Seguridad en Redes

M. Farias-Elinos

Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Dirección de Posgrado e Investigación
Universidad La Salle
Grupo de Seguridad de RedCUDI (Internet-2 México)
e-mail: elinos@ci.ulsa.mx
http://seguridad.internet2.ulsa.mx/

April 21, 2009

Hacker vs Cracker

Hacker Experto ó que es especialmente hábil en el manejo de un sistema, que sabe como aprovechar al máximo sus capacidades, todo por el bien de la comunidad.

Cracker Se adentra en el terreno de lo ilegal, se aprovecha del conocimiento de los hackers; denominado tambien **Hacker Dark Side**

Qué es seguridad?

Seguridad - (sust. fem.) Certeza, firmeza, conafianza. (locución adverbial). Sin riesgo

Seguridad - (sust.) Dícese de las cosas ciertas, firmes y/o libres de peligro o riesgo. Estado de las cosas bajo protección.

Seguridad - (lat. Securitis) Confianza, tranquilidad de una persona procedente de la idea de que no hay ningún peligro que temer.

Qué es seguridad?

- El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado de gas venenoso y cuidado por guardas muy bien armados y pagados. Aún así no apostaría mi vida por él[a]
- Para que lo sepan, la seguridad en la Internet no existe[b]

[a] Eugene Spafford
[b] Scott McNealy

Obscurantismo vs Seguridad

- Si guardo una carta en una caja, y dicha caja la pongo en un lugar de la ciudad de México ...
  - ... y les pido localizarla, y leer la carta (Oscurantismo)
  - ... les doy las especificaciones de la caja, y aun así no pueden leer la carta (Seguridad)

Historia eventos seguridad

1969 Nace ARPANet

1971 John Dreaper (*Captain Crunch*) and bluebox

1973 75% del tráfico lo ocupa el e-mail
Christmas Day Lockup - problema de routeo tráfico a Hardvard

1980 Progragación del primer mensaje de virus (*status-message "virus"*)
Jürgen Kraus tesis de maestria "*Selbstreproduktion bei Programmen*" (*programas que se autoreproducen*)

Historia eventos seguridad

1983 Se acuña el término *virus* por Frederick Cohen

1986 1er. virus para PC (Brain)

1988 1er gusano en Internet (*Morris Worm*) afecta 10%
Se crear el CERT (Computer Emergency Response Team)
1ra. victima de fraude por cómputo First National Bank of Chicago

1993 WWW Worms (W4)

1995 Crackean ”The Spot”, ”Hacker movie page”

Historia eventos seguridad

1996 Crackean DoJ, CIA, Air Force, NASA, entre otros.

1997 Crackean sitio del gobierno d Indonesia, NASA, Conservatorio UK, Spice Girls

1998 Crackean DoC, NY Times, UNICEF, entre otros.

1999 Virus: Melissa y ExploreZip
Crackean StarWars, USIA, e-Bay, Senado US, Microsoft, Gob. Paraguay, entre otros

Historia eventos seguridad

2000 Ataque masivo de DoS afecta a Yahoo, Amazon, e-bay entre otros
Crackean Apache, Wester Union, Microsoft, entre otros
Virus: Love Letter

2001 Virus: CodeRed, Nimda, SrCam, BadTrans

2002 Un ataque de DDoS afecta a 9/13 servidores raices de DNS

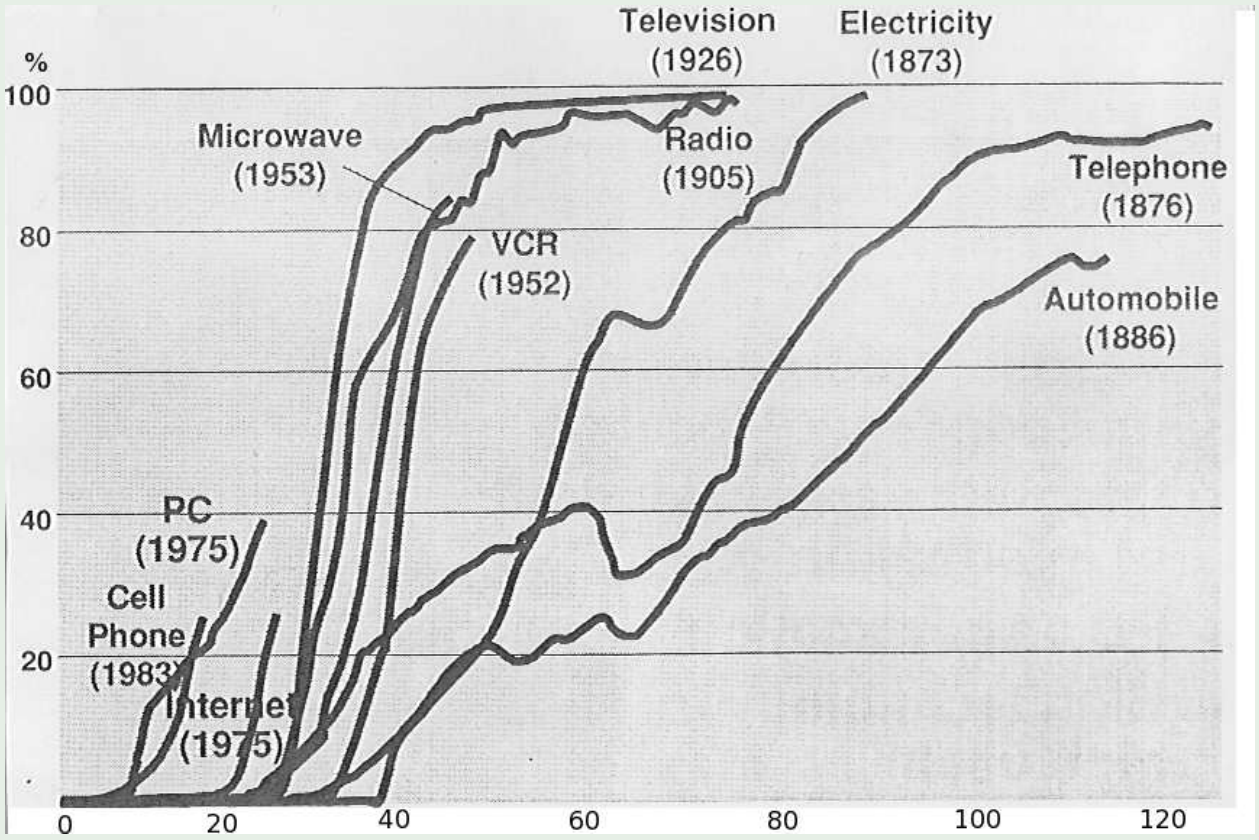
2003 Gusano SQL Slammer genera un DDoS

Diversidad

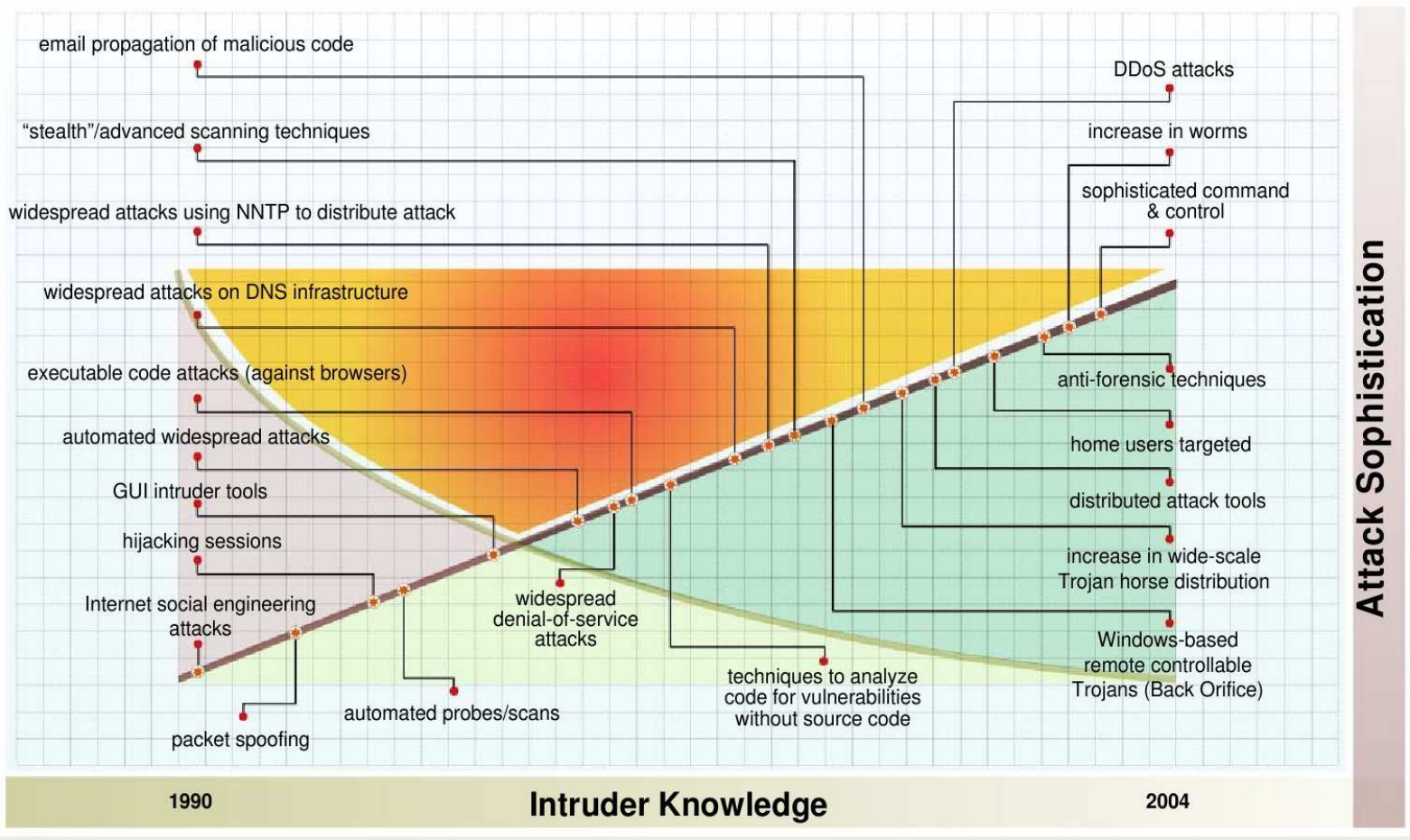
- 1,463,632,361 usuarios actualmente[a]
- Muchas formas de pensar
- Diferentes culturas
- Un sólo punto en común La Red
- 1% maliciosa

[a] Internet World Statistics

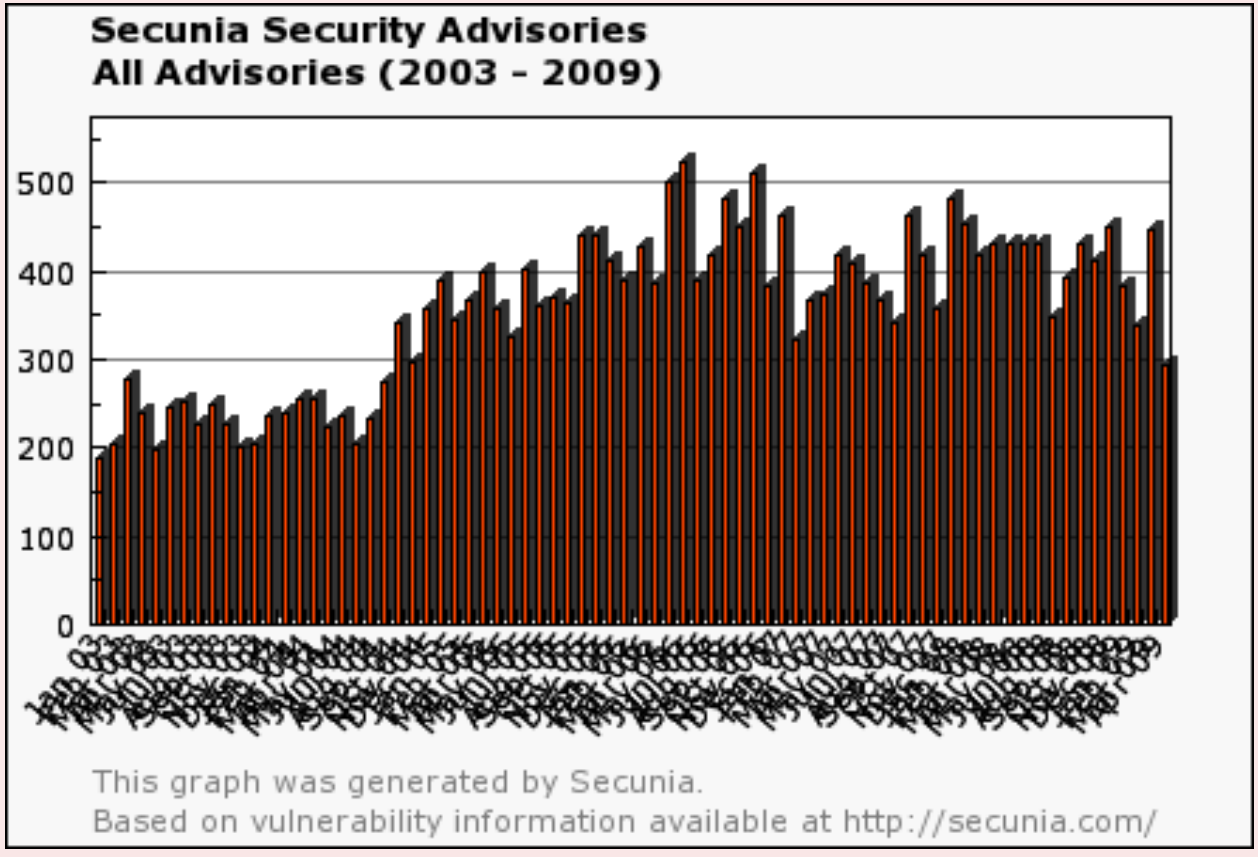
Tecnología y sociedad



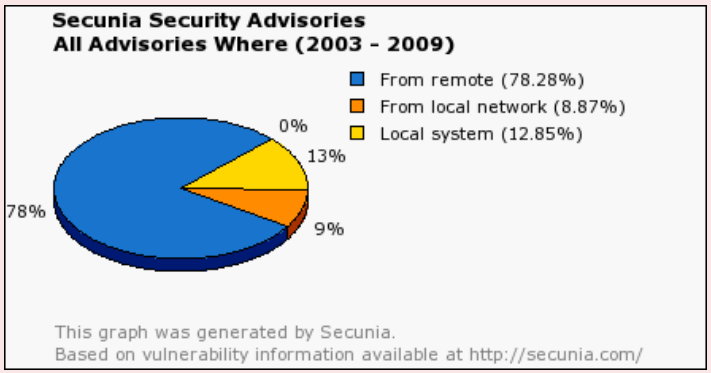
Evolución de los ataques

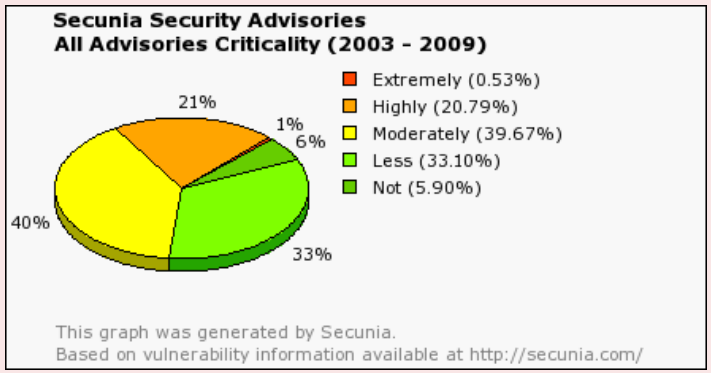


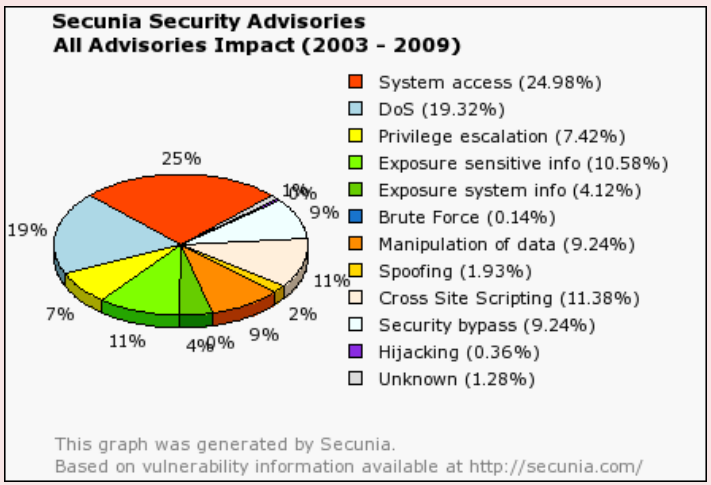
Vulnerabilidades



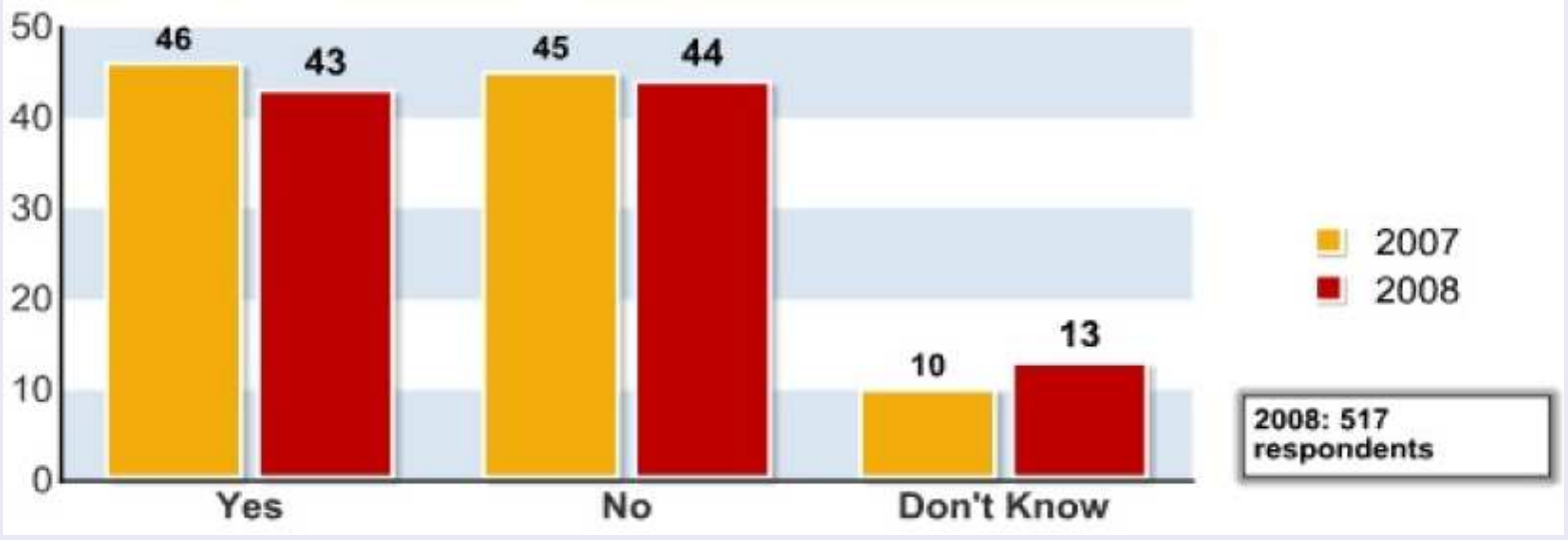
Vulnerabilidades



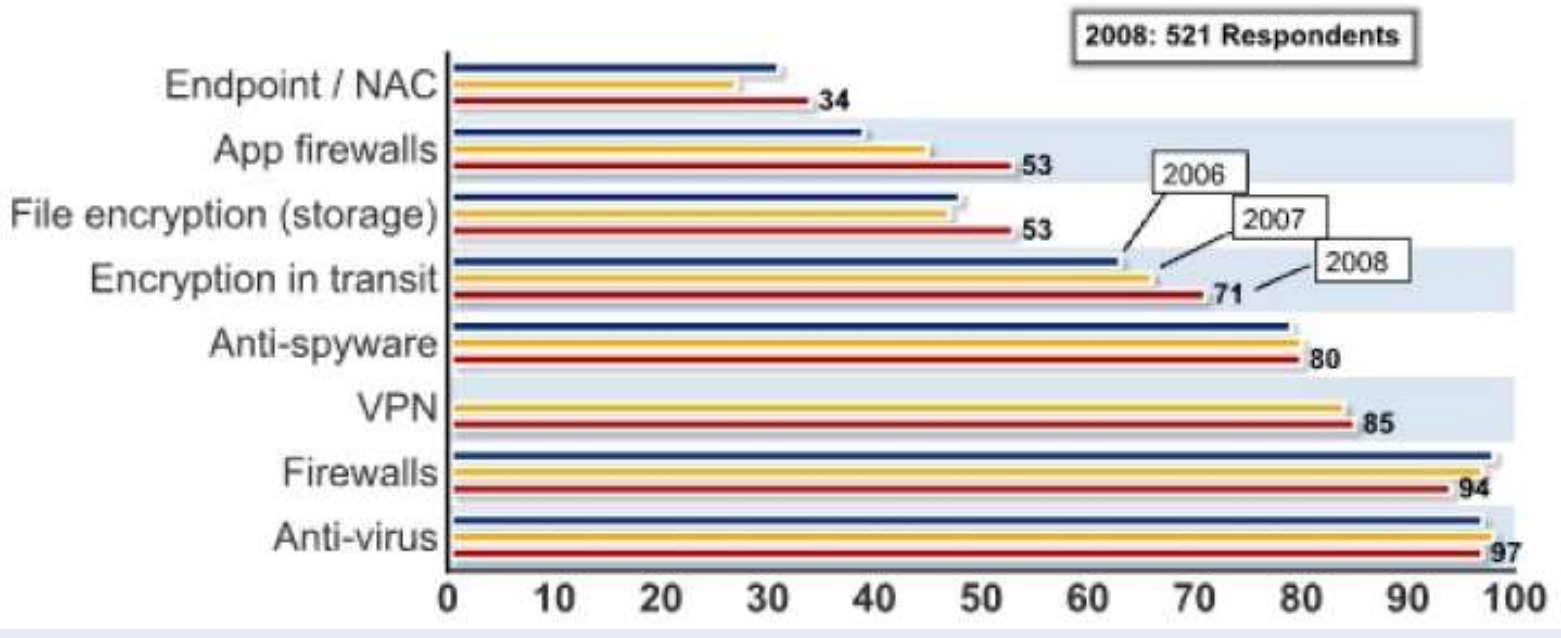




Incremento de incidentes



Herramientas utilizadas



Niveles de seguridad

Nivel	Descrip	Procesos	Políticas	Tecnologías	Métricas
0	Caos	No hay procesos	Pocas o inexistentes	Requerimientos inexistentes	ninguna
1	Ad-Hoc	Procesos no estandarizados	1ra. revisión de políticas	Uso de paquetes	ninguna
2	Adm. del riesgo inicial	Responsabilidad identificacion de amenazas	Politicas basadas en amenazas	Uso de herramientas básicas	ninguna
3	Monitoreo auditorias	Procesos de control y	Politicas iniciales de	Estudio de amenazas	amenazas vulnerabilidades
4	Seguridad adaptiva (ANS)	Análisis de mejoras cont. de procesos	Politicas ANS y prevención integradas	Entorno ANS Encriptación bajo nivel	Respuesta conciencia
5	Avanzadas	no adicionales	avanzadas	encriptación autenticación	no adicionales

Analfabetismo digital

- Pemsamiento en lo concreto, palpable
- No se ve, no pasa nada
- 30 años aceptación tecnológica
- menos de 15 años la computadora
- Ignorancia en el uso de las TIC's

Legales

- Falta de una legislación informática
- Falta de convenios internacionales

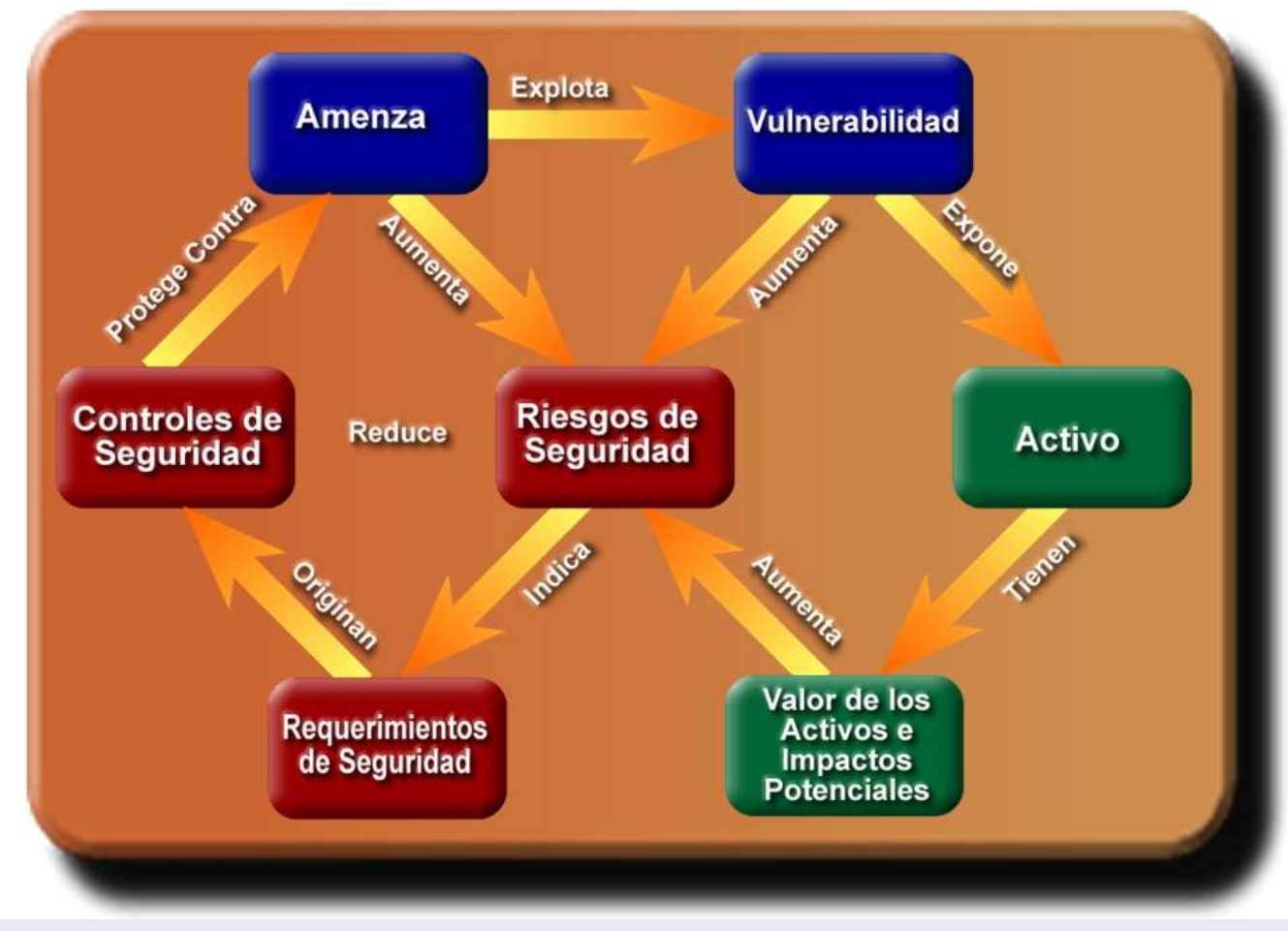
Con simple IE y google

- Explotación de vulnerabilidades
- Motor de búsqueda de información

Que pasa por el medio

- *Snifer* del medio
- Conecciones no autorizadas
- Flujos en la red

Integración de la seguridad



Aspectos a tomar en cuenta

Existe la Seguridad?

- ☞ Enfoque debe ser hacia la Seguridad de la Información

Es un problema esclusivamente técnico?

Aspectos a tomar en cuenta

Seguridad - Todo aquello que hacemos para dificultarle las cosas al intruso

- Aspectos de la seguridad
  - Tecnológico
  - Socio-cultural
  - Jurídico (Legal)

Todo es crackeable

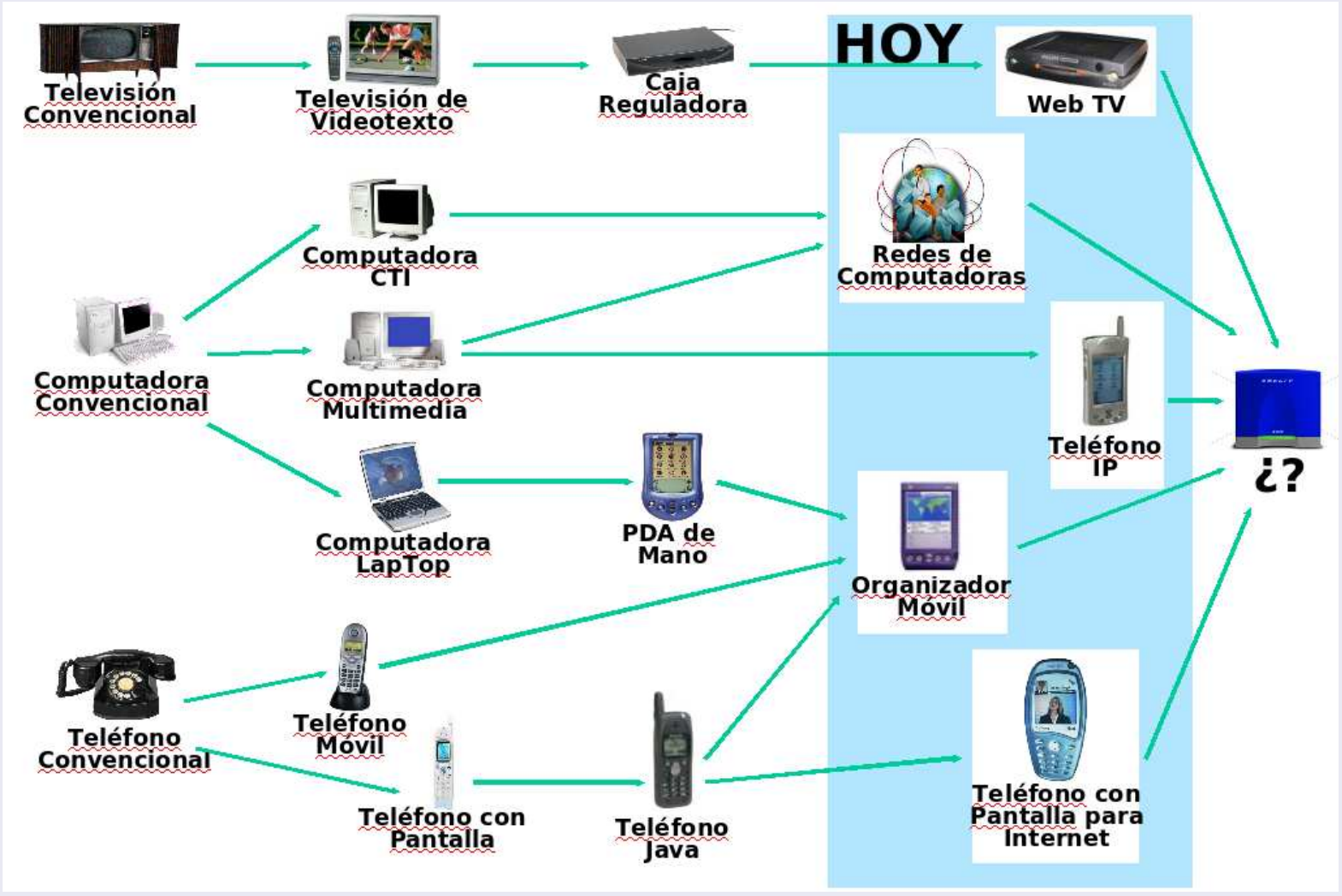
Conclusiones

- Inexistencia de una cultura de seguridad
  - Controles de acceso insuficientes o débiles (ej: inalámbrica)
  - Comunicación no cifrada (no encriptada)
  - Facilidad de conexión
  - Abusos y usos excesivos de las TIC's
  - Mal manejo de la basura (papeles, equipos de cómputo)
- Grupos con poca y nula ética
  - Información en la red que la mal utilizamos
  - Usuarios vengativos
- No hay control de la información existente en la red
- Retraso en cuanto a Legislación Informática en México

Perfil del Oficial de Seguridad

- Técnico con conocimientos generales de todas las áreas
- Habilidades de hacker
- Mentalidad de cracker
- Conocimientos legales de la informática

Convergencia en redes globales



Seguridad en Redes

M. Farias-Elinos

Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Dirección de Posgrado e Investigación
Universidad La Salle
Grupo de Seguridad de RedCUDI (Internet-2 México)
e-mail: elinos@ci.ulsa.mx
http://seguridad.internet2.ulsa.mx/

April 21, 2009