GUÍA DE ESTUDIO TEMA 6.

SEGURIDAD EN LAS COMUNICACIONES

OBJETIVOS

- La seguridad de las redes (de comunicaciones e industriales) es fundamental y está permanentemente comprometida.
- Para minimizar los efectos de los potenciales ataques, hay que conocer los factores de inseguridad de las redes y cómo solventarlos.
- Se presenta el concepto de política de seguridad, los tipos de defensas existentes y se terminará con la seguridad en los protocolos industriales.

FACTORES DE INSEGURIDAD

- **Red** =sistemas + dispositivos de comunicaciones + aplicaciones en ejecución ⇒ todos son importantes desde el punto de vista de la seguridad.

1. Problemas de seguridad física

- En sistemas servidores:
  - Por mala ubicación física ⇒ destrucción del equipo.
  - Por posibilitar acceso no permitido al S.O. = posibilitar el arranque mínimo del S.O. (secuencia de arranque físico especial sin contraseña).
- En sistemas clientes:
  - Generar ataques desde el cliente al sistema entero (incluidos los virus y troyanos).
  - Mala ubicación física ⇒ destrucción del equipo.
  - Acceso a los datos sensibles almacenados en el cliente.
  - Acceso no permitido al servidor desde el cliente.

2. Problemas generales en S.O. y aplicaciones

- Causas: son cada vez más extensos, más modulares y permiten más interconexiones.
- Vulnerabilidades por mala codificación:
  - Inevitables al 100% y continuos ⇒ muy graves.
  - Los fabricantes deben descubrirlos, anunciarlos y crear y distribuir los parches adecuados.
- Ingeniería Social: técnicas que aprovechan la buena voluntad o inconsciencia de la gente. Ej. "pishing" bancario.

3. Problemas comunes en S.O.

- Configuración insegura
  - De los ficheros de autorización:
    - Incorrecta protección del fichero ⇒ cracking
    - Nombres y contraseñas no seguros
    - Configuración incorrecta de la compartición de ficheros
  - De los permisos de sistemas de ficheros.
- Inexistencia de copias de seguridad.

4. Problemas comunes en aplicaciones

- Implementación incorrecta de protocolos:
  - Ataques de denegación de servicio. Ej. "ping de la muerte"⇒ desbordamiento de memoria de la víctima (recibe ping).
  - Del protocolo SMTP: responsable de mensajes de correo.
  - Puertas falsas: código que sólo conoce su autor y que permite el acceso a cualquier sistema o aplicación.
- Diseño peligroso de protocolos y aplicaciones:
  - Aplicaciones sin control de autenticación: TFTP, SMTP, DNS, SNMP y RIP.
  - El mecanismo de conexión TCP/IP:
    - "smurf": genera tráfico broadcast suplantando la identidad de una víctima que aparece como emisor y recibe respuestas de toda la red, bloqueándose.
    - "SYN FLOOD": colapsa al servidor enviándole falsas peticiones de conexión que llenan su tabla de conexiones embriónicas y le impiden atender las conexiones reales.
  - Otros peligros potenciales se encuentran en macros, facilidades de uso (autoarranques), los applets de Active X y las cookies.

4. Problemas comunes en aplicaciones

- Incorrecta selección de protocolos de aplicación: en casi todos los casos existen alternativas más seguras
- Otros:
  - Virus y caballos de Troya
  - Ataques combinados. Ej. loki o ataques de denegación de servicio distribuidos.

Inseguro	Seguro
Telnet	SSH
http	https
FTP	SFTP
RIP	RIPv2, OSPF, EIGRP

5. Inseguridad en dispositivos de comunicaciones

- Afecta fundamentalmente a conmutadores (nexo entre dispositivos de la misma red IP) y encaminadores (unión de redes).
- Efectos de los ataques a estos elementos:
  - Aprovechando vulnerabilidades ⇒ parar la red o mal reparto del ancho de banda
  - Mala ubicación física ⇒ perder la cohesión de la red o acceso no autorizado.
  - Gestión remota con protocolos no seguros ⇒ reconfiguración no deseada.
  - Configuraciones de seguridad incorrectas ⇒ ataques
  - Protocolos de encaminamiento no fiables ⇒ encaminamiento incorrecto

SOLUCIONES

PROBLEMAS DE SEGURIDAD	DEFENSAS POSIBLES
Inseguridad Física	Establecer perímetro de seguridad
Vulnerabilidades del software	Método seguro de actualización del software
Pérdida de datos sensibles	Política correcta de copias de seguridad
Ataques de acceso no permitido a sistemas	• Selección de contraseñas • Tarjetas token • Autenticación AAA • Firma digital • Sistemas biométricos
Virus, troyanos, *spyware*, etc.	Sistemas antivirus y antispyware actualizados
Ingeniería social	Formación básica para usuarios
Problemas de seguridad en redes en general	• Cortafuegos • Sistemas de detección de intrusiones • Detectores de vulnerabilidades

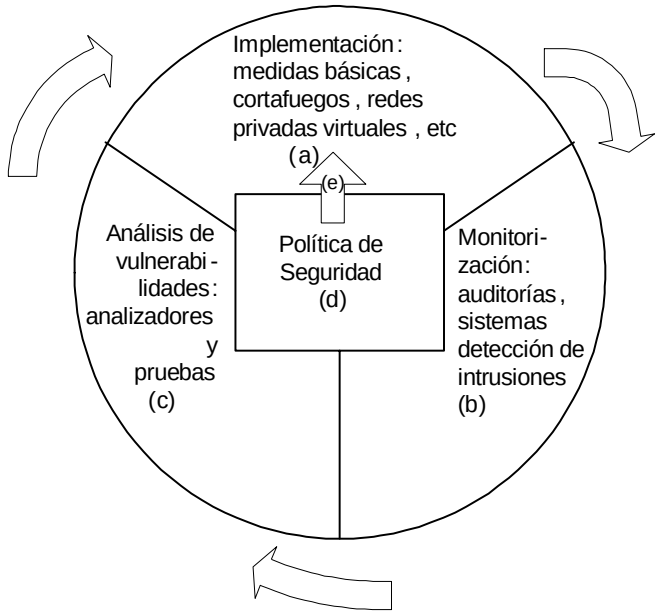
POLÍTICA de SEGURIDAD para REDES

- Serie de sentencias formales, o normas, que deben ser cumplidas por todas las personas de una organización que dispongan de acceso a cualquier información, datos o tecnología que sean propiedad de la organización.
- Debe poderse implantar sin alterar la actividad habitual.
- Debe entenderse fácilmente.
- Debe hacerse cumplir y definirse claramente los distintos grados de responsabilidad.
- Debe cumplir la legislación (LOPD y LSSICE).
- Debe incluir mecanismos de respuestas a incidentes y de actualización de la propia política.
- Deben participar grupos de técnicos, de negocio, legales e incluso consultores externos

POLÍTICA de SEGURIDAD para REDES

- Debe dar respuesta a:
  - Qué se quiere proteger
  - Quiénes son los potenciales atacantes
  - Cómo se usan los sistemas y herramientas seleccionados
  - Disponibilidad económica

- Las etapas del proceso de seguridad son:



DEFENSAS NO CRIPTOGRÁFICAS

1. CORTAFUEGOS

- Todo tráfico entre las dos redes debe pasar a través del cortafuegos.
- Solo el tráfico autorizado por el cortafuegos debe dejarse pasar.
- El cortafuegos debe ser completamente inatacable.

👍 Sitio habitual para implantar la política de seguridad	👎 Puede relajar la implantación de medidas en otros dispositivos
👍 Soporta técnicas de autenticación	👍 Pueden requerir compleja configuración
👍 Buen sitio para centralizar alarmas y registros de auditoría de tráfico	👍 Pueden ser un cuello de botella
👍 Necesitan poca administración de usuarios	👍 Ningún cortafuegos puede evitar ataques originados en la parte protegida de la red y cuyo objetivo reside en la misma parte.

- Tecnologías en cortafuegos
  - Basadas en **filtros de paquetes:** Operan al nivel IP y de transporte. Filtran mensajes IP, dejándolos pasar o no, a través de cada interfaz, basándose para ello en los valores de algunos de los campos más importantes de las cabeceras IP, TCP y UDP de cada mensaje.
  - Basada en **servidores *proxy*** por cada uno de los protocolos que se quiere filtrar. Nivel de red.
  - Basada en inspección dinámica de tráfico por sesión y completa o "***stateful inspection***". En estos cortafuegos se obtiene, almacena y manipula información de todos los niveles de comunicación. Esta información, completa para cada mensaje y gestionada dinámicamente, se utiliza para decidir si se permite el paso del tráfico o no.
  - Muchos cortafuegos combinan varias tecnologías.
  - Además existen cortafuegos personales: una aplicación que se instala en el ordenador que se quiere proteger y se configura de manera que le protege individualmente frente a los posibles ataques provenientes del resto de la red.

2. SISTEMAS de DETECCIÓN de INTRUSIONES

- Una intrusión puede definirse como un mensaje, o serie de mensajes, que implementan, de muy diferentes formas posibles, ataques a sistemas o dispositivos en la red.
- Un sistema de detección de intrusiones o IDS suele ser un sistema en la red especializado en detectar y parar ese tipo de intrusiones.
- Métodos:
  - Detección de anomalías: basadas en perfiles creados previamente para todo tipo de tráfico aceptable.
  - Detección de firmas de ataque: basadas en búsquedas de patrones creadas a partir de ataques previos.

3. DETECCIÓN de VULNERABILIDADES

- Programa que busca, de manera automatizada, vulnerabilidades y debilidades de entre una gran lista que conoce y que se actualiza.
- Su resultado final es un informe sobre los problemas encontrados y qué se debe hacer para subsanarlos.
- También deben informar de todo aquello que no son capaces de analizar.

DEFENSAS CRIPTOGRÁFICAS

- **Autenticación:** propiedad que permite demostrar que uno es quien dice ser.
- **Privacidad:** propiedad que permite que un mensaje solo sea legible, entendible, por los dos extremos origen y destino; si es interceptado en un punto intermedio no es legible.
- **Integridad:** propiedad que permite garantizar que un mensaje enviado no ha sido modificado en su transito al sitio de destino o detectar si ha sido modificado.
- Una vez elegidas las propiedades deseadas para el sistema, se cuenta con una serie de algoritmos utilizados por protocolos criptográficos cuya selección determinará el tipo de sistema que se deba utilizar. Los algoritmos deben ser públicos (estandarizados).

1. Un algoritmo de clave privada (o de **criptografía simétrica**) utiliza una única clave, que sirve tanto para cifrar un texto como para descifrarlo, clave compartida únicamente entre los participantes del sistema.

- 👍 Más rápidos que los algoritmos de clave pública y son los usados tradicionalmente en sistemas hardware de cifrado.
- 👎 Necesidad de un sistema de distribución de la clave muy seguro

2. Las **funciones de una sola vía** basadas en enviar el mensaje convertido mediante una función hash.

- Su uso más habitual es el de garantizar la integridad. Las más utilizadas dependen, para mayor seguridad, de una clave privada compartida
- El procedimiento es simple: se envía el mensaje junto con su *hash* y el receptor, al recibir el mensaje, separa éste del *hash*, aplica la misma función empleada en el origen del mensaje y compara el *hash* resultante. Si no son iguales, el mensaje ha sido modificado en el camino.

3. Un algoritmo de criptografía de clave pública (o de **criptografía asimétrica**) se basa en las siguientes características:
   - Cada participante del sistema genera de manera simultánea, mediante el algoritmo, una pareja de claves íntimamente relacionadas entre sí, la clave pública del participante y la clave privada del participante.
   - La clave pública puede ser conocida por todos los participante sin problema alguno de seguridad.
   - La clave privada sólo es conocida por el propio participante.
   - Cualquiera que conozca la clave pública del participante A puede cifrar mediante ella un mensaje y enviarlo a la red, pero únicamente el participante A podrá descifrarlo pues esta operación sólo se puede realizar mediante la clave privada de A
   - Presenta un problema de gestión de claves para garantizar la autenticación de la clave pública.

- En el modelo de firma digital más extendido, el basado en el algoritmo RSA de criptografía pública:
  - El emisor genera un *hash* del mensaje, H1, mediante una función de una sola vía previamente pactada con el receptor.
  - Este H1 se cifra mediante RSA usando la clave privada del emisor y el resultado es lo que se conoce como firma digital, FD, del mensaje, que se adjunta al mensaje. Nótese que la firma digital cambia cada vez que se envía un mensaje diferente.
  - Cuando el mensaje llega a su destino, el receptor separa el mensaje de la firma digital.
  - Calcula el *hash* del mensaje mediante la función pactada y obtiene un *hash* H2 y descifra la firma digital mediante RSA y la clave pública del emisor obteniendo H1, el *hash* original.
  - Si H1 y H2 son idénticos, puede afirmarse que el mensaje fue enviado por el propietario de la clave pública usada (autenticación) y que no fue modificado en transito (integridad).

4. Protocolos criptográficos: SSL, IPSec y otros

- Un protocolo criptográfico es simplemente un protocolo de comunicaciones que, como parte de sus funciones, usa métodos criptográficos
- Protocolo **SSL**. Propiedades:
  - **Autenticación**, el estándar del protocolo la marca como opcional, pero se debe utilizar siempre que se pueda. Se utiliza normalmente RSA.
  - **Privacidad**
  - **Intercambio seguro de claves:** para asegurar las propiedades anteriores.
- Protocolo **TLS**: mejora del anterior.
- Protocolos **IPSec**:
  - Permiten comunicaciones seguras a distintos niveles entre dos puntos cualesquiera de una red IP.
  - Ofrece integridad, autenticación del origen, privacidad y protección contra repetición de mensajes
  - Tres protocolos independientes:
    - **AH** que proporciona integridad y autenticación.
    - **ESP** proporciona privacidad y opcionalmente integridad y atenticación.
    - **ISAKMP** administración e intercambio seguro de todas las claves.
  - Procedimiento: previamente hay un intercambio de mensajes emisor-receptor para crear una Asociación de Seguridad (= resultado de pactar los algoritmos que se van a utilizar), después se autentican y completan la Asociación para iniciar la comunicación.

REDES PRIVADAS VIRTUALES

- Una red privada virtual (RPV) es una conexión segura entre dos o más partes de una red privada, creada a través de una red pública. Tiene tres usos principales:
  - **Intranet:** sirve para conectar piezas disjuntas de la misma red privada.
  - **Extranet:** Parte de las redes disjuntas unidas mediante la RPV no pertenecen a la misma organización sino a otra o a otras que colaboran con la primera.
  - Como una **red de usuarios móviles** de una organización para proporcionar una conexión segura con la red.
- Utilizan SSL, IPSec o MPLS.
- También otros componentes:
  - Componente de autenticación por usuario o de control de acceso.
  - Componente de auditoría y registro de actividades, para asegurar el funcionamiento correcto y capacidad de recuperación.
  - Componente de calidad del servicio.

SEGURIDAD EN PROTOCOLOS INDUSTRIALES

- **OPC**: define una serie de interfaces opcionales de seguridad para los objetos OPC que sólo detallan controles de acceso y no entran en confidencialidad ni integridad. S
  - Se basan en el modelo de seguridad de Windows de Microsoft.
  - Un servidor OPC puede implementar uno de entre tres posibles niveles de seguridad:
    - Seguridad deshabilitada: no se obliga a cumplir ningún criterio de seguridad.
    - Seguridad DCOM: permisos para un cierto conjunto de clientes.
    - Seguridad OPC: El servidor OPC sirve como monitor de referencia para controlar el acceso a objetos de seguridad específicos que gestiona el servidor.
- **MMS:** norma del nivel de aplicación para la comunicación mediante mensajes a y desde dispositivos o PLCs en un entorno de fabricación gestionada informáticamente.
  - Comunicaciones cliente/servidor y entre iguales.
  - Define una serie de características de control de acceso basadas en una autenticación simple mediante contraseñas.
  - No se dice nada sobre la confidencialidad o la integridad.
  - La red de comunicación es Ethernet.
  - La mayor parte de las implementaciones actuales asumen la pila de comunicaciones TCP/IP.
  - Se puede incluir seguridad de cifrado mediante protocolos SSL o IPSec.

SEGURIDAD EN PROTOCOLOS INDUSTRIALES

- **IEC 61850:** especifica modelos de datos, servicios, protocolos y formatos de datos para la automatización de subestaciones de las redes de potencia eléctrica.
  - Las características de seguridad se basan en las opciones de control de acceso, basado en la identificación del nodo, y en la autenticación de usuario y de control de acceso al sistema para usuarios... junto a la asociación de protocolos de comunicaciones.

- **IICP:** estándar para la comunicación en redes de área amplia entre centros de la red de transmisión eléctrica. Es similar a la norma de OPC pero no está ligada a ningún sistema operativo en particular.
  - La mayor parte de las implementaciones del ICCP funcionan sobre MMS y TCP y, como consecuencia, debe implementarse las funciones de control de acceso de MMS.
  - Para proteger la comunicación entre centros se recomienda el uso del protocolo SSL.
  - Se define también la encapsulación de mensajes SSL en paquetes ISO, no TCP.

SEGURIDAD EN PROTOCOLOS INDUSTRIALES

- **Normas y organismos involucrados en el desarrollo de políticas de seguridad para entornos de comunicaciones industriales:**
  - IEEE 1402: Es la norma de seguridad de subestaciones, especialmente dedicada la seguridad física.
  - *Process Control Security Requirements Forum* (PCSRF): Puesta en marcha por el NIST, tiene como objetivo crear conjuntos de normas de seguridad en la creación de nuevos sistemas de control de procesos. Ha desarrollado ya normas para sistemas DCS o SCADA como la SCP-ICS (*Industrial Control System Security Capabilities Profile*) y la SPP-ICS (*Industrial Control System System Security Profile*).
  - ISA SP99: El comité SP99 del ISA (*Instrumentation Systems and Automation*), conocido como "*MAnufacturing and control systems security*", intenta crear documentos de guía para introducir la seguridad informática en los sistemas de control automatizado. Tiene ya dos guías publicadas sobre seguridad en sistemas PLCs, SCADA, etc.
  - IEC TC65: El subcomité técnico 65C del IEC lleva desde 2004 trabajando sobre normas de seguridad para buses de campo y otras redes de comunicación.

CONCLUSIONES

- Los problemas de seguridad más habituales que suelen aparecer en las redes de comunicaciones industriales son, esencialmente, los mismos de cualquier red actual de ordenadores.
- Así resulta importante conocer los problemas y sus soluciones, así como definir, implantar y actualizar continuamente una política de seguridad adecuada.
- La estandarización de soluciones garantiza que éstas estén probadas y avaladas por investigaciones previas y que tienen un control de calidad.