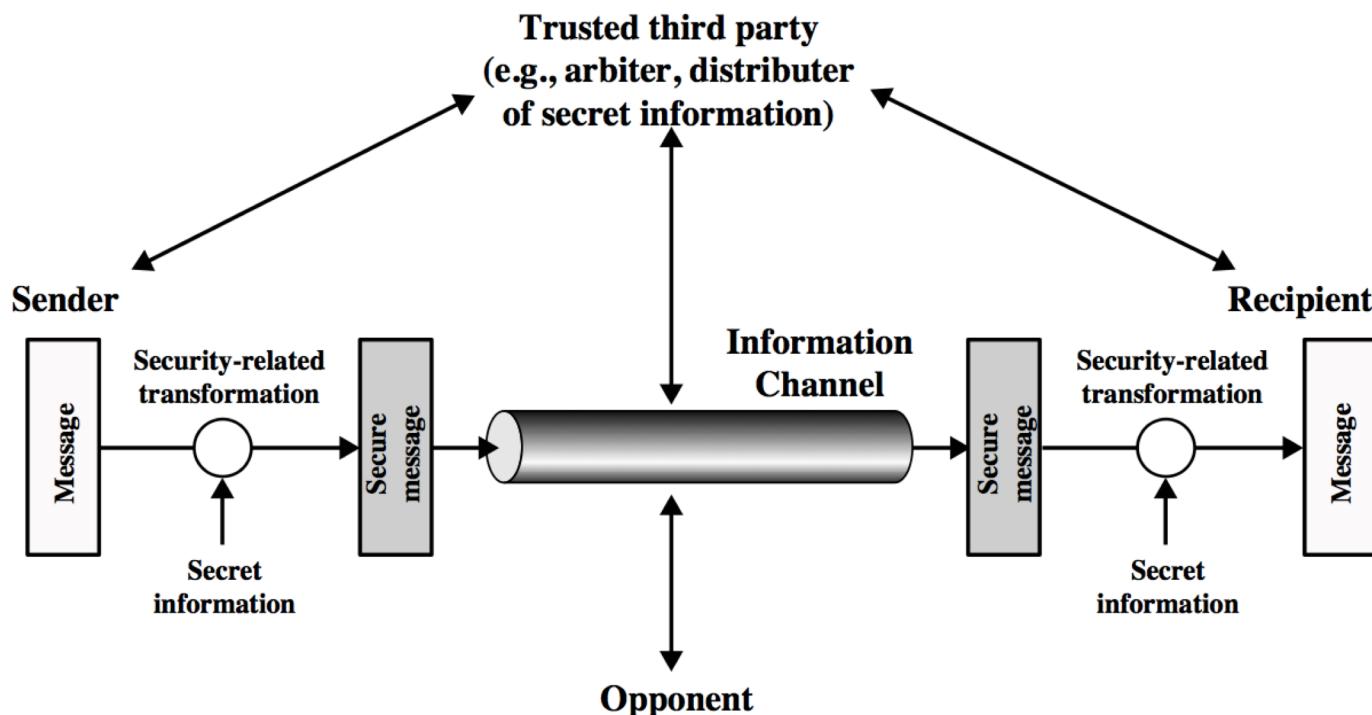
keeping information secret from all but those who are authorized to see it.
ensuring information has not been altered by unauthorized or unknown means.
corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
corroborating the source of information; also known as data origin authentication.
a means to bind information to an entity.
conveyance, to another entity, of official sanction to do or be something.
a means to provide timeliness of authorization to use or manipulate information or resources.
restricting access to resources to privileged entities.
endorsement of information by a trusted entity.
recording the time of creation or existence of information.
verifying the creation or existence of information by an entity other than the creator.
acknowledgement that information has been received.
acknowledgement that services have been provided.
a means to provide an entity with the legal right to use or transfer a resource to others.
concealing the identity of an entity involved in some process.
preventing the denial of previous commitments or actions.
retraction of certification or authorization.

Fuente: “Handbook of Applied Cryptography”

- La política de seguridad es sólo una de las fases del **ciclo de vida de la seguridad**. El modelo general de ciclo de vida se incluye en el estándar ISO-7498-2, y consta de cinco pasos:
 1. Definición de una **política de seguridad** que contiene una serie de requisitos genéricos de seguridad para el sistema
 2. Análisis de **requisitos de seguridad**, incluyendo el análisis de riesgos, y un análisis de los requisitos legales, gubernamentales y normativos
 - 3. Definición de los **servicios de seguridad necesarios** para satisfacer los requisitos de seguridad
 - 4. Diseño del sistema e implementación, así como la selección de los **mecanismos de seguridad** que van a proporcionarnos los servicios de seguridad definidos en la etapa anterior
 5. Administración y mantenimiento de la seguridad

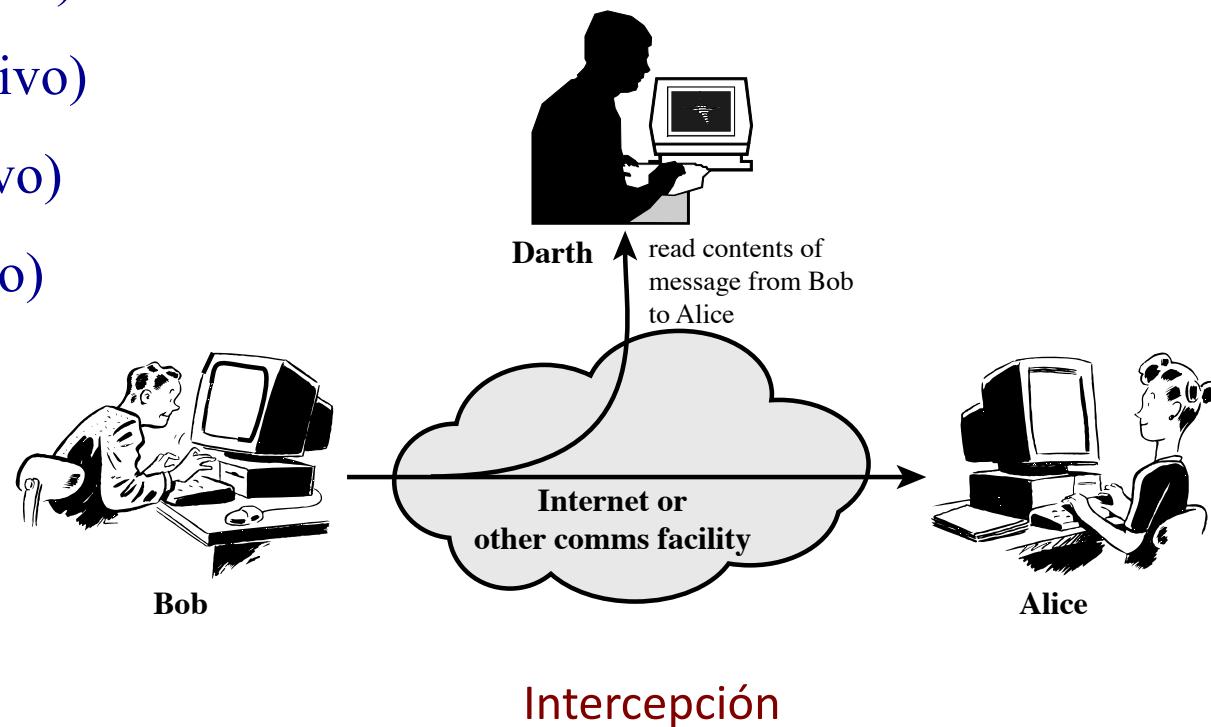
Modelo de escenario de Seguridad

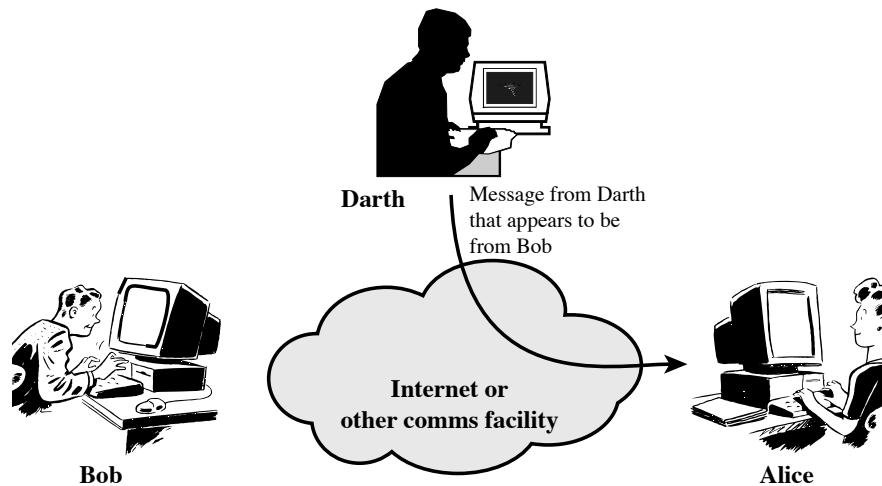
- Es necesario un escenario básico para empezar a razonar sobre:
 - las amenazas que pueden existir y los ataques que se pueden sufrir
 - las soluciones (servicios y mecanismos) de seguridad que podemos utilizar



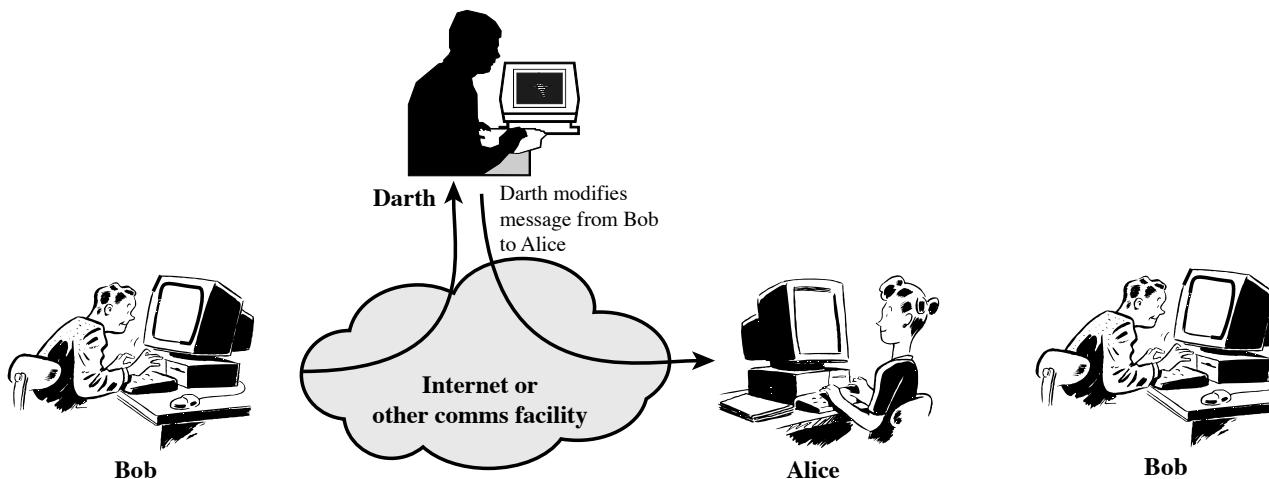
- ¿Quiénes pueden ser el emisor y el receptor en un escenario real?
 - Navegador web y Servidor web para transacciones electrónicas (por ejemplo, compra on-line)
 - Banca on-line (cliente y servidor)
 - Servidores DNS
 - Routers intercambiando tablas de enrutamiento
 - Dos usuarios en un chat, o enviándose e-mails, ...
 - Etc.

- Los ataques se pueden clasificar en **activos** y **pasivos**
- Más concretamente, se pueden considerar los siguientes cuatro tipos:
 - Intercepción (pasivo)
 - Modificación (activo)
 - Interrupción (activo)
 - Generación (activo)

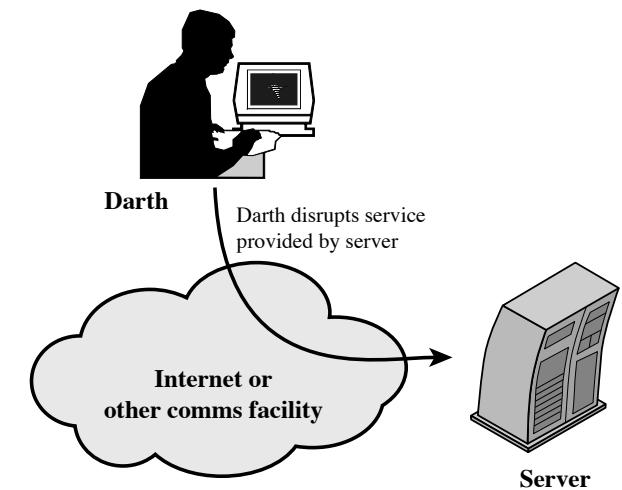




Generación



Modificación



Interrupción

SERVICIOS Y MECANISMOS DE SEGURIDAD

- Los servicios de seguridad ponen en funcionamiento las políticas de seguridad
- Algunas definiciones más precisas para este concepto:

“A processing or communication service that is provided by a system to give a specific kind of protection to system resources”

RFC 2828: Internet Security Glossary

“A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or the data transfers”

ISO 7498-2: Basic Reference Model -- Part 2: Security Architecture

ITU X.800: Security Architecture for Open Systems Interconnection for CCITT Applications

- Los estándares ISO 7498-2 e ITU X.800 dividen los servicios de seguridad en **cinco categorías**, y a partir de ahí distinguen **catorce servicios específicos**
- Las categorías son:
 - Confidencialidad de datos
 - Autenticación
 - Integridad de datos
 - No-repudio
 - Control de acceso

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality

The protection of all user data on a connection.

Connectionless Confidentiality

The protection of all user data in a single data block

Selective-Field Confidentiality

The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-flow Confidentiality

The protection of the information that might be derived from observation of traffic flows.

- **Otros ejemplos:**

- Coca-Cola no desea que se conozca su fórmula
- Las empresas quieren proteger sus tecnologías
- Los gobiernos quieren mantener en secreto sus planes

Se usa este servicio porque no deseo que otros usuarios conozcan:

- mails que envío o chats
- mi DNI o número de la Seg. Social
- mi número de tarjeta de crédito
- mis datos médicos
- las webs que visito, lo que compro y dónde viajo
- mi salario
- lo que voto
- mis gustos (música, cine, ...)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

- Se usa este servicio porque quiero estar seguro de que las entidades con las que interactúo son quienes dicen ser:
 - mi amiga Alice
 - mi médico
 - Amazon
 - ...
- Es decir, quiero tener garantías de que nadie está suplantando la identidad de mi interlocutor

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery

As above, but provides only detection without recovery.

Selective-Field Connection Integrity

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.



- Se usa este servicio porque no deseo que:
 - los mails o chats que envío o recibo sean modificados o falsificados
 - alguien borre (conscientemente o no) una parte de mis registros médicos
 - se puedan falsificar las órdenes que envío a mi banco para realizar pagos/cobros
 - alguien pueda modificar mi declaración de Hacienda cuando la relleno/envío por la Web

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin

Proof that the message was sent by the specified party.

Nonrepudiation, Destination

Proof that the message was received by the specified party.

- **Se usa este servicio porque deseo:**
 - tener pruebas de que ha ocurrido cierto evento:
 - envío de un ítem específico de información
 - recepción de un ítem específico de información
 - tener pruebas del instante exacto en que ha tenido lugar ese evento
 - tener pruebas de qué entidades han intervenido en el evento

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

- Se usa este servicio porque deseo:
 - Permitir el acceso a mis recursos de usuarios autorizados
 - Denegar acceso a mis recursos de usuarios desconocidos
 - Limitar y monitorizar el uso de cierto recurso
 - Definir reglas de acceso
 - Garantizar el uso de credenciales correctos de acceso
 - en forma
 - en tiempo

- Dentro de una comunicación, estos servicios de seguridad se pueden proporcionar en distintas capas del modelo de referencia OSI, como indica la siguiente tabla:

Service / Layer	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5/6	Layer 7
Entity authentication			Y	Y		Y
Origin authentication			Y	Y		Y
Access control			Y	Y		Y
Connection confidentiality	Y	Y	Y	Y		Y
Connectionless confidentiality		Y	Y	Y		Y
Selective field confidentiality						Y
Traffic flow confidentiality	Y		Y			Y
Connection integrity with recovery				Y		Y
Connection integrity without recovery			Y	Y		Y
Selective field connection integrity						Y
Connectionless integrity			Y	Y		Y
Selective field connectionless integrity						Y
Non-repudiation of origin						Y
Non-repudiation of delivery						Y

- Por otro lado, un **mecanismo de seguridad** proporciona soporte a un servicio de seguridad
- Definición:

*“A process (or a device incorporating such a process) that can be used in a system to **implement a security service** that is provided by or within the system”*

RFC 2828: Internet Security Glossary
- Los estándares ISO 7498-2 e ITU X.800 distinguen entre dos tipos de mecanismos de seguridad:
 - **específicos**: están implementados en una capa específica de la pila de protocolos
 - **ubicuos**: no son específicos de ninguna capa en particular

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
<p>May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.</p>	<p>Mechanisms that are not specific to any particular OSI security service or protocol layer.</p>
<p>Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.</p>	<p>Trusted Functionality That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).</p>
<p>Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).</p>	<p>Security Label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.</p>
<p>Access Control A variety of mechanisms that enforce access rights to resources.</p>	<p>Event Detection Detection of security-relevant events.</p>
<p>Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.</p>	<p>Security Audit Trail Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.</p>
<p>Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.</p>	<p>Security Recovery Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.</p>
<p>Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.</p>	
<p>Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.</p>	
<p>Notarization The use of a trusted third party to assure certain properties of a data exchange.</p>	

Mechanism Service	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y	.	.	Y	.	.	.
Data origin authentication	Y	Y
Access control service	.	.	Y
Connection confidentiality	Y	Y	.
Connectionless confidentiality	Y	Y	.
Selective field confidentiality	Y
Traffic flow confidentiality	Y	Y	Y	.
Connection Integrity with recovery	Y	.	.	Y
Connection integrity without recovery	Y	.	.	Y
Selective field connection integrity	Y	.	.	Y
Connectionless integrity	Y	Y	.	Y
Selective field connectionless integrity	Y	Y	.	Y
Non-repudiation. Origin	.	Y	.	Y	.	.	.	Y
Non-repudiation. Delivery	.	Y	.	Y	.	.	.	Y

- The mechanism is considered not to be appropriate.

Y Yes: the mechanism is considered to be appropriate, either on its own or in combination with other mechanisms.

Note – In some instances, the mechanism provides more than is necessary for the relevant service but could nevertheless be used.

- Resumiendo, un servicio de seguridad está basado de:
 - Un **protocolo de seguridad*** (opcional) es un conjunto de reglas y formatos que determinan la información que se intercambian dos (o más) entidades con objeto de proporcionar un servicio de seguridad
 - Los **mecanismos de seguridad** son las piezas básicas con las que se construyen protocolos de seguridad
 - Los mecanismos de seguridad se apoyan en **técnicas criptográficas**



Referencias bibliográficas

Bibliografía básica

- "User's Guide To Cryptography And Standards"
Alex W. Dent, Chris J. Mitchell
Artech House, 2004
- "Handbook of Applied Cryptography"
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone,
CRC Press, 1996

Bibliografía complementaria

- *ISO 7498-2*
 - Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, 1989.
- *RFC 2828*
 - RFC2828: Internet Security Glossary, R. Shirey, May 2000.
- *ITU-T X.800*
 - Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications, ITU, 1991.
- *ITU-T X.509*
 - Recommendation X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU, 2005