# Introducción a la Seguridad de Redes

**Ing. Pedro Escudero**

Telf: 0994667184
Mail: pedro.escudero@unach.edu.ec
Web: https://www.researchgate.net/profile/Pedro-Escudero-3/research

Abril - 2025

# Contenido

# **1.** Que es la seguridad?

# • Que es la seguridad?

**Conceptos generales**

Libre y exento de todo peligro, daño o **riesgo**.

**Mecanismos que garantizan el correcto funcionamiento y previenen fallos, asegurando que los recursos y la información sean accesibles y utilizados adecuadamente por los usuarios previstos**

Sinónimo: protección, invulnerabilidad, defensa, robustez

**Funcionamiento de sistemas**

**Corrección**

Ante una entrada de usuario, se genera la salida esperada.

Más funcionalidades => mejor sistema

**Seguridad**

Ante una entrada inesperada de un atacante, el sistema no falla.

Más funcionalidades => más posibilidades de fallos

# • Que es la seguridad?

**Tipos**

- Seguridad personal
- Seguridad de la información
- Seguridad de ordenadores o de sistemas
    - Proteger la información en ordenadores compartidos
- Seguridad de redes cerradas o propietarias
    - Proteger sistemas distribuidos y las comunicaciones entre ellos
- Seguridad en la interconexión de redes
    - Proteger los intercambios entre redes

**Objetivos**

- Protegerse de actuaciones de usuarios malintencionados
- Permitir el acceso y uso del sistema a usuarios conocidos o de confianza
- Dotar de privacidad
- Definir las políticas o reglas de uso
- Anticipar cualquier posible fallo en el sistema Garantizar que los servicios no se interrumpen

# • Que es la seguridad?

## Terminología

- ITU X.800 y RFC 2828 sistematizan metodología para definir la seguridad de un sistema

**Conceptos**

- Amenazas o riesgos de seguridad
  - Potencial violación de la seguridad, resultado de la cual se explotan vulnerabilidades.
- Ataques de seguridad
  - Cualquier acción que pueda comprometer la seguridad de la información de una organización
- Mecanismos de seguridad
  - Proceso o dispositivo diseñado para detectar, prevenir o recuperarse de un ataque
- Servicios de seguridad
  - Solución que permite mejorar y garantizar la seguridad en el procesado y transmisión de datos entre sistemas.
  - Resultado de la integración de varios mecanismos de seguridad

- **Que es la seguridad?**

## Áreas de la seguridad

- **Seguridad física**
  - Instalaciones
  - Equipamiento
    - Manipulación
    - Variaciones Tª, voltaje, en momento preciso
- **Seguridad lógica**
  - Seguridad de la información
    - Criptografía
    - Seguridad de las comunicaciones (protocolos)
  - Control de acceso
    - Autenticación y autorización
  - Seguridad de sistemas

# 2. Evolución histórica

- **Evolución histórica**

## Historia de las redes de computadores

- **1960**
  - ARPANET – Creación de Internet usando Network Connect Protocol
- **1970**
  - Primeros protocolos: email, Ethernet, TCP, FTP, etc.
- **1980**
  - Definición de la pila TCP/IP
  - DNS
- **1990**
  - Incremento del número de nodos en la red
  - Redes de comunicaciones móviles
  - Origen de la WWW => boom del .com
- **2000**
  - Acceso global a la red

- **Evolución histórica**

## Historia de las redes de computadores

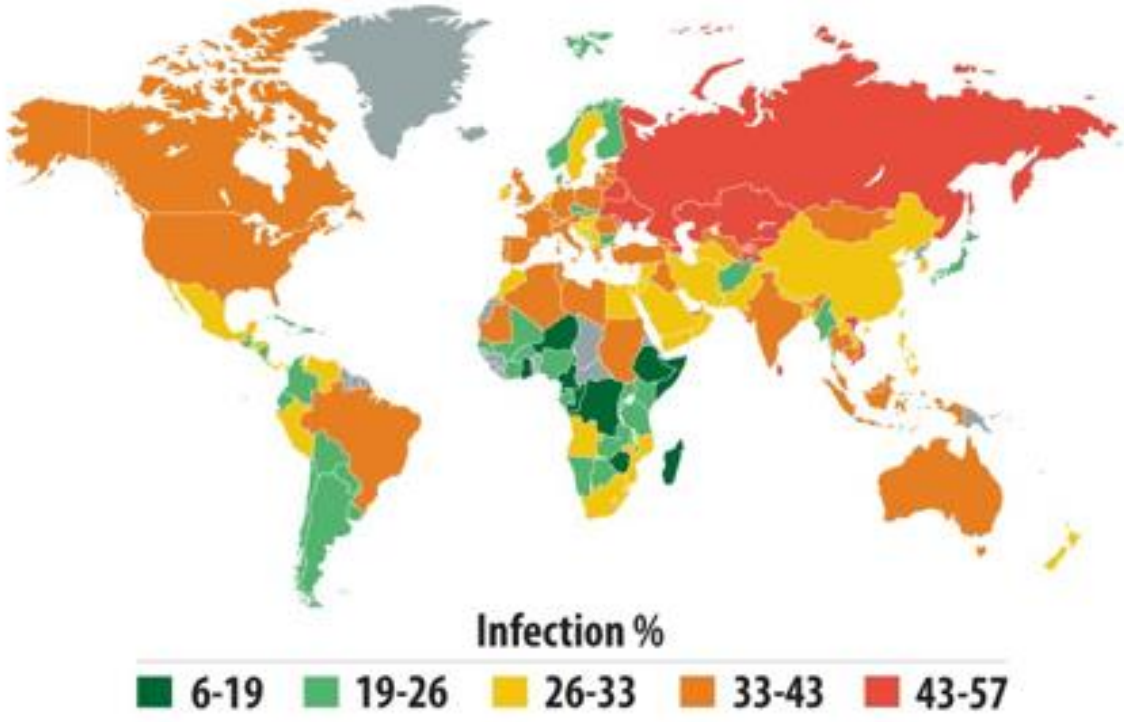
- **1960**
  - Definición de los términos hacker y cracker (hacker malicioso)
- **1970**
  - Phreaking => Blue boxes para la realización de llamadas gratuitas
  - RFC 602 => ARPANET es susceptible de ataques
- **1980**
  - Cucko’s egg => Ataque por uso agujero en programas
  - Morris Worm => 1er gusano
  - Creación del CERT (Computer Emergency Response Team)
- **1990**
  - Spoofing de TCP
- **2000**
  - Gusanos, virus, reemplazos de identidad, phising, etc

## Tipos de vulnerabilidades

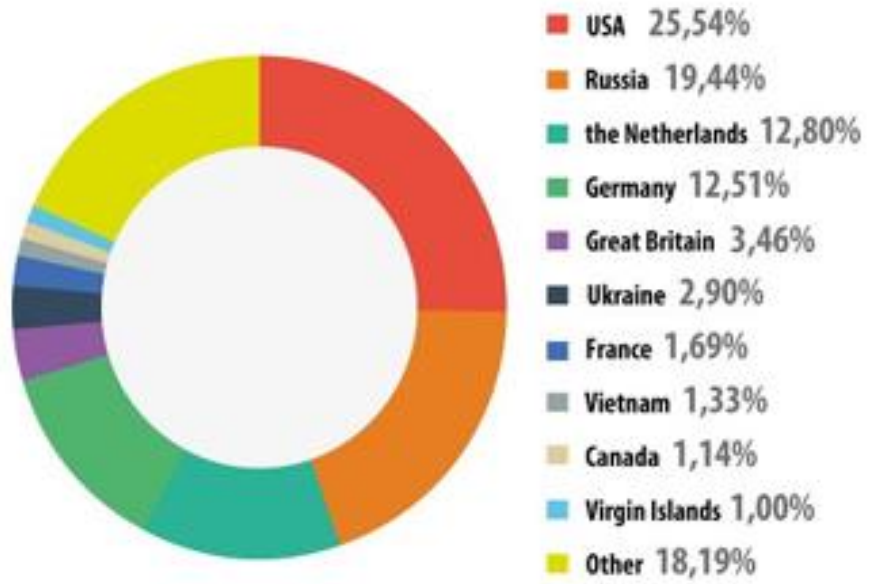
- Errores humanos
- Diseño de los protocolos y/o software
  - Puertas abiertas
  - No validan la identidad en el acceso
  - Seguridad no considerada desde el inicio
- Implementación de protocolos y/o software
  - Puertas traseras
  - No comprobación datos de entrada/salida (contenido, tamaño, …)
- Configuración del sistema y/o red
  - Políticas de seguridad

- **Evolución histórica**

**Vulnerabilidades** **2013**



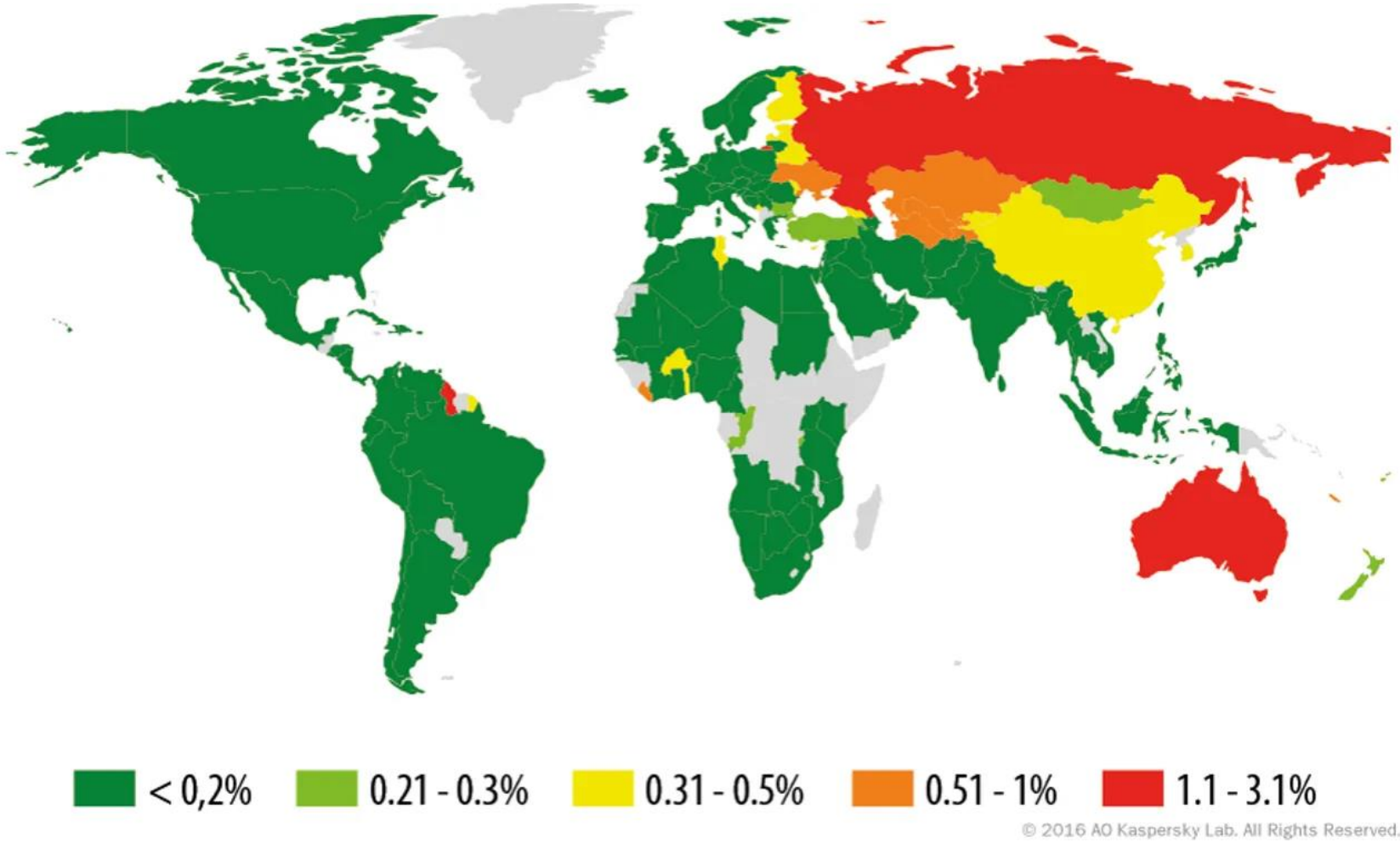

Riesgo de infección




Origen infecciones WWW

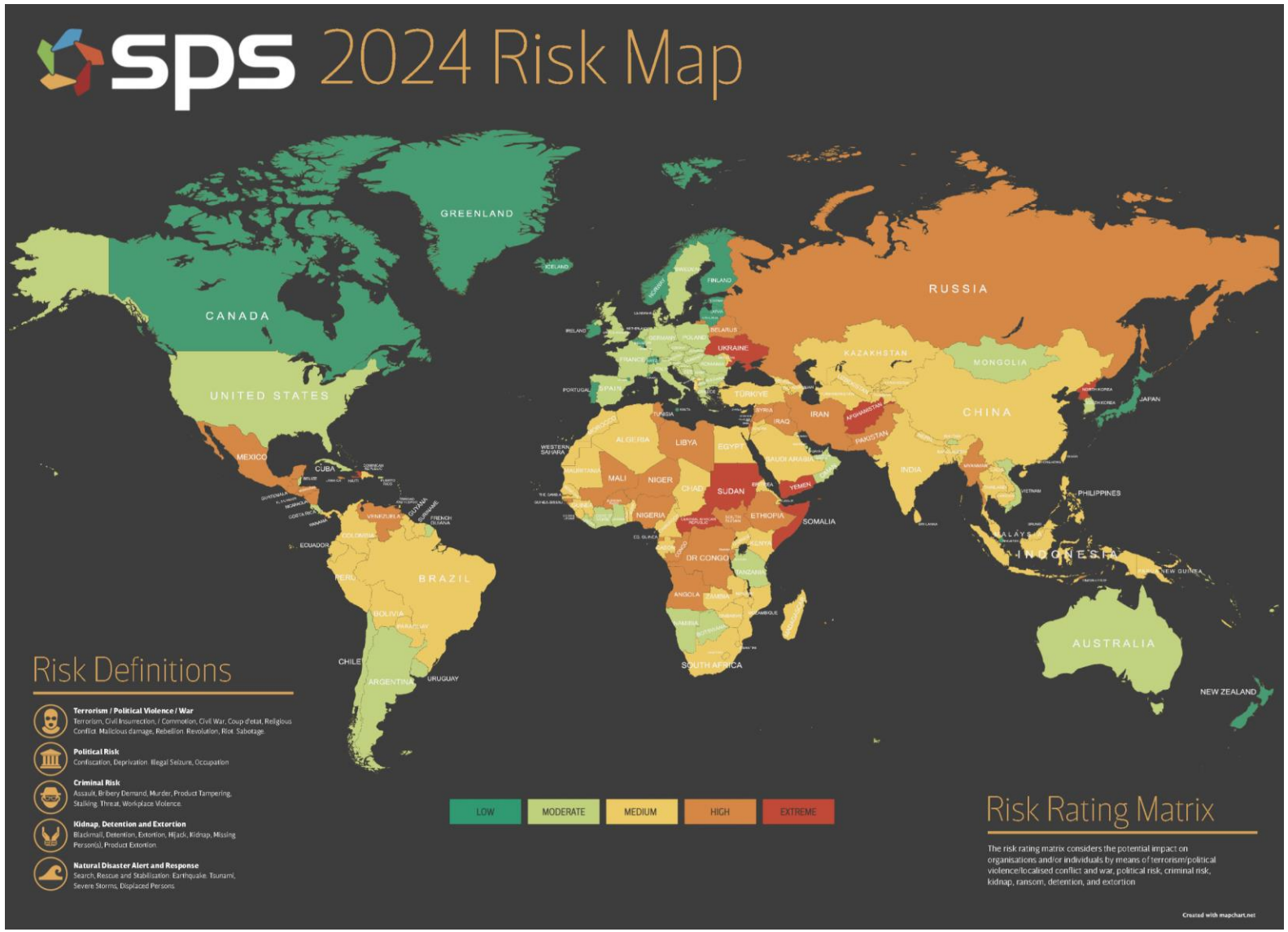
- **Evolución histórica**

**Vulnerabilidades** **2016**



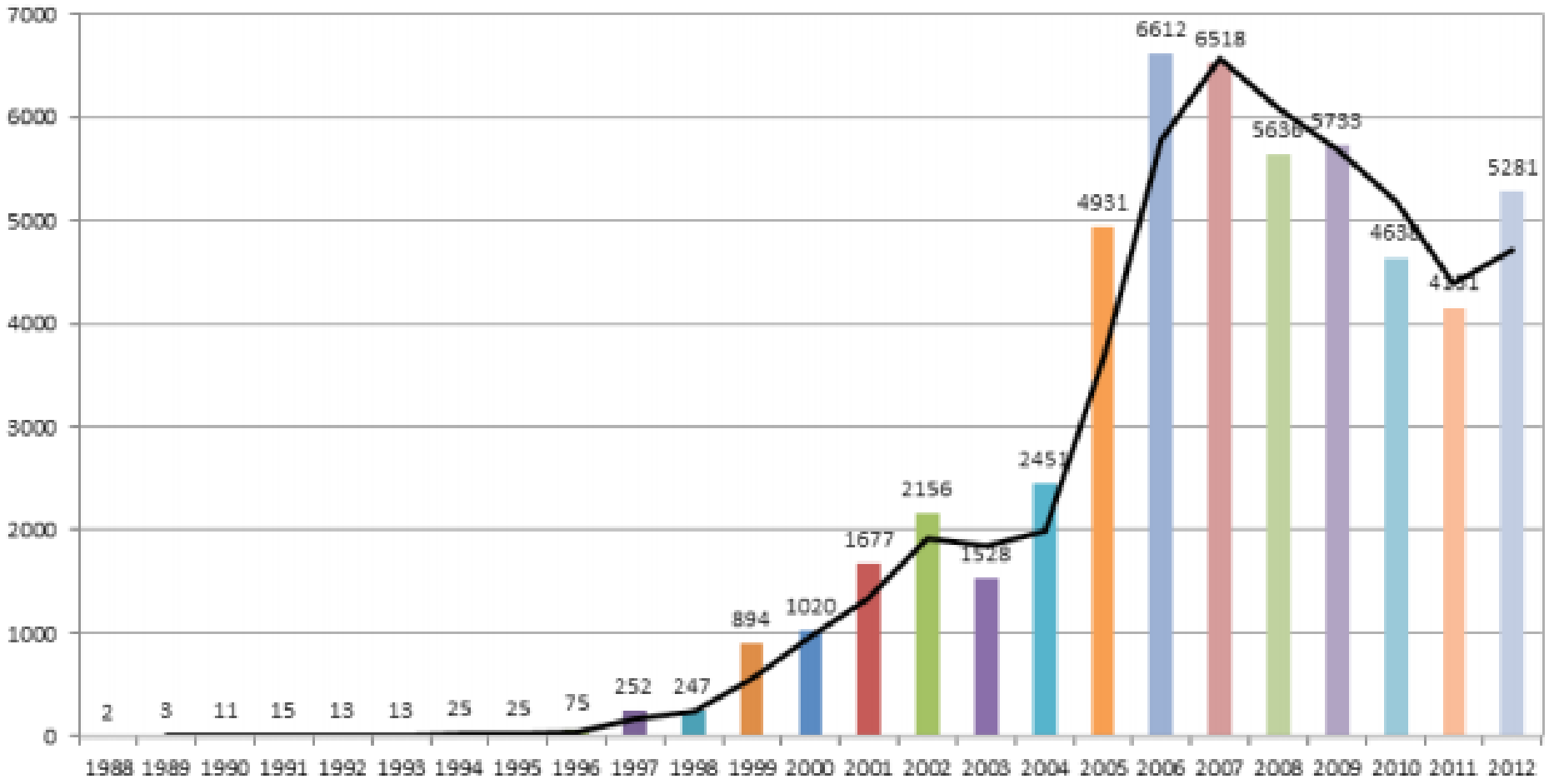
- **Evolución histórica**

## Vulnerabilidades

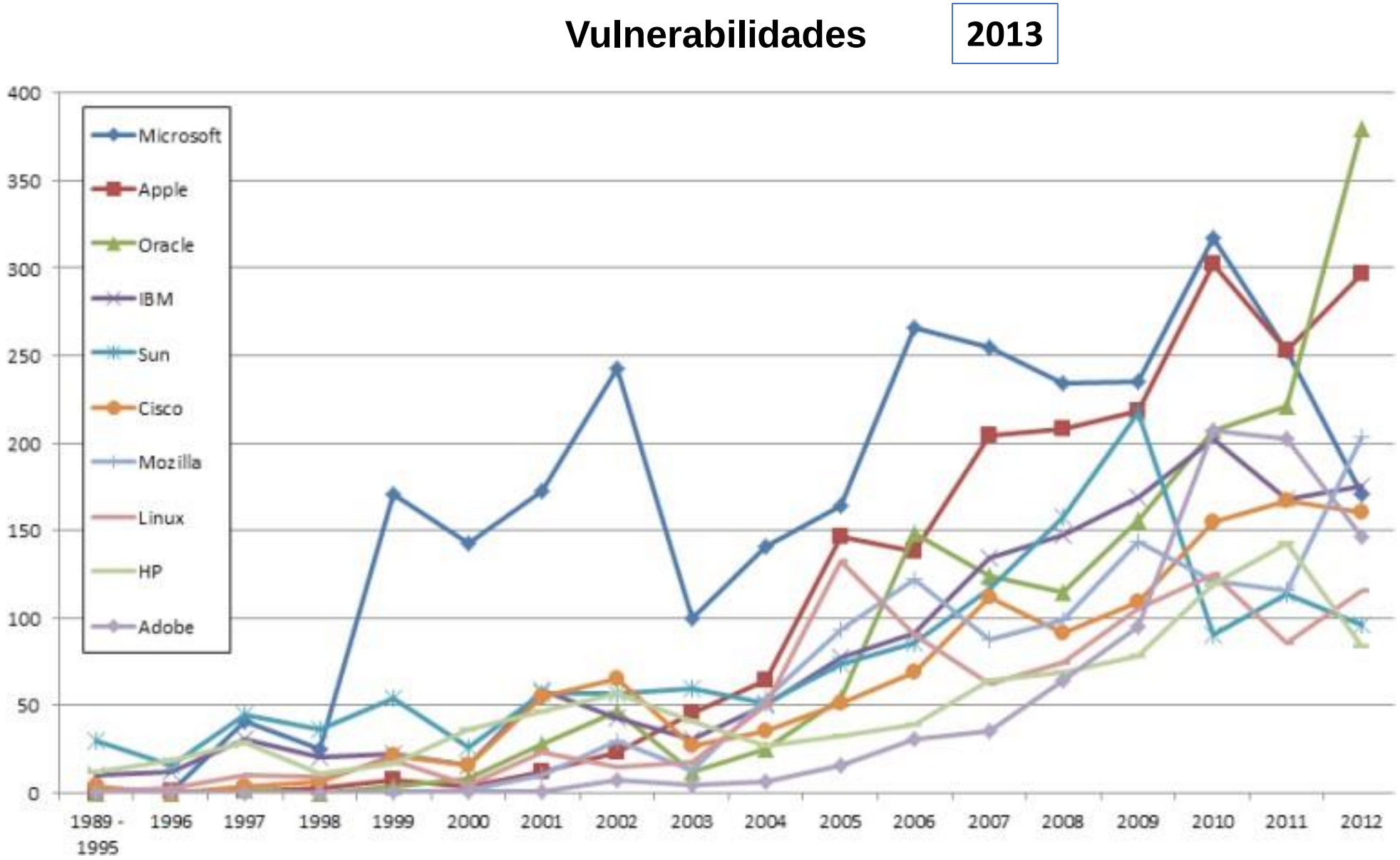


# • Evolución histórica

- Autenticación
- Configuración
- Condiciones raciales
- Credenciales
- Errores numéricos
- Filtrado de información
- Crypto CSRF



- **Evolución histórica**



# **3.** Amenazas y ataques

# • Amenazas y ataques

**Personas atacan por:**

**Motivación**

- Reto personal
- Uso totalmente malintencionado
- Económica

**Tipos**

- Hacker
- White hat
- Black hat or Cracker
- Phreaker
- Spammer
- Phisher

**Tipos de ataques:**

**Por reconocimiento**

- Información abierta
- Barridos
- Escaneo de puertos
- Inspección de paquetes (*packet sniffer*)

**De acceso a la red**

- Claves o cuentas comprometidas
- Sondas
- Explotar la confianza
- Redirección de puertos
- Hombre en el medio
- Secuestro de conexiones
- *Spoofing*

- **Amenazas y ataques**

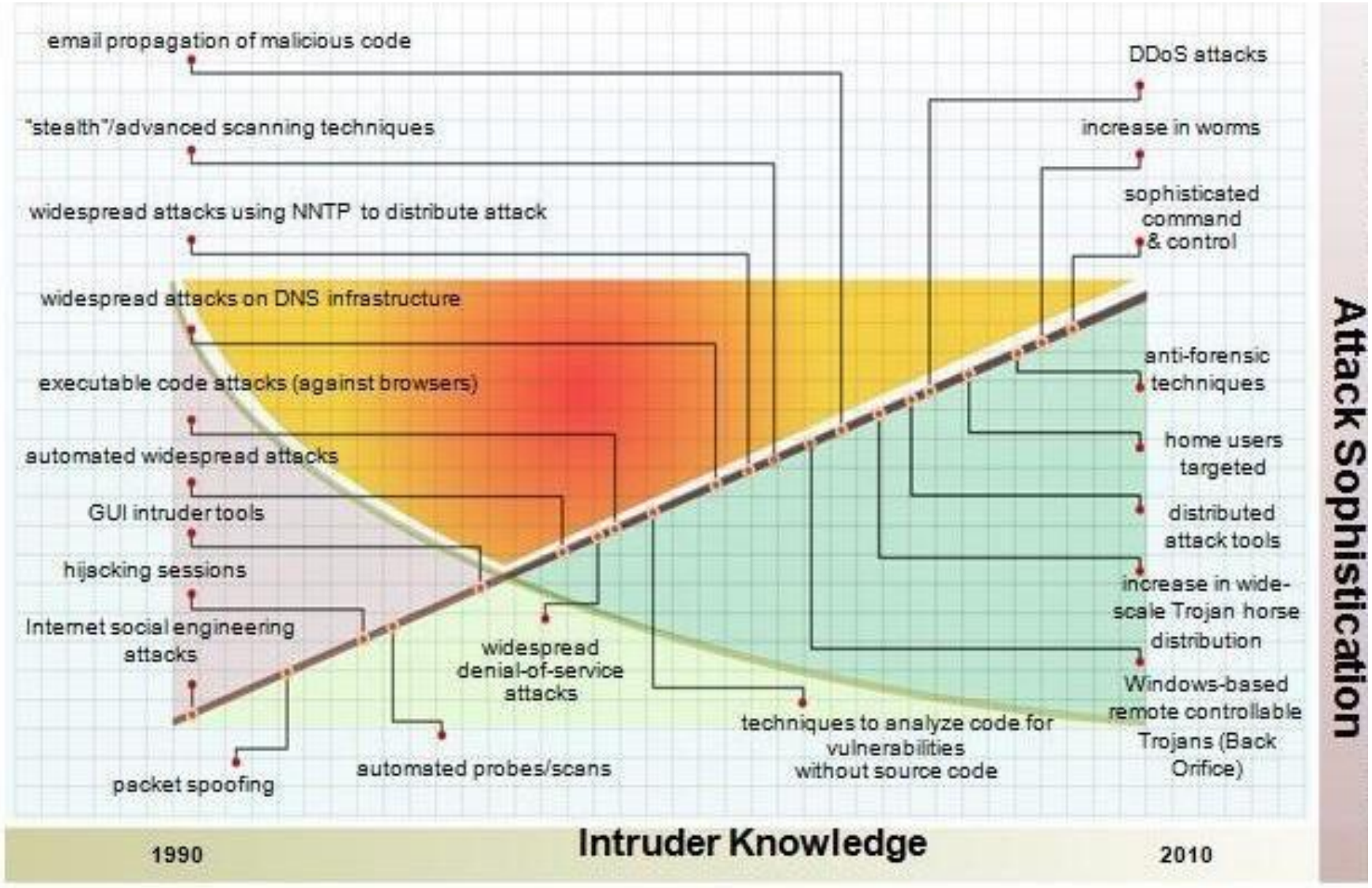
**Tipos:**

Denegación de servicio
- Inundación ICMP, SYI
- Llenado de buffers - lectura lenta
- Distribuidos

Código malicioso
- Gusanos
- Virus  Troyanos

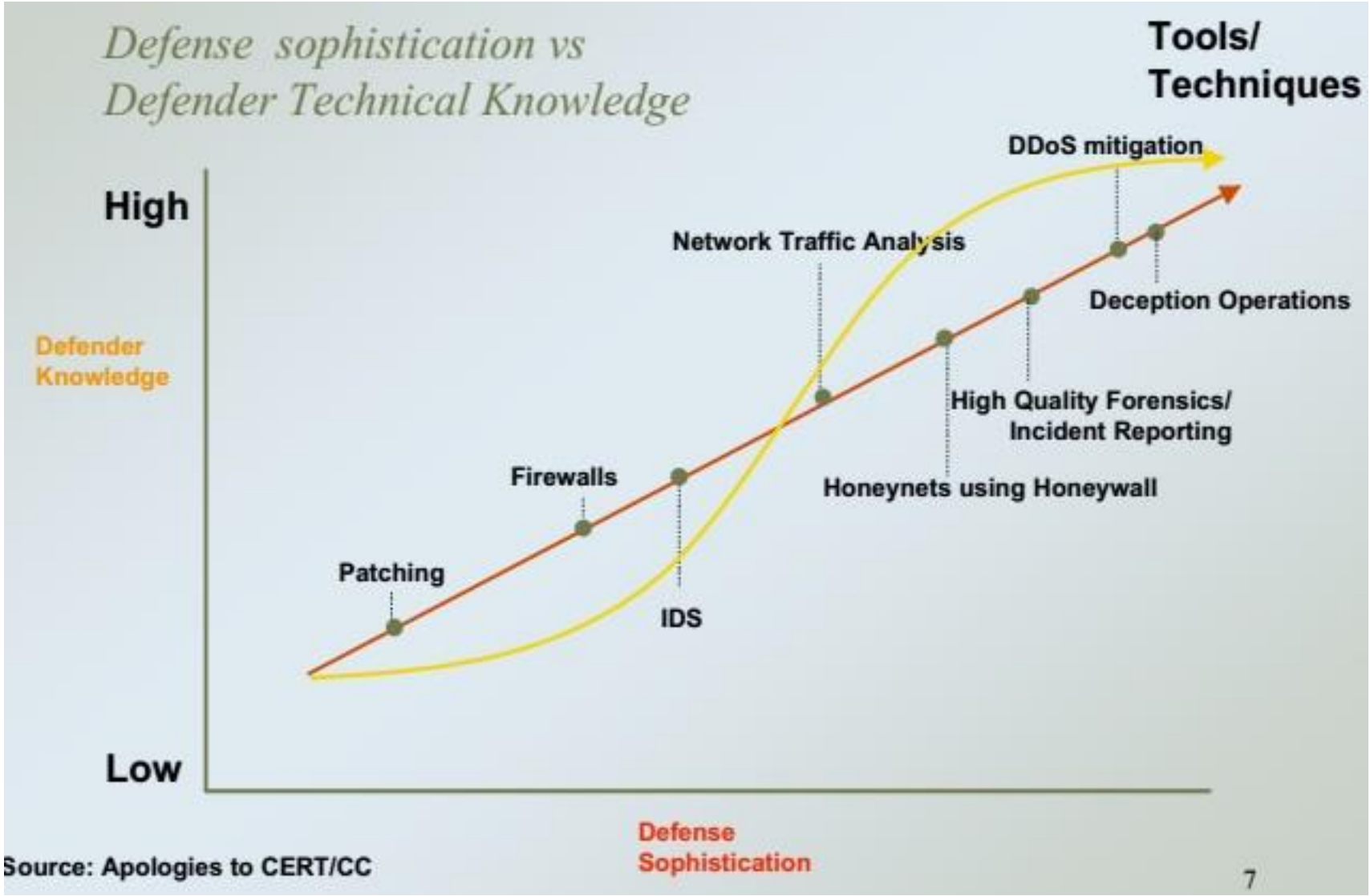
Psicológicos
- Pretexto
- Phising
- Culturales

**Visión Global de amenazas y ataques**



- **Amenazas y ataques**

**Visión Global de amenazas y ataques**



## Comparativa con la vida cotidiana

- Similitudes
  - Candado ⇒ ocultar datos
  - Leyes ⇒ reglas a seguir

- Diferencias
  - $\partial tecnología / \partial tiempo$ ⇒ rápidos cambios en poco tiempo
  - Ataques rápido y baratos
  - Leyes en constante cambio
    - Ambiguas
    - Normas no especificadas

# 4. Entornos de comunicación seguros

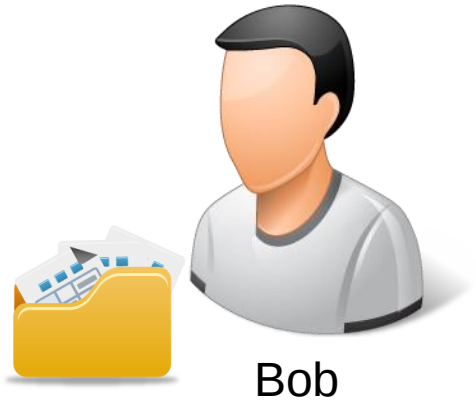
# • **Entornos de comunicación seguros:** Sistemas de comunicación


- Alice y Bob se transfieren datos a través de la red
  - Canal inseguro
  - No incluyen medidas de seguridad adicionales

- **Entornos de comunicación seguros:** Sistemas de comunicación

Eve

Alice

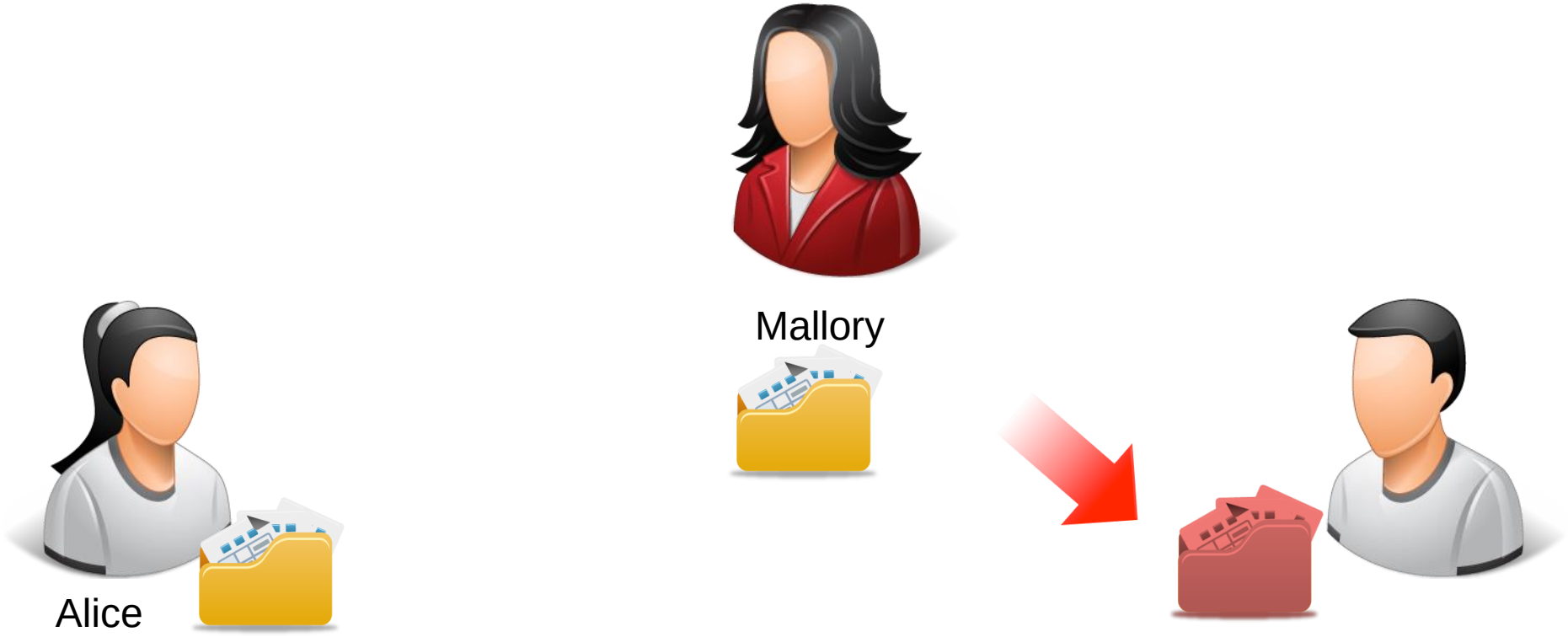


Bob

Ataque pasivo – Eve (espía o *eavesdropper*)

Leer el contenido de los mensajes  Analiza los patrones de los mensajes

- **Entornos de comunicación seguros:** Sistemas de comunicación




Ataque activo – Mallory (malintencionado o *malicious*)

- Reemplazo de identidad
- Retransmisión de mensajes
- Modificación de mensajes
- Denegación de servicio

# • Servicios de Seguridad

## Requerimientos

Autenticar
- Extremos de la comunicación
- Origen de los datos

Autorizar
- Controlar el acceso a un servicio

Confidencialidad de los datos
- Protección de ataques pasivos  Evitar análisis de los flujos de datos

Integridad de los datos
- Detectar modificación, borrados, inserciones, repeticiones, …  Con o sin recuperación de los datos originales

No repudio
- De origen o destino

Trazabilidad (accountability)
- Registro de actividades
- Comprobación de asignaciones y políticas

Disponibilidad
- Sistema accesible para usuarios autenticados
- Mantener unas condiciones de calidad de servicio y experiencia de uso

# • **Servicios de Seguridad:** Autenticación

Escenario

- Alice quiere enviar un mensaje a Bob
- Bob quiere garantizar que el mensaje es de Alice

Opciones

- Alice le dice a Bob que es ella
- Pero también lo puede decir Eve o Mallory
- Alice le envía una información a Bob que “solo” conocen ellos
- Pero Eve o Mallory han podido aprender la información y enviarla también
- Alice le envía a Bob la clave cifrada como prueba de identidad
- Pero Eve o Mallory han podido hacer lo mismo. No necesitan descifrarla

Ninguna de las anteriores es válida

# • **Servicios de Seguridad:** Confidencialidad

Escenario

- Alice quiere enviar un mensaje a Bob
- Alice quiere garantizar que nadie conoce el contenido real del mensaje

Opciones

- Alice y Bob establecen un procedimiento de cifrado propio
  - Pero Eve o Mallory al haber variabilidad reducida pueden llegar a aprenderlo
- Alice y Bob emplean procedimientos de cifrado estándar
  - Pero ¿cómo se han intercambiado las claves? Eve o Mallory han podido obtenerlas
- Alice y Bob emplean una misma clave todo el tiempo
  - Pero Eve o Mallory la han obtenido y leen sus mensajes
- Alice y Bob emplean algoritmo y procedimientos intercambio muy robusto
  - Pero Mallory ha podido modificar el contenido del mensaje

Ninguna de las anteriores es válida

# • **Servicios de Seguridad:** Integridad y No Repudio

Escenario

Alice quiere enviar un mensaje a Bob

Alice quiere garantizar que Bob recibe lo que ha enviado

Opciones

Alice añade datos adicionales al mensaje que permiten a Bob verificar el contenido

Pero Mallory puede conocer la función aplicada y modificar el mensaje y el código de verificación

Pero Eve o Mallory pueden volver a remitir el mensaje en otro momento

Ninguna de las anteriores es válida

# • Mecanismos de seguridad

- Cifrado  Resúmenes (*Hash*) Firma digital
- Intercambios de autenticación Control de acceso
- Terceras parte de confianza Aleatoriedad
- Control de rutas

# • **Mecanismos de seguridad:** Criptografía

Del griego *krypto* (~esconder) y *graphein* (escribir)

Conjunto de técnicas para escribir enmascarando el contenido real de un mensaje

Previene que terceros no autorizados puedan leer el contenido

- **Mecanismos de seguridad:** Criptografía

¿Algoritmos abiertos y públicos o cerrados y propietarios?

En privados, los errores se descubrirían inicialmente por usuarios, pero si un malicioso los descubre, los usuarios no se enteran

En públicos, los errores serán abiertos también

Algoritmos de cifrado abiertos  uso de códigos secretos  Rotura de sistemas de cifrado

A partir de un mensaje cifrado

A partir de duplas <mensaje en claro, mensaje cifrado>  A partir de mensajes conocidos

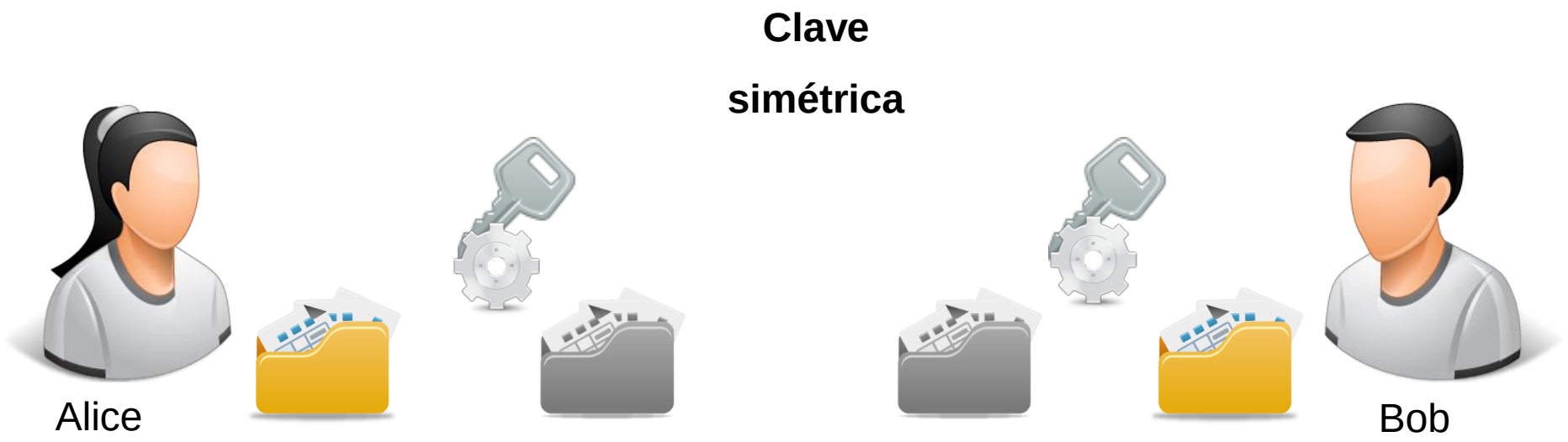
# • **Mecanismos de seguridad:** Criptografía de clave simétrica

Misma clave para cifrar y descifrar Ventajas

- Algoritmos operan a velocidades relativamente altas

Inconvenientes

- Distribución de la clave en canales inseguros
- Mensajes cifrados con apariencia similar al mensaje en claro



# • **Mecanismos de seguridad:** Criptografía de clave asimétrica

Claves diferentes para cifrar y descifrar
Clave pública conocida por todo el mundo
Clave privada personal (y conocida por el dueño)
Inconvenientes
Algoritmos operan a velocidades relativamente lentas
Ventajas
Distribución de la clave en canales inseguros

PúblicaP
$U_X$

Privada
$PR_X$

- **Mecanismos de seguridad:** Criptografía de clave asimétrica

Alice usa las claves para …

Clave pública de Bob: cifrar el mensaje que manda a Bob (confidencialidad)

Clave privada de Alicia: firmar el mensaje (integridad y no repudio)

Bob usa las claves para …

Clave pública de Alicia: comprobar la validez del mensaje enviado por Alicia (integridad y no repudio)

Clave privada de Bob: descifrar el mensaje que Alicia le ha enviado (confidencialidad)

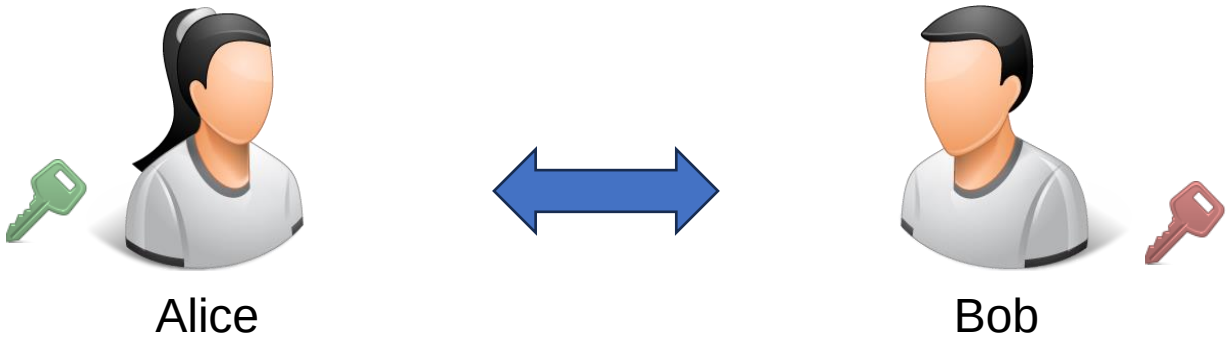
Alice Bob

# • **Mecanismos de seguridad:** Sistemas Híbridos

Criptografía simétrica y asimétrica son complementarias y no excluyentes

Asimétrica se emplea para cifrar claves

Simétrica para cifrar grandes volúmenes de datos



# • **Mecanismos de seguridad:** Funciones Unidireccionales (hash)

Transformación matemática que a partir de un mensaje de una longitud arbitraria calcula un resumen de una longitud fija.

- Dado x es sencillo calcular f(x)
- Dada f(x) es difícil o imposible calcular x
- Dados x e y, f(x) será distinta de f(y)

Utilidad

- No para cifrar un mensaje
- Generar una huella única de un mensaje (integridad)

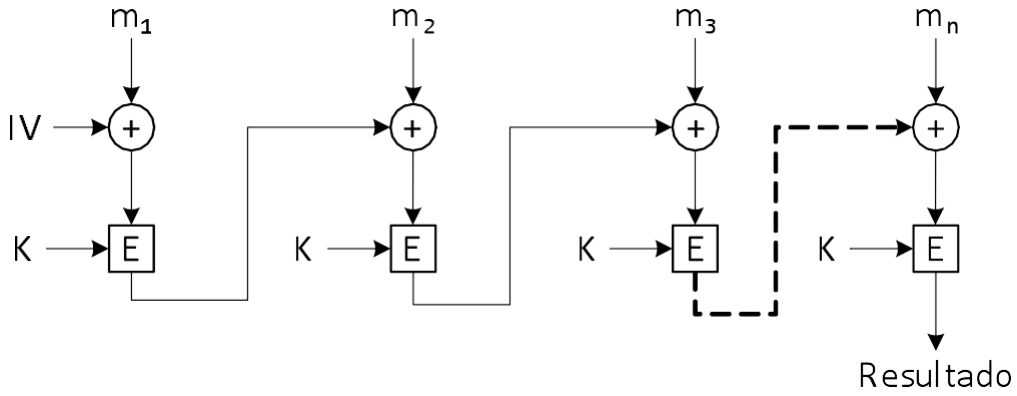
Algoritmos más conocidos

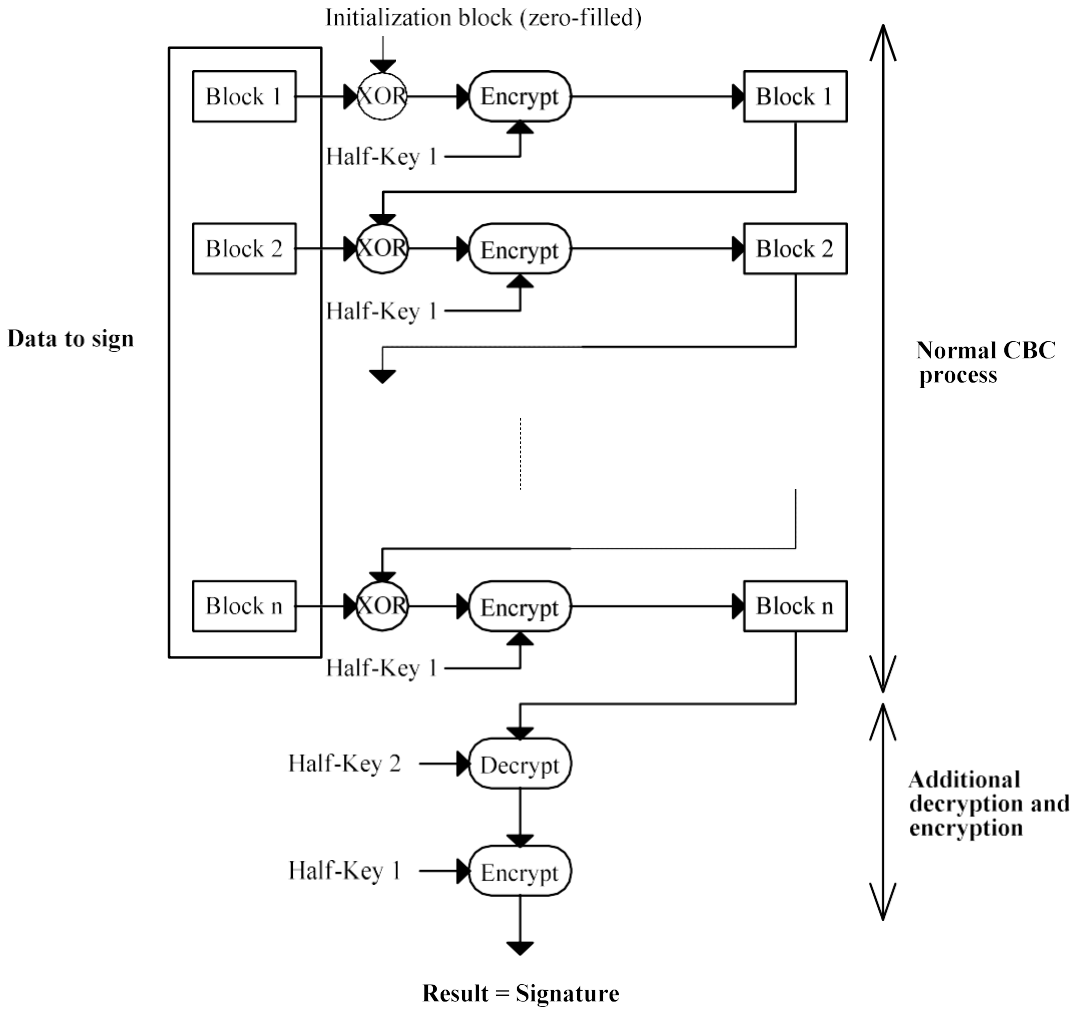
- MD5, SHA-0, SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512), SHA-3

Message Authentication Code (MAC)

- Hash usando una clave y procedimientos criptográficos $\Rightarrow$ H(K, m)

- **Mecanismos de seguridad:** Funciones Unidireccionales (hash)



# • **Mecanismos de seguridad:** Generación de números aleatorios

Nonce

- Numero proporcionado por el usuario que solo se usa **una** vez

Un número será estadísticamente independiente

- Generación de claves, un solo uso, etc.

Pseudo-aleatorios

- Lo mejor que un ordenador puede realizar $\Rightarrow$ parecen aleatorias
  Secuencia con periodo de repetición suficientemente elevado
- Uso de criptografía para cifrarlas, las hace más robustas $\Rightarrow$ impredecible

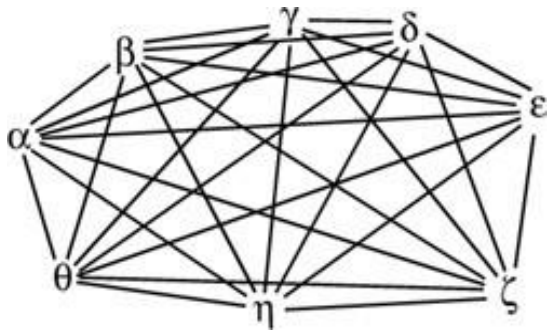
Aleatorios

- Ni pueden ser reproducidas
- Mecánica cuántica $\Rightarrow$ el mundo es determinista, ¿los ordenadores no?

# • **Mecanismos de seguridad:** Entidades de confianza

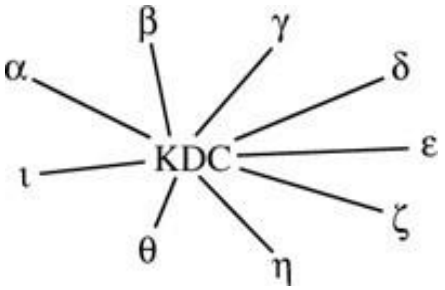
**No todos pueden confiar en todos**

N nodos ⇒ N-1 claves
(punto a punto)




**Tercera entidad de confianza (TTP, *Trusted Third Party*)**

- Centros de distribución de claves (KDC, *Key Distribution Center*)
- Autoridades de certificación (CA, *Certification Authority*)
- Servidores de tiempo (*timestamp*)
- Organizaciones jerarquizadas o por dominios




**Delegación**

Autenticación y control de acceso

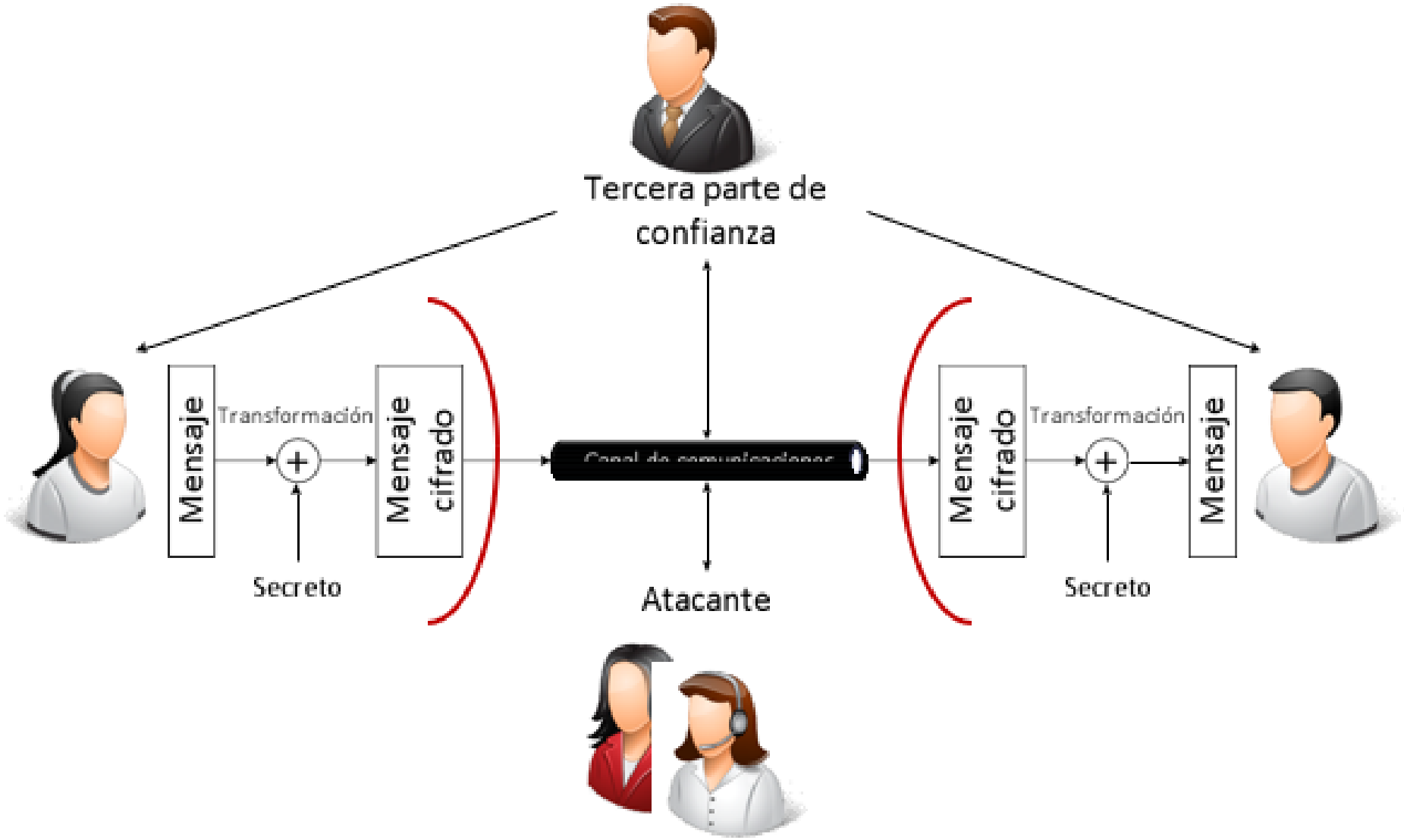
- **Mecanismos de seguridad:** Procedimientos adecuados

Mecanismos de seguridad

Servicios de seguridad

| | Cifrado | Firma digital | Control acceso | TTP | Control rutas | Aleatoriedad |
|---|---|---|---|---|---|---|
| **Autenticación** | X | X | | X | | |
| **Autorización** | | | X | | | |
| **Confidencialidad** | X | X | | | X | X |
| **Integridad** | X | X | | | | |
| **No repudio** | | | | X | | |

- **Consideraciones de diseño:** “Sistema de Comunicación seguro”



# • **Consideraciones de diseño:** Diseño de un entorno seguro

Ser paranoico
- Aplicación de la ley de Murphy

Tener en cuenta el entorno
- Existen entradas y salidas

Plan de contingencia
- Seguridad reactiva ante detección de ataques

Seguimiento de los procesos
- Vinculado a la trazabilidad

El eslabón más débil son las personas
- No leen, no prestan atención, no pensamos, …

Configuraciones por defecto óptimas
- Ante reinicios estado de máxima restricciones

Características del sistema criptográfico empleado

Algoritmo, longitud de claves, etc.

Elementos externos de apoyo

Gestión de claves

Token criptográfico: tarjetas inteligentes, etc.

Actualizaciones de sistema operativo

# • **Consideraciones de diseño:** Seguridad del sistema

Las tres leyes de Shamir (uno de los inventores de RSA) sobre la seguridad de sistemas:

- No existen sistemas absolutamente seguros
- Para reducir a la mitad tus vulnerabilidades, tienes que doblar tu inversión
- La mayor parte de los ataques más que atacarlas, evitan las protecciones criptográficas

Es más fácil atacar los elementos no criptográficos (el factor humano, p.ej.) que los algoritmos

**Seguridad Multicapa**

Física
Espectro ensanchado, …

Enlace
WEP, WPA, BT PIN,

Red
IPSec, Tunel, VPN, …

Transporte
SSL, TLS, …

Aplicación
SSH, HTTPS, …

# • **Consideraciones de diseño:** Seguridad de Red (Resumen)

**Aspectos básicos de la seguridad de redes**

- Control de acceso
- Segmentación de la red
- Seguridad perimetral
- Cifrado de datos

**Tipos de seguridad de la red**

- *Firewalls*
- Sistemas de detección y prevención de intrusiones (IDPS)
- *Software* antivirus o *antimalware*
- Control de acceso a la red (NAC)
- Seguridad en la nube
- Redes privadas virtuales (VPN)
- Prevención de pérdida de datos (DLP)
- Protección de puntos finales "*endpoints*"
- Gestión unificada de amenazas (UTM)
- Puerta de enlace web segura (SWG)

**Áreas vulnerables:**
**¿Dónde suele fallar la seguridad de una red?**

- Cualquier intercambio de archivos riego de ser infectado por un malware
- El correo electrónico, riesgo de malware
- Uso de sistemas operativos y programas desactualizados, malware
- Las extensiones ocultas que aparecen al descargar y abrir archivos supuestamente seguros
- Las plataformas de mensajería y los chatbots también pueden transmitir malware mediante archivos adjuntos y enlaces.
- La seguridad en redes inalámbrica

- **Tareas**

  - **Hacer un glosario de terminos sobre seguridad en redes**

Mail: pedro.escudero@unach.edu.ec
Telf: 0994667184