

Taller: Software Libre, Cibercontrol y hacktivismo

**Jornadas Solidaridad en Red
Elkartasuna Sarean
Jardunaldiak
Vitoria-Gasteiz, 2004**

Introducción al Software Libre

- ¿Qué es el software?
- ¿Qué es un Sistema Operativo?
- Breve historia del software
- El software libre frente al software privativo
- Práctica: X-Evian, una distribución de GNU/Linux por Metabolik BioHacklab

¿Qué es el Software?

- El software y la gastronomía
 - Un programa es “una manera ordenada de hacer algo”, es decir, una receta:
 - Receta:
 - Batir huevos
 - Freir patatas
 - ...
 - Programa:
 - Freir enemigo
 - Sumar 500 puntos
 - ...
 - A la receta, en informática se le llama **código fuente**, mientras que al pastel, **código binario o ejecutable**.

¿Qué es el Software?

- El software y la gastronomía

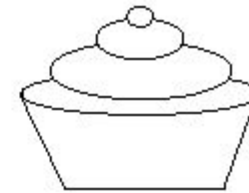
- Gastronomía:



Receta



Horno



Pastel

- Software:

**Código
fuente**

Compilador

**Código
ejecutable**

¿Qué es un Sistema Operativo?

- Un Sistema Operativo es un conjunto de **programas** que nos **facilitan** el uso de la máquina.
- Ejemplo práctico:
 - El S.O. de un móvil nos permite enviar cómodamente SMS, aunque el proceso sea bastante complejo (antenas, facturación, etc.).
- Ejemplos de S.O.s para PCs:
 - Microsoft Windows, GNU/Linux o MacOS

Breve historia del software

- Años 70:
 - Muchas máquinas enormes, difíciles y diferentes.
 - Nace UNIX, un S.O. que funciona en muchos ordenadores diferentes: una especie de “esperanto” de los ordenadores.
 - Los *hackers* de universidades y centros de investigación **colaboran libremente**, ayudándose a que sus programas funcionen en ordenadores tan diferentes.

Breve historia del software

- Años 80:
 - Nace el PC: los ordenadores dejan de ser diferentes (¡y dejan de ser caros!).
 - Cambio del modelo de negocio: se dejan de vender ordenadores carísimos y se comienza a vender software:
 - Empresas de software fichan a hackers con contratos millonarios y con **cláusulas de no divulgación**.
 - Algunos se hace MUY ricos así, otros no aguantan esa situación y fundan la Free Software Foundation.

Breve historia del software

- La Free Software Foundation:
 - Quiere crear programas LIBRES, que puedan ser copiados, modificados, regalados, vendidos o lo que nos apetezca hacer con ellos.
 - Su proyecto más importante es hacer un S.O. libre, es el proyecto GNU (GNU's Not UNIX).
 - Richard Stallman comienza solo, pero a través de la naciente Internet se le van sumando colaboradores (modelo bazar).

Breve historia del software

- Años 90:
 - El proyecto GNU estaba casi terminado:
 - La gente de la FSF tomó un UNIX comercial y fue cambiando cada pieza por una pieza libre.
 - Faltaba sólo el “cerebro” del S.O., el núcleo o kernel.
 - Linus Torvalds, un estudiante de informática, programa “Linux”, un núcleo de un S.O. (por hobby, “just for fun”).
 - GNU + Linux = GNU/Linux, un S.O. completamente libre.

¿Qué es el Software Libre?

- Es aquel que cumple 4 libertades:
 - Libertad 0: libertad de usar el programa, con cualquier propósito.
 - Libertad 1: libertad de estudiar cómo funciona el programa y adaptarlo a tus necesidades.
 - Libertad 2: libertad de distribuir copias, con lo que puedes ayudar a los demás
 - Libertad 3: libertad de mejorar el programa y hacer públicas esas mejoras.

¿Cómo se protege todo esto?

- “El software libre es gratis, así que cualquiera puede copiarlo, cambiar el nombre y cerrarlo, para forrarse”.
- No, el software libre está protegido por el **copyleft**.

¿Qué es el copyleft?

- Copyleft:
 - Es un copyright, pero en donde se especifican las condiciones de copia, en lugar de decir “prohibida toda copia por cualquier medio blablabla...” dice “permitida la copia blablabla...”.
 - No es un cuento chino, se basa en el copyright, así que lo amparan leyes internacionales.
 - © Copyright, all rights reserved.
 - ☺ Copyleft, all rights reversed ;-)

Software libre vs. privativo

- Libre:
 - Uso ilimitado
 - Permitida la copia
 - Permitida la modificación
 - Formatos abiertos
 - Sin garantía
- Privativo:
 - Uso restringido
 - Prohibida la copia
 - Prohibida la modificación
 - Formatos cerrados
 - Sin garantía

Práctica: X-Evian GNU/Linux

- ¿Qué es X-Evian?
 - Una distribución de GNU/Linux auto-arrancable y auto-instalable.
 - Es copyleft, producto de saberes libres.
 - Es un dispositivo hacktivista para la desobediencia, la autonomía digital y el activismo social.
 - Es tecnopolítica, mezcla de lo técnico y lo social.

Práctica: X-Evian GNU/Linux

- X-Evian
 - Funciona desde el CD-ROM (Live-CD).
 - Se puede instalar (todavía en pruebas).
 - Optimizada para ordenadores viejos (Pentium, Pentium II).
 - Descargable gratuitamente:
 - <http://www.x-evian.org>

Práctica: X-Evian GNU/Linux

- X-Evian

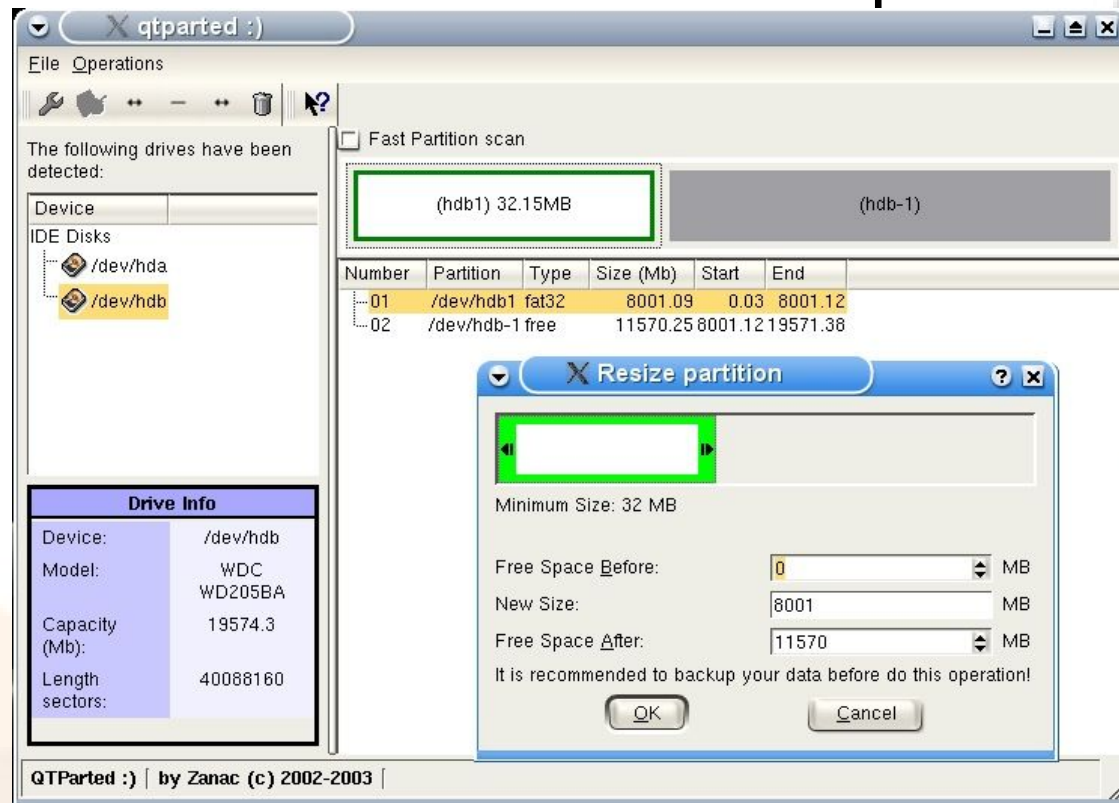


Práctica: X-Evian GNU/Linux

- Instalar GNU/Linux:
 - Dos problemas si tienes otro Sistema Operativo instalado:
 - Dividir el disco en al menos dos particiones, una para cada Sistema Operativo.
 - Configurar el menú de arranque para que nos permita cargar uno u otro Sistema Operativo.

Práctica: X-Evian GNU/Linux

- Particiones con X-Evian y qtParted:
 - hacer “hueco” en el disco duro para GNU/Linux.



Práctica: X-Evian GNU/Linux

- Configurar el arranque:
 - El instalador de X-Evian o cualquier distribución de GNU/Linux lo hace automáticamente.
 - Este es un punto crítico, en el que deberíamos prestar mucha atención, porque podríamos dejar otros Sistemas Operativos inaccesibles.

Práctica: GNU/Linux

- ¿Cuál es el equivalente en GNU/Linux de...?
 - <http://alts.homelinux.net/index.php>
 - Ejemplo:
 - Acrobat Reader:
 - gpdf
 - xpdf
 - gv
 - KGhostView

Práctica: GNU/Linux

- ¿Qué distribución es la mejor para empezar?
 - Ubuntu Linux es muy sencilla.
 - Tiene dos versiones:
 - Versión para instalar.
 - Versión Live-CD para probar.
 - Puedes descargarla desde www.ubuntu.org
 - Puedes solicitar un pedido de CDs gratuitamente en esa misma dirección.
 - Funciona en PC y Mac, entre otros.

Cibercontrol social

- Analizaremos...
 - Medidas de control social en globales en Internet.
 - Medidas de control social en nuestro propio PC.
 - Medidas de control social en telefonía móvil.
 - Medidas de control social sin el uso de tecnología.

Cibercontrol social

- ¿Qué es el cibercontrol social?
 - El control social gracias a las nuevas tecnologías, cada vez más capaz y más simple para quienes disponen de la infraestructura adecuada.
 - Ejemplos:
 - Red de espionaje internacional Echelon.
 - Sistemas de localización geográfica por telefonía móvil.
 - Pasaporte digital con RFID.

Cibercontrol social

- Cibercontrol social global gracias a Internet.
 - Las nuevas usuarias y usuarios de Internet tienen una falsa sensación de anonimato en la Red, creen que nadie vigila su navegación, que podrían hacerse pasar por cualquiera.
 - Hay redes especializadas en vigilar/espiar:
 - Echelon
 - Carnivore
 - Sistemas Single-Sign-on
 - Sistemas de correo electrónico gratuito

Cibercontrol social

- Echelon
 - Sistema de espionaje al ciudadano de a pie en su vida cotidiana, todo el mundo es un enemigo potencial.
 - No sólo las comunicaciones personales por Internet son filtradas y espiadas, sino muchas conversaciones telefónicas, móviles, fax y GPS.
 - Funcionaba con un sistema de "palabras clave" que activan el filtrado (Ejemplo: "he bombed!").

Cibercontrol social

- Echelon

- Participan Estados Unidos, el Reino Unido, Canadá, Australia y Nueva Zelanda.
- El Parlamento Europeo hizo pública su existencia en mayo de 2001
(http://www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf).

Cibercontrol social

- Echelon
 - Técnicamente le lleva 10 años de ventaja a Internet:
 - Cuando ARPANet se abrió al público, la red "Platform" que sustenta Echelon ya era mucho más potente (sistemas de satélites y cables submarinos).

Cibercontrol social

- Echelon

- Echelon descartó ya en los 80 el sistema de palabras clave que utiliza actualmente Google (¡¡en los 80 yo grababa mis juegos de Spectrum de la radio!!).
- Actualmente ha solicitado la patente para un método de búsqueda basado en campos semánticos, por lo que ya será obsoleto y estarán utilizando otro.
- Han hecho lo mismo con un sistema de reconocimiento de voz automatizado global.

Cibercontrol social

- Echelon

- Margaret Newsham (arrepentida):

- "Ya en 1979 podíamos rastrear a una persona determinada y captar su conversación telefónica en tiempo real".
 - En 1984, los satélites de inteligencia norteamericanos "lograron fotografiar un sello de correos en el suelo, por lo que es casi imposible imaginar la versatilidad de los sistemas de hoy".
 - "Con la tecnología actual, toda comunicación electrónica es un objetivo para los servicios de inteligencia: tus transferencias de dinero, tus operaciones de Bolsa, tus conversaciones políticas y tu comunicación privada. Todo es puesto al descubierto".

Cibercontrol social

- Carnivore
 - Sistema de espionaje creado por la NSA, Agencia de Seguridad Nacional de Estados Unidos, y el FBI.
 - Colaboración con empresas como Microsoft o Cisco, líderes en el mercado del software y el hardware de equipamientos de red respectivamente.

Cibercontrol social

- Carnivore
 - En palabras del propio FBI:
 - "Carnivore es un sistema computacional diseñado para permitir al FBI; en colaboración con un proveedor de Internet (ISP) se haga valer una orden judicial que exige la recolección de cierta información en relación al correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación".
 - La manera de funcionar y sus implicaciones son similares a la nueva Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

Cibercontrol social

- Sistemas Single Sign On:
 - Sistemas de solamente una autenticación:
 - Introduces una vez tu usuario y contraseña en un sistema (hotmail, por ejemplo).
 - El resto de sistemas asociados (Amazon.com, Ebay.com, etc.) reconocen tu “pasaporte virtual” y no solicitan autenticación.
 - Bastante cómodo.

Cibercontrol social

- Sistemas Single Sign On: Passport.Net
 - Microsoft Passport.Net amenaza contra la intimidad de los "netizens".
 - Con ese pasaporte vamos dejando un rastro en muchos sitios simultáneamente.
 - Problema: correlaciones y data-mining. Ejemplo:
 - Comprar medias: ¿regalo a tu hermana?
 - Comprar rifle de caza: ¿tienes un coto de caza?
 - Comprar sierra de metal: ¿bricomania?
 - Suma de todas: ¿atracó a un banco?

Cibercontrol social

- Correo electrónico gratuito:
 - Existe actualmente una lucha por ser el correo gratuito que más MB da de buzón a sus usuarios:
 - Hotmail duplica el tamaño de sus buzones.
 - Yahoo ha ampliado recientemente su buzón a 100 MB.
 - Gmail, el correo gratuito de google, dota a sus usuarias de un buzón de 1000 MB.

Cibercontrol social

- Correo electrónico gratuito: Gmail
 - Gmail ha conseguido muchos usuarios:
 - Es el que mayor tamaño de buzón ofrece (1 GB).
 - + Técnica de márketing:
 - No es posible solicitar una cuenta en gmail, tienes que ser invitado por otro usuario.
 - Las cuentas de gmail se convierten virtualmente en un bien preciado.

Cibercontrol social

- Correo electrónico gratuito: Gmail
 - Política de Gmail:
 - No borres nada, no hace falta, en lugar de pulsar en “Borrar”, pulsa en “Archivar”.
 - Invita a tus amigas y amigos a Gmail.
 - Consecuencias:
 - Gmail tiene una base de datos enorme de e-mails de mucha gente, perenne, porque nadie borra sus e-mails.
 - Gmail tiene una red de gente generada por sus propios usuarios al hacer las invitaciones.

Cibercontrol social

- Sistemas de control social en nuestros Pcs:
 - Sistemas Software:
 - Códigos troyanos
 - Sistemas de activación por Internet
 - Sistemas Hardware:
 - Computación confiable, Trustworthy Computing.

Cibercontrol social

- Códigos troyanos:
 - Un troyano es un programa que además de hacer su labor, hace otras sin nuestro consentimiento.
 - Como el Caballo de Troya: regalo y trampa a la vez.
 - Ejemplo:
 - La última versión del Windows Media Player para ver películas y escuchar música, se conecta a Internet para informar de los ficheros que vemos. En principio para ofrecer información extra.

Cibercontrol social

- Códigos troyanos: "Magic Lantern"
 - Desarrollado por el FBI y la CIA. Con el beneplácito de los dos grandes pesos pesados de Internet: Microsoft y CISCO.
 - Con la colaboración de expertos en seguridad como el grupo "Cult of the Dead Cow", famoso por el troyano "Back Oriffice".
 - Las empresas de antivirus se mantienen en una extraña ambigüedad: ¿detectan el troyano? ¿fidelidad al cliente o al Gobierno de USA? Microsoft y CISCO ya han decidido.

Cibercontrol social

- Sistemas de activación por Internet:
 - Antiguamente se utilizaban números de serie, "mochilas", etc. para activar los programas.
 - Todo eso está olvidado, activación por Internet.
 - ¿Cuánta información personal revelan tus programas al conectarse con la empresa que los creó?
 - Muchos posibles objetivos: Marketing, combatir la piratería, espionaje industrial.
 - Windows XP se conecta de 20 formas diferentes y espía software de terceros (comprobado gracias al programa tecDUMP).

Cibercontrol social

- Sistemas de control hardware en nuestros PCs: Computación Confiable
 - Varios nombres:TC / TCG / TCPA / LaGrande / Palladium. Se ha cambiado varias veces por las protestas en Internet contra cada sistema, por atentar contra la privacidad de las netizens.
 - El “Grupo para la Informática Fiable” es una alianza entre Microsoft, Intel, IBM, HP y AMD.

Cibercontrol social

- Sistemas de control hardware en nuestros PCs: Computación Confiable
 - Objetivo: Conseguir un ordenador "más seguro"
 - ¿Para quién?
 - Más seguro para las empresas de software y contenidos audiovisuales (Microsoft, Disney).
 - Más inseguro para su propietario. Stallman lo califica de Informática Traidora (TC is Traitor Computing).
 - Su aplicación inicial era el Control de Derechos Digitales (DRM): venderte un DVD que sólo funciona en 1 PC y el día de tu cumpleaños.

Cibercontrol social

- Sistemas de control hardware en nuestros PCs: Computación Confiable
 - ¿Pero todo esto no se puede hackear?
 - En una primera fase se podría "escuchar" digitalmente el flujo de datos entre el procesador y el chip Fritz, encargado de realizar el cifrado necesario para esta tecnología.
 - Cuando el chip Fritz se integre dentro del procesador esto será inviable (¡Intel y AMD están dentro del Grupo para la Computación Confiable!).

Cibercontrol social

- Sistemas de control hardware en nuestros PCs: Computación Confiable
 - ¡Pues nos negamos a usarlo!
 - Quizá tu proveedor de Internet te obligue a conectarte desde un ordenador "seguro".
 - Quizá tu banco te obligue a lo mismo.
 - ¡¡¡PROTESTAR, PROTESTAR y PROTESTAR!!!

Cibercontrol social

- Sistemas de control hardware en nuestros PCs: Computación Confiable
 - ¿Cuándo llegará todo esto?
 - ATMEL ya está vendiendo un chip Fritz.
 - Puedes comprarlo de serie en un IBM Thinkpad.
 - Algunas de estas maravillosas características ya están implementadas en WindowsXP y la X-Box.
 - El Enterprise Rights Management ya se incluye con todos los Windows 2003 Server.
 - Guardad vuestros viejos PCs en el desván, nos harán falta cuando las cosas se pongan duras ;-)

Cibercontrol social

- Sistemas de control social por telefonía móvil: localización geográfica
 - La propia tecnología que sustenta la telefonía móvil necesita la localización geográfica del móvil.
 - Roaming:
 - Cambio automático y transparente al cliente de telefonía móvil de una estación de telefonía a otra.
 - Cuando hablamos por el móvil en un autobús, no se corta al alejarnos de una antena, el móvil está conectado a varias y hace roaming entre ellas.

Cibercontrol social

- Sistemas de control social por telefonía móvil: localización geográfica
 - La localización se basa en:
 - Las antenas de telefonía móvil cubren 360°, pero están sectorizadas en 3 antenas de 120° normalmente.
 - Los tiempos de retardo para cada antena a las que está conectado un móvil.

Cibercontrol social

- Sistemas de control social por telefonía móvil: localización geográfica



Cibercontrol social

- Sistemas de control social por telefonía móvil: localización geográfica
 - En el diagrama:
 - El móvil está conectado a 3 estaciones.
 - Con A tiene un retardo de 50 ms.
 - Con B tiene un retardo de 30 ms.
 - Con C tiene un retardo de 45 ms.
 - Conclusiones:
 - Se encuentra en el triángulo comprendido entre A, B y C.
 - Está más cerca de B que del resto, y un poco más cerca de C que de A.

Cibercontrol social

- Sistemas de control social por telefonía móvil: localización geográfica
 - Actualmente se ofrece comercialmente en España por el RACC o servicios como "¿Dónde?" de Amena:
 - Seguimiento sólo a móviles que hayan dado su "consentimiento": flota de camiones, adolescentes...
 - Coste mínimo, SMSs.
 - Vuestros móviles son como la bola roja que se saca Schwarzenegger en Desafío Total por la nariz (yo no tengo móvil ;-)

Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - RFID es IDentificación por Radio Frecuencia.
 - En los años 80, investigadores del MIT pretendieron hacer sistemas de reconocimiento de objetos comunes, pero tuvieron muchísimos problemas, así que decidieron que fueran los propios objetos los que se identificaran.

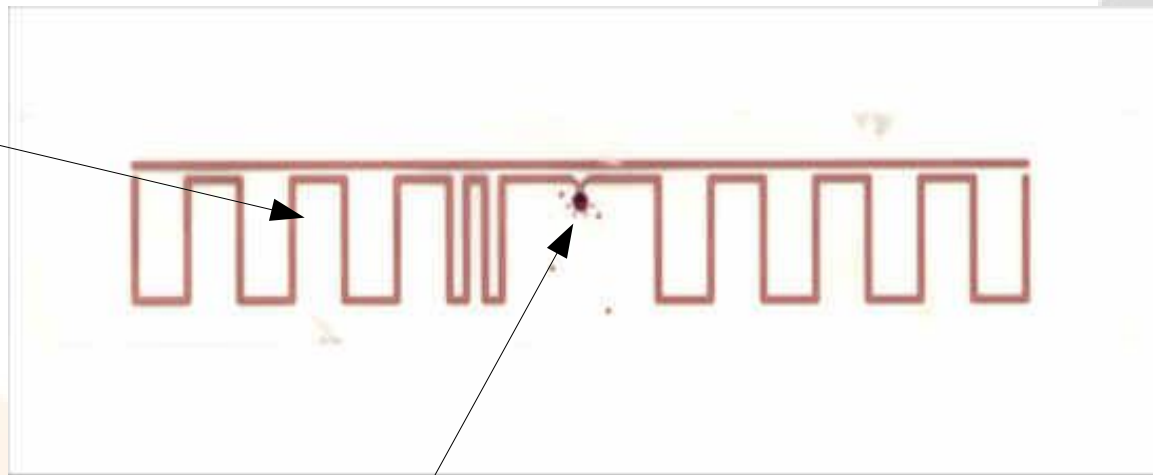
Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - Un chip RFID puede ser:
 - activo: si necesita alimentación eléctrica (pilas), con un alcance de unos 10 Km.
 - pasivo: si no necesita alimentación eléctrica y rebota la señal de radio que recibe, modificada. Su alcance es de unos 15 metros.

Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - Los chips se componen del chip y la antena:

Antena



Chip RFID

Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - En principio podrían valer para hacer inventarios automáticos, detectar pequeños robos (las de Yomango las conocen bien), etc.
 - En la práctica sirven para cibercontrolar:
 - Se han implantado en colegios privados de USA: ya no hace falta pasar lista, controlar a los niños en cada momento, ¡es genial!
 - Se han etiquetado con RFID todos los libros de la Biblioteca Pública de Berkeley.

Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - ¿Es esto otra paranoia?
 - Sí, claro, pero ya están aquí...
 - Gillete comercializa maquinillas con RFID para controlar el hábito de sus consumidores... ¿lo sabíais?
 - Wall-Mart, la cadena de supermercados más grande de USA lo comenzará a obligar a sus proveedores dentro de 3 años.
 - Zara tiene un modelo de zapatos de caballero con un chip RFID en el tacón.
 - Caben unos 4 chips RFID en una lentilla (0.4mm x 0.4mm), desconfiad hasta de las pegatinas de los plátanos.

Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - Los chips RFID son resistentes al calor y al agua, pueden utilizarse en prendas de vestir.
 - Para deshabilitarlos hay que separar el chip de su antena, para que no pueda emitir.
 - Para localizarlos deberemos estar atentos a posibles mallas metálicas o utilizar Rayos-X si pudiéramos (si somos veterinarios o quiroprácticos, por ejemplo).

Cibercontrol social

- Ejemplos de chips RFID: en cajas de plástico.



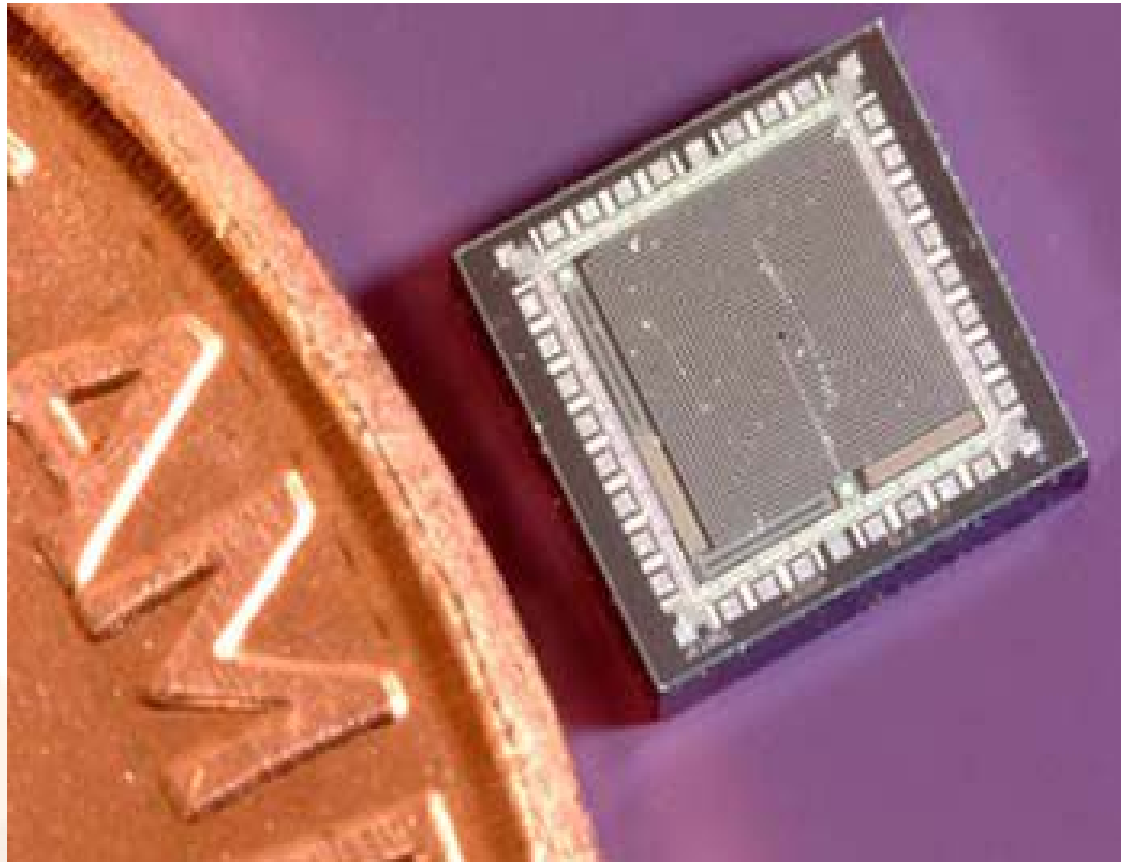
Cibercontrol social

- Ejemplos de chips RFID: en S, para cartón.



Cibercontrol social

- Ejemplos de chips RFID: con un penique.



Cibercontrol social

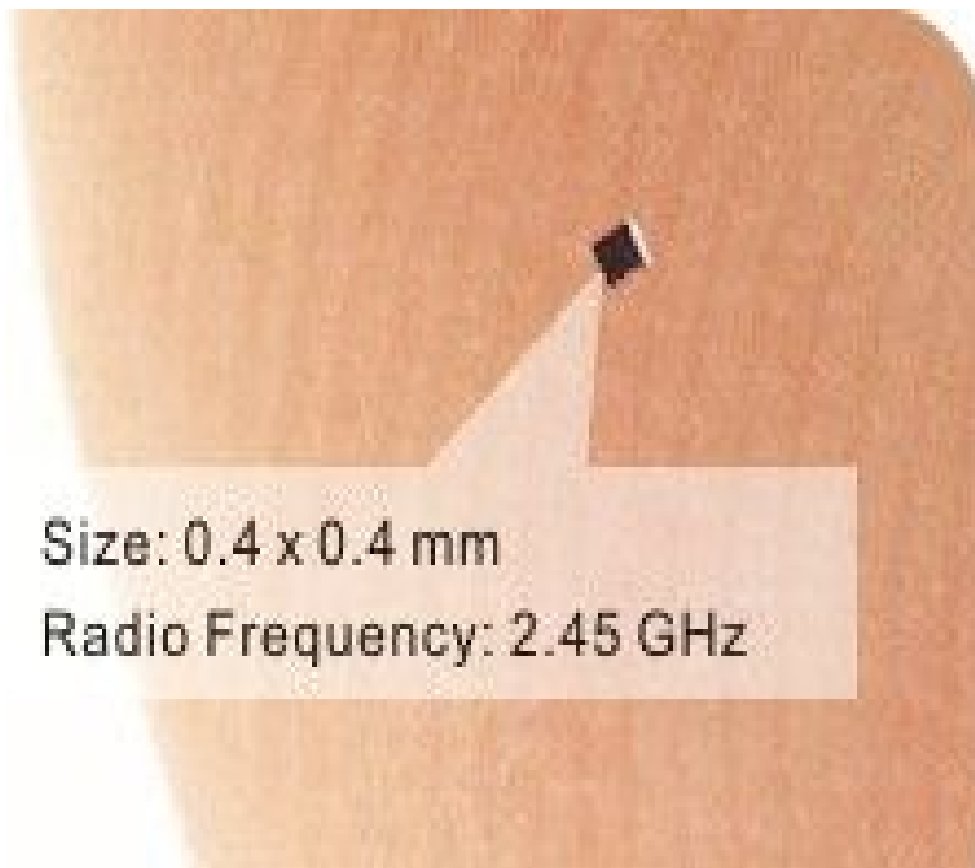
- Ejemplos de chips RFID: miniaturización.



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Cibercontrol social

- Ejemplos de chips RFID: ¿billetes?



Application Example: Gift Certificate



Cibercontrol social

- Ejemplos de chips RFID: miniaturización, radiografía de una hormiga con RFIDs.



Cibercontrol social

- Lectores / Grabadores de RFID, de venta en Internet



Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - Un caso grave: el nuevo pasaporte digital.
 - Existen dos maneras de hacer un pasaporte digital:
 - SmartCard: como el chip de las “tarjetas monedero”, precisan introducir el chip en un lector, como las tarjetas de crédito.
 - RFID: no precisan introducir el chip en el lector, pueden leerse a distancia y sin nuestro consentimiento.
 - Estados Unidos ha elegido RFID, que no aporta ninguna ventaja sobre SmartCard al poseedor del pasaporte y sí desventajas para su intimidad.

Cibercontrol social

- Sistemas de control social sin el uso de la tecnología: RFID
 - Un caso grave: el nuevo pasaporte digital



Cibercontrol social

- Katherine Albretch, protestando por los RFID en productos Gillette



Cibercontrol social

- Niño protestando contra las etiquetas RFID en sus juguetes.



Práctica: Navegar sin dejar rastro

- Funcionamiento de una petición web:
 - Cuando un navegador pide una página web a un servidor web, envía:
 - Su dirección IP en Internet. Ej: 130.206.100.12
 - La página web que quiere. Ej: www.google.com
 - Desde qué página web viene. Ej: www.terra.es/deportes
 - Desde qué navegador está accediendo. Ej: Internet Explorer.

Práctica: Navegar sin dejar rastro

- Funcionamiento de una petición web
 - Al navegar es posible que no nos interese dejar todos estos datos en el servidor al que accedemos.
 - Por ello podemos utilizar un servidor Proxy, que hará de “recadista” entre el servidor web y nuestro navegador.
 - El problema es que los servidores Proxy normales dicen “de parte de quién” vienen.
 - Necesitamos proxies anónimos.

Práctica: Navegar sin dejar rastro

- Funcionamiento de una petición web
 - Un proxy anónimo permite navegar anónimamente a través de él, es decir, acepta recados web sin informar a nadie de quién se los pidió.
 - Normalmente suelen ser gratuitos, aunque hay servicios especiales que son de pago.

Práctica: Navegar sin dejar rastro

- Funcionamiento de una petición web
 - Proxies anónimos:
 - El de Autistici, en desuso:
<http://anonymizer.autistici.org/english/>
 - Sencillos de utilizar:
 - <http://www.the-cloak.com/login.html>
 - <https://www.proxyweb.net/antilog.php>
 - <http://anonymouse.ws/anonwww.html>
 - Oculta la página que pides:<http://www.calcmaster.net/>
 - Listado completo:
http://www.freeproxy.ru/en/free_proxy/cgi-proxy.htm

Práctica: GnuPG

- GnuPG nos permite...
 - Cifrar cualquier texto para enviar correos electrónicos privados.
 - Cifrar ficheros de nuestro disco duro para que nadie pueda abrirlos sin nuestro consentimiento.
 - Es Software Libre, así que:
 - Tenemos la certeza de que no tiene puertas traseras.
 - Es estándar.
 - Es gratuito.

Práctica: GnuPG

- Criptografía simétrica y asimétrica
 - Simétrica:
 - La clave para cifrar es la misma que para descifrar.
 - Ejemplo: un candado sólo tiene una llave, tanto para abrirlo como para cerrarlo.
 - Asimétrica:
 - La clave para cifrar es distinta pero complementaria a la clave para descifrar.
 - Ya no tengo solamente una clave, tengo siempre un par de claves: clave pública y clave privada.

Práctica: GnuPG

- Criptografía asimétrica
 - Imaginemos unos candados especiales:
 - Al comprarlo me dan una llave negra y una llave blanca.
 - Si cierro el candado con la negra, solamente podré abrirlo con la blanca complementaria (ni siquiera con la negra).
 - Si cierro el candado con la blanca, solamente podré abrirlo con la negra complementaria (ni siquiera con la blanca).
 - Los candados aceptan cualquier par de llaves, valdrían las de alguien que tuviera uno igual.

Práctica: GnuPG

- Criptografía asimétrica
 - Imaginemos unos candados especiales:
 - Yo guardo la llave negra en mi casa a buen recaudo y hago copias de la llave blanca a todo el que me la pida.
 - Cuando alguien quiera mandarme algo que solamente yo pueda abrir, no tiene más que comprar un candado especial, perdirme una copia de la llave blanca y cerrarlo.
 - Solamente la llave complementaria a esa llave blanca lo podrá abrir, y solamente yo la poseo.

Práctica: GnuPG

- Criptografía asimétrica
 - La llave blanca es la clave pública, que podemos dar a todo el mundo. Representa a “la manera que a mí me gusta que me cifren los mensajes”.
 - La llave negra es la clave privada, que no daremos a nadie.

Práctica: GnuPG

- Criptografía asimétrica
 - Cuando quiero mandar un mensaje cifrado a alguien...
 - Le pido su clave pública (llave blanca)
 - Cifro el texto con esa clave
 - Lo envío
 - Si alguien lo intercepta, como no tiene la clave privada complementaria a esa clave pública, no lo puede abrir (no tiene la llave negra de mi destinatario).
 - Al recibirlo, lo descifra con su clave privada (negra).

Práctica: GnuPG

- GnuPG:
 - Existen versiones tanto para Microsoft Windows como para GNU/Linux.
 - En Windows se llama WinPT, Windows Privacy Tools.
 - Manuales de uso:
 - <http://winpt.sourceforge.net/es/>
 - http://www.nautopia.net/nautopia_old/gnupg.htm

Hacktivismo

- El hacktivismo...
 - ¿Suma de hacking + activismo?
 - Comenzó siendo despreciado por los hackers y activistas:
 - hackers: "sois tecnológicamente patéticos, peores que los 'script kiddies'".
 - activistas: "usais la tecnología, un instrumento del poder".
 - Ha realizado diferentes campañas en la red, sin eficiencia práctica pero con mucha eficiencia mediática.

Hacktivism

- **Contraataque: Netstrike!!!**
 - Frente al control existen varias reacciones:
 - **Iniciativas y campañas:**
 - Campañas contra la aprobación de las patentes de software. Campañas de sensibilización acerca del Software Libre, la privacidad en Internet, etc.
 - Portales de (contra)información (normalmente basados en "open publishing").
 - **Hacktivism:**
 - Netstrikes: Ataques por saturación (DoS: Denial of Service) a sistemas gubernamentales normalmente.
 - Acciones tipo www.hactivist.com.

Hacktivism

- Hacklabs, Hack-in-the-streets, Hackmeetings
 - ¿Qué es un hacklab?
 - *"Para mi tanto los hackmeetings como los hacklabs representan una interesantísima y fructífera tensión-interacción entre lo social, lo tecnológico y lo político y nacieron con la idea de integrar y contaminar mutuamente a gente de estos campos y aprovechar las sinergias específicas de cada uno."* AZALAI
 - ¿Laboratorio de Hackers?
 - Social + Tecnológico + Político = Sinergia

Hacktivism

- Hacklabs
 - Nacen en Italia, dentro de Centros Sociales Okupados.
 - Coincidiendo con la celebración del primer "Hackmeeting" surge el hacklab de Barcelona, Kernel Panic.
 - Rápidamente el fenómeno se extiende:
 - Wau Holland Cielito Lindo Hacklab (Madrid)
 - Metabolik BioHacklab (Leioa)
 - ... www.hacklabs.org

Hacktivism

- Hacklabs



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Hacklabs



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Hacklabs



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Hacking the streets
 - Surgen con la misma idea que los "Reclaim the streets":
 - La idea es retomar la calle como un espacio político tecnológico.
 - ¿Por qué?, porque precisamente la tecnología es lo que está estructurando políticamente nuestra sociedad, tanto en los medios de comunicación, como en la vida cotidiana de la gente.
 - Acercar la tecnología a la gente de la calle.
 - Demostrar que no es tan inaccesible como pudiera parecer.

Hacktivism

- Hacking the streets



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Hacking the streets



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Hackmeetings

- No sólo es un encuentro de hackers.
- Es un encuentro de gente interesada en las nuevas tecnologías y en sus aspectos sociales que se realiza normalmente en un espacio liberado o CSOA.
- Varias ediciones:
 - 2000: Barcelona, Les Naus.
 - 2001: Leioa, Udondo Gaztetxea.
 - 2002: Madrid, Labo03, Lavapiés.
 - 2003: Pamplona, Jai Alai Gaztetxea.
 - 2004: Sevilla, CSOA Casas Viejas.

Hacktivism

- Hackmeetings



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Hackmeetings



Pablo Garaizar Sagarminaga. Copyleft, all rights reversed

Hacktivism

- Sistemas de Publicación Abierta: Indymedia
 - ¿Qué es el "open-publishing" o "publicación abierta"?
 - Es un sistema que permite a cualquiera (periodistas profesionales o no) publicar las noticias de forma instantánea en un sitio web accesible globalmente.
 - Los propios "actores" de la noticia pueden publicar sus versiones.
 - El criterio de lo "noticiable" no está regido desde "arriba".

Hacktivism

- Sistemas de Publicación Abierta: Indymedia
 - Características de este modelo de comunicación:
 - Se tratan gran cantidad de temas (no todo lo publicado tiene que estar "en el candelerero").
 - El filtrado es mínimo (en principio no hay censura).
 - La información así generada es libre de ser reproducida cómo y dónde se quiera, pero si es en un sistema de publicación abierta, mejor.

Hacktivism

- Sistemas de Publicación Abierta: Indymedia
 - Paralelismo con el Software Libre:

Software Libre
(GNU/Linux)



Publicación Abierta
(Indymedia)



Software Proprietario
(Microsoft)



Publicación Cerrada
(CNN)



Práctica: Publicar en Indymedia

- Es un proceso muy sencillo:
 - Acceder desde un navegador a <http://euskalherria.indymedia.org>.
 - Seleccionar el idioma en el que queremos trabajar en la columna de la izquierda, por ejemplo castellano.
 - Pulsar en el enlace “publicar” en la columna de la derecha:
 - NEWSWIRE: Este es un espacio de publicación abierta. Si quieres, puedes [publicar](#) tu noticia.

Práctica: Publicar en Indymedia

- Una vez en el formulario de publicación...
 - 1) Lo primero que se pregunta es el número de ficheros multimedia (fotos, videos, documentos, etc.) que tendrá la noticia. Si no vamos a incluir más de cinco, dejamos esto como está.
 - 2) Escribimos el título, autor, entradilla y noticia.
 - 3) Definimos opcionalmente datos como el idioma, una dirección de contacto, etc.
 - 4) Añadimos, si queremos, ficheros multimedia.
 - 5) Pulsamos el botón de publicar.
 - 6) Esperamos: como mínimo tardará 5 minutos en salir.

Referencias

- SinDominio: <http://sindominio.net>
- Hacklabs: <http://hacklabs.org>
- Hackmeetings:
<http://sindominio.net/hackmeeting>
- Nodo50: <http://nodo50.org>
- Indymedia: <http://indymedia.org>
- Netstrike: <http://netstrike.it>
- Autistici: <http://autistici.org>