OWASP Spain Local Chapter

Trust, Security and Usability

Roger Carhuatocto
rcarhuatocto [at] intix.info

6.Julio.2007

Definiciones

- Trust
- Security
- Usability

trust (*plural* **trusts**)

1. Confidence in or reliance on some person or quality.
   - **1671**: O ever-failing **trust** / In mortal strength! — John Milton, *Samson Agonistes*
2. Dependence upon something in the future; hope.
   - **1611**: Such **trust** have we through Christ. — *Authorised Version*, 2 Corinthians iii:4.
3. Confidence in the future payment for goods or services supplied; credit.
   *I was out of cash, but the landlady let me have it on **trust**.*
4. (*rare*) Trustworthiness, reliability.
5. (*law*) The confidence vested in a person who has legal ownership of a poperty to manage for the benefit of another.
6. A group of businessmen or traders organised for mutual benefit to produce and distribute specific commodities or services, and managed by a central body of trustees.

Synonyms [edit]

- belief
- confidence
- expectation
- faith
- hope

Etymology

use + -ability

Noun

usability (*uncountable*)

1. The degree to which an object or device is easy to use with no specific training
2. (*computing*) the degree to which a software application or a website is easy to use with no specific training

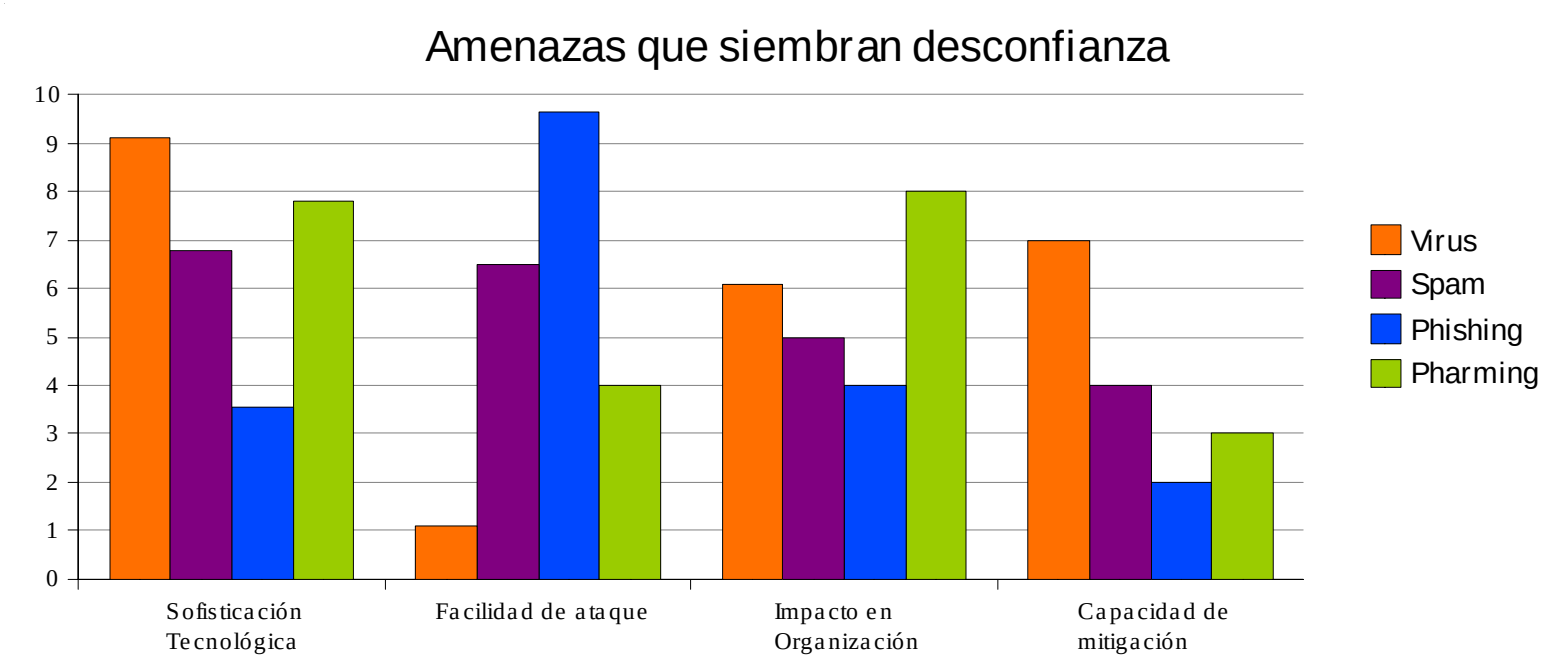
Related terms

- usable

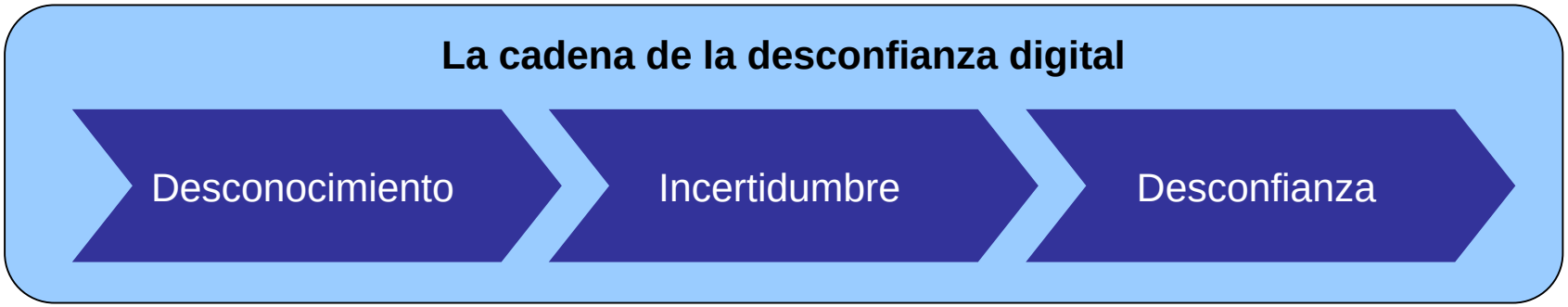
Translations

- French: facilité d'utilisation *f*
- Swedish: a

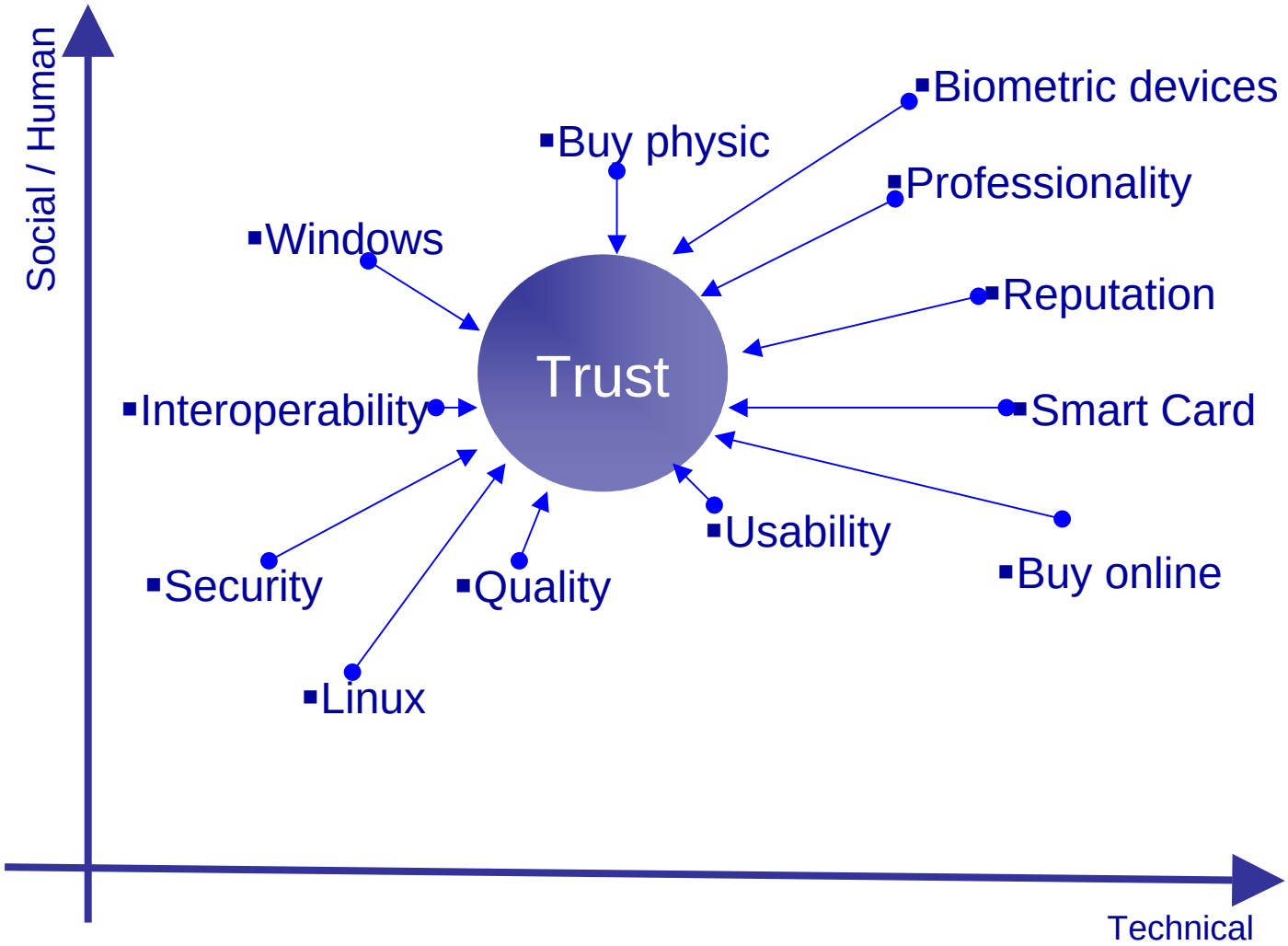
Amenazas que siembran desconfianza en el mundo IT



La cadena de la desconfianza digital



Cómo medimos la confianza



Tecnologías de seguridad… la solución?

El 23% de la gente no presta ninguna atención a lo que dice la barra de dirección del navegador, la barra de estado o los indicadores de seguridad.

El 68% de la gente no hace caso de los avisos de su navegador en referencia a un certificado digital caducado o falso.

Factores como la edad, el sexo, la educación o las horas de utilización de un ordenador no se han mostrado como estadísticamente significativos en relación a la vulnerabilidad ante ataques de phishing.

Fuente: *Why phishing works?* , de los profesores Racha Damija, de Harvard, y J.D. Tygar y Martin Hearst, de Berkeley

Reformulemos la confianza digital

Nos inspira confianza aquello que es conocido o que está inequívocamente relacionado con algo conocido.

Confiamos en lo que percibimos como creíble.

La credibilidad no es una cualidad objetiva, ya que resulta de la percepción subjetiva de las personas.

Factores que aumentan la confianza

Sensación de pertenencia al mundo real

- Fotos de personas conocidas
- Referencias a localizaciones físicas
- Marcas de prestigio

Facilidad de uso

- Menos complejidad comporta menos incertidumbre
- La sensación de control genera confianza
- Los mensajes directos generan confianza

Imagen de profesionalidad

- Funcionamiento perfecto: los errores generan desconfianza
- Contenidos actualizados
- Enlaces a webs prestigiosas
- Ausencia de errores ortográficos

Transparencia

- Información clara y concisa de las implicaciones económicas
- Mostrar objetivos y motivos de la web

Los factores que menguan la confianza

Implicaciones comerciales

- Presencia de publicidad de marcas desconocidas
- Obligatoriedad de registros y petición de datos personales
- Un fenómeno nuevo: la ceguera a los banners

El amateurismo

- Alojamiento en sitios gratuitos
- Cuentas de correo gratuitas (Hotmail, Yahoo...)
- Tratamiento de imagen infantil

El reto de la confianza digital

La mejora objetiva de la seguridad tecnológica NO es la única vía para generar confianza.

El conocimiento que posee el usuario de los mecanismos de seguridad digital es insuficiente y los convierte en ineficaces.

El reto que se nos plantea obliga a diseñar políticas de generación de confianza que traten los aspectos subjetivos que construyen la credibilidad:

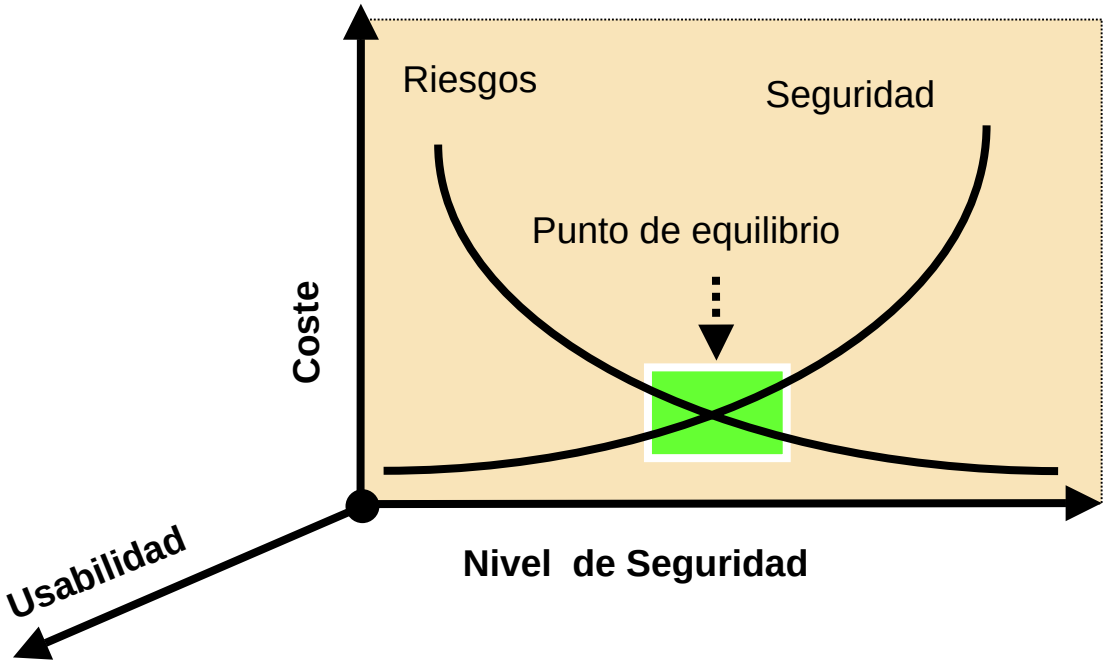
- -Elementos familiares de reconocimiento fácil
- -Contexto relacional
- -Multi-modalidad

Holistic approach in IT Security

- Abordar los problemas de seguridad usando un enfoque más completo, donde se consideren elementos subjetivos y no sólo prime la tecnología.

Seguridad vs. Usability vs. Coste

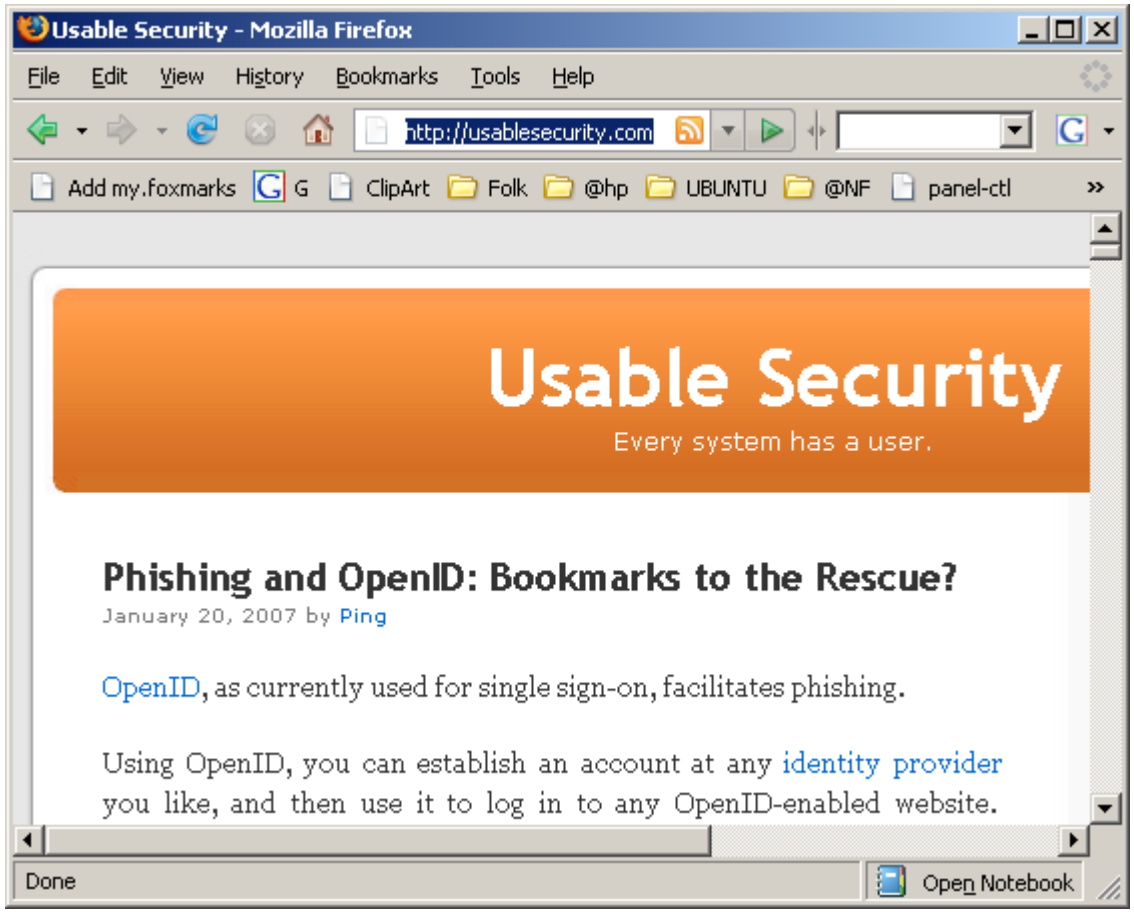
- Costs Versus Benefits in Securing Your Applications
  http://www.scmagazine.com/scmagazine/sc-online/2002/article/50/article.html
- Se busca controlar el riesgo y minimizarlo
  http://www.infosecnews.com/opinion/2002/09/11_03.htm
- 100% de seguridad no existe
- Mayor nivel de seguridad, es probable que no sea usable



Casos de la vida real …

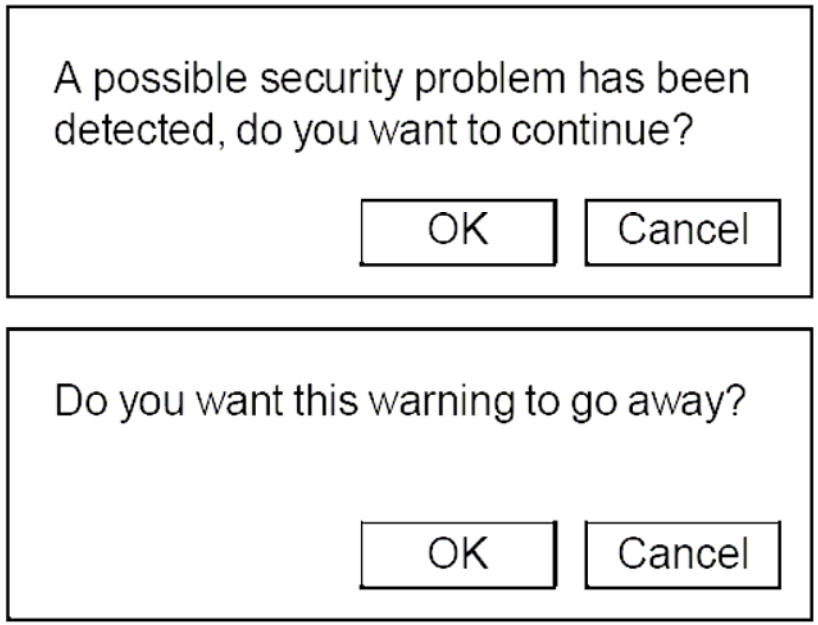
Every system has a user

- Siempre ponernos en el lado del usuario



Qué ve el usuario y qué el programador?

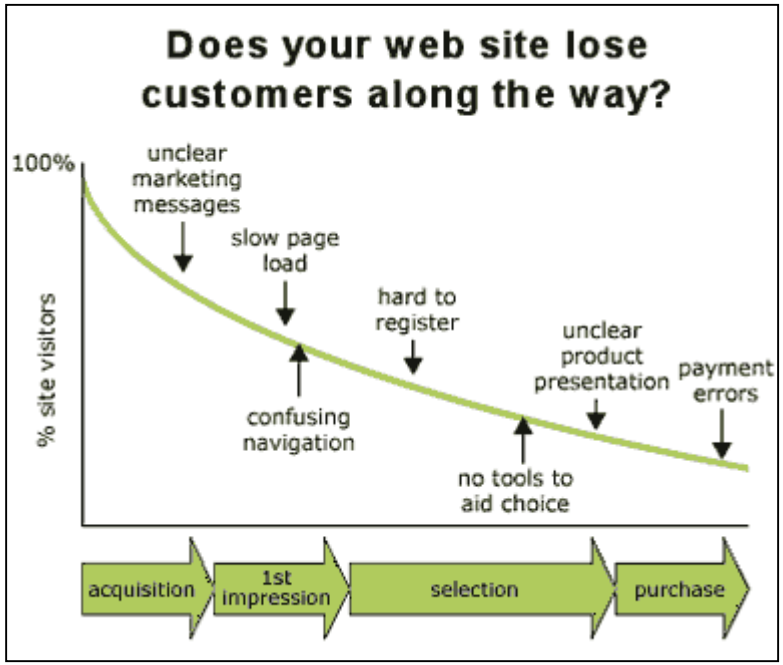
- Es importante saber identificar el momento que debemos pensar como técnico y como usuario

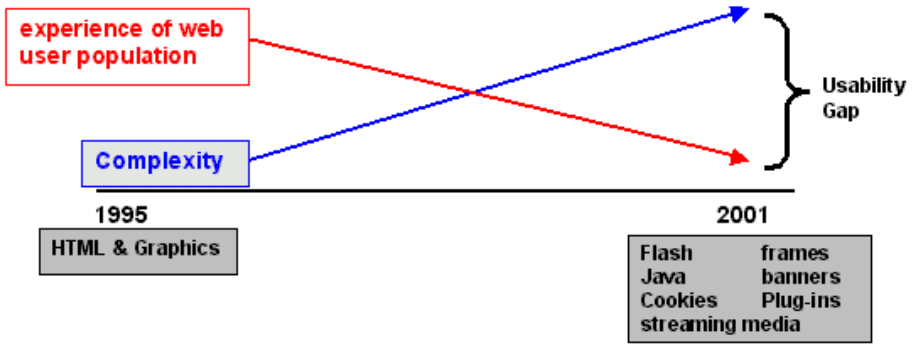


http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf

Cryptography, PKI, Digital Certificates and poor Usability

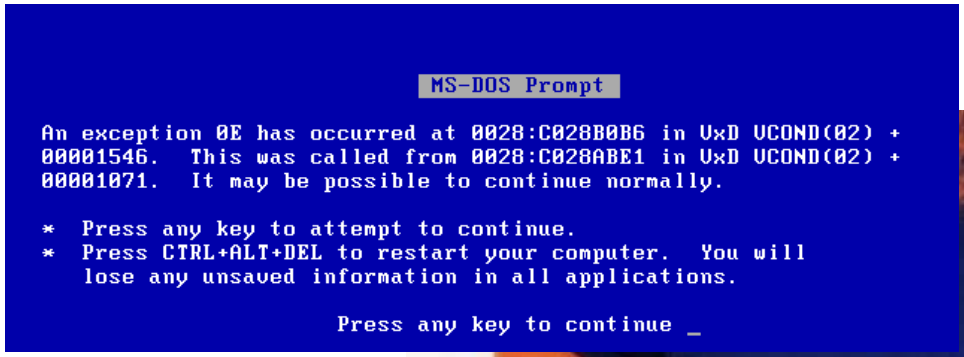
- La probre usabilidad mató a …
  - PGP ?, PKI ?, e-Commerce, …

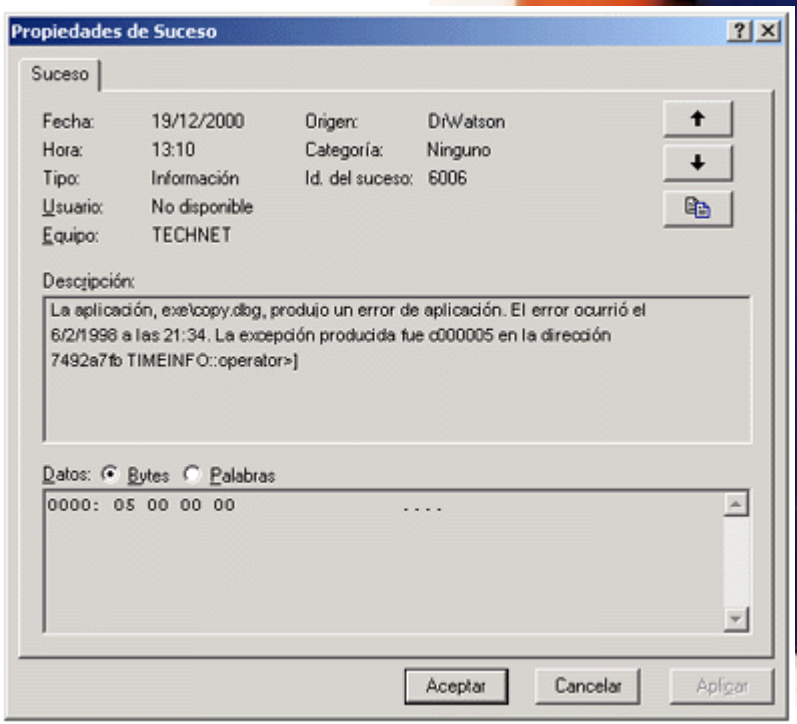




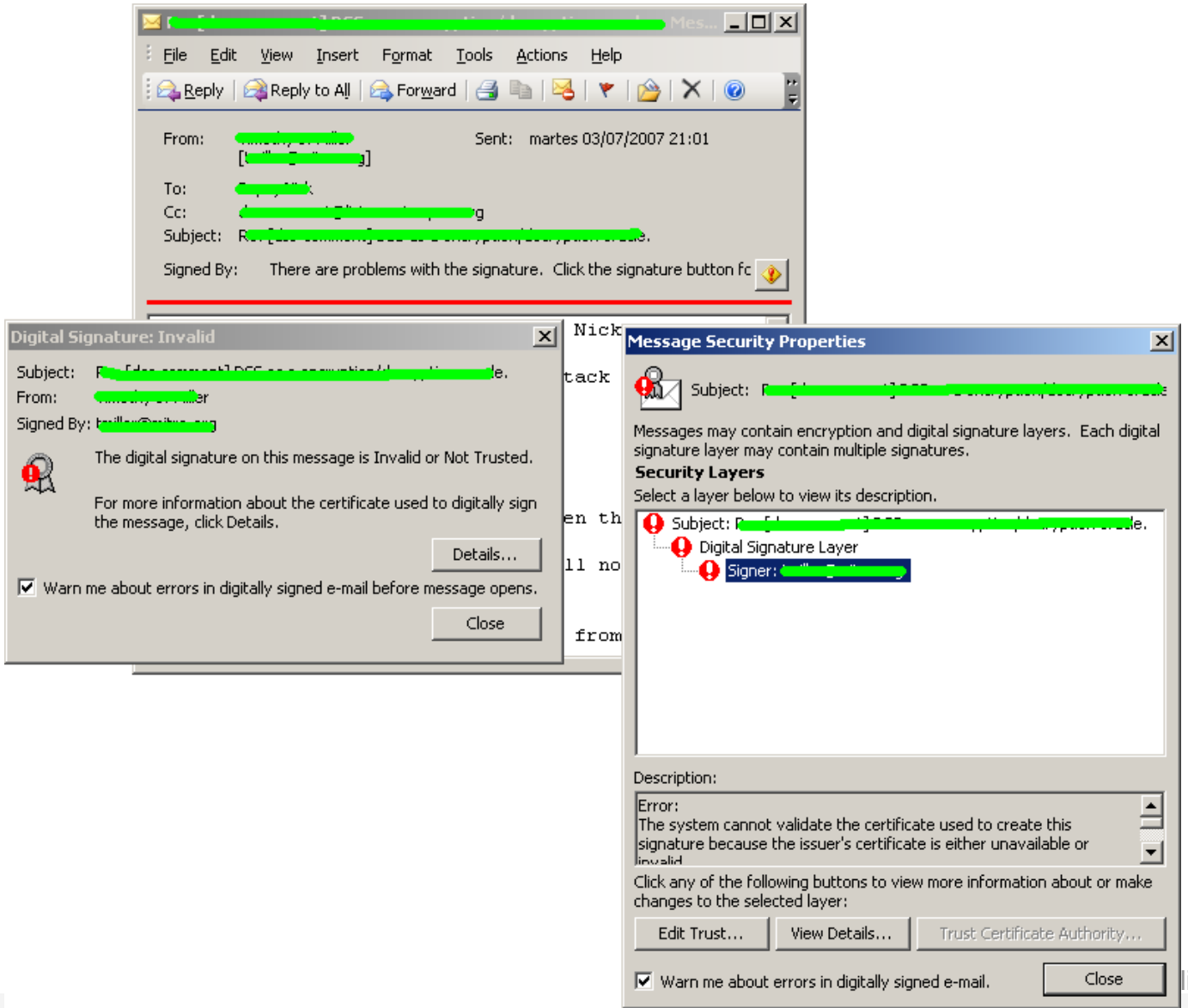
http://www.uservision.co.uk/usability_articles/usability_usability2.asp

De Blue Screen al Dr. Watson





Correo electrónico seguro no usable



Correo electrónico seguro, confiable y usable?

"La mosca"

Cabecera del mensaje: La tendencia es que el usuario inicie la lectura por la parte superior

Cuerpo del Mensaje: Representa el contenido clásico del mensaje

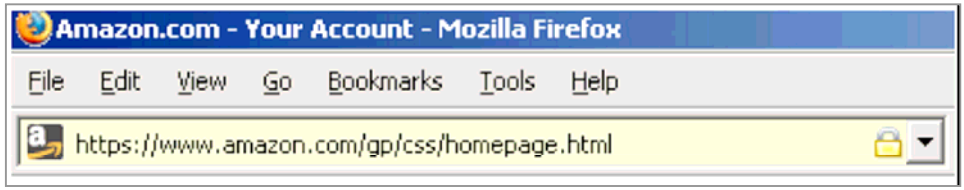
Pie del mensaje: Nos permite mostrar información textual y visual de confianza (elementos basados en principios criptográficos)

Los clásicos

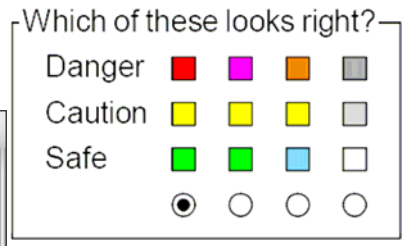
- Users are not the enemy – by Anne Adams and M. Angela Sasse
- Usability and privacy: A study of KaZaA P2P file Sharing – by Nathaniel S. good and Aaron Krekelberg
- Why Johnny can’t encrypt – by Alma Whitten and J. D. Tygar
- …

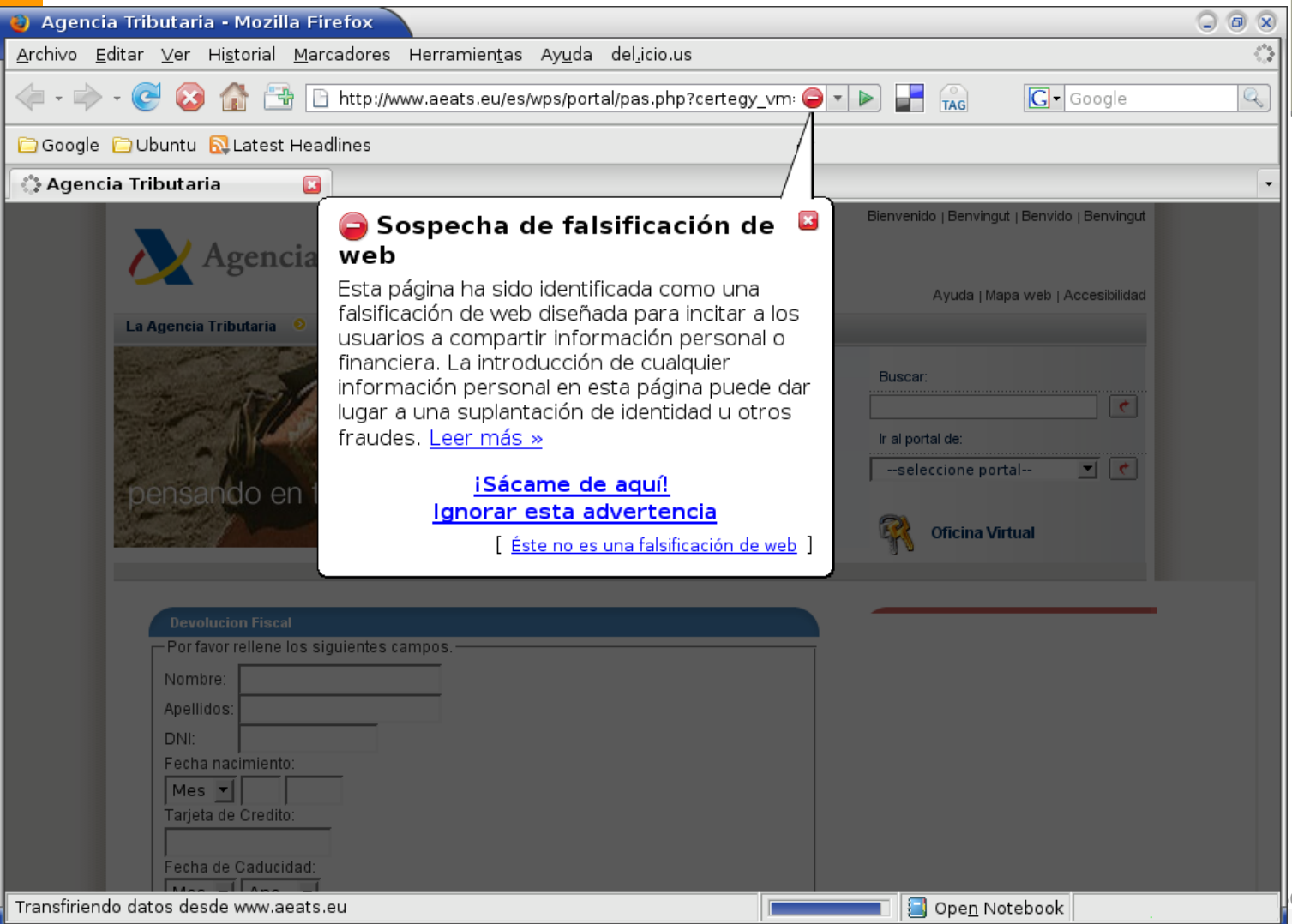
Algunas soluciones …

Pistas visuales



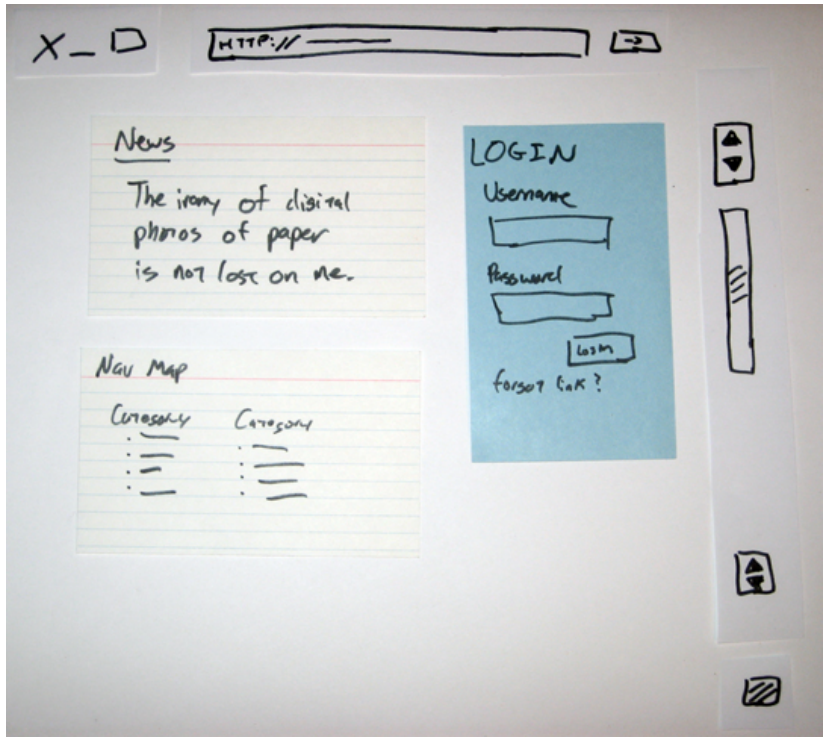
- Diferenciación del nivel de riesgo basada en colores





Testing de la usabilidad

- Testing en la etapa del diseño (muck-up on paper, GUI prototyping)
- Testing con perfiles de usuarios (estereotipos)
- Feedback de usuarios
- Testing post-implementación: ver reacciones de usuarios cuando maneja la aplicación



Conclusiones ...

La usabilidad, argumento que refuerza la venta

- Existe una tendencia de mejorar la usabilidad para que el usuario tenga una mejor “experiencia”, no motivado por la seguridad, motivado por la acción comercial:
  - Web 2.0, Semántica, User Experience, SaaS, …

Comercializando Usabilidad:

•ZoneAlarm: Creating usable security products for cosumers
•Firefox and worry-fre web
•Users and Trust: A Microsoft case of study

Security and Usability Book

Referencias

- Usable security – http://usablesecurity.com
- Symposium on Usable Privacy and Security - http://cups.cs.cmu.edu/soups/2007
- Slashdot // Are Usability & Security Opposites in Computing? - http://it.slashdot.org/article.pl?sid=04/11/15/1420246&tid=172&tid=218
- Usability in web development - http://www.uservision.co.uk/usability_articles/usability_usability2.asp
- Stanford Web Credibility Research - http://credibility.stanford.edu
- Justaddwater || Instant usability & web standars - http://justaddwater.dk
- Security and Usability | Designing Secure systems that People Can Use (Edited by Lorrie Faith Cranor & simson Garfinkel, O'Reilly)