TEMA 1

Fundamentos de Seguridad

Índice

- Amenazas y vulnerabilidades
- Ciclo de vida de software de seguridad
- Evaluación de la seguridad
- Normativas de seguridad

AMENAZAS Y VULNERABILIDADES

Amenazas y vulnerabilidades

- Una **Amenaza** es un evento que puede producir un daño material o inmaterial en el sistema.
  - El primer paso para protegerse ante posibles amenazas es saber reconocerlas.
- Una **Vulnerabilidad** o fallo de seguridad, es todo aquello que provoca que nuestros sistemas informáticos funcionen de manera diferente para lo que estaban pensados, afectando a la seguridad de los mismos.
  - En un plano más formal el término vulnerabilidad, se puede definir como la posibilidad de que una amenaza se materialice.
- Tres elementos principales a tener en cuenta: **Software**, **Comunicaciones** y **Usuarios**

Software confiable vs. Malware

- Una de las mayores amenazas es el propio sistema operativo.
  - Omisión de parches de seguridad, backdoors, bugs, etc.
- El Malware es realmente efectivo cuando se puede ejecutar sobre un S.O. sin modificar.

https://nakedsecurity.sophos.com/es/2013/12/03/d-link-patches-joels-backdoor-security-hole-in-its-soho-routers/

Código malicioso (Malware)

- Programas creados para ***manipular*** el normal funcionamiento de los sistemas, sin el ***conocimiento*** ni ***consentimiento*** de los usuarios.
- Ejemplos:
  - Virus
  - Gusanos
  - Troyanos
  - Ransonware
  - Keyloggers
  - …

https://www.osi.es/es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus

Malware

- Un **código malicioso** es un conjunto de instrucciones que comprometen la seguridad de un sistema. Ejemplo:

  El siguiente script UNIX tiene por nombre “ls”:

```
cp /bin/sh /tmp/.xxsh
chmod o+s,w+x /tmp/.xxsh
rm ./ls
ls $*
```

- Tanto los virus, gusanos, como los troyanos son herramientas efectivas con las que atacar sistemas informáticos.

Virus Informáticos

Es un programa que se **inserta** en uno o más archivos y puede realizar algunas **acciones** en el sistema que lo hospeda. Suele seguir el siguiente esquema de funcionamiento:

```
if condiciones_propagación then begin
   for conjunto_archivos do begin
     if not archivo_ya_infectado then begin
       determinar donde colocar las instrucciones víricas
       copiar instrucciones desde virus_inicio hasta virus_fin
       modificar archivo para que pueda ejecutar el virus
     end;
   end;
end;
realizar algunas acciones
goto inicio_programa_infectado
```

Tipos de Virus Informáticos

- **Infecciones en el sector de inicio**. Un código insertado en el sector de inicio es ejecutado al acceder el sistema al mismo. El código real correspondiente al sector de inicio es movido a otra ubicación del disco, posiblemente otro sector.

- **Infecciones en archivos ejecutables**. Es un tipo de virus que infecta archivos ejecutables

Tipos de Virus Informáticos

- **TSR.** Siglas de "Terminate and Stay Resident", definen un tipo de virus que **permanece activo** en memoria después de que la aplicación que lo hospeda haya **terminado**.

- Pueden infectar tanto el sector de inicio como las aplicaciones.

- Los virus no TSR únicamente se ejecutan cuando la aplicación que lo hospeda se inicia y finalizan su ejecución cuando dicha aplicación lo hace.

Tipos de Virus Informáticos

- **Virus Stealth.** Este tipo de virus se caracteriza por **esconder** la infección de archivos.
  - Interceptan las llamadas al sistema que acceden a los archivos. Controlan aspectos como: atributos, datos del archivo y su ejecución.
- **Virus cifrado.** Intentan hacer frente a los antivirus que **reconocen** las cadenas víricas que se adhieren a las aplicaciones.
  - Para ello, cifran todo el código vírico excepto una pequeña **rutina de descifrado**. Ej: 1260

Tipos de Virus Informáticos

- **Virus Polimórficos.** Un virus polimórfico es aquel que **cambia de forma** cada vez que se inserta en una aplicación. Muy relacionados con los virus cifrados donde además de emplear una **clave de cifrado distinta** cambian las **instrucciones** de descrifrado para que este proceso no pueda ser detectado por un antivirus.

- Suelen emplear operaciones que no realizan ninguna variación sobre el algoritmo, como por ejemplo: “add 0 to operand”, “or 1 with operand”, “no operation” y “subtract 0 from operand”.

- El polimorfismo puede darse a varios niveles: distintos algoritmo de descifrado o una implementación diferente del virus. La creación de virus polimórficos está automatizado

Gusano

- Su objetivo es replicarse de forma rápida y distribuirse por todos los medias posibles para expandir su radio de acción los más rápidamente posible.

http://luissubiabre.wordpress.com/2014/04/22/virus-gusanos/

Troyanos

- Es un programa con funcionalidades públicas y conocidas, y otro conjunto de funcionalidades **ocultas**.

Ransomware

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Ransomware

- Bloquean el acceso a sistemas informáticos hasta que se page un “rescate”
- Suelen consistir en el cifrado del disco duro del ordenador.
- Las claves solo las conoce el atacante y después del pago este proporciona tanto la clave como el programa de descifrado.
- Afecta tanto a usuarios como a empresas.

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/EnfrentandonosRansomware

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Ransomware_de_cifrado

Keylogers

- El objetivo es registrar todas las pulsaciones de teclado de la victima. También pueden registrar movimientos de ratón o incluso hacer capturas de pantalla.
- Está relacionado con herramientas de monitorización que también tienen un uso legítimo, p.e. vigilar uso del ordenador de los menores para protegerlos.

Riesgos en Smartphones

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/informe_de_situacion_del_malware_para_android

Fraudes SMS

HOW
TOLL FRAUD SMS MESSAGES
WORK
User inadvertently downloads malicious app
START
Malware sends premium SMS without the user's knowledge
Via Aggregator and Wireless provider, a message is sent to user to confirm the order *
66555
66555
Malware writer makes money
$
$5
User is billed fraudulently
Malware blocks message and confirms charge
* depending on country
THE PLAYERS
Users are your everyday smartphone user.
Wireless providers run the network and send you bills.
Aggregators are "middlemen" for premium SMS transactions, who maintain the technical and service level requirements of each wireless network.
Malware is software that performs malicious actions when installed.
Malware writers are people who create malware.

Suplantación de Ads

Promoción de Apps

APT: Advanced Persistent Threats

- Las APTs suelen manifestarse como un programa diseñado para mantenerse oculto y realizar un ataque de forma mucho más paciente frente a un objetivo muy concreto.
- Amenaza a objetivos de cierta envergadura, a gran escala.
- Es persistente en el sentido que se debe realizar un trabajo previo de preparación para poder acceder al objetivo
- Es avanzada porque aporta novedades frente a las técnicas utilizadas o a los objetivos atacados.

https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/apt_amenaza_oculta

https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf

Proceso de Ataque

Estudio e infección de la víctima
Utilizando ingeniería social como phishings o correos dirigidos, se incita a un usuario a abrir un fichero o enlace fraudulento que aprovecha una vulnerabilidad para infectar el equipo.

Propagación del ataque
Utilizando la agenda de contactos del primer infectado, el correo se reenvía a los demás trabajadores mientras se activa el malware que intentará acceder a redes, máquinas y/o datos de la empresa.

Acceso a los recursos
El malware podrá acceder a los recursos internos de la empresa según los accesos permitidos de los usuarios infectados.

Botnets y servidores de control(C&C)

- El atacante nunca accede a los bots directamente sino a través de una red jerárquica para evitar que puedan localizarlo.
- La red de equipos C&C se suele alojar en la nube, con cuentas gratuitas, para evitar se puedan enlazar con el atacante.

Técnicas comunes usadas por APT

Ingeniería Social

Oficinistas, departamentos, servicio técnico... cualquier persona o grupo que permita acceder a la empresa.

0-days

Vulnerabilidades no conocidas o de alto éxito de explotación que permiten adentrarse mediante un adjunto en un email o la visita de websites fraudulentos.

Intrusiones

Intrusión en los sistemas a través de inyecciones en websites / bases de datos de la empresa publicados en Internet o Intranet, su perímetro externo

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Ejemplo de APT: Stuxnet

Ejemplo de APT: Darkhotel

- Usan las redes wifi de los hoteles para engañar a directivos.
- Usando certificados falsos para que crean que las conexiones son seguras.
- Instalan malware en el ordenador del directivo para robarle información valiosa.

https://securelist.com/blog/research/66779/the-darkhotel-apt/

Ejemplo de APT: Carbanak

https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

Ejemplo de APT: Turla

https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

Comunicaciones

- LAN
- Internet
- Wifi
- Bluetooth

Elementos de Interconexión de Redes

- HUB (Concentrador)

  La función del HUB es repetir las señales físicas que entran por cada uno sus puertos en el resto de puertos. Es un multiplicador a nivel eléctrico. Lo que se envía por un puerto lo reciben todos los equipos que están conectados a el.

- SWITCH (Conmutador)

  La función del SWITCH es conmutar los puertos que necesitan comunicarse, es decir, establecer un enlace físico o puente entre los puertos en los que están conectados los equipos que se están comunicando. Lo que se envía por un puerto, solo lo ve el puerto de destino.

- ROUTER (Enrutador)

  Un ROUTER es un elemento que une varias redes diferentes. Tiene un puerto en cada red, de forma que hace de puente de conexión entre las redes. Es un tipo especial de SWITCH.

Amenazas en redes locales

IP Spoofing y ARP Poisoning

Routing under normal operation

Routing subject to ARP cache poisoning

MAC Spoofing

Wifi

Tipos de Redes:

- Abierto
- WEP
- WPA - WPA2

Internet

1969

2011

Comunicaciones en Internet

- En redes complejas como internet los problemas de seguridad se agravan ya que la información pasa por múltiples nodos de red antes de llegar al destino.
- Es imprescindible utilizar mecanismos de seguridad para proteger la información en transito.

Usuario, el eslabón más débil.

Contraseñas

http://thepasswordproject.com/

http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php

- PIN (4 dígitos)
- Alfanuméricos
  - Minúsculas
  - Mayúsculas
- Caracteres especiales
  - #$%&/.-()?¿|
- Evitar repeticiones

Técnicas de Ingeniería Social

http://www.social-engineer.org/framework/general-discussion/

Phising

http://appletoncreative.com/2014/03/04/how-not-to-be-duped-by-seo-spam/

Ej. Bancos

Identificación de usuarios
Introduzca sus datos de identificación.
Número de DNI/NIE
Fecha de nacimiento
Datos de la tarjeta
Número tarjeta
CVV
PIN de cajero
FIRMA
Borradores
Enviados
Eliminados
Comentarios
PHP
Nueva carpeta
Santander
Estimado cliente:
Notificamos que su tarjeta de Banco Santander se ha suspendido temporalmente debido a intentos fallidos de uso.
Como medida de seguridad hemos decidido desactivar su tarjeta temporalmente.
Para asegurarnos de su autenticidad rogamos reactivar su tarjeta desde el siguiente enlace el cual presentamos :
https://www.bancosantander.es/cssaSatellite?pagename=verification_cliente43287jkru43i4rhf
202.91.12.181/SUPFPA_ENS/
© 2014 Microsoft
Términos
Privacidad y cookies
Desarrolladores
Español
Spam Loco

Ej. Hacienda

GOBIERNO DE ESPAÑA

Agencia Tributaria

Bienvenido a Agencia Tributaria Formulario de Reembolso

Por favor ingrese su información exactamente donde el 244,79 EUR se reembolso.

Después del último cálculo anual de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 244,79 EUR
Por favor, rellene el formulario y nos permiten 5-9 días laborales con el fin de procesarlo.

Aceptamos : MasterCard VISA

Nombre* :

Identificador Fiscal (NIF/CIF/NIE)* :

Teléfono* :

Número de Tarjeta* :

Fecha de Caducidad (de la tarjeta)* : /

Código de Seguridad (CVV2/CSC)* :

Código PIN (Contraseña)* :

Fecha de nacimiento (mm/dd/aaaa)* :

Enviar

VeriSign Secured VERIFY

http://www.policia.es/org_central/judicial/udef/alertas/20110404_1.html

Spear Phising (phising dirigido)

Vishing (Voice Phising)

http://www.thehindu.com/news/cities/chennai/vishing-fraud-gang-targeting-senior-citizens/article5929320.ece

Impersonación

- Empleados
- Clientes
- Inspectores
- Técnicos

Ciclo de vida de la Ingeniería Social

http://www.securestate.com/Services/Profiling/Pages/Social-Engineering.aspx

Estafas Online

WHERE SCAMS ORIGINATE
In complaints where perpetrator location was known, nearly 66% were from the U.S. in 2010. Take a look where the other complaints originated, and find out which countries are known for certain scams.
Country is known for:
Auction fraud
The Nigerian scam
Grandparent scams
Lottery scams
Phishing scams
Canada
2.4%
United States
65.9%
Spain
0.8%
United Kingdom
10.4%
China
3.1%
Romania
South Africa
Ghana
0.7%
Cameroon
0.6%
Nigeria
5.8%
Malaysia
0.8%
Australia
0.5%

Inversión en Seguridad

- Las medidas efectivas de seguridad no se implantan.
- No se realizan actualizaciones.
- No se monitoriza ni restringe el acceso correctamente.
- Los proveedores de servicios se rigen por el mercado y los servicios, no por la seguridad
- Los usuarios toman pocas precauciones.
- Las organizaciones no dedican
  - suficiente personal ni recursos
  - a mejorar la seguridad

Ataques informáticos en tiempo real

http://map.norsecorp.com/

CICLO DE VIDA DE SOFTWARE DE SEGURIDAD

Definiciones de interés

- *"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

- *"Computer security is the protection of a company's assets by ensuring the safe, uninterrupted operation of the system and the safeguarding of its computer, programs and data files"*

  Prof. Harold J Highland, State University of New York

- *"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

Conceptos básicos

- Las definiciones anteriores obligan a definir otros nuevos conceptos
- Activos (assets): Todo lo que forma parte de un sistema de información, incluyendo hardware, software y personas
- Amenaza (threat): Alguna cosa o circunstancia que pone en riesgo potencial la seguridad del sistema y sus activos
  - Accidentales: fuego, fallo eléctrico, error humano, etc.
  - Deliberados: hacking, malware, eavesdropping, etc.
- Vulnerabilidad: Debilidad en el sistema que influye en la probabilidad de que la amenaza sobre los activos se convierta en realidad
- Ataque: Consumación de la amenaza

Common Criteria for Information Technology Security Evaluation
ISO/IEC 15408: Evaluation criteria for IT security -
Part 1: Introduction and general model

http://wwwusers.di.uniroma1.it/~parisi/Risorse/CC.pdf

Asset
Software
Hardware
People
Threat
Deliberate
Accidental
Environmental
Vulnerability
Risk
Security breach
Impact
Disclosure, Denial,
Destruction, Modification
Consequence
E.g. Financial Loss, Breach of
Confidentiality, Legal Liability,
Disruption to activities

Prevención, detección y reacción

De lo anterior se desprende que las medidas de seguridad han de contemplarse desde distintas perspectivas, como se comenta a continuación

- Prevención: medidas que previenen el problema
- Detección: medidas que permiten detectar que se ha producido un problema, cómo se ha producido y quién lo ha producido
- Reacción: medidas que permiten recuperarse del problema

Políticas de Seguridad

Cuando se diseña un sistema seguro, es fundamental conocer el conjunto de reglas que gobiernan el comportamiento del sistema en lo que a seguridad se refiere.

- Ese conjunto de reglas constituye la política de seguridad

Algunas definiciones:

- *"The set of criteria for the provision of security services"*

  (Fuente: ISO 7498-2)

- *"A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources"*

  (Fuente: RFC 2828)

- *"The set of rules laid down by the security authority governing the use and provision of security services and facilities."*

  (Fuente: ITU-T X.509)

Servicios de Seguridad

Los servicios de seguridad son los encargados de dar soporte a las políticas de seguridad.

Algunas definiciones:

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

  (Fuente: RFC 2828)

- *"A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or the data transfers."*

  (Fuente: ISO 7498-2 y ITU X.800)

Mecanismos de Seguridad

- Los mecanismos de seguridad proporcionan soporte a los servicios 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."*

    (Fuente: RFC 2828)
- 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

Categorías de servicios de seguridad

- 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**

Modelo de escenario de Seguridad

- Necesitamos un modelo de escenario para, desde una perspectiva general (por el momento), empezar a razonar sobre:
  - Las amenazas que pueden existir
  - Los servicios que podemos usar para prevenirlos

Instancias del modelo

- 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.

Tipos de ataques

- **Intercepción** (Pasivo)

- **Inserción** (Activo)

- **Modificación** (Activo)

- **Denegación** (Activo)

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.

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).

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.

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.

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.

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.

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.

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.

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.

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).

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
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.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
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).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**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.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Ciclo de vida de seguridad (ISO-7498-2)

- Definición de una política de seguridad que contiene una serie de requisitos genéricos de seguridad para el sistema
- Análisis de requisitos de seguridad, incluyendo el análisis de riesgos, y un análisis de los requisitos legales, gubernamentales y normativos
- Definición de los servicios de seguridad necesarios para satisfacer los requisitos de seguridad
- 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
- Administración y mantenimiento de la seguridad

El ciclo de vida del software (SEGURO)

Ej: Microsoft Security Development Lifecycle

Ingeniería de requisitos de seguridad

- La seguridad debe tratarse con la misma prioridad que cualquier otro requisito funcional
- Distintos enfoques:
  - Modelado de ataques/amenazas
  - Modelado de medidas de seguridad
  - …

Modelado de ataques/amenazas

- Analizan posibles ataques y amenazas en el sistema.
  - **Attacker Centric.** Se centra en las capacidades del atacante, requiere un conocimiento en detalle del atacante. Intenta predecir el comportamiento del atacante, basando en ataques previos dentro y fuera de la organización.
  - **Asset Centric.** Se centra en un activo en particular, permite simplificar el modelo. Su objetivo es encontrar vulnerabilidades y definir controles adecuados al valor del activo.
  - **System Centric.** Modela el sistema completo con todas sus relaciones, puede ser excesivamente complejo de analizar.

http://www.slideshare.net/RafalLos/threat-modeling-the-security-of-the-enterprise

http://www.slideshare.net/tonymartinvegue/how-to-improve-your-risk-assessments-with-attackercentric-threat-modeling

http://web.mit.edu/tweilu/www/eff-ssd-mockup/threatmodel.html

Modelado de ataques/amenazas

- Casos de abuso (abuse cases)
- Casos de uso malicioso (misuse cases)
- Árboles de ataque (attack trees)
- Árboles de errores (fault trees)
- Grafos de ataque (attack graphs)

Ej: Misuse and abuse cases

Ej: Attack tree

Análisis y Gestión de riesgos

- Es objetivo principal es controlar el riesgo, bajo un umbral aceptable, y analizar la probabilidad de las amenazas así como su potencial impacto sobre los activos.
- Además, en caso de que no se cumplan las políticas o la contramedidas no sean efectivas también deben considerar los planes de contingencia
- Al considerarse múltiples stakeholders aparecen riesgos diferentes: necesidad de priorizar y llegar a acuerdos
- El coste es un riesgo muy importante en proyectos reales. Hay que mantenerlo controlado a lo largo del SDLC
- Ejemplos de metodologías de gestión de riesgos:
  - NIST SP 800-30 - Risk Management Guide for Information Technology Systems
  - OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation
  - CORAS - Construct a platform for Risk Analysis of Security critical system
  - Magerit - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Matalobos Veiga, Juan Manuel (2009). Análisis de riesgos de seguridad de la información. Proyecto Fin de Carrera / Trabajo Fin de Grado, Facultad de Informática (UPM) http://oa.upm.es/1646/

Modelado de medidas de seguridad

- Buscan hacer explicitas las medidas de seguridad junto al diseño del modelo.
- Buscan cierto formalismo que permita validar las propiedades del sistema
- Se suelen basar en extensiones para lenguajes de modelado:
  - UML: UMLSec y SecureUML
  - BPMN: SecBPMN

    http://www.staff.science.uu.nl/~dalpi001/papers/saln-dalp-gior-14-bpmds.pdf

Ej: UMLSec

- Extensión UML (perfil) que define estereotipos, etiquetas y restricciones para varios diagramas.
- Intercambio justo, RBAC, cifrado de comunicaciones, etc

Customer machine :
Customer Apps :
Get Account and Pin
Browser :
Internet Link E1 1Mbps
<<Internet>>
<<secrecy>>
e-Banking Web Server :
Web Service :
<<LAN>>
DMZ firewall Link
<<encrypted>>
e-Banking Database Server :
e-Banking Database :
<<high>>
<<LAN>>
Internal network Link
e-Banking Application Server :
e-Banking Application :
Access Control :

Evaluación de la seguridad

- No existe una única metodología para la evaluación de la seguridad.
- Podemos destacar dos categorías en lo relativo a las pruebas de seguridad
  - **Métodos formales**: El objetivo de los métodos formales es definir un modelo del sistema para poder comprobar que se cumplen ciertas propiedades de seguridad
  - **Test de Intrusión**: El objetivo es someter al software a una batería de “ataques” dirigidos a comprometer la seguridad del sistema para poder observar hasta que punto los mecanismos de defensa son efectivos.

Evaluación de la seguridad

- Aparte de las pruebas de seguridad existen otros conceptos relacionados que permiten evaluar la seguridad de un sistema.
- Por un lado tenemos las **garantías de seguridad**, un proceso en paralelo al desarrollo del software que permite documentar las evidencias que dan soporte a las afirmaciones sobre la seguridad del sistema
- Otro concepto relevante es el de las certificaciones de seguridad, unas de las metodologías de certificación más importante es el **Common Criteria**. En este caso el proceso de documentación está regido por un estándar y es ”homologable”.

Model Checking

- Son **representaciones parciales** de los sistemas
  - Notación y semántica definida.
  - Describen los comportamientos posibles del sistema sin ambigüedades.
- Se representan mediante **grafos dirigidos**
- Los nodos representan los estados posibles y las flechas las posibles transiciones.

Model Checking

model checking:

all program state are explored until none left or defect found

Explosión de estados

La verificación de modelos presenta un problema conocido como la **explosión de estados**, presentes en la mayoría de los sistemas del mundo real.

Existen diversos métodos que pretenden combatir esta limitación:

- Algoritmos simbólicos.
- Limitación de las repeticiones o estados comprobados.
- Simplificación del modelo del sistema y refinado
- ...

Theorem Prover

- Theorem Prover es un método de verificación formal basado en demostraciones matemáticas mas o menos automatizadas.

- Se trata de implementar pruebas que verifiquen un razonamiento o problema mediante una serie de pasos demostrados

- Los retos principales son:
  - La representación del conocimiento o del sistema.
  - Las reglas para derivar nuevo conocimiento del que se tiene.
  - Las estrategias para controlar dichas reglas para evitar la explosión de estados.

Definiciones,
teoremas, etc
Usuario
Memory
Gates
Arith
Vectors
demostraciones
theorem
prover
Se demuestra

Características de los métodos formales

- Siempre se centran en un modelo simplificado del sistema debido al problema de la explosión de estados
- Son propensos a errores de especificación ya que suelen ser complejos.
- Requieren un conocimiento detallado del funcionamiento interno del sistema tanto en la componente software como en el hardware.
- Son muy útiles para verificar protocolos de seguridad simples que se puedan usar como elementos del diseño de sistema seguros.

Test de Intrusión

- El objetivo es realizar pruebas automatizadas en busca de vulnerabilidades dentro del sistema a analizar.
- Se distinguen tres aproximaciones principales:
  - **Caja Negra**. Al técnico no se le proporciona ninguna información sobre el sistema a analizar. Se hace más complicado poder explotar vulnerabilidades en el sistema pero se asemeja más a las situaciones reales. La empresa no tiene que dar información sensible al técnico que realiza el análisis.
  - **Caja Blanca**. Se le proporciona al técnico toda la información sobre el sistema: código fuente, documentación, esquemas de red, etc. Si bajo estas condiciones no se encuentran puntos flojos en el sistema, el sistema se puede considerar que está prácticamente blindado.
  - **Caja Gris**. Se le proporciona al técnico información parcial sobre el sistema. Intenta combinar las ventajas de ambos.

Características de los Test de Intrusión

- No requieren un conocimiento interno del sistema, aunque con ese conocimiento los test son más efectivos.
- Permiten evaluar un sistema en condiciones reales.
- Solo cubren los ataques o técnicas conocidas por el “pen-tester”, dependen mucho del experto que los realiza.
- Requieren de la firma de acuerdos de confidencialidad con las empresa ya que el “pen-tester” tiene acceso a información critica sobre la empresa, ya sea de forma directa o indirecta a consecuencia de los ataques realizados.

Garantías de seguridad

- Del inglés *assurance*: “A justified measure of confidence that a system will function as intended in its environment of use“
- Técnicas que más orientadas a la seguridad por construcción (security-by-construction) o por diseño (security-by-design)
  - Refinamiento a cada paso (stepwise refinement)
- Pueden (y deben) ofrecer métricas e indicadores de seguridad
- Usan escenarios de garantía de seguridad (assurance cases)

Escenarios de garantía de seguridad

- Demonstración estructurada, y generalmente informal y basada en argumentos, de que un sistema es suficientemente seguro y confiable en un determinado contexto.
  - Testing por sí mismo no puede ofrecer estos argumentos
- Argumentos, evidencias y afirmaciones
  - Evidencia: resultado de analizar, testar, simular y estimar las propiedades de un sistema del que se puede inferir alguna propiedad del mismo
  - Afirmación: algo que se dice sobre un sistema o sobre una propiedad del mismo
  - Argumento: explicación de cómo una evidencia se puede interpretar de forma razonable como la existencia de una operación aceptable

Escenarios de garantía de seguridad

SI Evidencia1, entonces Afirmación 1;
Si Evidencia 2, entonces Afirmación 2;
Si Evidencia 3, entonces Afirmación 3;
Si Afirmación 2 y Afirmación 3, entonces Afirmación 4;
Si Afirmación 1 y Afirmación 4, entonces Afirmación

Common Criteria

- Certificación de productos informáticos regulados por el ISO/IEC 15408

- Common Criteria ofrece la garantía de que el proceso de especificación, implementación y evaluación de un producto de seguridad informática se ha realizado de una manera rigurosa, estándar y repetible.

Common Criteria:TOE-Target of Evaluation

- En CC, un TOE es un conjunto de software, firmware y/o hardware que requiere una evaluación de seguridad.
- Un TOE puede ser:
  - Una parte de un producto informático.
  - Un producto informático (sistema operativo, aplicación software,…).
  - Un conjunto de productos informáticos.
  - etc.

Common Criteria: Grupos de interés

Hay tres grupos con un interés general en la evaluación de las propiedades de seguridad de los TOEs:

- **Consumidores**: pueden utilizar los resultados de las evaluaciones para ayudar a decidir si un TOE satisface sus necesidades de seguridad.
- **Desarrolladores**: Identificación de los requisitos de seguridad que deberán cumplir los TOEs
- **Evaluadores**: criterios que deben utilizar los evaluadores para determinar la conformidad de los TOE con sus requisitos de seguridad

Requisitos de seguridad

Derivados de:

- Análisis de los **objetivos** deseados de protección de privacidad, confidencialidad, etc.
- Análisis de **riesgos**, identificando amenazas para cuya mitigación se requiere el TOE.
- Análisis del **entorno**, identificando factores que pueden influenciar la consecución de los objetivos o la mitigación de los riesgos, pero que no están dentro del alcance del TOE.

Documentos principales

- Perfiles de protección (PP): Identifican requisitos de seguridad detallados que son relevantes para un propósito de protección particular, por ejemplo, un conjunto de casos de uso relacionados.
- Requisitos funcionales de seguridad (Security Functional Requirements, SFR): Especifica las funcionalidades individuales de seguridad que se proporcionan en un TOE.
- Objetivos de Seguridad (Security Target, ST): Identifica las propiedades de seguridad del TOE.

Perfiles de protección vs objetivos de seguridad

- Los Objetivos de Seguridad (ST) siempre describen las propiedades de un TOE específico (por ejemplo, el *MinuteGap v18.5 Firewall*) mientras que los Perfiles de Protección (PP) describen un tipo de TOE (por ejemplo, *firewalls*).
  - Un mismo PP se puede utilizar como plantilla para diferentes ST
- Un ST suele estar escrito por los desarrolladores del TOE mientras que un PP suele estar escrito por:
  - Una comunidad de usuarios.
  - Un promotor o un grupo de desarrolladores de un TOE
  - Un gobierno o una gran corporación.
- Ejemplo de Perfiles de protección:
  - https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/Perfiles_Proteccion_DNIe_UNE/?year=2012

Requisitos de Confianza (SAR)

- El proceso de evaluación intenta establecer el nivel de confianza (*Assurance*) que se le puede otorgar a la seguridad de un TOE.
- Los SAR (Security Assurance Requirements) detallan las acciones tomadas durante el desarrollo, implementación y funcionamiento del TOE que aseguran el cumplimiento de las funcionalidades de seguridad que se declaran.
- Los SARs están escritos en un lenguaje estandarizado para asegurar exactitud y facilitar la comparabilidad.

Nivel de Confianza de la Evaluación

- El Nivel de Confianza de la Evaluación (Evaluation Assurance Level, EAL) es una calificación numérica asignada al TOE para reflejar los requisitos de confianza (SAR) cumplidos. Cada nivel corresponde a la evaluación de un conjunto de requisitos de confianza, con una profundidad y un rigor determinado.

Organizaciones de pruebas

- Los gobiernos suelen usar Common Criteria como base para los sistemas de evaluación.
- Todos los laboratorios de pruebas deben cumplir con la norma ISO 17025, y las organizaciones de certificación (*certification bodies*) generalmente son aprobadas sobre el ISO/IEC Guide 65 o BS EN 45011.
- El cumplimiento del ISO 17025 es generalmente aprobado por una autoridad nacional:
  - En España, el Centro Criptológico Nacional (CCN) acredita laboratorios de prueba Common Criteria

Proceso de certificación