CULTURA & POLÍTICA @ CIBERESPACIO
1er Congreso ONLINE del Observatorio para la CiberSociedad
Grupo 11: Ética aplicada en Internet – Estudio de la ética hacker
Coordinación: Ramon Alcoberro & Enric Faura
http://cibersociedad.rediris.es/congreso

ALGUNOS HACKERS BUENOS

Mercè Molist

"Que es mi ordenata mi tesoro
que todo el mundo ha de temer.
Mi ley, el ratón y el módem.
Mi única patria, la red"

Adaptación anónima de la 'Canción del Pirata', de Espronceda

Había una vez unos hombres -y muy pocas mujeres- que construyeron un mundo a su medida, donde el ingenio, la libertad y la educación fueron las normas. Hackers y ética son términos indivisibles desde la primera red, ArpaNet, cuando se discutían con pasión los buenos y malos usos de la tecnología. Paradójicamente, en el exterior, crecía la demonización de esta tribu, quizás la más numerosa y mejor conectada del planeta.

La DefCon es una legendaria reunión de hackers. Se celebra a mediados de julio en Las Vegas y acoge a miles. Entre las competiciones que allí se desarrollan, como la de Ingeniería Social (mentir para conseguir información), este año destacó algo nuevo: el juego del Superviviente CiberÉtico, con dos equipos enfrentados a preguntas como: ¿Penetrarías en el ordenador de tu escuela para cambiar las notas?. Su artífice, Winn Schartau, es una autoridad en el estudio de la "infoguerra" y autor del nuevo libro "Internet & Computer Ethics for Kids".

Cuando ni cortafuegos ni sistemas de detección pueden evitar que se doblen anualmente los ataques a sistemas, la vieja moral hacker llega al rescate. Según el servicio de información SecurityFocus, "los expertos en seguridad y las fuerzas de la ley norteamericanos promocionan cada vez más que se eduque sobre ética en las escuelas, ante el aumento de ataques informáticos realizados por adolescentes". Estos, a quienes los hackers llaman, despectivamente, 'script-kiddies', son un paso más en la confusión que rodea a la comunidad.

Gisle Hannemyr, en su estudio "Considering Hacking Constructive", traza el camino: "Los hackers originales eran profesionales informáticos que, a mediados de los sesenta, adoptaron

la palabra "hack" como sinómino de trabajo informático ejecutado con cierta habilidad. En los setenta, emergieron los techno-hippies, que creían que la tecnología era poder que debía ser puesto en las manos de la gente. En la segunda mitad de los ochenta, apareció el llamado "underground", que cambió los significados: "hack" equivaldría a sabotear un sistema informático".

Lejos de desaparecer, el término ha integrado todos los sentidos y hoy se considera hackers a los buenos programadores, a los manitas del "hardware" y la electrónica o a los que se especializan en (in)seguridad. Juntos forman una comunidad, con sus webs, listas de correo, canales de chat, lobos solitarios e incluso una "escena" y su correspondiente "star-system". Unidos por una nebulosa de ideas compartidas, algo como una ética-práctica que es su esencia y que, a veces, gravita entre la ley y el lado oscuro.

La Ley de la Selva

La norma es no confiar en las normas, como escribe Bruce Sterling en el libro "The Hacker Crackdown", que narra la primera redada en Estados Unidos, en 1989: "Cuando eres un hacker, son las propias convicciones internas de tu estatus de élite las que te capacitan para romper o exceder la reglas. Habitualmente, las reglas rotas por los hackers no son importantes, son las reglas de los avariciosos burócratas de las compañías de telecomunicaciones y de la estúpida plana de los gobernantes".

En este sentido, Lluís Mora, experto en seguridad, cita a uno de los padres fundadores, Richard Stallman: "No sé si existe una ética hacker, pero sí existió una ética del Laboratorio de Inteligencia Artificial del MIT: no importaban las reglas, en la forma de candados en las puertas o seguridad en los ordenadores. Estábamos orgullosos de lo rápido que podíamos eliminar la más mínima burocracia que se cruzase en nuestro camino. Cualquiera que cerrase una terminal en su oficina, porque era profesor y pensaba que era más importante que el resto de la gente, a la mañana siguiente encontraría su puerta abierta".

Aquellos autodenominados hackers de los 60 compartían una forma de pensar que sigue siendo el corpus ético de referencia para sus hijos y nietos espirituales, descrito por Steven Levy en el libro "Hackers": "El acceso a los ordenadores y a todo lo que te pueda enseñar algo sobre como funciona el mundo debe ser ilimitado. Toda la información debe ser libre. Desconfía de la autoridad, promueve la descentralización. Los hackers deberían ser juzgados por su hacking, no por su edad, nivel, raza o posición. Puedes crear arte y belleza con tu ordenador. Los ordenadores pueden cambiar tu vida a mejor".

Siempre guardianes de su buen nombre, cuando éste empezó a salir en las páginas de sucesos inventaron el término "cracker", para quien rompe las protecciones de un sistema, y "script-kiddie" para quien, además, no tiene ni idea. Lo explica Jesús Cea, fundador y moderador de la más poblada lista de correo de hackers hispanos: "Hace quince años, te lo tenías que 'currar' para tener un módem, entrar en una BBS... Ahora, mi abuela se compra un PC y hace doble clic y se conecta". Para Manuel Medina, director del centro de seguridad esCERT, "al principio tenía sentido, la única posibilidad de comunicarte con libertad era pirateando, pero la cosa se ha ido exagerando. Lo de antes era usar recursos escasos y desaprovechados. Ahora abusan".

También criticaba el legendario Lee Felsenstein, a finales de los 80, a los que se quejan ahora: "De una misión colectiva de exploración se ha pasado a una orgía de egoístas que alardea de haber penetrado en ordenadores militares". Steven Levy describía entonces un abismo que aún se mantiene: "En el primer grupo, los que crean, en el segundo, los que destruyen. El primer grupo amaba tener el control de sus ordenadores, pero el segundo ama el poder que le dan. El primer grupo siempre buscó cómo mejorar y simplificar, el segundo sólo explota y manipula. El primer grupo era comunal, compartía abiertamente nuevos descubrimientos, el segundo es paranoico, aislado y secreto".

Que corra el código

Adriano Galano, 27 años, es de los pocos que defienden a la nueva generación: "Los script-kiddies algún día se convertirán en verdaderos hackers". Galano se mueve entre los mundos de la seguridad informática y del "software" libre, temas unidos por el sagrado ciclo de creación de programas y sistemas que deberán mantenerse, encontrar fallos, añadir código, escribir manuales... La comunidad de programas libres GNU (GNU's Not Unix) es la más numerosa de las que alimentan esta cadena, donde se entrecruzan las necesidades y, como Galano, es posible zambullirse en diferentes campos a la vez, también en blanco y negro.

La mayoría de hackers comparte el uso y defensa del "software" libre, especialmente GNU/Linux. Es una cuestión de principios, pero también de confiar en lo que ha creado uno mismo y de costumbre histórica, de cuando los programas se intercambiaban y se mejoraban entre todos. El veterano Vinton Cerf explica: "Tim Berners-Lee no patentó la World Wide Web. No le puso copyright. La ofreció abiertamente. Y éste fue el acicate para el gran desarrollo de la red y de innovadoras ideas. Hay una ética continua en la comunidad, de devolver a la red lo que ella te ha dado a tí".

Galano entiende esta ética como "ser coherente con las cosas que pienso y en las que creo. Compartir, colaborar, integrar, brindar, intercambiar... comunicar. Creemos en el software libre, que puedes copiar, distribuir, modificar y usar a tu antojo, sin limitaciones. Creemos en la capacidad de autoorganización de los individuos que persiguen objetivos claros y justos". En 1998, con unos amigos, Galano fundó el primer grupo de usuarios de GNU/Linux en Santiago de Cuba. Ahora, desde España, lleva el proyecto Linux Sin Fronteras, que quiere acercar el "software" libre a los países pobres.

Linus Torvalds, iniciador del fenómeno Linux, y Richard Stallman, fundador de GNU y la Free Software Foundation, son los gurús de este movimiento, surgido de una necesidad práctico-ética, según escribía el segundo en 1984: "No quiero seguir usando ordenadores con deshonor. He decidido crear un cuerpo suficiente de programas para que no tenga que volver a usar nunca "software" que no sea libre". Como marca la tradición de la Internet Engineering Task Force: "Sin reyes, sin sacerdotes, sólo un consenso suficiente y código corriendo".

También el diccionario "Jargon File" define la ética hacker como "la creencia en que compartir información es un bien poderoso y positivo. Hay un deber ético entre los hackers de compartir su experiencia, escribiendo código abierto y facilitando el acceso a la información y los recursos computacionales, siempre que sea posible. Grandes redes como la misma Internet pueden funcionar sin control central por este trato, en el que todos confían y que se refuerza con un sentido de comunidad, que podría ser su recurso intangible más valioso".

Comunidad donde, afirma Lluís Mora, "lo que sabes es lo que eres". Pekka Himanen lo confirma en su nuevo libro "The hacker ethic", donde habla de Internet como sistema público de educación y de los hackers como herederos de la ciencia: "La ética científica conlleva un modelo donde las teorías se desarrollan colectivamente y los fallos son percibidos por la potencia crítica de la comunidad. Además, no implica derechos de autor, sólo se pide que se mencionen las fuentes y que las nuevas investigaciones sean publicadas, para beneficio de la comunidad".

Rebeldes con causa

David Casacuberta, profesor de Filosofía y activista por los ciberderechos, comparte esta visión: "El hacker es un "científico informático", de aquí la defensa de la libertad de la información, vital para los científicos, mayoritarios en los primeros tiempos de Internet. Los ciberderechos son también un invento suyo, especialmente después del Hacker Crackdown, que se consideró un ataque directo a la comunidad y de donde nació la Electronic Frontier Foundation". Ésta y más antiguas instituciones, como la Internet Society y Computer Professionals for Social Responsability, que velan por los derechos de los net-ciudadanos, son emanaciones directas de la ética hacker.

Otros teóricos, como el respetado Eric S. Raymond, la definen como una "cultura del conocimiento", una meritocracia basada en la habilidad, en el regalo como forma de ganar reputación, la colaboración frente a la competencia, la diversión como fuelle... que va a cambiar el mundo: "Ningún nodo es indispensable. Otro hará lo que deja uno. Esta ecología tiene una respuesta más rápida a las demandas del mercado y más capacidad de resistir y regenerarse". Para Adriano Galano: "La comunidad del software libre ha creado, en sólo diez años, un poderoso sistema de operación que hace frente a lo que fríos laboratorios de I+D han ocultado durante años".

Aunque no forma parte de la "ética" estrica, muchos hackers coinciden en sus ideas sociales alternativas. Para Raúl Sánchez, del colectivo TrabajoZero, "en ellos tenemos el paradigma de una fuerza de trabajo indistinguible de una subjetividad singular, de una constelación ética, de una leyenda siempre abierta a la innovación y de una capacidad de tejer comunidades, que afirman su independencia y reproducen su potencia creativa y liberadora. No hace falta escarbar mucho para ver la politicidad intrínseca que presentan. Estamos ante un sujeto que se forma independiente y clandestinamente con respecto al sistema de producción y reproducción de la fuerza de trabajo capitalista".

Lo reconoce Jesús Cea: "Cierto espíritu de rebeldía, en general, sí lo hay. Un hacker es un curioso, alguien que hace algo teóricamente imposible, que piensa distinto". Y dice Galano: "El hacker es potencialmente un hacktivista, ya que la conciencia es parte de él". Virus contra Telefónica, contra las armas nucleares, contra ETA. Chistes contra Microsoft. Campañas contra leyes. Ir contra el sistema es un clásico de la red, que en los 90 se bautizó como "hacktivismo", de la mano del grupo Cult of the Dead Cow, la European Counter Network o los luchadores por la causa zapatista. El veterano odio tecnológico se llama ahora "desobediencia cibercivil" y se tolera a regañadientes, si no conlleva aburrimiento o destrucción.

Italia es el país europeo donde más fuerza tiene el 'hacktivismo'. Su arma secreta se llama "netstrike": poner de acuerdo a mucha gente para que acceda repetidamente a una web, hasta colapsarla. Los italianos la describen como "acción directa, un acto político de masas, una protesta legítima, el derecho de las personas a expresarse contra la pena de muerte, contra los políticos o contra la censura". Junto a la 'netstrike', se usan otras fórmulas como la creación de webs y comunicados, de virus mediáticos o de arte disidente.

De todas formas, la protesta más habitual sigue siendo el asalto y cambio de páginas web, muy devaluada como práctica preferida de los "script-kiddies", pero aún usada por grupos diversos, para la crítica política. En la pasada DefCon, se presentó el proyecto "Hacktivismo", orientado a ir más allá del cambio de páginas y concentrar esfuerzos en la construcción de un sistema anónimo y privado de difusión de información sobre derechos humanos. Cult of the Dead Cow trabaja actualmente en una aplicación, Peekabooty, que sería la base de esta red.

En España, los casos de hacktivismo son aislados, aunque persiste la conciencia de la fuerza que da la tecnología: "Poder para organizar movimientos ciudadanos nacionales e internacionales. Poder para controlar a tus 'representantes' en el Parlamento. Poder para ir directamente a las fuentes de información. Poder para difundir tu verdad al mundo, sin necesidad de pedir permiso. Cada vez que un hacker reivindica su entrada en un ordenador, debe ser para atraer la atención sobre las cuestiones importantes", escribe Paseante en el artículo "La importancia de llamarse hacker".

En blanco y negro

Este pensar crítico no se lleva bien con el poder establecido, que iguala hacker a criminal informático. Para alejar tal visión, en el resbaladizo campo de la seguridad, se inventó el término "hacker ético/blanco". Las empresas lo usan publicitariamente, refiriéndose a sus expertos en tests de penetración (simulación de la entrada de un hacker en un sistema). Lluís Mora, uno de ellos, aclara: "No tiene nada que ver con la "ética hacker" sino con la connotación positiva de esta imagen en la sociedad. Más bien, ofrecemos servicios a empresas para los que usamos una mentalidad y unas herramientas hacker".

El auténtico "hacker ético" puede trabajar o no como consultor de seguridad, pero sí sigue los principios enumerados por Jesús Cea: "Avisar a la empresa del fallo, darle un plazo razonable y publicarlo en una lista". También las FAQ del grupo de noticias es.comp.hackers, donde se reúnen los interesados en seguridad, dicen: "Los hackers gozan intentando acceder a otros ordenadores. Cuando más difícil sea, más disfrutan. A menudo, cuando lo consiguen, avisan a la empresa y explican cómo lo hicieron. Así, mejoran el sistema, y tienen un nuevo reto".

Este verano, era noticia un informático de 20 años, Adrien Lamo, que informó a Excite de un grave agujero en su red. Excite escuchó a Lamo y, posiblemente, lo contrató. Pero esta reacción no es normal: "Las empresas tienden a denunciar a quien les avisa y hay gente que se está cansando de tener buen rollo", asegura un anónimo habitante del 'underground'. José de la Peña, director de la revista "Seguridad en Informática y Comunicaciones", confirma que "existe un gran desconocimiento por parte de las empresas, no distinguen un intruso peligroso de un hacker como reto".

Si no se roba ni destruye, la comunidad consiente tácitamente el curiosear en redes. Claudio Hernández, "hardware cracker" y autor de numerosos libros, considera que "piratear sistemas con buenas intenciones, para probar tu astucia o la seguridad, no es un crimen. La gente que elude sus impuestos causa más daños que los hackers". Manuel Medina, director del esCERT, discrepa: "Entrar en un ordenador es violar la propiedad privada, aunque sólo mires. Es como robar, a no ser que se pueda entrar sin forzar nada".

Pero las sentencias judiciales en España no han seguido esta línea: de tres supuestas intrusiones, sólo una mereció castigo, porque se robaron datos. En su defensa del caso !Hispahack, que acabó en absolución, el abogado Carlos Sánchez Almeida apeló a las bondades del "hacking blanco": "Sus descubrimientos son beneficiosos para una mayor seguridad. ¡Cuántos fallos han podido ser reparados gracias a hackers que no buscaban causar daño sino investigar!. Para que pueda ser penado, debe estar orientado a la obtención de secretos, o bien a la causación de daños. El acceso en sí mismo no puede ser considerado a priori como delito, porque no existe un precepto penal que lo castigue".

Hoy, la batalla está en Europa, donde el futuro Tratado de Cibercrimen penaliza la posesión de programas de 'hacking', si no se está autorizado. Ironiza Jesús Cea: "Es una tontería. ¿Y quién certifica que eres un profesional y puedes usarlos? ¿Pedirán exámen? ¿Y el profesional que por la noche usa estas herramientas para hacer hacking?". Cuando se les provoca, los hackers recuerdan que, por suerte, funciona mejor su ética que las leyes: "Yo puedo tirar Internet entera pero, si me la cargo, ¿con qué juego?. Por eso no ha pasado nada catastrófico hasta ahora. Internet es muy frágil, pero a la gente con recursos no le interesa atacarla porque, precisamente, conforma su hábitat: su entorno social, su biblioteca, su fuente de noticias, su trabajo diario...".

- Jesús Cea
  http://www.argo.es/~jcea

- Claudio Hernández
  http://perso.wanadoo.es/snickers/

- Carlos Sánchez Almeida
  http://www.bufetalmeida.com

- !Hispahack
  http://hispahack.ccc.de

- Linux Sin Fronteras
  http://www.universala.org/~sinfronteras

- Lista de correo Hacking
  http://www.argo.es/~jcea/artic/hack-faq.htm

- Canción del Pirata
  http://www.fortunecity.es/ilustrado/infinito/40/textos/pirata.htm

- La Taberna de Van Hackez
  http://www.vanhackez.com/

- Hacker Crackdown.es
  http://www.globaldrome.org/textos/hackercrack/

- esCERT
  http://escert.upc.es

- Computer Professionals for Social Responsability
  http://www.cpsr.org/chapters/spain/

- Electronic Frontier Foundation
  http://www.eff.org

- Internet Society
  http://www.isoc.org

- Internet Engineering Task Force
  http://www.ietf.org

- Jargon File
  http://www.tuxedo.org/jargon

- 2600
  http://www.2600.com

- Phrack
  http://www.phrack.com

- Cult of the Dead Cow
  http://www.cultdeadcow.com

- Netstrike
  http://www.netstrike.it

- Electronic Civil Disobedience
  http://www.thing.net/~rdom/ecd/ecd.html

- Chaos Computer Club
  http://www.ccc.de

- GNU
  http://www.gnu.org

- Free Software Foundation Europe
  http://www.fsfeurope.org/

- Sourceforge
  http://sourceforge.net/

- "A Brief History of Hackerdom"
  http://www.oreilly.com/catalog/opensources/chapter/ch01.html

- "Old hackers, new hackers: what's the difference?"
  http://www.eff.org/pub/Net_culture/Hackers/old_and_new_hackers.article

- "Ambiguous Definitions of Hacker: Conflicting discourses and their impact upon the possibilities of resistance"
  http://www.nd.edu/~akreider/essays/hackers.htm

- "The hacker ethic and the spirit of information age".
  http://www.hackerethic.org

- "Internet&Computer Ethics for Kids"
  http://www.nicekids.net

Grupo 11: Ética aplicada en Internet – Estudio de la ética hacker

Coordinación: Ramon Alcoberro & Enric Faura

http://cibersociedad.rediris.es/congreso