Seguridad en Sistemas de Información

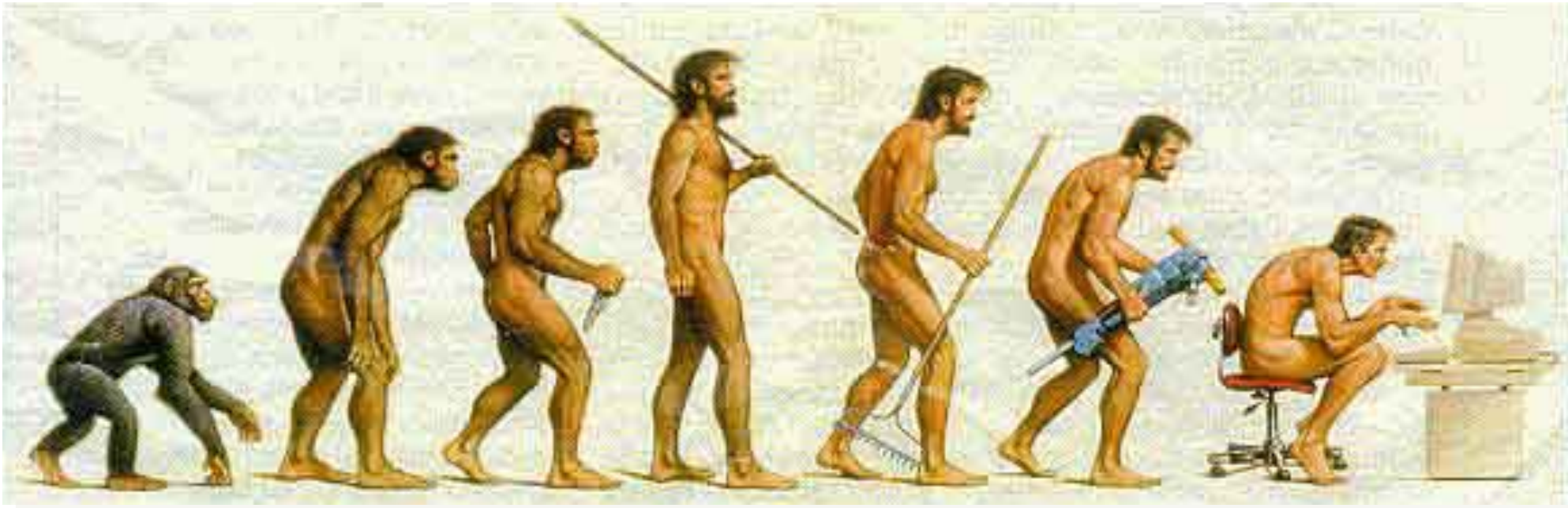
Curso en Zacatenco y Tamaulipas [Q2 2013]

Luis Gerardo de la Fraga, Arturo Díaz, y Luis Julián Domínguez

Cinvestav, Mayo 13 de 2013

Contenido, sección 1

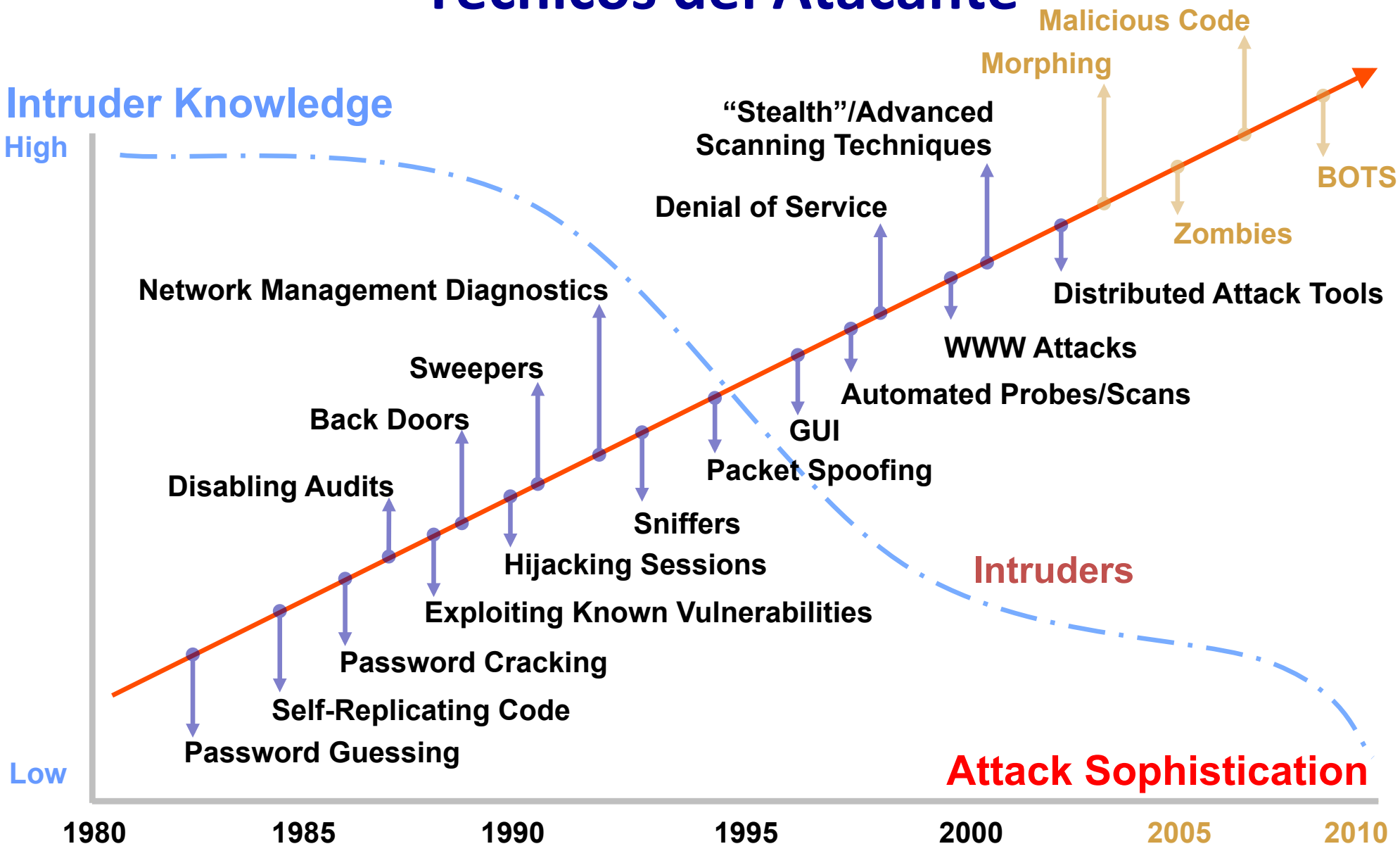
Seguridad Informática, ¿Para Qué?



La Evolución a la Era de la Información

Aspectos de Seguridad Informática

Sofisticación de Ataques vs. Conocimientos Técnicos del Atacante



Sources: *Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005*

Terminología

Activos

Los elementos que pertenecen a la empresa y que se quieren proteger

- Datos, instalaciones, software, hardware, personal, servicios

Amenazas

- Interrupción
- Interceptación
- Modificación
- Fabricación

Riesgo

La posibilidad de que se materialice una amenaza aprovechando una **vulnerabilidad**

Ataque

La materialización de una amenaza

Impacto

Consecuencia de un ataque

¿Por qué seguridad?

Errores reales

Vulnerabilidades

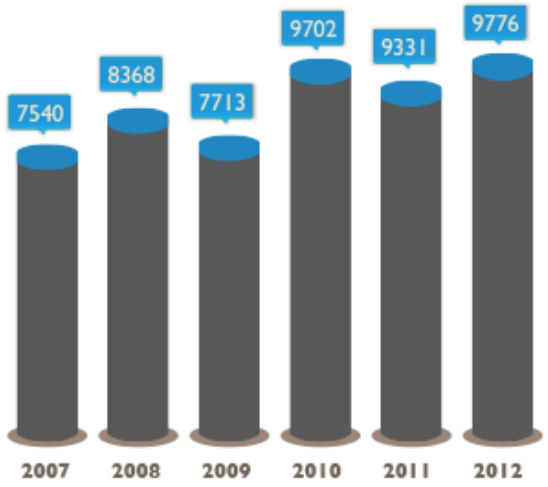
Definición

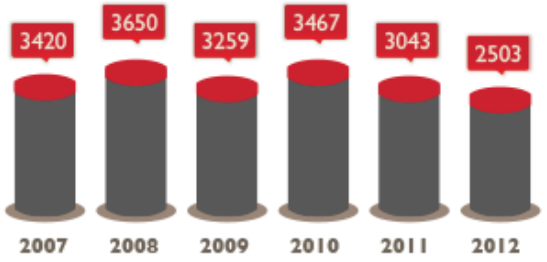
Una vulnerabilidad está definida en el estándar ISO 27002 como: "Una debilidad de un activo o un grupo de activos que puede ser explotada por una o más amenazas" (International Organization for Standardization, 2005).

El ISO/IEC 27002 es un estándar para la seguridad de la información: "Information technology - Security techniques - Code of practice for information security management".

Reporte sobre Vulnerabilidades

Fuente: Secunia Vulnerability Review 2013. secunia.com





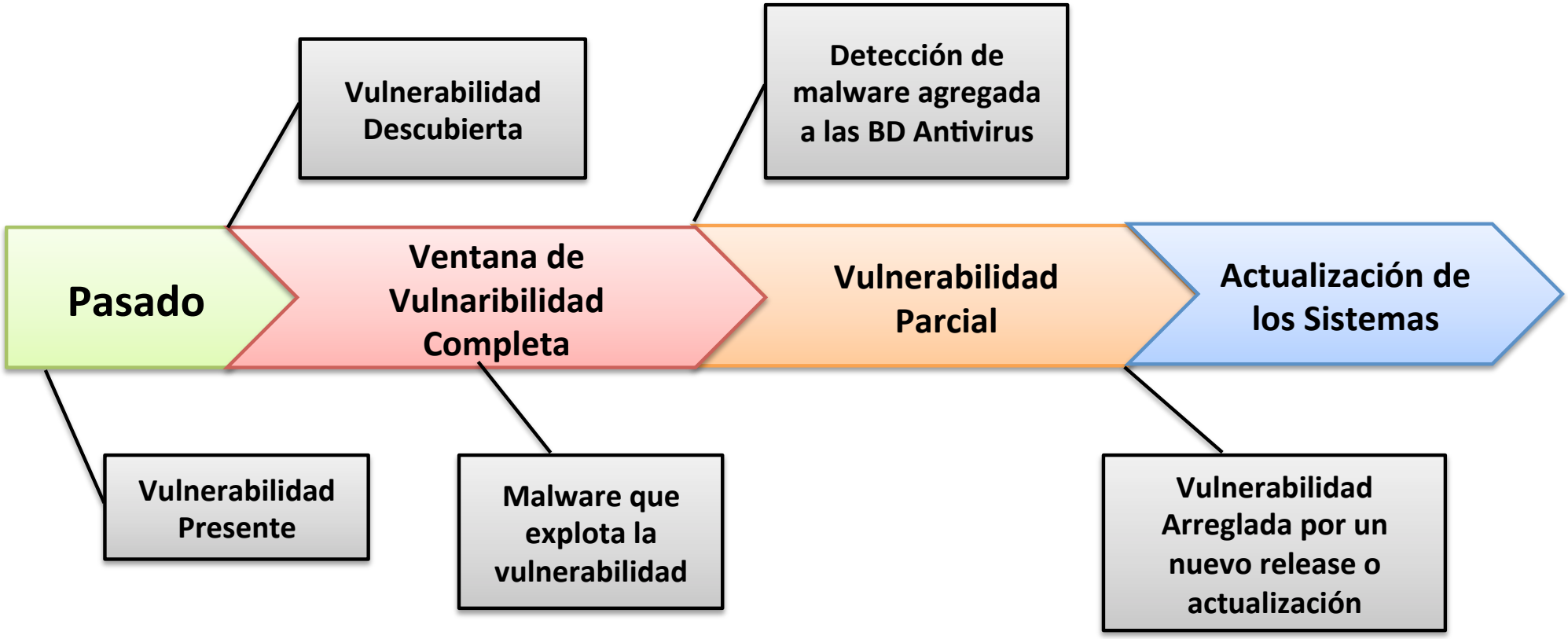
There is an increase in vulnerabilities, and a decrease in the number of vendors and products vulnerabilities are discovered in.

How dangerous are the vulnerabilities for all products/vendors?

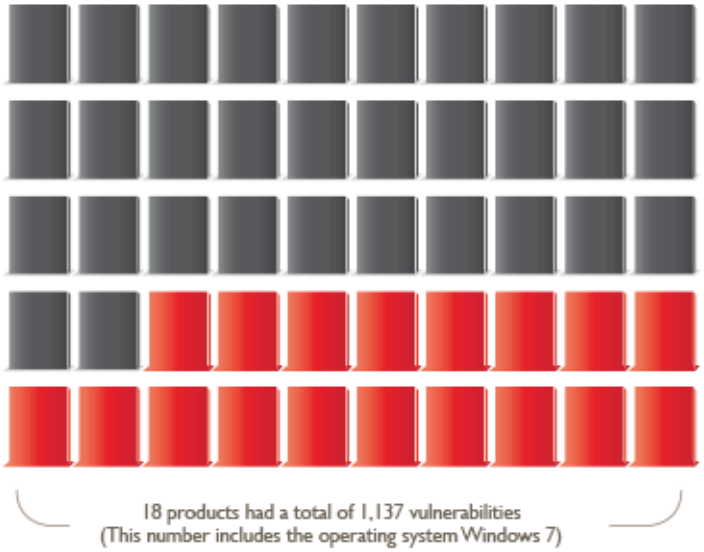
Vulnerabilidad

Es un fallo en el diseño o configuración de un software

Una vulnerabilidad genera un expedinte de seguridad identificado por su CVE (Common Vulnerabilities and Exposure)

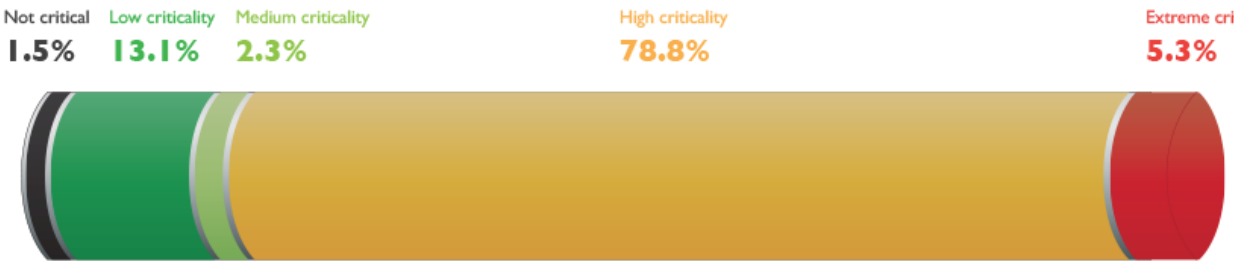


Vulnerabilidades en los programas más usados



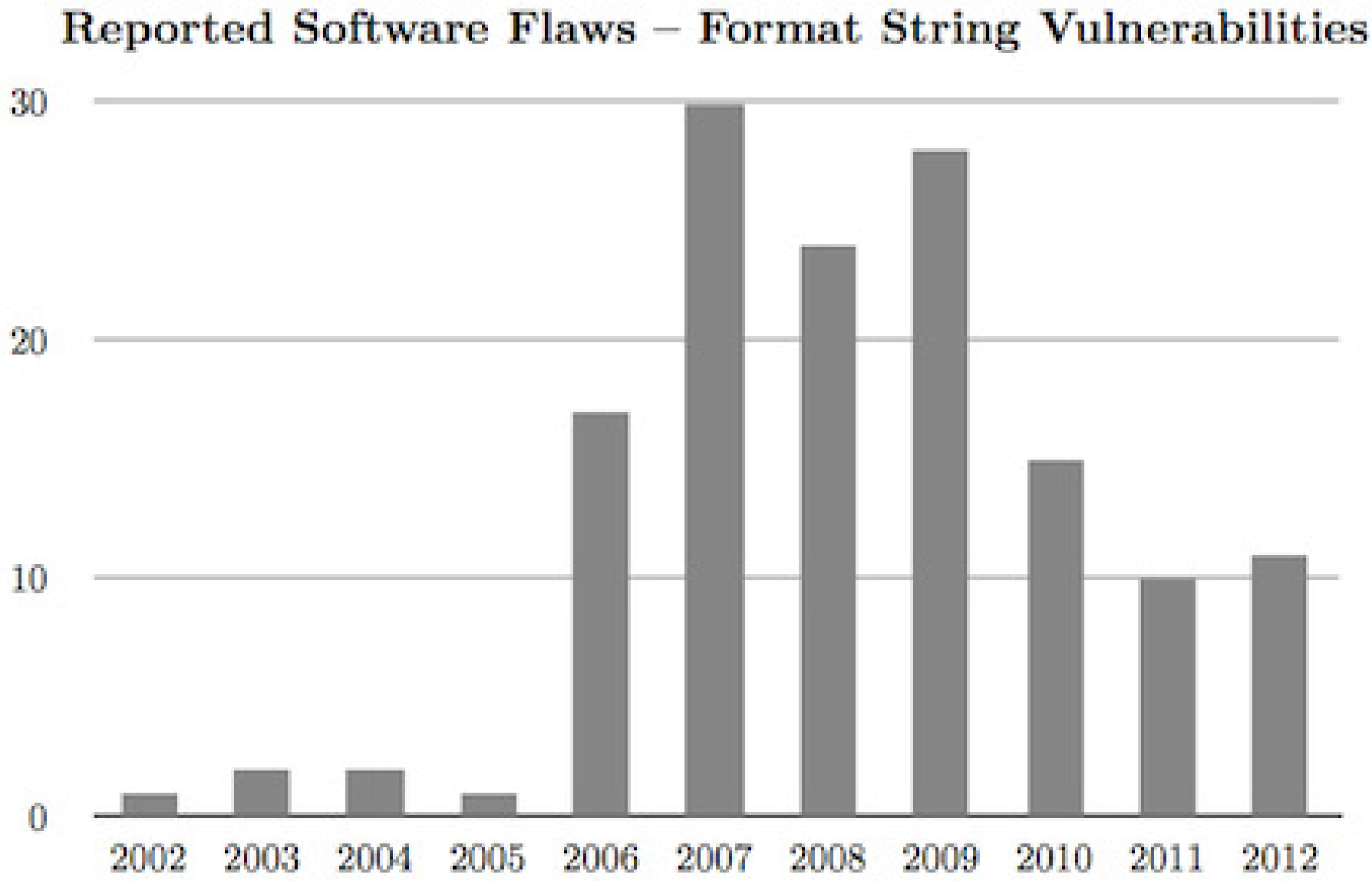
18 products had a total of 1,137 vulnerabilities
(This number includes the operating system Windows 7)

GOOGLE CHROME	291
MOZILLA FIREFOX	257
APPLE ITUNES	243
ADOBE FLASH PLAYER	67
ORACLE JAVA JRE SE	66
ADOBE AIR	56
MICROSOFT WINDOWS 7	50
ADOBE READER	43
MICROSOFT INTERNET EXPLORER	41
APPLE QUICKTIME	29
MICROSOFT .NET FRAMEWORK	14
VLC MEDIA PLAYER	11
MICROSOFT EXCEL	10
MICROSOFT VISIO VIEWER	7
MICROSOFT SILVERLIGHT	5
MICROSOFT WORD	3
SKYPE	1
MICROSOFT XML CORE SERVICES (MSXML)	1

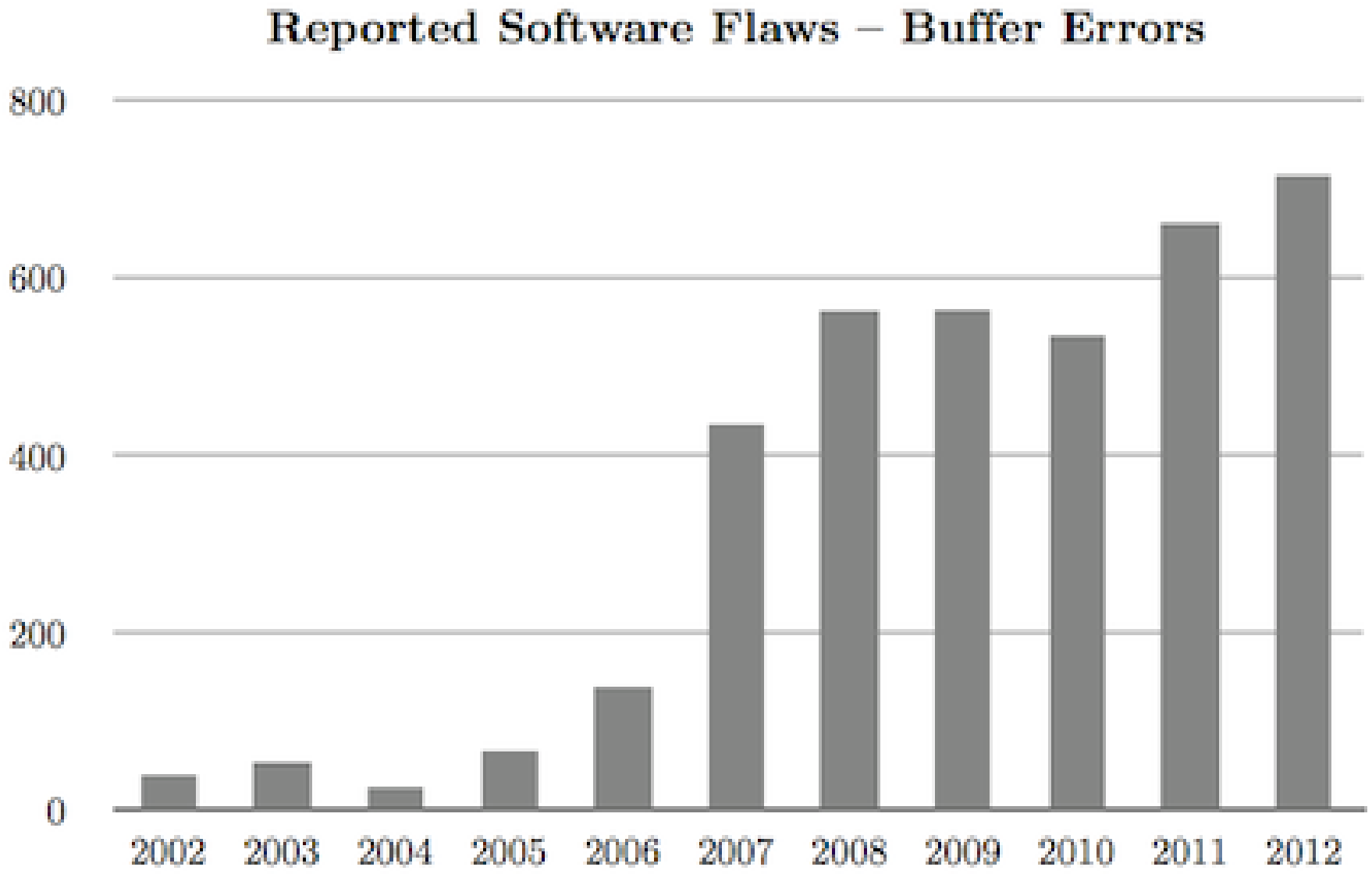


Fuente: Secunia Vulnerability Review 2013. secunia.com

Vulnerabilidades de formato de cadena



Vulnerabilidades de formato de cadena



Vulnerabilidades Zero-Day

Definición

Es una vulnerabilidad previamente desconocida, y por la que no existe una solución.

Lo de zero-day viene dado a que las empresas tienen cero días para preparar una solución.

Ataque Zero-day

Es un ataque o amenaza que explota una vulnerabilidad desconocida.

Un atacante utiliza una vulnerabilidad desconocida por los fabricantes para entrar a sistemas externos o internos.

El negocio de las vulnerabilidades Zero-day

- Un hacker brillante, podría encontrar una vulnerabilidad en el, digamos, iPad, iPhone, etc., reportarle a Apple, dar una conferencia, y ser famoso por un tiempo.
- Alternativamente, podría reportar la vulnerabilidad a HP Zero Day's Initiative, y ganarse unos $10,000 USD.

En ambos casos, Apple corregiría el error, y en un tiempo razonable, tendríamos la actualización en todos los dispositivos.

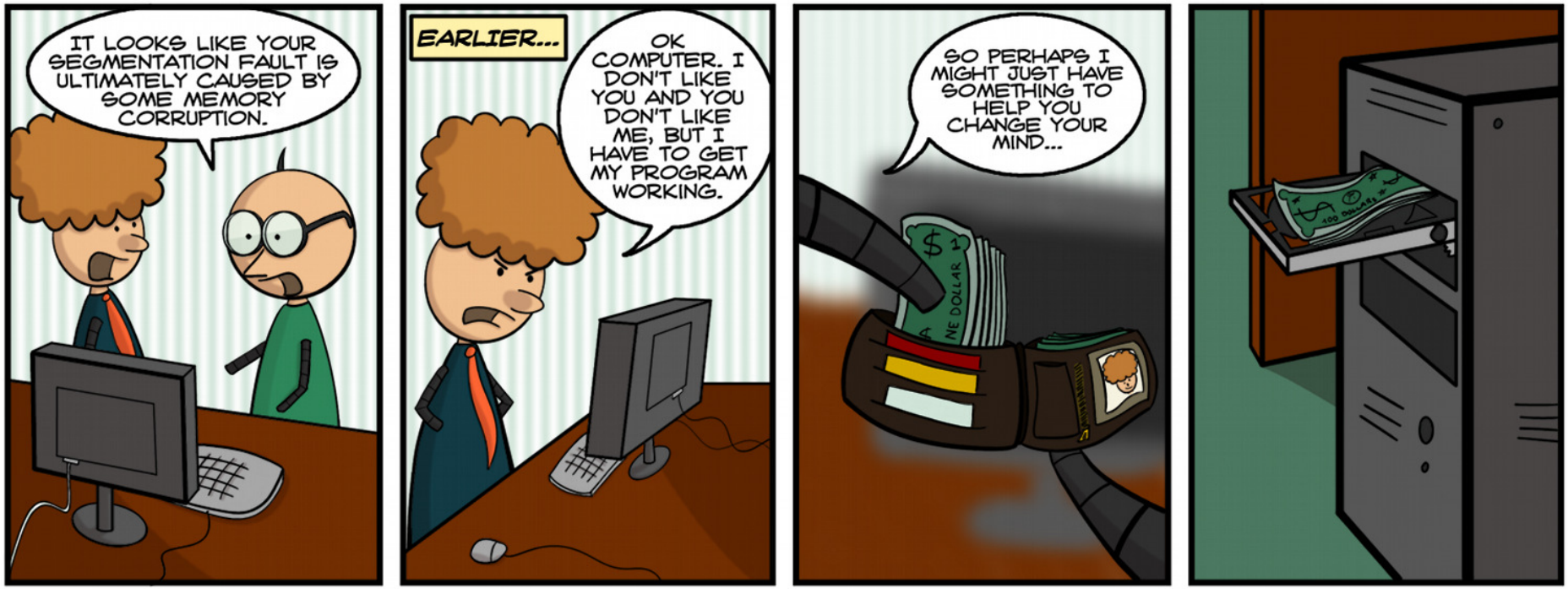
El negocio de las vulnerabilidades Zero-day 2

- Sin embargo, si uno conoce a un agente de colocación, uno tiene una tercera opción: venderla anónimamente a una agencia gubernamental (de cualquier gobierno). Los precios varían:

Adobe Reader	$\$5,000 - \$30,000$
Mac OS X	$\$20,000 - \$50,000$
Android	$\$30,000 - \$60,000$
Flash/Java plugin	$\$40,000 - \$100,000$
Word	$\$50,000 - \$100,000$
Windows	$\$60,000 - \$120,000$
Firefox / Safari	$\$60,000 - \$150,000$
Chrome / IE	$\$80,000 - \$200,000$
iOS	$\$100,000 - \$250,000$

  - a Sep. 2012.

Corrupción de memoria. . .



Ejemplo

Gets

```
#include <stdio.h>
int main () {
    char username[8];
    int allow = 0;
   printf external link("Enter your username, please: ");
    gets(username);
    if (grantAccess(username)) {
        allow = 1;
    }
    if (allow != 0) {
        privilegedAction();
    }
    return 0;
}
```

Ejemplo 2

Symlink

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define MY_TMP_FILE "/tmp/file.tmp"


int main(int argc, char* argv[])
{
    FILE * f;
    if (!access(MY_TMP_FILE, F_OK)) {
        printf external link("File exists!\n");
        return EXIT_FAILURE;
    }
    tmpFile = fopen(MY_TMP_FILE, "w");

    if (tmpFile == NULL) {
        return EXIT_FAILURE;
    }

    fputs("Some text...\n", tmpFile);

    fclose(tmpFile);

    return EXIT_SUCCESS;
}
```

Resolviendo una vulnerabilidad

Cronología sobre una vulnerabilidad crítica del Internet Explorer en el 2012:

- Septiembre 14, 2012 – El investigador de seguridad, Eric Romang, descubre una vulnerabilidad
- Septiembre 16, 2012 – Se publican los detalles específicos de la vulnerabilidad
- Septiembre 17, 2012 – Metaploit publica un exploit de juguete para dicha vulnerabilidad. El mismo día, Microsoft libera un aviso de seguridad, y recomienda a los usuarios utilizar el Enhanced Mitigation Experience Toolkit.
- Septiembre 18, 2012 – El CVE asigna el código CVE-2012-4969 a esta vulnerabilidad

Resolviendo una vulnerabilidad 2

- Septiembre 19, 2012 – Microsoft libera un artificio para darle la vuelta a la vulnerabilidad, configurando al Internet Explorer a ejecutarse en modo seguro (sin plug-ins). La solución temporal sólo funcionó para la versión de 32-bits.
- Septiembre 21, 2012 – Microsoft libera un parche de emergencia para arreglar esta vulnerabilidad en el Internet Explorer.

Resolviendo una vulnerabilidad 2

- Septiembre 19, 2012 – Microsoft libera un artificio para darle la vuelta a la vulnerabilidad, configurando al Internet Explorer a ejecutarse en modo seguro (sin plug-ins). La solución temporal sólo funcionó para la versión de 32-bits.
- Septiembre 21, 2012 – Microsoft libera un parche de emergencia para arreglar esta vulnerabilidad en el Internet Explorer.

- Sin embargo, Eric Romang no fue citado por encontrar la vulnerabilidad. . . ya que Microsoft sabía de la misma de 1 mes a 1 año antes.

Resolviendo una vulnerabilidad 2

- Septiembre 19, 2012 – Microsoft libera un artificio para darle la vuelta a la vulnerabilidad, configurando al Internet Explorer a ejecutarse en modo seguro (sin plug-ins). La solución temporal sólo funcionó para la versión de 32-bits.
- Septiembre 21, 2012 – Microsoft libera un parche de emergencia para arreglar esta vulnerabilidad en el Internet Explorer.

- Sin embargo, Eric Romang no fue citado por encontrar la vulnerabilidad. . . ya que Microsoft sabía de la misma de 1 mes a 1 año antes.
- ¿Porqué Microsoft no la arregló antes?

Common Vulnerabilities and Exposures — CVE

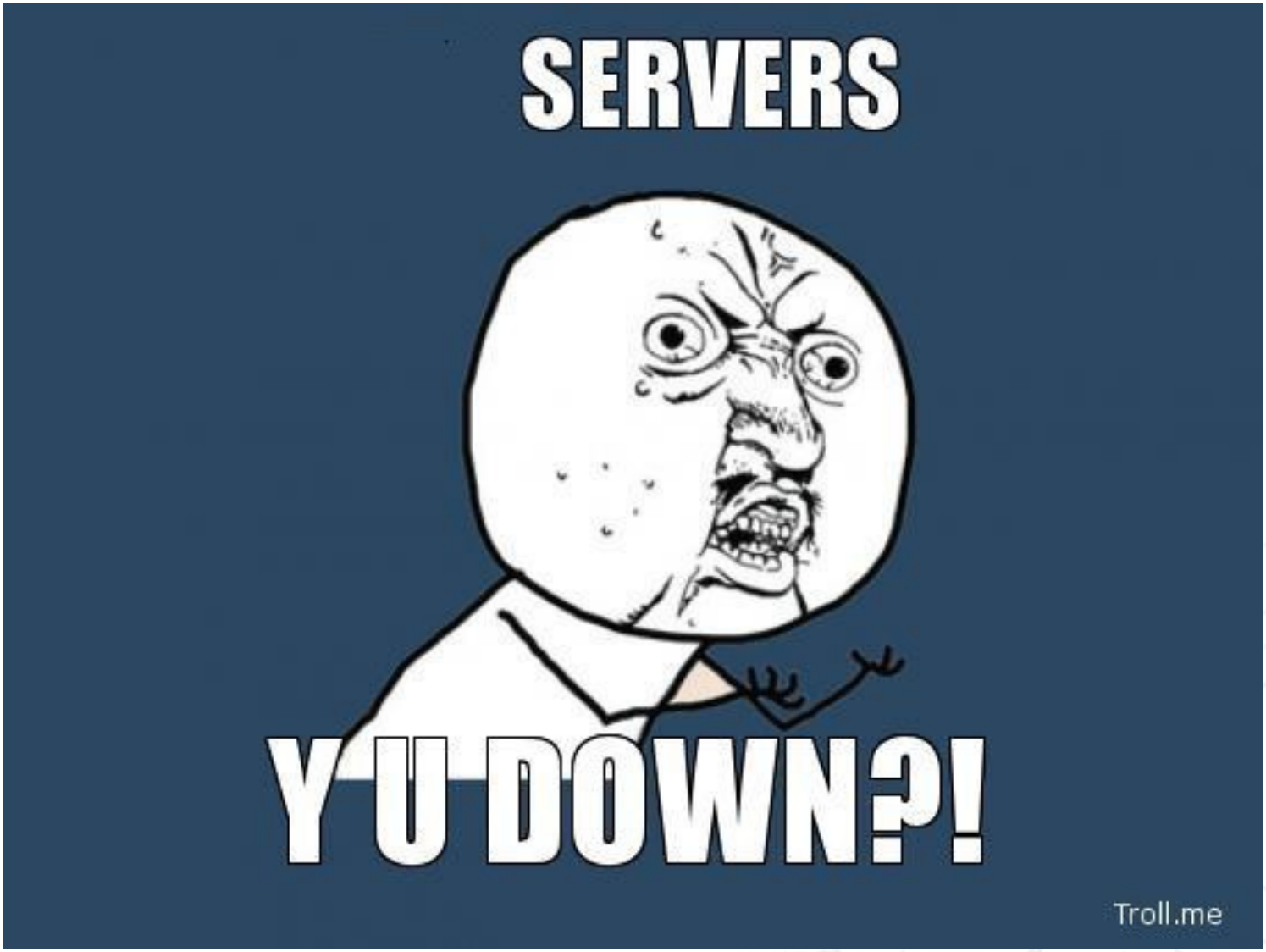
- CVE comenzó en 1999 cuando cada proveedor asignaba y medía sus vulnerabilidades a conveniencia.
- CVE es el estándar industrial para identificar las vulnerabilidades.
- Provee identificadores únicos.
- Establece criterios comunes para evaluar vulnerabilidades, herramientas y servicios.

Consecuencias de las vulnerabilidades

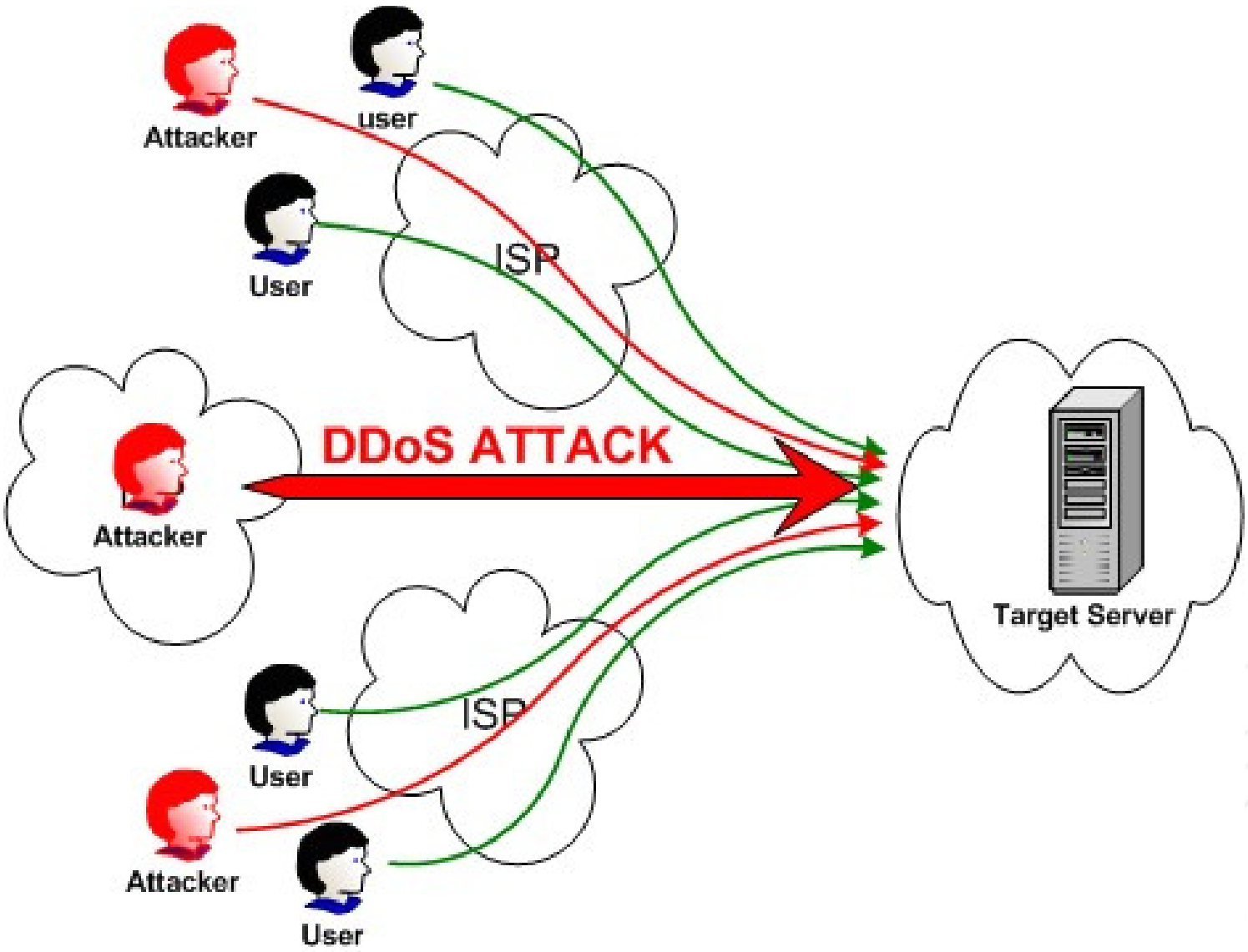
- Existen muchas consecuencias como resultado de una vulnerabilidad:

Consecuencias de las vulnerabilidades

- Existen muchas consecuencias como resultado de una vulnerabilidad:



Ataque DOS

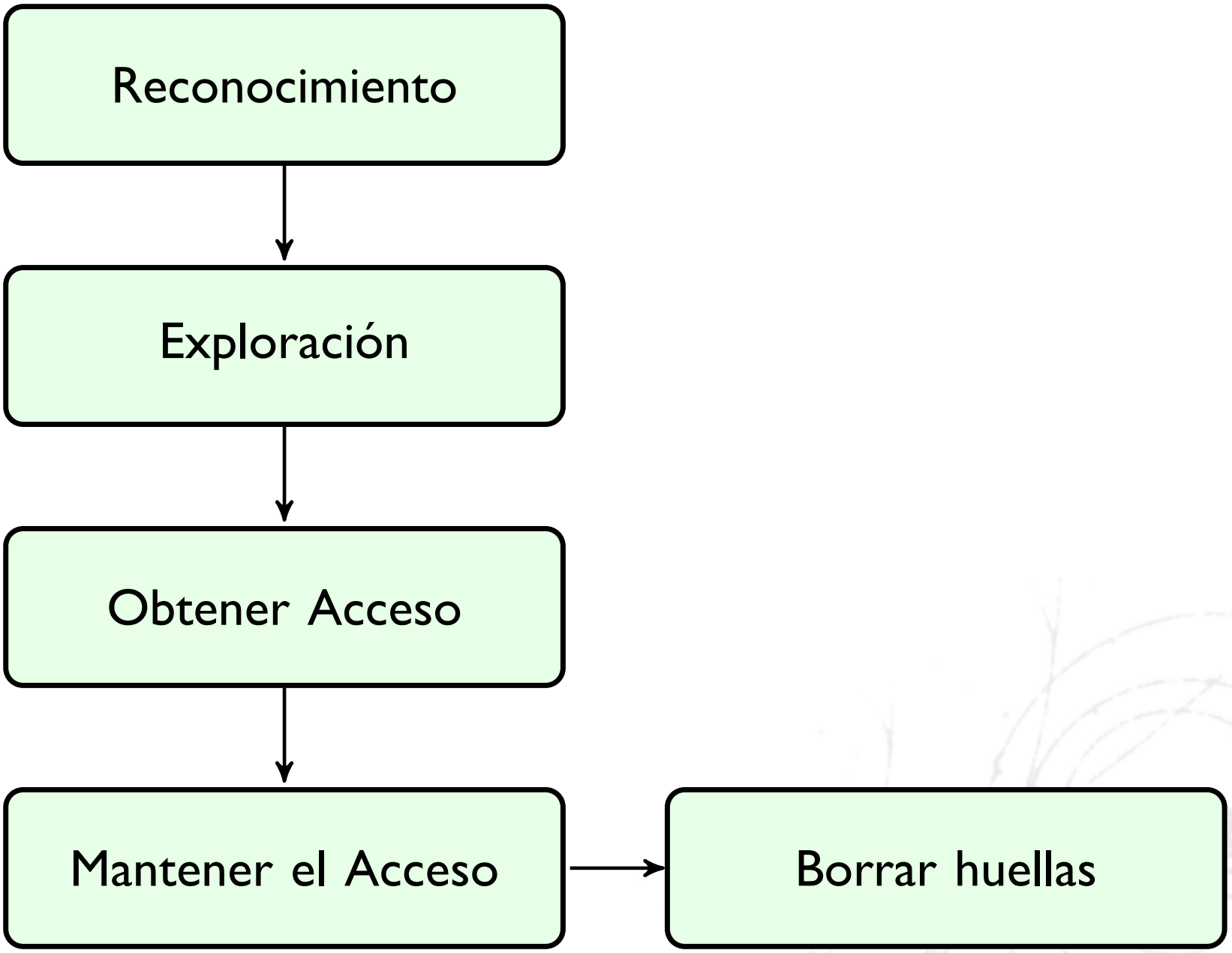

Attacker
user
User
ISP
DDoS ATTACK
Attacker
Target Server
User
ISP
Attacker
User

Ataques de red

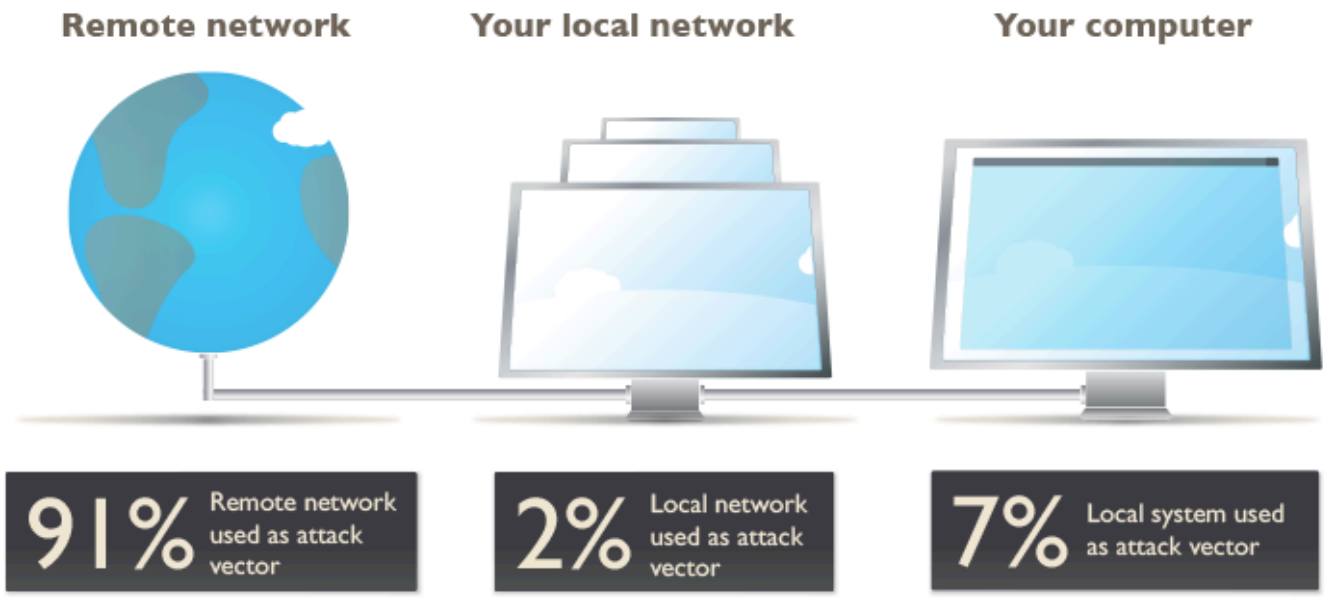
Existen muchos tipos de ataques en la red.

- Denegación de servicio
- Man-in-the-middle
- XSS
- Overflow
- Mail relay
- DNS hijacking
- IP spoofing
- Eavesdropping
- Sniffing
- Modificación de datos
- Destrucción de infraestructura
- etc.

Etapas de un ataque



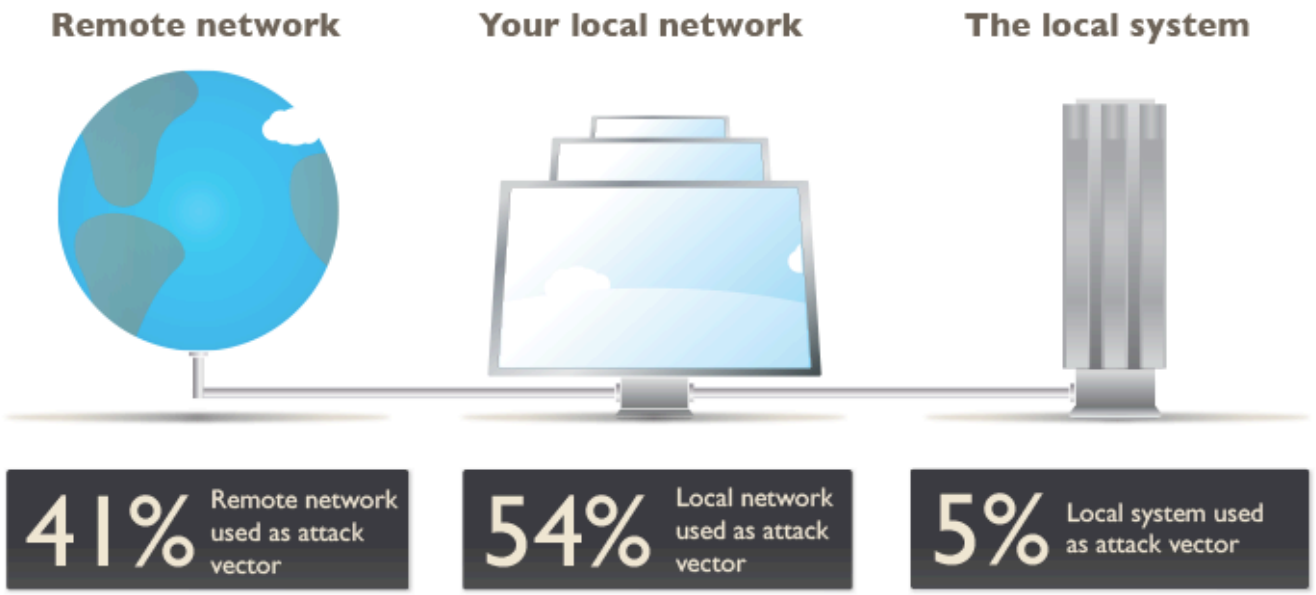
Origen de los Ataques



The majority of attacks are carried out by a hacker from a remote network, where the attacker is not required to have access to the system or a local network in order to exploit the vulnerability.

Fuente: Secunia Vulnerability Review 2013. secunia.com

Seguridad SCADA



Fuente: Secunia Vulnerability Review 2013. secunia.com

¿Quiénes hacen el hacking?

- Hay muchos involucrados en los ataques, por instancia:
  - White hat
  - Black hat
  - Grey hat
  - Elite hacker
  - Script kiddie
  - Neophyte
  - Blue hat
  - Hacktivist
  - Nation state
  - Organized criminal gangns
  - Bots

Hacktivistas vs. Criminales

Discusión: ¿Son criminales? ¿Porqué sí, y porqué no?

Otras razones

Los ataques en la red vienen dados por diferentes razones:

- Errores de diseño de los protocolos de red
- Errores de implementación de los protocolos de red
- Errores de diseño de la arquitectura de red
- Falta de presupuesto
- Descuidos en la configuración de los equipos
- Factores externos (e.g. vulnerabilidades, pero otras más también)

Mecanismos de contensión 1/2

Salvo que se tenga una importante suma de dinero en infraestructura, la mayoría de los ataques podrían ser efectivos. Sin embargo, un ataque se puede evitar si existen suficientes factores que lo desmotiven.

Esto es, no existe una fórmula 100% efectiva, y salvo que se trate de un ataque específico contra la compañía, se pueden activar prácticas adecuadas para que un ataque automatizado, o de un amateur desista.

Mecanismos de contensión 2/2

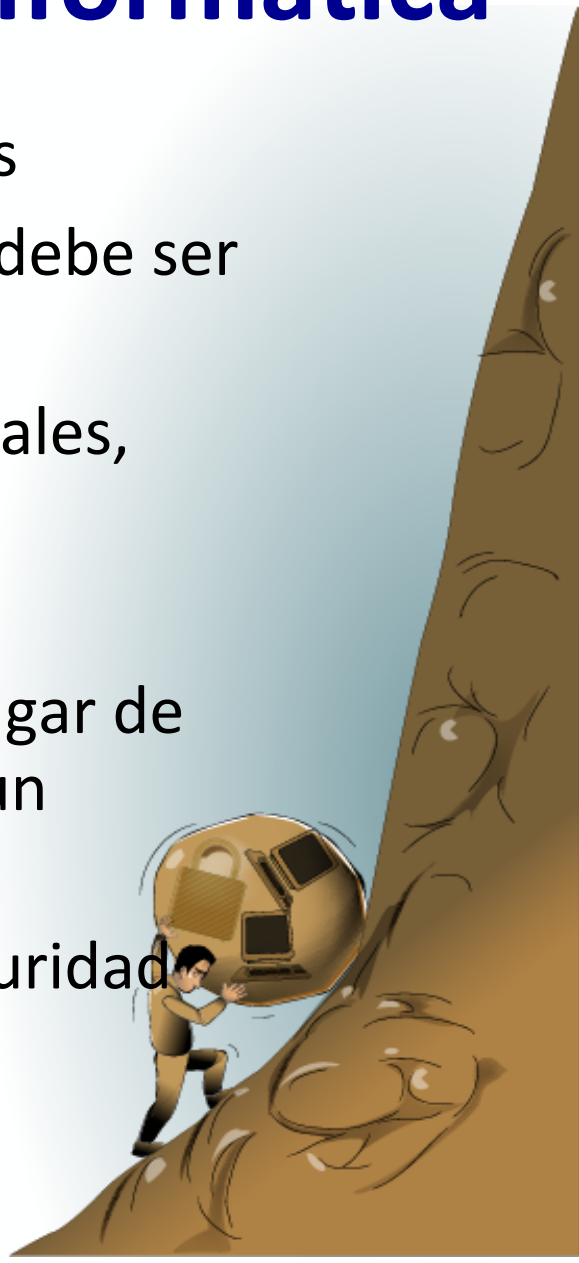
Además de prácticas seguras, existen mecanismos palpables a instalar en la red:

- Firewall
- Detector de intrusiones
- Prevensor de intrusiones
- Pasarela de aplicación
- Bitácoras
- Políticas
- etc.

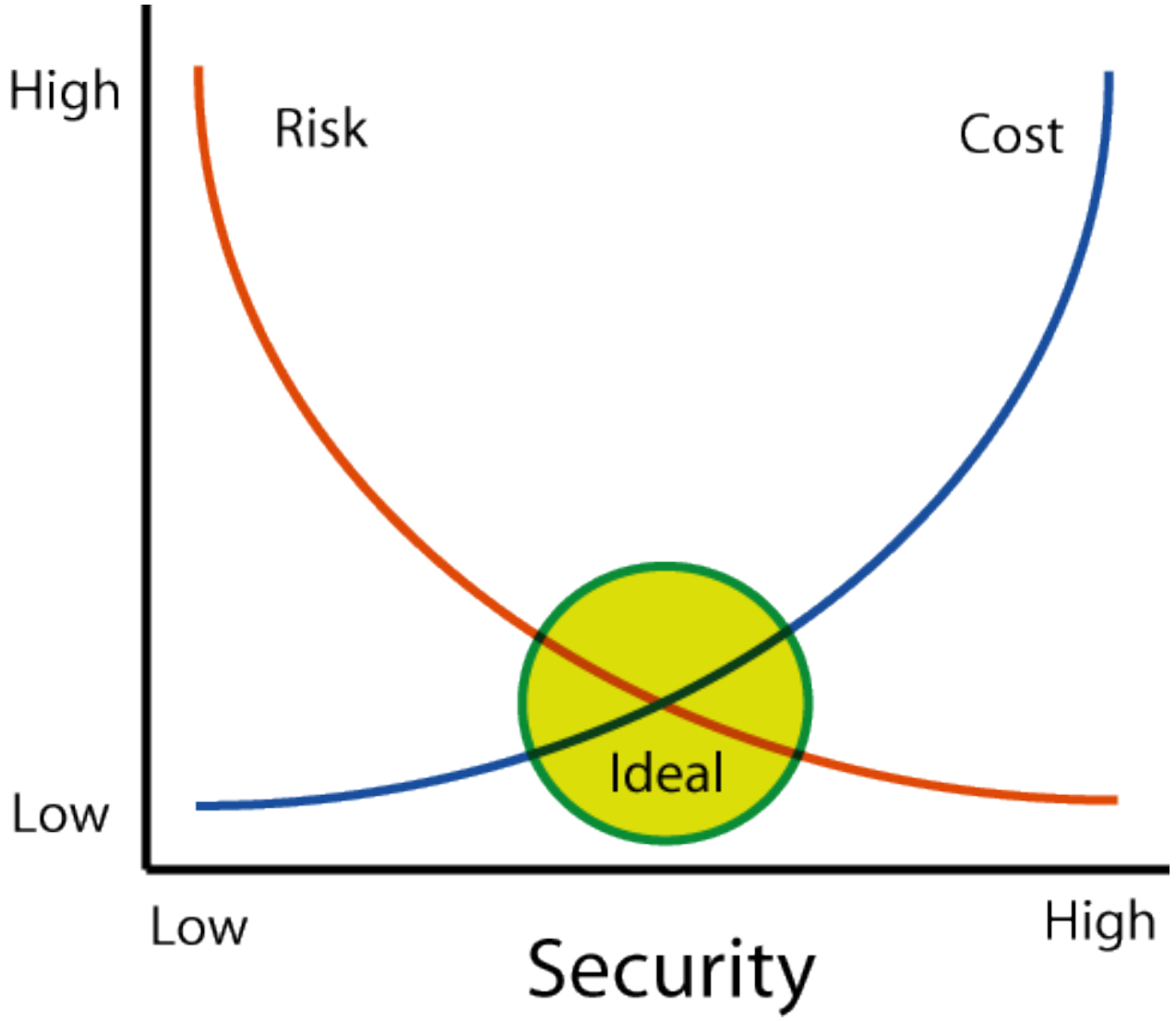
Contenido, sección 2

El Problema de la Seguridad Informática

- Abstracto, tiene que ver con eventos hipotéticos
- Un problema no solamente técnico; la solución debe ser holística, a nivel organizacional
- Intervienen aspectos tecnológicos, organizacionales, normativos, económicos y sociales
- No existen métricas ampliamente aceptadas
- Una estrategia de prevención de desastres en lugar de beneficios directos para la organización (como un seguro)
- La instalación de mecanismos de control de seguridad puede tener aspectos negativos
  - Costos adicionales, disminución en el rendimiento, inconvenientes por parte de los usuarios

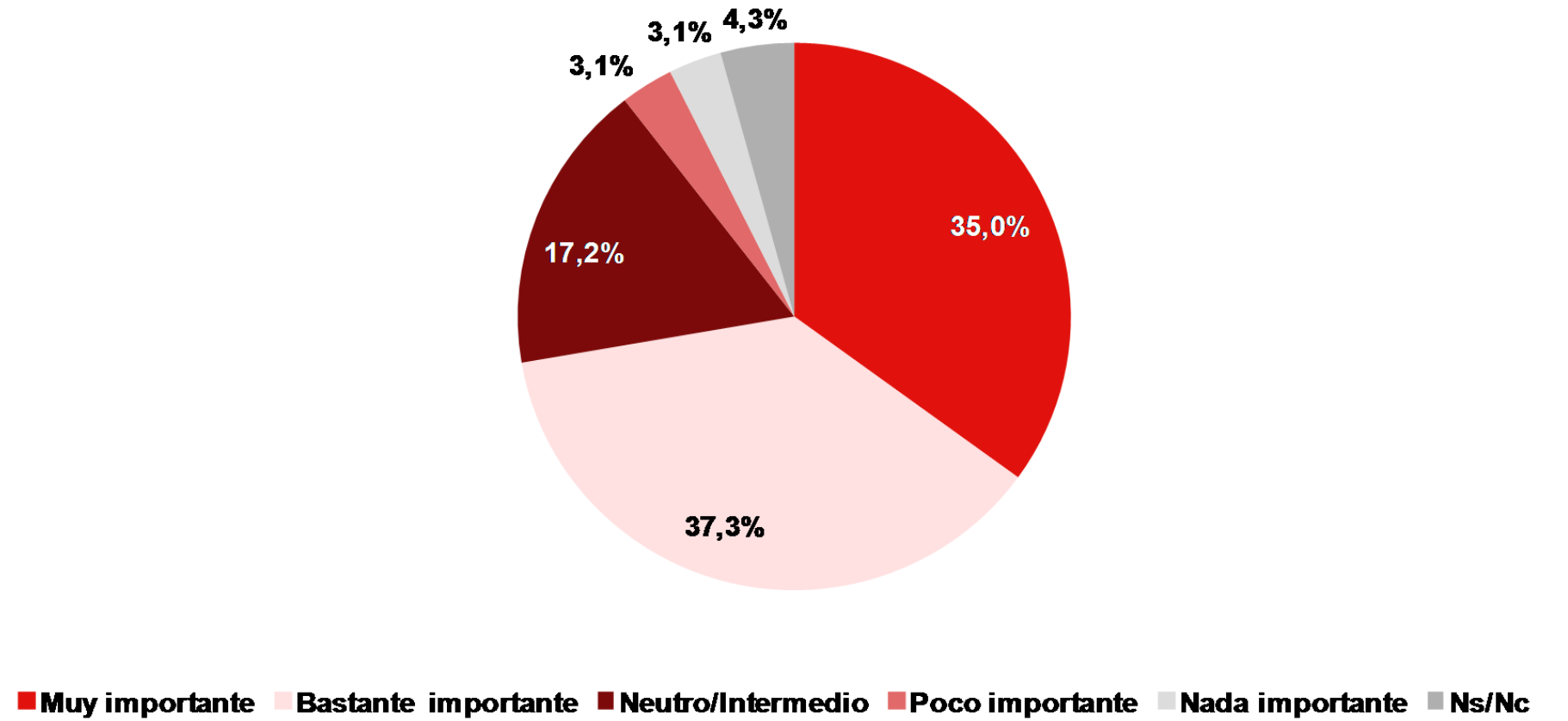


Costo vs Riesgo



Medidas de Seguridad Informática

Nivel de importancia que la Dirección de la empresa otorga a la seguridad de la información

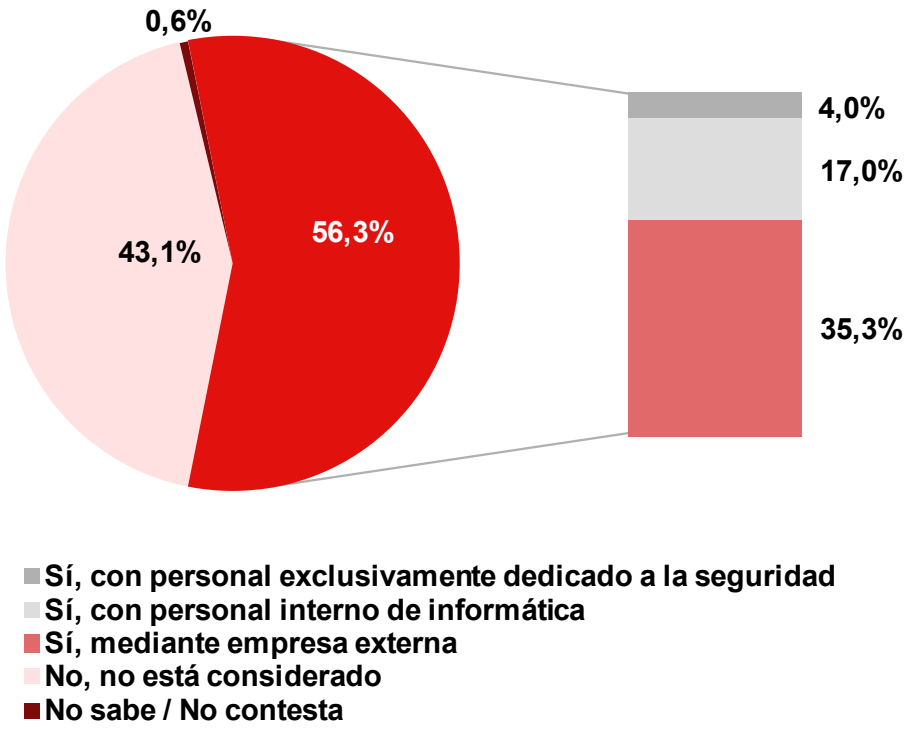


Base: total empresas que responden al cuestionario de seguridad (n=1.144)

Fuente: ***Estudio sobre la seguridad en la información y continuidad en el negocio de empresas españolas***. INTECO. 2012. www.inteco.es.

Medidas de Seguridad Informática

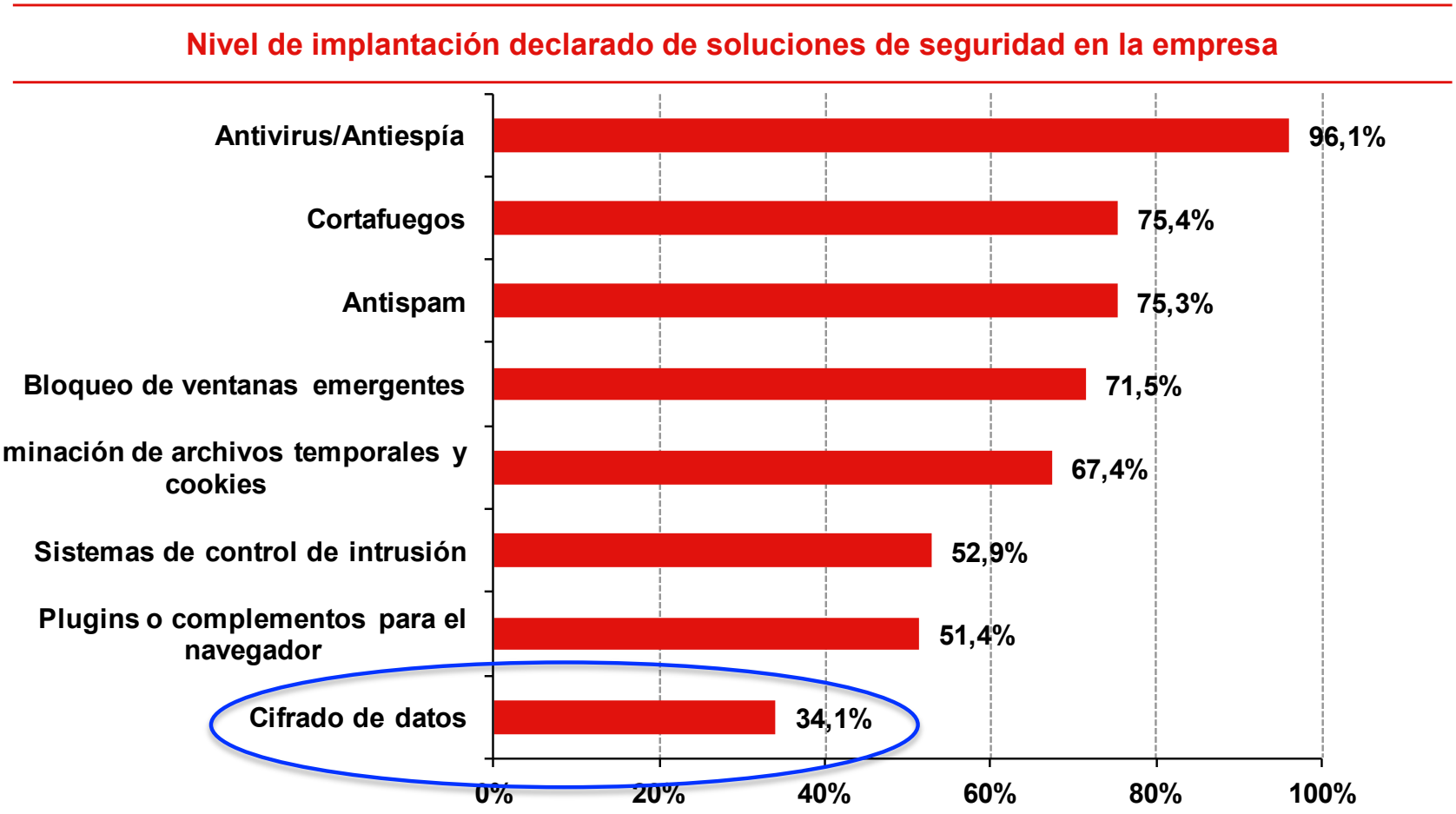
Personal dedicado a la seguridad de la información



Base: empresas que participan en el cuestionario de seguridad (n=1.144)

Fuente: ***Estudio sobre la seguridad en la información y continuidad en el negocio de empresas españolas***. INTECO. 2012. www.inteco.es.

Medidas de Protección



Fuente: ***Estudio sobre la seguridad en la información y continuidad en el negocio de empresas españolas***. INTECO. 2012. www.inteco.es.

Medidas de Seguridad Informática

Motivos para no aplicar medidas de seguridad

Soluciones	% Empresas que no lo utilizan	No conoce	No necesita	Precio	Ineficaces	Entorpecen	Otros	No contesta
Antivirus / Antiespía	3,9	2,3	39,6	0,4	5,1	17,4	14,9	20,3
Cortafuegos	24,6	35,6	27,2	3,2	0,8	2,8	0,2	30,2
Antispam	24,7	28,0	38,8	0,1	0,8	3,8	0,2	28,3
Plugins	48,6	37,0	28,4	0,5	0,5	2,0	0,4	31,2
Bloqueo de ventanas emergentes	28,5	33,3	29,7	0,0	0,9	2,9	0,2	33,0
Sistemas de control de intrusión	47,1	38,0	26,0	1,4	0,4	2,1	0,2	31,9
Cifrado de datos	65,9	35,1	35,2	0,4	0,5	1,6	0,8	26,4
Eliminación de archivos temporales y cookies	32,6	29,1	32,5	0,7	1,1	3,1	1,5	32,0

Base: empresas que no utilizan las herramientas y soluciones de seguridad

Fuente: ***Estudio sobre la seguridad en la información y continuidad en el negocia de empresas españolas***. INTECO. 2012. www.inteco.es.

Seguridad Informática

- El conjunto de **servicios y mecanismos** que aseguren la **integridad** y **privacidad** de la **información** que los sistemas manejen
- El conjunto de servicios, mecanismos y **políticas** que aseguren que el **modo de operación** de un sistema sea **seguro.** El que se especificó en la fase de diseño o el que se configuró en tiempo de administración
- El conjunto de **protocolos** y mecanismos que aseguren que la **comunicación** entre los sistemas esté **libre de intrusos**

Servicios de la Seguridad Informática

- Un conjunto de recursos destinados a lograr que los activos de una organización sean confidenciales, íntegros, consistentes y disponibles a sus usuarios, autenticados por mecanismos de control de acceso y sujetos a auditoría.
  - Confidencial
  - Íntegro
  - Consistente
  - Disponible
  - *Autenticado*
  - *Control de acceso*
  - *Auditoría*

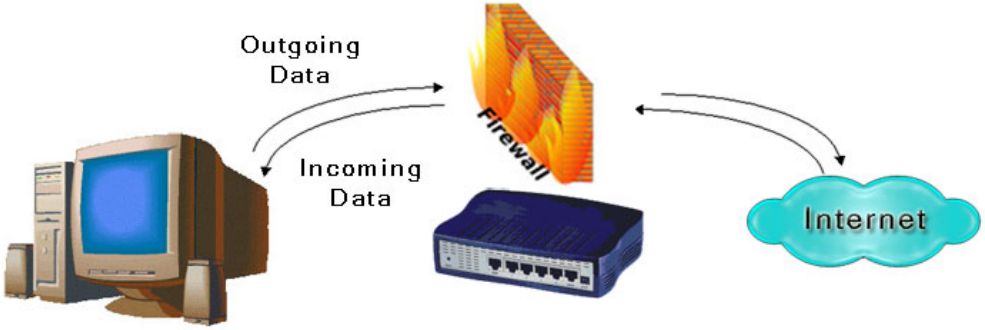
Clasificación de la Seguridad Informática

Física

Lógica

Pasiva

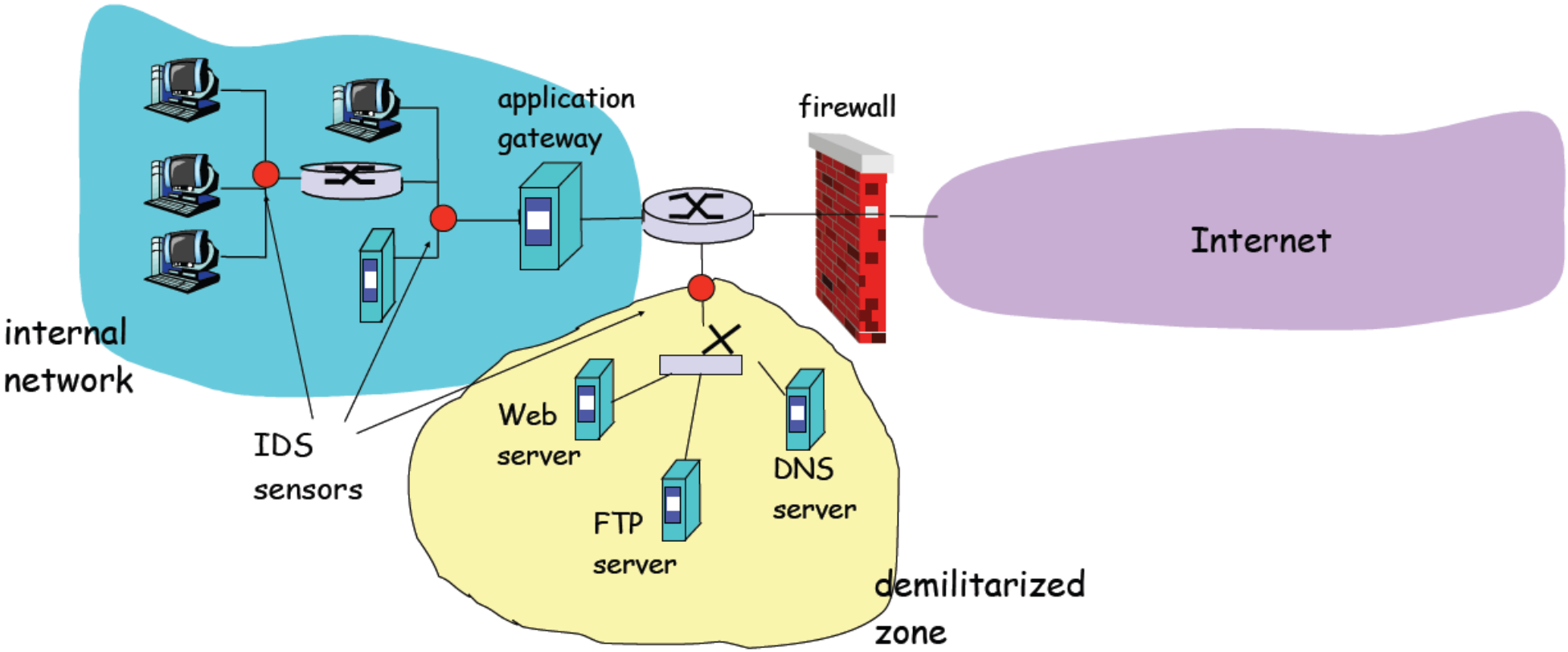
Activa



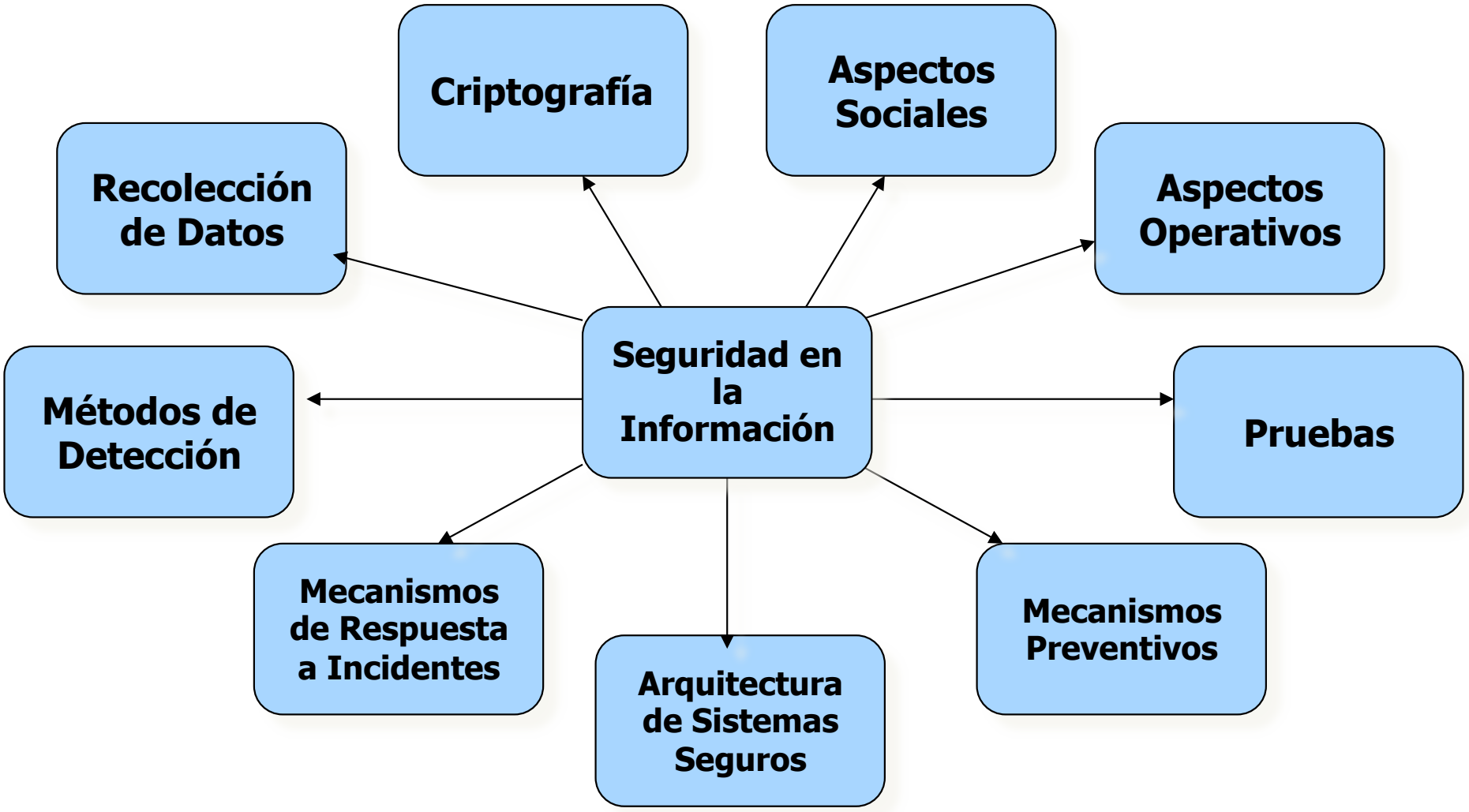
Mecanismos en la Seguridad Informática

- Autenticación
- Autorización
- Verificación de la integridad de la información
- Cifrado/Descifrado
- Certificados/Firmas Digitales
- Copias de seguridad
- Software anti-malware
- Firewall
- IDS/IPS
- Auditoría
- Políticas: inspección de información

Sensores para un IDS



Areas Relacionadas



Fundamentos de Seguridad Informática

Criptografía

- ❑ Mecanismos y algoritmos básicos para la
- ❑ Protección de la información.

Protocolos Seguros

- ❑ Servicios de Autenticación
- ❑ Comunicaciones seguras y transacciones

PKI – Infraestructura de Llave Pública

- ❑ Generación, distribución y administración de certificados de llave pública.

Políticas de Administración de Servicios

- ❑ Servicios de autorización y control de acceso
- ❑ Políticas y normas de seguridad
- ❑ Plan de continuidad en el negocio

Modelo de Capas para Sistemas de Seguridad

Herramientas, Políticas y Aplicaciones: cortafuegos, plan de continuidad en el negocio, políticas de uso de la firma electrónica, monedero digital, elecciones electrónicas, cómputo en la nube seguro, etc.

Protocolos de Comunicación: SSL/TLS/WTLS, IPSEC, IEEE 802.11, etc.

Servicios de Seguridad: Confidencialidad, Integridad de Datos, **Autenticación**, No-Repudio, Firmas Digitales, CD

Funciones Criptográficas: Cifrar/Descifrar, Firmar/Verificar: SHA-1, MD5

Criptografía de Llave Pública: RSA, ECC
Criptografía de Llave Simétrica: AES, DES, RC4, etc..

Aritmética Computacional con Números Grandes

Autenticación

Password authentication
Single sign on authentication
Lightweight Directory Access Protocol (LDAP) authentication
Access Control authentication
Network authentication
Biometric authentication
Weak authentication
Strong authentication
Two-factor authentication

PKI authentication
Security token authentication
Smart card authentication
Wireless authentication
Message authentication
Document authentication
Transaction authentication
Federated authentication
Authentication management

Autenticación en la Práctica:

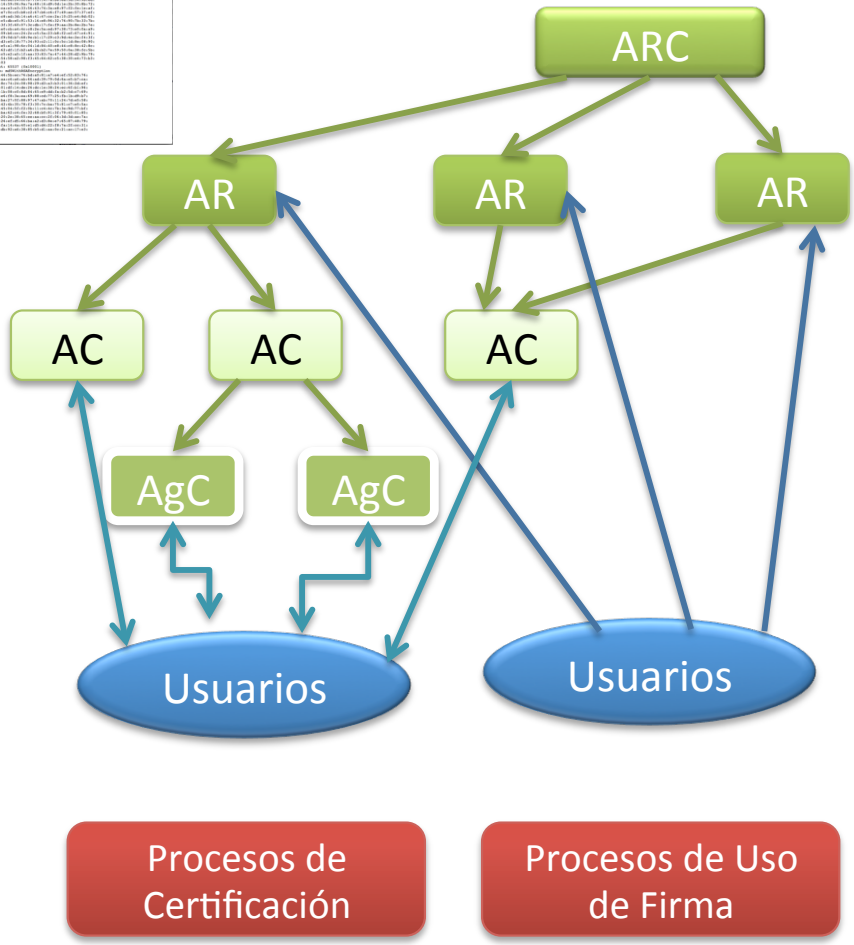
Algunas Iniciativas en México

Servicio de Administración Tributaria SAT

- FIEL, Firma electrónica avanzada
- CIEC, Clave de Identificación Electrónica Avanzada
- Servicios
  - Obligatorios: Pedimentos aduanales, dictámenes fiscales, expediente integral del contribuyente, comprobantes fiscales digitales
  - Opcionales: Declaración anual de personas físicas, declaraciones estadísticas, reimpresión de acuses, consulta de transacciones, consulta de devoluciones, etc.
- Basada en PKI

Banco de México: Infraestructura Extendida de Seguridad

- IES
  - Un sistema diseñado y administrado por Banco de México con el propósito de fortalecer la seguridad de la información que se transmite tanto en los sistemas de pagos como entre el sistema financiero mexicano y el Banco Central.
  - Clave pública a través de certificados digitales
- Firma Electrónica
  - El signatario y el destinatario deben contar, respectivamente, con dispositivos de creación y verificación de firmas electrónicas, los cuales deben ser sistemas de cómputo cuya función principal sea la aplicación de algoritmos criptográficos.
  - Dichos sistemas deben mantener comunicación con la IES, en particular con una AR, para estar en posibilidad de solicitar y verificar la validez de los certificados digitales de los usuarios involucrados en los procesos de firma y cifrado de documentos.



Gobierno del Estado de Colima: Firma Electrónica Avanzada

"

La Firma Electrónica Certificada, constituye el instrumento para dotar de seguridad, validez y certeza jurídica a los documentos que entonces serán documentos electrónicos y que generan las dependencias del Poder Ejecutivo.

El proceso para consolidar lo anterior, inicia con la solicitud que realizan los funcionarios públicos mediante un formato dirigido a la ***Autoridad Certificadora****, que corresponde al Poder Ejecutivo del Estado; como respuesta, la propia* ***Autoridad Certificadora*** *evalúa el cumplimiento de los requisitos establecidos en* ***la Ley Sobre el Uso de Medios Electrónicos y Firmas Electrónicas*** *para el Estado de Colima y su Reglamento para con base en ello, emitir un* ***Certificado que incluye dos llaves, una llamada "pública" y otra "privada", es decir, dos claves diferentes.***

"

Marco Jurídico

1.- Constitución Política del Estado Libre y soberano de Colima.
2.- Decreto No. 4 se reforma y deroga diversos artículos de la Ley Orgánica de la Administración Pública del Estado. (Decreto No. 5)
3.- Ley Sobre el uso de medios electrónicos y firma electrónica para el Estado de Colima.
4.- Reglamento Interior de la Secretaría de Administración.
5.- Reglamento de la Ley sobre el uso de medios electrónicos y firma electrónica para el Estado de Colima.
6.- Acuerdo para la adopción y uso por la Administración Pública Estatal de la Clave Única de Registro de Población.

UNAM: Firma Electrónica Avanzada

"

Avanzar en el marco jurídico que regule e implemente la Firma Electrónica Avanzada al interior de la institución basada en una tecnología que garantice la autenticación de las partes que se involucra, la integridad y confidencialidad de la información transmitida, así como el no repudio de la misma en sus trámites, solicitudes y comunicaciones electrónicas.

… la Universidad pretende establecer una equivalencia funcional entre el consentimiento expresado por medios electrónicos y la firma autógrafa con el objeto de realizar trámites en forma segura.

"

ACUERDO POR EL QUE SE IMPLEMENTA EL USO DE LA FIRMA ELECTRÓNICA AVANZADA EN LA UNAM

JUAN RAMÓN DE LA FUENTE, Rector de la Universidad Nacional Autónoma de México, con fundamento en lo previsto por los artículos 9° de la Ley Orgánica y 34 fracciones I, IX y X del Estatuto General, y

CONSIDERANDO

Que la Universidad Nacional Autónoma de México es una corporación pública, organismo descentralizado del Estado, que tiene por fines impartir educación superior para formar profesionistas, investigadores, profesores universitarios y técnicos útiles a la sociedad, organizar y realizar investigaciones y extender con la mayor amplitud posible los beneficios de la cultura.

Que la Universidad en cumplimiento de sus funciones sustantivas, no puede ser ajena al desarrollo y avances tecnológicos de los medios de comunicación electrónica.

Que la digitalización de la información, la difusión mundial de Internet como red abierta de comunicaciones y de transferencia de información, la automatización de procesos, la creciente importancia del aspecto inmaterial de la riqueza producida, son el resultado de los avances tecnológicos actuales.

Que reconocer este fenómeno de las nuevas tecnologías, conlleva a avanzar en el marco jurídico universitario que regule e implemente la Firma Electrónica Avanzada al interior de la Institución, basada en una tecnología va bajo su control su clave privada y la utiliza para firmar electrónicamente un Mensaje de Datos;

XIII. Lineamientos: Lineamientos para la Implementación y Uso de la Firma Electrónica Avanzada en la Universidad Nacional Autónoma de México;

XIV. Mensaje de Datos: Es la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o magnéticos, y

XV. Sistema de Administración de Identidades (SAI): Es una solución informática de alto impacto que permite la autenticación y autorización de acceso a diversos sistemas de información universitarios a través de la consolidación de un padrón único y fidedigno de la Comunidad Universitaria que contiene los datos generales, perfiles y permisos de sus miembros, lo que permitirá el reforzamiento de diversos aspectos de seguridad de las aplicaciones informáticas que se utilicen en la Universidad.

CUARTO. La implementación del uso de la FEA en la UNAM tiene los siguientes objetivos:

I. Permitir su utilización para la gestión de asuntos administrativos y académicos universitarios que determine el Comité;

II. Equipararla a la firma autógrafa siempre que la FEA se encuentre amparada en un Certificado Digital válido y vigente a la fecha de la firma;

III. Crear e implementar una infraestructura de certificación en la UNAM;

IV. Utilizar un mecanismo que otorgue seguridad técnica y certeza

Contenido, sección 3

Objetivo

- Seguridad en Sistemas de Información
  - Revisar los temas más importantes relacionados con la seguridad informática que afectan a los sistemas de información

Descripción del curso

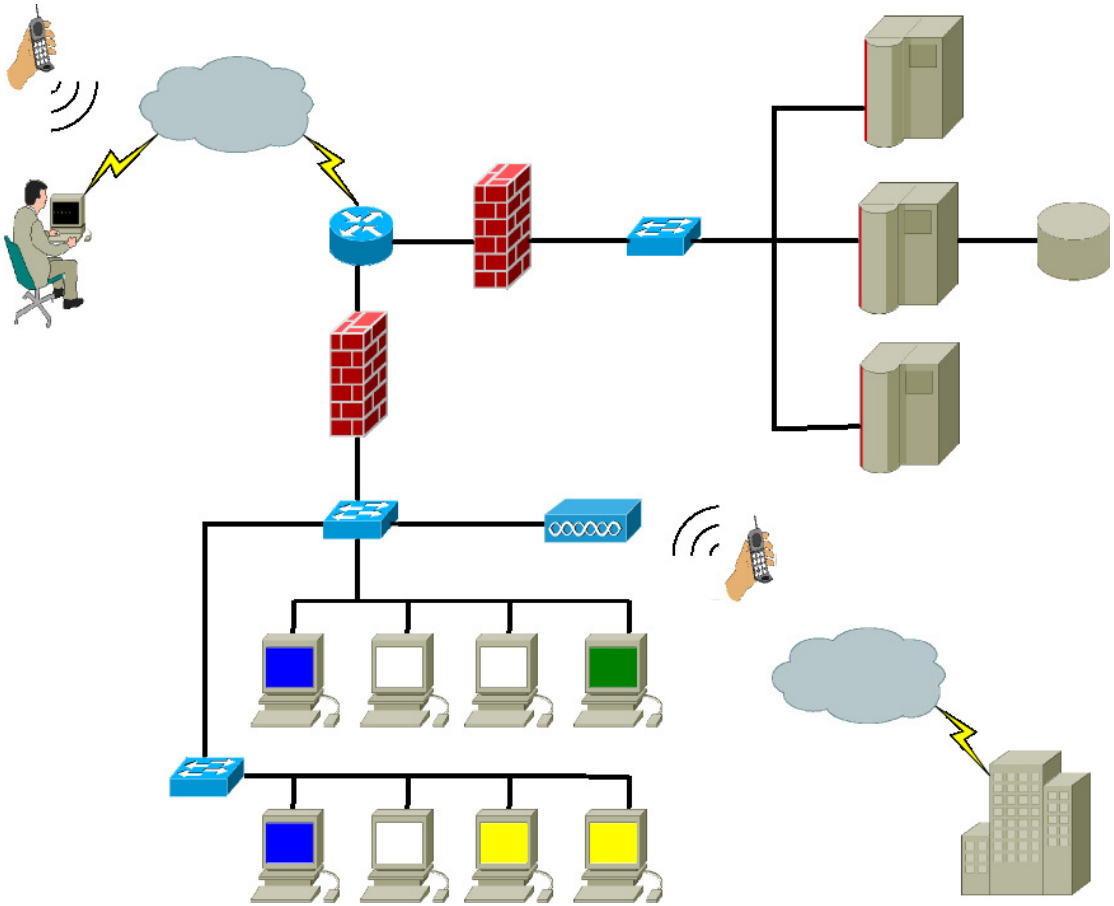
- El curso está organizado en cuatro partes fundamentales:
  - Introducción a los tópicos de seguridad informática
  - Aspectos fundamentales de un cortafuegos
  - Fundamentos criptográficos para servicios de seguridad
  - Herramientas para garantizar la seguridad informática

Organización del curso

- Cada parte es expuesta por un profesor diferente.
- Cada parte se evalúa por separado
  - Examen práctico
  - Examen de conocimientos
- Para la evaluación final, se juntarán las calificaciones de las partes, y se les dará un peso proporcional al número de clases.

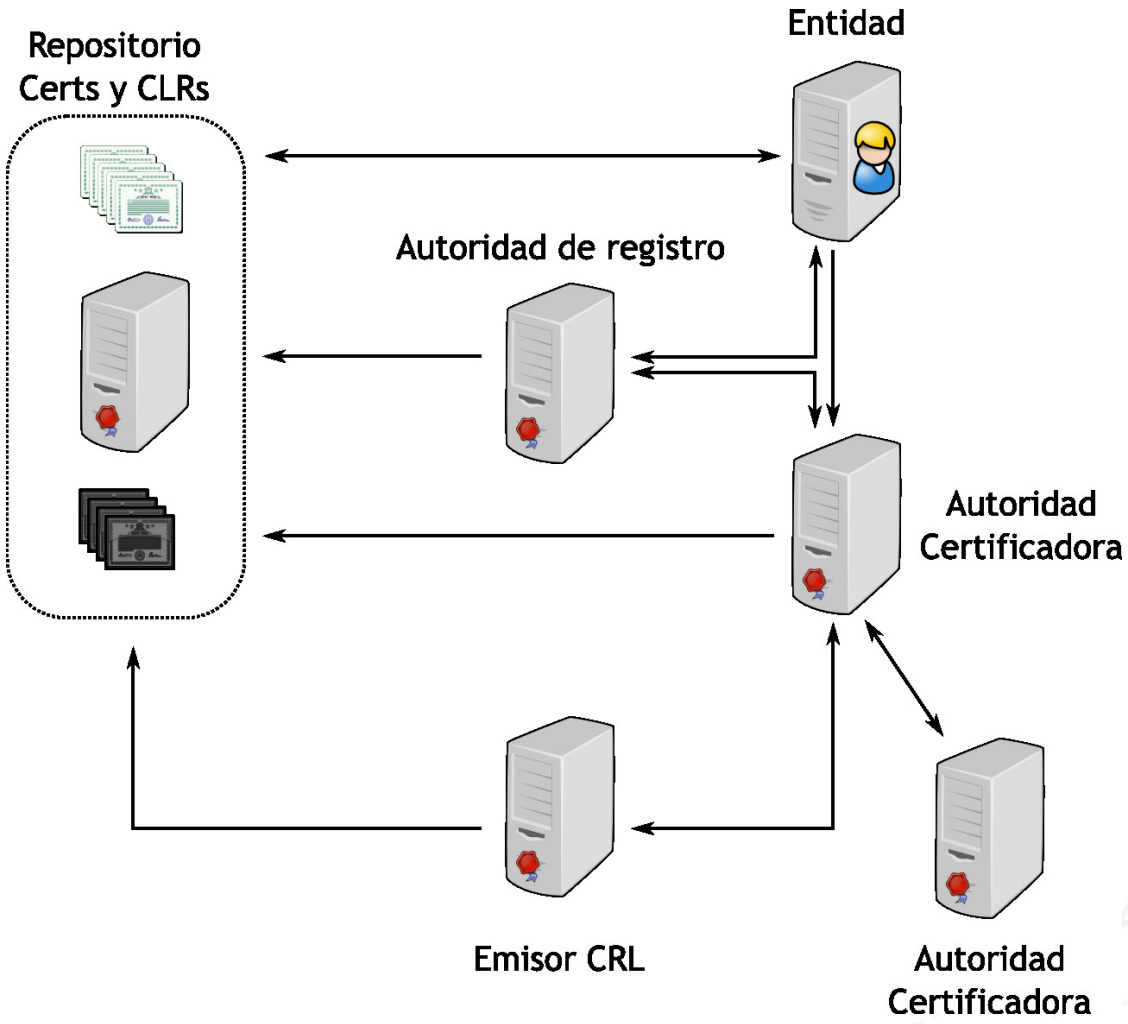
Aspectos fundamentales de un cortafuegos

- Se realizará una instalación de un sistema mínimo de protección de red



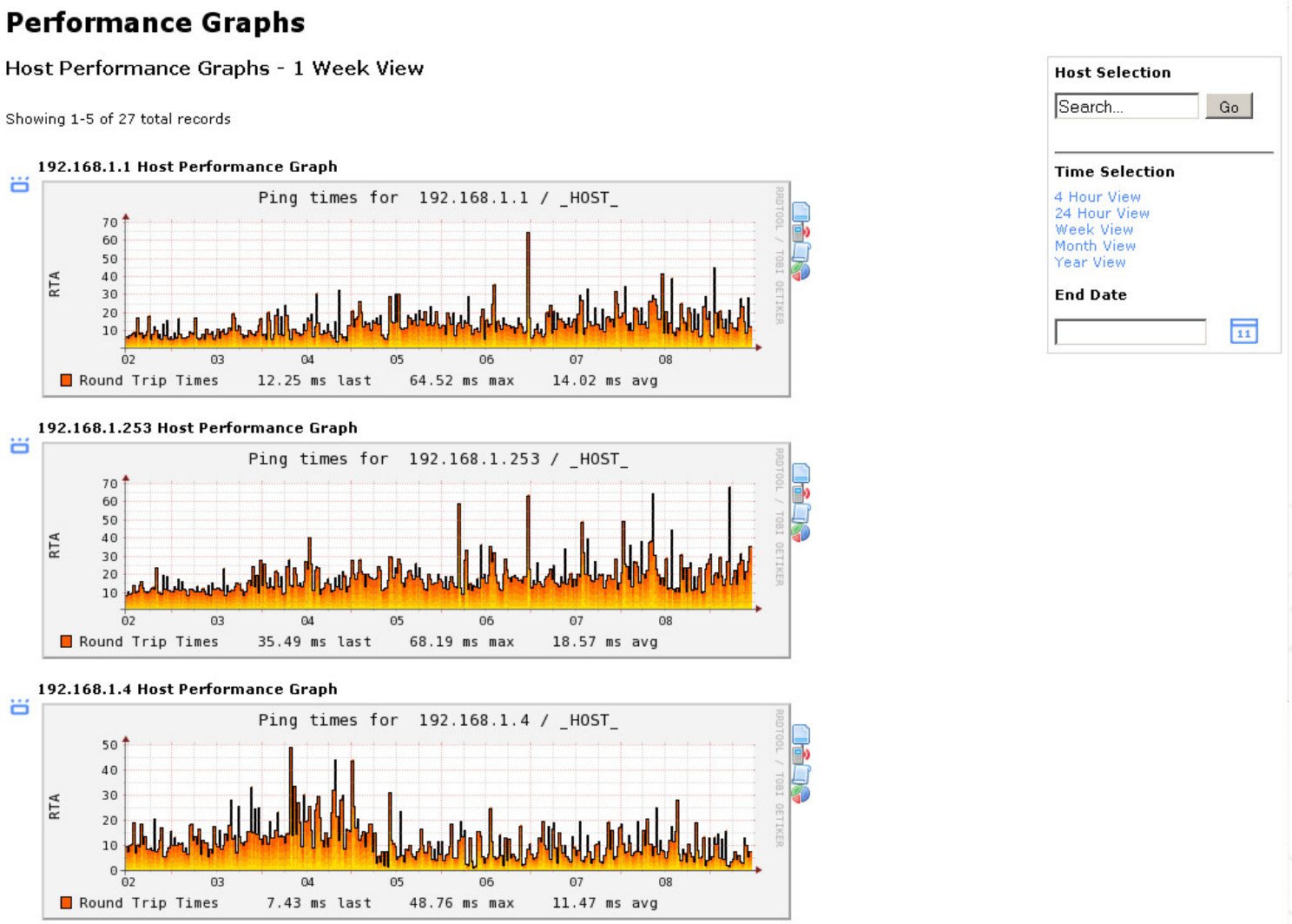
Fundamentos criptográficos para servicios de seguridad

- Se cubrirán aspectos de criptografía de los protocolos de seguridad vigentes, y criptografía de siguiente generación



Herramientas para la seguridad informática

- Se revisarán las herramientas que ayudan a detectar y corregir los problemas de seguridad informática en un sistema de información



Contenido, sección 4

Plataforma de Pruebas para el Curso de Seguridad en Sistemas de Información

Arturo Díaz Pérez
Laboratorio de Tecnologías de Información
Departamento de Computación
Centro de Investigación y de Estudios Avanzados del IPN

Laboratorio

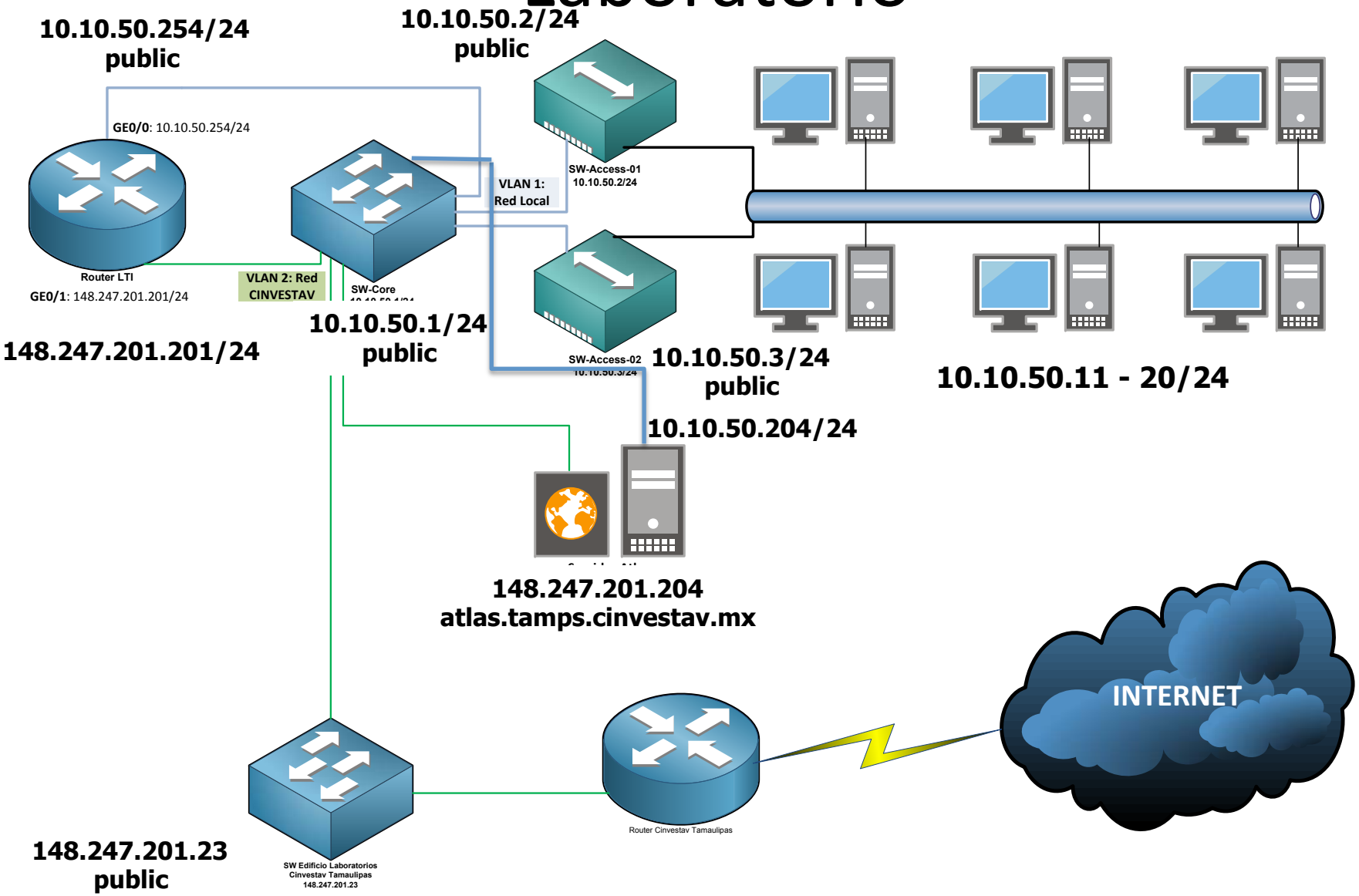


Diagrama de red			
REV.	Red Local MIC	19/07/2012	CINVESTAV TAM

atlas.tamps.cinvestav.mx

Usuarios de atlas

Usuario	Contraseña
lti01	2012
lti02	2012
lti03	2012
lti04	2012
lti05	2012
lti06	2012
lti07	2012
lti08	2012
lti09	2012
lti10	2012

El archivo /etc/hosts atlas.tamps.cinvestav.mx

```
#Hosts usuarios
10.10.50.11     lti01
10.10.50.12     lti02
10.10.50.13     lti03
10.10.50.14     lti04
10.10.50.15     lti05
10.10.50.16     lti06
10.10.50.17     lti07
10.10.50.18     lti08
10.10.50.19     lti09
10.10.50.20     lti10

#Equipos red

10.10.50.254    router
10.10.50.1      sw-core
10.10.50.2      sw-access-1
10.10.50.3      sw-access-2
```

Estaciones de Trabajo

Nombre del Equipo	Nombre del Usuario	Contraseña	Contraseña del root	Dirección IP	VLAN
Lti01	Lti01	2012		10.10.50.11	1
Lti02	Lti02	2012		10.10.50.12	1
Lti03	Lti03	2012		10.10.50.13	1
Lti04	Lti04	2012		10.10.50.14	1
Lti05	Lti05	2012		10.10.50.15	1
Lti06	Lti06	2012		10.10.50.16	1
Lti07	Lti07	2012		10.10.50.17	1
Lti08	Lti08	2012		10.10.50.18	1
Lti09	Lti09	2012		10.10.50.19	1
Lti10	Lti10	2012		10.10.50.20	1

Instalación

- apt-cache search nombreapp #aptitude show nombreapp
  - Ejemplo:

    #apt-cache search postfix
- Instalación
  - apt-get install nombreapp
  - aptitude install nombreapp
    - Ejemplo:

      #apt-get install honeyd
- Listar archivos instalados por la aplicación:

  #dpkg –L nombreapp

Aplicaciones

Servidor web: Apache2
Archivos de configuración:
/etc/apache2/

Servidor de correo:
MTA: Postfix
Archivos de configuración:
/etc/postfix/main.cf
/etc/postfix/master.cf

IMAP: Dovecot
Archivos de configuración:
/etc/dovecot/dovecot.conf

Filtrado de contenido: Amavis-new
Archivos de configuración:
/etc/amavis/conf.d/15-content_filter_mode

Anti-SPAM: Spamassassin
Archivos de configuración:
/etc/spamassasin/local.cf

Antivirus correo: ClamAV
Archivos de configuración:
/etc/clamav/clamd.conf

Webmail: Roundcube
Archivos de configuración:
/etc/roundcube/main.inc.php

Honeyd:
Archivos de configuración:
/etc/honeypot/honeyd.conf

Mrtg:
Archivo de configuración:
/etc/mrtg.conf

Conclusiones

- El área de seguridad informática ha cobrado importancia en el pasado reciente.
- Seguridad informática tiene que ver con activos, amenazas, riesgos, ataques e impactos.
- Hay una variedad muy amplia de amenazas a la seguridad informática. Es cada vez menos complicado generar ataques.
- Aunque el tema de seguridad ha permeado entre la comunidad directiva de TI, hay muchas áreas de oportunidad para implantar mecanismos de seguridad informática.
- Las barreras para la implantación de mecanismos de seguridad informática se deben a desconocimiento o falta de previsión
- La tecnología se encuentra ya madura y en constante evolución.
- Caso de estudio: existen mecanismos de autenticación más robustos que pueden ser adoptados más allá de los basados en nombre de usuario y contraseña.
  - Protocolos de autenticación y control de acceso basados en un KDC
  - Servicios de autenticación y control de acceso basados en Certificados Digitales
- Los mecanismos de seguridad informática consisten de un conjunto de protocolos, servicios, herramientas, políticas y estrategias que constituyen las “buenas prácticas”.


Cinvestav
Gracias
www.tamps.cinvestav.mx
www.cinvestav.mx