Tema 1: Fundamentos de seguridad

Introducción

¿Qué es la Seguridad de la Información?

Existen algunas definiciones:

- La seguridad de la información es la **protección de la información de un amplio rango de amenazas** para asegurar la continuidad de una empresa, minimizar el riesgo y maximizar el beneficio de las inversiones y oportunidades.
- La **protección de los activos de informació**n a través de tecnología, procesos y entrenamiento.
- La habilidad de un sistema de **gestionar, proteger y distribuir información sensible**.

Fallo de seguridad/vulnerabilidad: un error en la fase de análisis, diseño, desarrollo o implementación puede producir, a posteriori, un fallo de seguridad.

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. La **política de seguridad** es el conjunto de reglas/requisitos que gobiernan el comportamiento del sistema, en lo que ha seguridad se refiere.

Ciclo de vida de la seguridad

La política de seguridad es solo una de las fases del **ciclo de vida de la seguridad**. El modelo general de ciclo de vida se incluye en el estándar ISO-7492-2 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.
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.

El **emisor y receptor** pueden ser:

- Navegador web y servidor web para transacciones electrónicas.
- Banca online.
- Servidores DNS.
- Routers intercambiando tablas de enrutamiento.
- Dos usuarios en un chat, o enviándose emails…

Los **atacantes** se pueden clasificar en **activos y pasivos**. En realidad hay cuatro tipos:

- **Intercepción** (pasivo): lee mensajes que van de Alice a Bob.

- **Modificación** (activo): modifica mensajes que iban de Alice a Bob.
- **Interrupción** (activo): interrumpe el servicio proporcionado por un servidor.
- **Generación** (activo): envía mensajes simulando que Bob es el origen.

Servicios y mecanismos de seguridad

Servicios de seguridad

Los **servicios de seguridad** ponen en funcionamiento las políticas de seguridad. Algunas definiciones más precisas:

- Un **servicio de proceso o comunicación** proporcionado por un sistema **para aportar algún tipo de protección** a los recursos del sistema.
- Un servicio, proporcionado por una capa de sistemas abiertos en comunicación, que **asegura la adecuada seguridad del sistema** o transferencias de datos.

Los estándares ISO 7498-2 y ITU X.800 dividen los servicios en **cinco categorías** y a partir de ahí distinguen **catorce servicios específicos**. Las categorías son CIA^2N:

Confidencialidad de datos

Es la **protección de los datos** de su divulgación no autorizada.

Deseo de que otros usuarios no conozcan: emails que envío o chats, mi DNI o número de la seguridad social, número de tarjeta de crédito… Coca-Cola no desea que conozcan su fórmula, las empresas quieren proteger sus tecnologías, los gobiernos quieren mantener en secreto sus planes.

Autenticación

La seguridad de que **la entidad en comunicación es quien dice ser**.

Se usa este servicio porque quiero estar seguro de que las entidades con que interactúo son quienes dicen ser. Quiero tener garantías de que nadie está suplantando la identidad de mi interlocutor.

Integridad

La seguridad de que **los datos recibidos están exactamente iguales** que cuando fueron enviados por una entidad autorizada, no contienen modificación, inserción, eliminación o respuesta.

No deseo que los mails o chats que envío o recibo sean modificados o falsificados, alguien borre una parte de mis registros médicos, se puedan falsificar las órdenes que envío a mi banco para realizar pagos/cobros…

No repudio

Provee protección contra la **denegación**, por parte de una de las entidades involucradas en una comunicación, **de haber participado en toda o parte de la comunicación**.

Tener pruebas de que ha ocurrido cierto evento (envío de item, recepción de un item), tener pruebas del instante exacto en que ha tenido lugar ese evento, tener pruebas de qué entidades han intervenido en el evento, conocer cualquier información adicional específicamente asociada al evento…

Control de acceso (autorización)

La prevención del **uso no autorizado de un recurso**. Este servicio controla quién tiene acceso a un recurso, bajo qué condiciones puede ocurrir el acceso y qué pueden hacer aquellos que acceden al recurso.

Se usa 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 (forma y tiempo).

Dentro de una comunicación, estos servicios de seguridad se pueden proporcionar en distintas capas del modelo de referencia OSI:

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

Mecanismos de seguridad

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

- Un proceso (o un dispositivo incorporando dicho proceso) que puede ser usado en un sistema para **implementar un servicio de seguridad** proporcionado por o en el sistema.

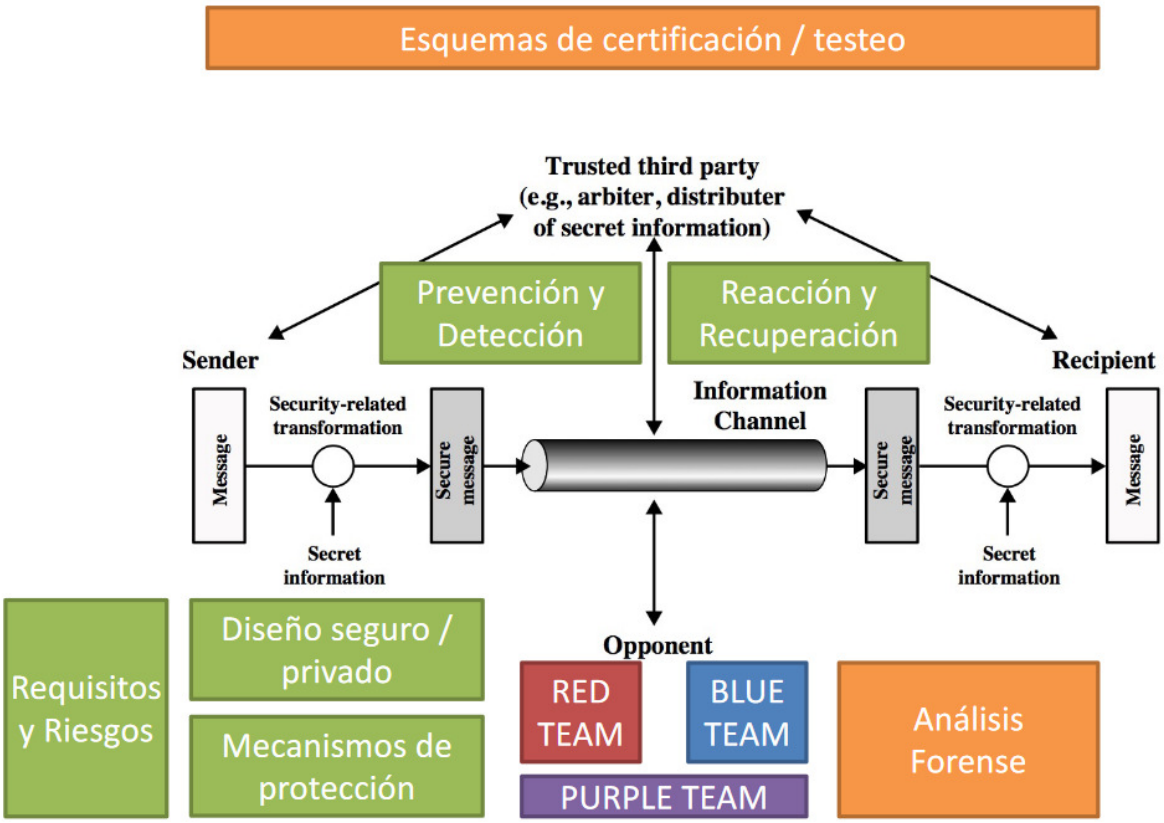
Los estándares distinguen entre dos tipos de mecanismos:

- **Específicos**: están implementados en una capa específica de la pila de protocolos. Ejemplos: cifrado, firma digital, control de acceso, integridad, autenticación, padding, control de enrutamiento, tercera persona de confianza (*Trusted Third Party*).
- **Ubicuos:** no son específicos de ninguna capa en particular. Ejemplos: controles de seguridad, etiqueta de seguridad, certificación, validación, simulación, detección y prevención de eventos, auditoría, forense, gestión de la confianza…

Resumiendo, un servicio de seguridad está basado en:

- Un **protocolo de seguridad:** 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.

El ecosistema de la seguridad



Organizaciones de estandarización:

- ISO (*International Organization for Standardization*)/IEC (*International Electrotechnical Commision*)
- ETSI (*European Telecommunications Standards Institute*)

Gobiernos, alianzas…

- NIST (*National Institute of Standards and Technology*)
- ENISA (*EU Agency for Cybersecurity*)
- INCIBE (Instituto Nacional de Ciberseguridad): para empresas y ciudadanos.
- CCN-CERT: para empresas públicas, organismos del estado, y otras empresas.