Ética y Seguridad en la red

Fernando Tricas García

ftricas@unizar.es

Dpto. de Informática e Ingeniería de Sistemas del Centro Politécnico Superior

Universidad de Zaragoza, España

http://www.cps.unizar.es/~ftricas/

Principios de Investigación en Medicina y Cirugía. Internet.

Burgos – 30 de enero de 2004

Índice

- Algunas definiciones
- Modos de atacar la seguridad y la privacidad
- Algunas reglas de autoprotección
- Confidencialidad y autenticidad
- Para saber más
- Conclusiones

Algunas definiciones

ESPASA([ESP]):

PRIVADO, DA adj: Que se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna || Particular y personal de cada uno.

INTIMIDAD: Parte personalísima, comúnmente reservada, de los asuntos, designios, o afecciones de un sujeto o de una familia.

Algunas definiciones

Oxford English Dictionary, ([oxf]):

> PRIVACY (from private) The state or quality of being private. The state or condition of being withdrawn from the society of others, or from public interest; seclusion. || The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion. Also attrib. designating that which affords a privacy of this kind. ‘one’s right to privacy’.

Privacidad vs. Seguridad Pública

Algunas objeciones

- Existen herramientas para ayudarnos a proteger nuestra privacidad.
- Esas herramientas, ¿no serán una ayuda para que gente con pocos escrúpulos cometa sus ‘fechorías’?

Privacidad vs. Seguridad Pública

Pero ...

- También se puede comprometer esa seguridad con otras tecnologías (teléfono, cartas, anuncios en la prensa, ...)
- La tecnología está disponible, prohibirla no impide su uso.
- Nosotros también podemos necesitar protegernos.

Ataques a la privacidad/seguridad

- La mayoría de los usuarios son gente común *‘como nosotros’*.
- ¿A quién pueden interesar mis datos?
- ¿Quién puede querer hacerme daño?

Ataques a la privacidad/seguridad

Ojo!!

- Puedo tener acceso a información importante.
- Alguien puede utilizarme como intermediario.
- Romper sólo porque es posible (y fácil a veces).

Pero ... ¿la red es mala o buena?

¿Con qué debo tener cuidado?

- Acceso físico a los recursos
  ¿Quién tiene acceso?
  - Conocidos.
  - Desconocidos.
  - Computadores compartidos.
  - Servicios de mantenimiento.

  ¿Dónde están?
  - En un despacho cerrado
  - En un laboratorio común
  - En ...

¿Con qué debo tener cuidado?

- Técnicas de ingeniería social
  - Cuidado con gente muy ‘amistosa’.
  - Si en la calle no se lo dirías, ¿en la red si?.
  - Si normalmente se hace de una manera, ¿por qué cambió?.
  - ¿Qué datos puede pedirme un técnico?

Ingeniería social

- Un poco + otro poco + varios pocos = mucha información
  - Primera llamada: nombre del jefe.
  - Con el nombre del jefe: localización de un recurso.
  - Con el nombre del jefe y la localización del recurso . . .

Confidencialidad de los datos

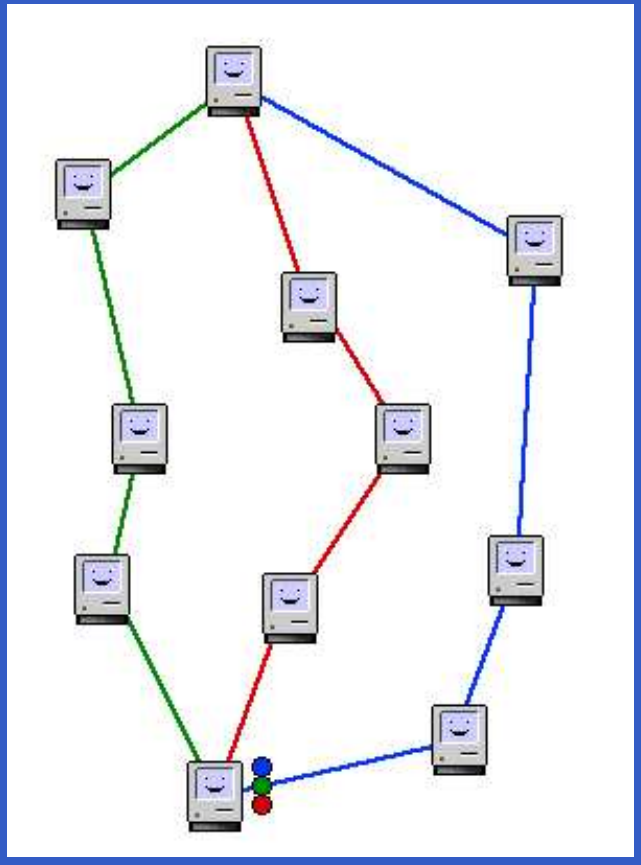
- La prudencia nos ayuda a disminuir los peligros
- Pero queremos comunicarnos!!!

Además ....

. . . ¿Cómo viaja la información por la red?

¿Cómo viaja la información por la red?

Las malas noticias siguen (?)



¿Cómo viaja la información por la red?

¿Entonces?

- Objetivo: transmisión de información, fiabilidad y robustez, no seguridad.
- No sabemos por dónde viaja nuestra información (ni tenemos control sobre ello).

Puertos (sin mar)

- Habitualmente, una sola conexión (dirección)
- Muchos servicios (mail, web, compartir archivos, ...)
- Solución: asignarles diferentes números (como a los buzones de una oficina)
- Conexión $\longrightarrow$ dirección + servicio

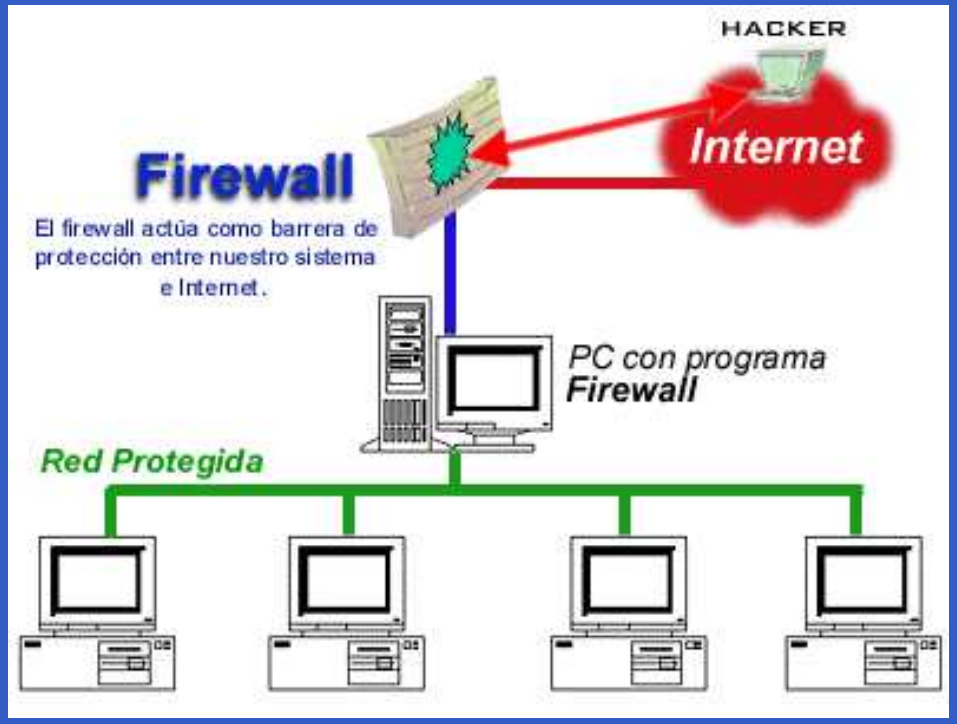
¿Y?

Puertos (¿Y?)

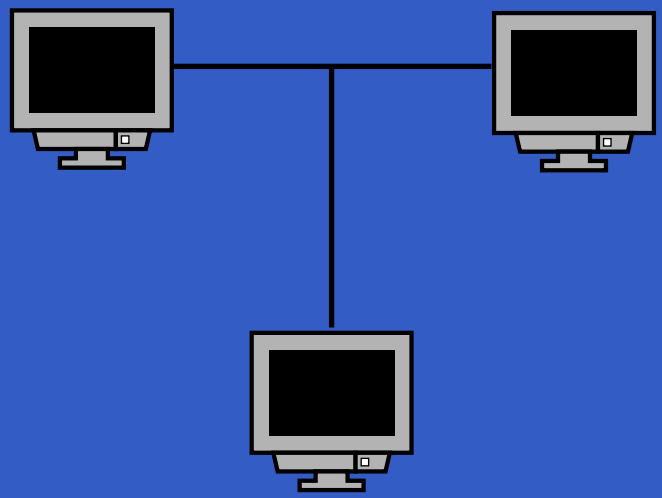
- Si no damos los servicios, es mejor que no estén abiertos los puertos correspondientes.
- ¡Usar un cortafuegos!
- Uno, general (a la entrada de la red)
- Uno, personal (en cada PC)

`http://www.seguridadenlared.org/es/zone.php`

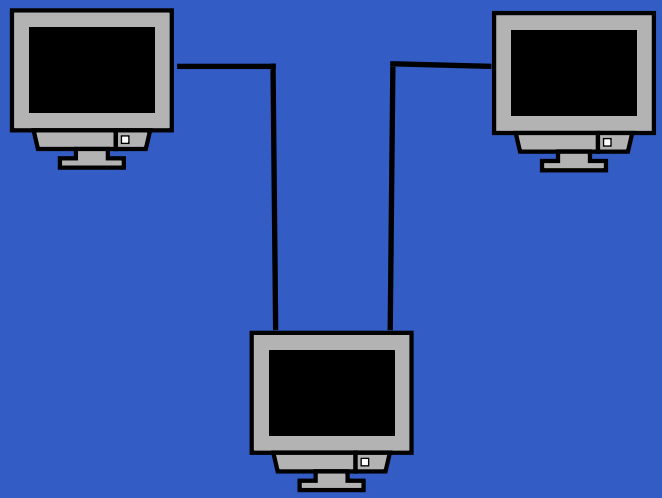
El cortafuegos



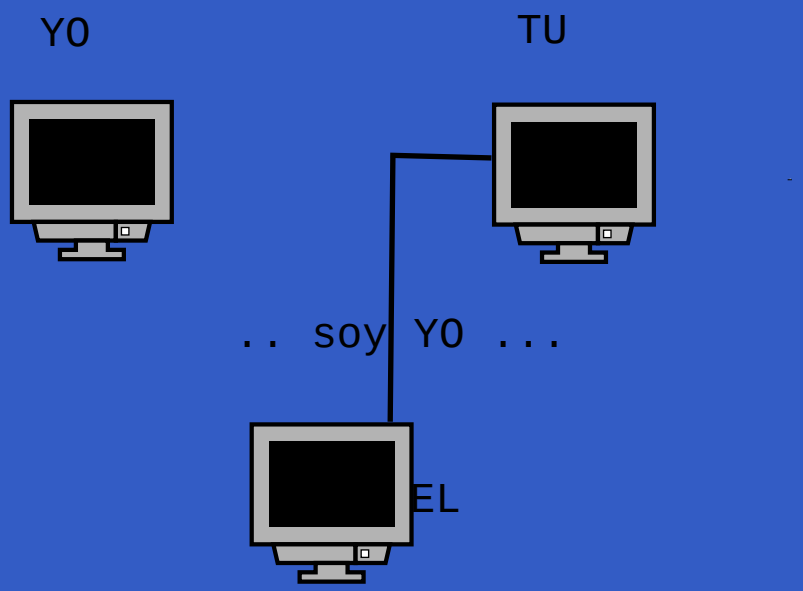
Escuchas



Modificación



Suplantación



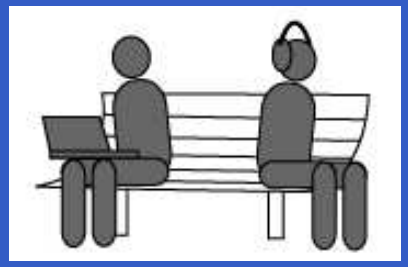
¡Los virus y troyanos hacen eso!

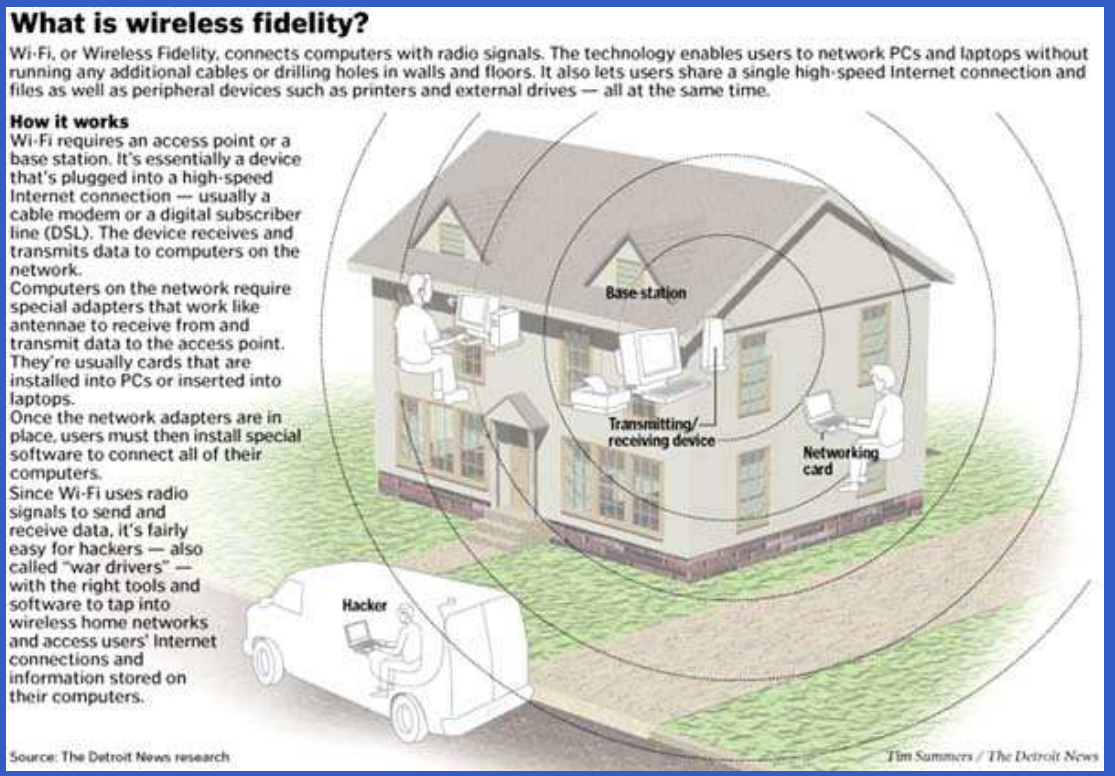
Repudio

Yo no fui!

Redes inalámbricas

La información se transmite por el aire (radio)





Precauciones WiFi

- Cuidado con las claves
- Control de acceso con autentificación bidireccional
- Configuración WEP (128 bits)
- Variación en las claves a lo largo del día
- Control de radio de transmisión
- Estar atentos ... todo cambia muy rápido todavía

¿Tiene remedio?

- Siempre que dos se comunican puede haber un tercero interesado.
- Siempre que se esconde algo, hay alguien dispuesto a encontrarlo (criptografía vs. criptoanálisis).

¿Tiene remedio?

Breve historia de la criptografía (muy breve)

- Julio César: ‘desplazamiento en el alfabeto’

$$\text{MEDICINA} \longrightarrow \text{OGFKEKPC}$$

- Variaciones sobre el tema: reordenamiento del alfabeto, modificaciones más sofisticadas.
- II Guerra Mundial: Enigma, computadores, grandes avances, pero basados en sistemas similares.

¿Tiene remedio?

Inconvenientes

- Solamente confidencialidad.
- Muchas claves
- ¿Cómo intercambiar las claves?

Ventajas

- Simplidad
- Rapidez

¿Tiene remedio?

¿Sólo confidencialidad?

Afortundadamente, no.

¿Cómo?

¿Tiene remedio?

Criptografía de clave pública

- Basada en dos claves:
  - Una pública
  - La otra, privada

Propiedades

Propiedad:

Secreto

- ¿Cómo se usa?

1. Secreto $\longrightarrow$ Codifico con la clave pública del receptor.
   - ¡Sólo él puede leer!
   - Cualquiera puede haberlo escrito

Autenticidad

- ¿Cómo se usa?

1. Autenticidad $\longrightarrow$ Codifico con mi clave privada.
   - Sólo yo puedo haberlo escrito
   - Cualquiera puede leerlo

Autenticidad + Secreto

- ¿Cómo se usa?

1. Es posible combinar las dos .
   - Sólo yo pude escribirlo
   - Sólo el receptor puede leerlo

¿Y el receptor?

- ¡Al revés!

1. Decodifica con su clave privada (sólo él puede).
2. Comprueba la autenticidad con mi clave pública.

Vamos bien

Ventajas

- Mi clave pública es conocida por todos.
- Mi clave privada no se transmite.
- La clave pública del receptor garantiza que sólo él podrá leerlo.
- Mi clave privada garantiza que sólo yo he podido generarlo (salvo robo).
- Sólo necesitamos una clave por cada interlocutor.

Pero ...

Inconvenientes

- Más complicado.
- Más lento (elevar números a pontencias grandes).
- ¿De quién es la clave pública?

¿Tiene remedio?.

- Recordar: ‘Mi clave privada garantiza que sólo yo he podido generarlo (salvo robo).’ Entonces ...
- Si codifico con mi clave privada, cualquiera puede comprobar la veracidad con la pública (no hay secreto, pero si verificación).
  ¡Vaya lío!
- Se puede simplificar (en realidad, acelerar).

Firma digital

No quiero codificar todo el mensaje:

- Mucho trabajo (cálculos).
- Confusión (X$&7Ji43).
- No es secreto

La solución

mensaje $\longrightarrow$ mensaje + ‘resumen del mensaje’

$\longrightarrow$ mensaje + ‘resumen del mensaje cifrado’

Firma digital

¿Y ahora?

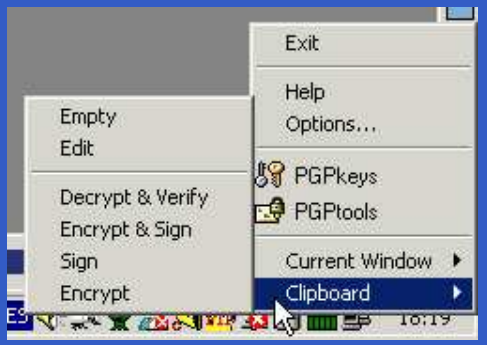
- Cualquiera puede leerlo (si codifico sólo con mi clave, también).
- Cualquiera puede comprobar su autenticidad.

¿Cómo lo hago?

- PGP

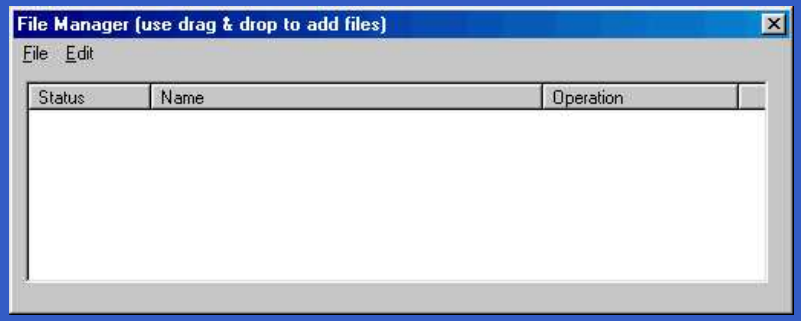
  http://www.pgp.com/products/freeware.html

  http://www.seguridadenlared.org/es/pgp.php



¿Cómo lo hago?

- GnuPG `http://www.gnupg.org/(es)/index.html`
  `http://www.seguridadenlared.org/es/gnupg.php`



¿Preguntas?

¿?

Referencias

[ESP] *ESPASA, Diccionario Enciclopédico Abreviado*. ESPASA.

[oxf] *Oxford English Dictionary*. Oxford University Press, second edition (electronic database version) edition. http://www.oed.com/.