LA VERDADERA MATRIX VI (10/12/03)

Estimados Internautas:

Voy a comenzar esta nueva versión de "La Verdadera Matrix" con tres noticias que afectan al software de código libre y las cuales muchos ya se habrán enterado en su momento.

Creo que no es ocultando estas cosas, como el software libre pueda gozar de mejor prestigio que el software propietario, al contrario, notificar de estos hechos quiere decir que se está alerta ante posibles problemas y que rápidamente son solucionados para evitar mayores perjuicios a los usuarios.

Cada vez se ven más intentos de desprestigiar el software libre, será que hay más interesados ó que los intereses crecen cada vez más, en igual propoción al crecimiento del software libre.

Por eso que cada vez hay que estar más atentos a las distintas amenazas que puedan ir surgiendo. Sin duda la competencia no duerme.

FUENTE: INFOHACKERS.ORG

Han intentado colar una puerta trasera en LINUX

Enviado el Jueves, 6 de Noviembre del 2003 (23:46:29) por polgibot

Acaban de darse a conocer los primeros detalles de una tentantiva de incorporación de una puerta trasera en el nucleo de Linux. Según desvela "Slashdot" acaba de darse a abortarse un peligroso intento de incorporar una puerta trasera al nucleo del sistema operativo libre.

La puerta trasera, incluída en el archivo kernel/exit.c, modificaba el sistema de comprobación y autentificación de usuarios, permitiendo al conocedor del boquete cambiar arbitariamente de usuario y obtener cómodamente privilegios de root.

Los cambios fueron detectados en el "Linux BitKeeper Kernel Repository", y falsamente atribuidos al veterano desarrollador de Linux David Miller (davem).

Según publica el "Linux Kernel Archive", el intento nunca supuso un auténtico riesgo, ya que la modificación maliciosa en el CVS fué rápidamente detectada y eliminada.

Los usuarios del repositorio BKCVS deberán resincronizar sus árboles para eliminar de los mismos el código malicioso.

FUENTE: INFOHACKERS.ORG

¡Las máquinas DEBIAN han sido crakeadas!

Enviado el Sábado, 22 de Noviembre del 2003 (11:55:59) por polgibot

Varias máquinas de la infraestructura Debian han sido 'crackeadas' durante el último día. El archivo *no está* comprometido ya que Auric, la máquina donde se almacenan los paquetes no parece haber sido 'crackeada'. Más información a continuación sobre este desgraciado incidente.

Las siguientes máquinas están bajo sospecha:

· master (Bug Tracking System)

· murphy (Listas de correo)

· gluck (web, cvs)

· klecker (security, non-us, busqueda web, www-master)

Para mayor desgracia, la revisión r2 de Debian Woody ya se había lanzado a los 'mirrors' para hacer el anuncio esta mañana, lo que hace que muchos servidores estén intentando actualizar paquetes clave tales como bsdutils. Pero el archivo *no* está comprometido.

security.debian.org no estará disponible hasta que se hayan verificado los paquetes que contiene.

FUENTE: DIARIO TI.COM

Detectan agujero en Linux

(03/12/2003 11:58): Las principales distribuciones de Linux -Red Hat, Debian y Mandrake- han publicado parches para el sistema operativo.

SANTIAGO: Según Linus Torvalds, el error afecta al kernel de Linux anterior a la versión 2.4.23 y sólo tiene carácter crítico si el sistema ya hubiera sido intervenido por intrusos.

El agujero es similar al usado durante un ataque realizado en noviembre contra los servidores de Debian. En su momento, el ataque fue neutralizado y aislado.

Posteriormente, también durante noviembre, hackers intentaron instalar un troyano en la base de datos usada por la comunidad de desarrolladores de Linux para guardar el código fuente.

En los círculos de especialistas y desarrolladores de Linux, se considera que el ataque fue realizado de manera tan torpe, que sólo motivó risas y burlas.

En esta noticia, que por suerte es muy alentadora, corroboramos una vez más el gran auge del software libre (Linux). Aunque creo que Microsoft debe tener algun as en la manga como para evitar llegar a este extremo. Sería asumir una dorrota.

FUENTE: HISPMP3.COM

Venderá Microsoft productos para Linux ?.

Machine, 09/12/2003 (08:13).

La consultora estadounidense Meta Group pronostica que el año próximo Microsoft se verá obligada a comenzar a desarrollar software para la plataforma rival Linux.

Según informa "DiarioTi" a mediano plazo Microsoft se verá obligada a desarrollar software para el segmento servidores de la plataforma Linux, con la intención de poder mantenerse vigente cuando el crecimiento de Linux verdaderamente despegue.

Meta Group prevé que para el año próximo Microsoft introducirá software diseñado para Linux, en los segmentos de servicios web y otras aplicaciones para servidores. Según la consultora, Linux será empleado en prácticamente la mitad de todos los nuevos servidores a partir de 2007.

Según ha señalado Meta Group: "Estimamos que para fines del año próximo Microsoft comenzará a trasladar parte de su funcionalidad al entorno Linux; entre otros, sus componentes de la plataforma .NET. Luego incorporará gradualmente los principales productos de back office de Microsoft, como por ejemplo SQL Server, IIS (Internet Information Server y Exchange Server".

Interrogado al respecto Peter Houston, director de la División Servidores de Microsoft, señaló que desconocía que hasta la fecha se esté llevando a cabo alguna labor destinada a migrar algún producto a Linux.

La noticia que faltaba para cerrar un año redondo en cuanto a los problemas con Windows. Espero que sea la última mala del año, aunque en las fiestas siempre los hackers hacen de las suyas, y sin duda vayan a dar algún último golpe de fin de año.

FUENTE: HISPASEC.COM

Algunos problemas de Windows, sin posible solución?.

Una aplicación que se ejecuta en Windows básicamente lo que hace es procesar los mensajes que va recibiendo. Cualquier programa tiene la capacidad de enviar mensajes a otros programas y no existe ningún sistema de autenticación, lo que abre la posibilidad a un nuevo mundo de vulnerabilidades de seguridad.

"Exploiting design flaws in the Win32 API for privilege escalation - or Shatter Attacks - How to break Windows" es un artículo que presenta un nuevo método para atacar los sistemas basados en Win32 (y con la posibilidad que otros entornos basados en el proceso de mensajes se ven igualmente afectados). Lo más importante de esta vulnerabilidad es que no tiene una solución fácil. Al menos no mediante la aplicación de un simple parche, ya que se trata de un problema en el propio diseño del entorno.

Es posible que los lectores recuerden que hace unos meses, en pleno proceso antimonopolio, un vicepresidente de Microsoft indicó que no era posible publicar el código fuente de Windows ya que esto pondría al descubierto la existencia de algunos problemas de seguridad, especialmente en la gestión de mensajes por parte del núcleo. De ser identificados estos problemas, argumentaba, se pondría la seguridad nacional (de los EE.UU.) en compromiso.

Si bien las declaraciones de este vicepresidente fueron rápidamente desmentidas, el autor del artículo al que hacemos referencia, empezó a investigar como funciona la gestión de mensajes en los sistemas operativos Windows.

La estructura de un programa Windows se puede simplificar, muy superficialmente, de la siguiente forma: el programa está constantemente recibiendo mensajes que son enviados por el núcleo y los otros programas en ejecución. Su misión consiste en procesar todos aquellos para los que el programador ha incluido alguna acción. Por ejemplo, cada vez que se pulsa una tecla, Windows envía el mensaje WM_KEYDOWN a la aplicación que está en primer plano. Todos los mensajes generados se sitúan en una cola y son procesados de forma secuencial por cada aplicación.

El problema de seguridad se encuentra en el h echo que Windows permite a una aplicación en ejecución enviar un mensaje a cualquier ventana abierta en el mismo ordenador (o escritorio, para ser más exactos), con independencia de si la ventana receptora tiene alguna relación con la aplicación que emite el mensaje o de sí el receptor de mensajes desea recibir los mensajes que le son enviados. Adicionalmente, Windows no facilita a las aplicaciones ningún mecanismo para determinar la autenticación del emisor del mensaje.

Es justamente esta falta de funciones de autenticación la que puede ser aprovechada en este tipo de ataques. Una aplicación maliciosa puede enviar un mensaje a un programa que se está ejecutando con el que puede manipular las ventanas y los procesos del programa receptor del mensaje.

La buena noticia es que este tipo de ataques, hoy por hoy, sólo pueden realizarse en local.

Microsoft parece estar preparando el terreno para su nuevo sistema Longhorn, el cual ya he comentado en versiones anteriores y el cual pretende unifcar el software y el hardware con la excusa de obtener un sistema más seguro, pero que lo que en realidad hace es cohartar la libertad de los usuarios y su privaciad.

FUENTE: HISPAMP3.COM

El SP2 de XP ligará software con hardware

Juggler, 04/11/2003 (12:27).

Microsoft ha anunciado que el Service Pack 2 para Windows XP incorporará una novedosa característica de seguridad ligada a una tecnología de protección asociada al hardware.

La novedosa tecnología, que ha sido bautizada como NX, ha sido presentada por Microsoft como un sistema de seguridad asociado al hardware y que soportarán tanto el AMD K8 como el Intel Itanium, esperándose que los futuros procesadores tanto de 32 y 64 bits sean compatibles con el mismo.

Según Microsoft, NX dotará a Windows XP de un mejorado sistema de seguridad, que ligará parte de la seguridad de su sistema operativo al hardware, dotando a este de zonas de seguridad claramente diferenciadas.

Básicamente NX permitirá al sistema operativo separar código de programa con los datos de los mismos, estableciendo una clara separación desde el hardware que pretende en lo posible impedir los cada día más frecuentes problemas de seguridad y virus de Windows.

¿ Los primeros pasos en pro de DRM ?...

Hay algo que no me cierra, y es con respecto al nuevo sistema operativo de Microsoft, Longhorn. Desde el año pasado (2002) se está hablando de este sistema, este año el Sr. Bill Gate ha hablado mucho a la prensa. Se han dado a conocer impresiones de pantalla. Ahora estas noticias que ya se están vendiendo en asia copias piratas, cuando en realidad está anunciado para el 2005 ó 2006.

Creo que es simplemente una estrategia de marketing, crear polémica y espectativa en el público para que cuando salga a la venta todos se enloquescan por comprarlo.

Estas dos noticias que siguen a continuación, en particular las veo como una forma de que penetre el mercado, ya que por ejemplo China ya dijo que no quiere saber nada con Microsoft y ese es el mercado más codiciado.

Si analizamos la posible forma en que adquirieron el producto vemos que hay algo raro, se pudo haber evitado si se hubiese querido. Parece que mordieron el anzuelo.

FUENTE: CNNESPANOL.COM

Piratas informáticos asiáticos venden el próximo Windows de Microsoft

2 de diciembre, 2003 JOHOR BAHRU, Malasia (Reuters) -- Piratas informáticos de Malasia están vendiendo la próxima versión del sistema operativo Windows de Microsoft años antes de que salga a la venta.

Para enfatizar aún más la relevante escalada de problemas con los derechos de autor de compañías de Estados Unidos en Asia, los CDs que contienen el programa de Microsoft con el código "Longhorn" están a la venta por seis ringgit (1,58 dólares) en el sur de Malasia.

La actual versión de Windows XP de Microsoft se vende por un cantidad superior a los 100 dólares en Estados Unidos.

El software es una versión anticipada de "Longhorn", mostrado y distribuido en una conferencia para programadores de Microsoft en Los Angeles en octubre, dijo el abogado de Microsoft, Jonathan Selvasegaram.

"No es un producto preparado", dijo desde Malasia. "Incluso si funciona por un tiempo, creo que es muy arriesgado" instalarlo en una computadora en casa, añadió.

El presidente de Microsoft, Bill Gates, dijo que Longhorn, que no saldría a la venta antes de 2005, ocupará un lugar prioritario como el mayor programa de Microsoft lanzado esta década.

El programa está a la venta en el mayor centro comercial de Johor Bahru, la ciudad malasia fronteriza con Singapur, junto a miles de programas pirateados, CDs y DVDs.

"Longhorn" promete nuevos métodos de guardar archivos, mejores vínculos con Internet, una mayor seguridad y menos reinicios de sistema, ha declarado Microsoft.

FUENTE: IBLNEWS.COM

Microsoft colabora con Malasia para eliminar las copias piratas de 'Longhorn'

Miércoles, 3 diciembre 2003

Microsoft está colaborando de forma muy estrecha con el Gobierno malayo después de comprobar que en ese país están a la venta copias piratas de su próximo sistema operativo, que responde al nombre clave de 'Longhorn', aun cuando todavía faltan años para que salga al mercado su versión definitiva.

IBLNEWS, EUROPA PRESS A principios de esta semana se supo que el nuevo sistema operativo, diseñado para sustituir al 'Windows XP', se vende en Malasia por menos de dos dólares, aunque la compañía informática precisó que se trata de una versión incompleta del programa, cuya distribución está prevista para 2006.

"Microsoft está preocupada por las copias piratas de 'Longhorn' que se están comercializando en el país", declaró la filial malaya del gigante de Redmon a través de un comunicado.

Según la compañía, "la versión disponible hasta la fecha es un código para desarrolladores, y no está preparada para su uso en empresarial o por particulares ya que no se trata de un producto completo", por lo que los usuarios que instalen la copia ilegal "lo harán bajo su propia responsabilidad" y "se expondrán a riesgos y vulnerabilidades".

"Estamos trabajando con el Ministerio de Comercio Interior y Consumo para asegurar que nuestros clientes y empresas están protegidas", añadía la nota.

Cómo lo copiaron

Una portavoz de Microsoft señaló que los piratas pudieron hacerse con este 'software' bien a través de una filtración de parte del código detectada en Internet el año pasado o bien a través el contenido de un cederrón distribuido en una conferencia de desarrolladores profesionales celebrada en Los Angeles (Estados Unidos) el pasado mes de octubre.

Como en otros países asiáticos, en Malasia se encuentran a veces en las calles discos piratas de música y películas de estreno antes incluso de que lleguen a la gran pantalla y a un precio de alrededor de un dólar por copia.

De a poco Microsoft ha tenido que ir cediendo, al ver que pierde mercado. Por eso cada vez a más estados, empresas, particulares, etc, les está abriendo el código. Es mejor eso a que dejen de consumir sus productos y se corte la cadena monopólica por la que tanto lucha.

Además su afán recaudador vuelve a quedar de manifiesto, ya que pretende licenciar la tecnología Clear Type y el sistema de archivos FAT. No importa, tengamos en cuenta que siempre hay alternativas open source.

FUENTE: NOTICIASDOT.COM

Microsoft muestra el código de sus aplicaciones XML

El XML es un lenguaje que permite que distintas aplicaciones compartan información, y puedan comunicarse, por ejemplo, con los sistemas de gestión corporativos. De esa manera, facilita enormemente el intercambio de datos dentro de una compañía.

Microsoft anunció que revelará el código de los desarrollos en XML usados por sus aplicaciones Word, Excel e Infopath, que forman parte de la suite de productividad Office 2003.

Hasta ahora, Microsoft se venía negando a revelar los "esquemas" que usaban sus desarrollos en XML en Office 2003. Sin esa información, los clientes corporativos de Microsoft sólo tenían acceso a aspectos básicos del intercambio de información entre aplicaciones, pero sin poder adaptarlas enteramente a las necesidades de la compañía.

Debido a las protestas de una importante cantidad de clientes corporativos, Microsoft ahora ha decidido abrir el desarrollo de XML de Office. Esta decisión facilitará el trabajo de sus clientes, pero seguramente también provocará la aparición de software de terceras partes, que estará diseñado para interactuar y extender las funciones XML de Office.

Otra de las razones que podría haber impulsado a Microsoft a abrir parte del código de Office 2003 son las presiones que está sufriendo por parte de la Unión Europea (UE). Allí prosigue el ju0icio contra Microsoft por presuntas prácticas monopólicas, que, a diferencia de Estados Unidos, podrían terminar con sanciones para la compañía. De hecho, es sabido que la UE está impulsando fuertemente la adopción de estándares unificados de gestión, y podría haber presionado a Microsoft para que hiciera más abierto su desarrollo de XML.

Nuevas licencias para la tecnología ClearType y otra para el sistema de archivos FAT

Asimismo Microsoft ha anunciado la disponibilidad de dos nuevos programas de licencias: uno para la tecnología ClearType y otra para el sistema de archivos FAT.

La tecnología ClearType mejora la lectura de textos en dispositivos de pantallas de cristal líquido hasta el punto de que las palabras parecen tan claras y nítidas como las que están impresas en un papel. La popularidad de esta tecnología y sus grandes posibilidades de aplicación en una amplia gama de dispositivos digitales propició que muchas empresas le pidieran licencias a Microsoft.

Por su parte, el sistema de archivos FAT es un formato de almacenamiento de archivos muy conocido que se utiliza para intercambios entre ordenadores y dispositivos digitales. A través de la tecnología de sistemas de archivo FAT, los sistemas operativos pueden identificar clusters de almacenamiento que no están siendo utilizados y controlar todas las partes del archivo en todo el almacenamiento. El resultado para las personas que implantan esta tecnología es que realizan una rápida identificación y acceso a cualquier parte de un archivo, a la vez que maximizan el uso del almacenamiento.

Licenciando la documentación, muestras de código y patentes de esta tecnología, Microsoft hace más sencillo para otras compañías sacar partido de las mejoras de compatibilidad en la transferencia de archivos y les facilita crear implementaciones compatibles y eficaces del sistema de archivos FAT dentro de sus ofertas comerciales. Esta política también amplía las condiciones de acceso de la comunidad académica a su propiedad intelectual bajo condiciones de exención de royalties para usos no comerciales de la misma.

El tema de los implantes de chip no es nuevo, pero cada vez se hace más mencionado, hasta que llegará el día que se materialice y pasemos a ser androides o las marionetas de Bill Gate.

Suena aterrador, y es por eso que estamos en esta lucha. Informando, formando conciencia, mostrando la verdad de las cosas, es como se pueden evitar. Es lo que trato de hacer desde "La Verdadera Matrix".

FUENTE: DIARIORED.COM

Chips subcutáneos:

¿una revolucionaria forma de pago, o la materialización del "Gran Hermano"?:

Una empresa de Florida (Estados Unidos) ha anunciado planes para desarrollar un sistema de pago que funcionaría mediante la lectura de chips implantados bajo la piel. El proyecto, que parece más sacado de una película de ciencia ficción que de la realidad, ya ha provocado polémica.

Applied Digital Solutions ha presentado el proyecto VeriChip, con el que pretende substituir los medios de pago tradicionales como el efectivo o la tarjeta de crédito, por un medio revolucionario: un microchip implantado bajo la piel (subcutáneo) que sería leído de una forma especial, y que contendría información personal y los mismos datos que tiene cualquier otra tarjeta de crédito.

Aunque se pone especial énfasis en su uso como medio de pago, el VeriChip puede contener -en principio- cualquier clase de información, como por ejemplo el historial médico del usuario.

En la página web del proyecto podemos ver como funciona: el chip, implantado justo por debajo de la piel, se encuentra "dormido" hasta que es "despertado" por el lector, que funciona emitiendo ondas de radio a una frecuencia muy baja, a las que el chip reacciona (identificación por radiofrecuencia, RFID).

Pero esto que nos puede parecer muy práctico lleva aparejado un grave problema: la posibilidad de una constante identificación y, por lo tanto, monitorización también constante de nuestras actividades. ¿Han visto el film "Minority Report", de Steven Spielberg con Tom Cruise como protagonista? En la película se nos muestra una sociedad futura, con lectores de la retina humana instalados en las calles que identifican constantemente a los transeúntes para ofrecerles publicidad a su medida. ¿Podríamos vernos así en un futuro gracias a los chips subcutáneos? ¿Y si la identificación constante nos lleva a un estricto control, entrando de lleno en el campo de una dictadura?

Todo esto y mucho más es lo que se preguntan los internautas preocupados con el tema.

La importancia que a tomado la red, que ahora hasta la ONU pretende tomar control de ella. Que pretenden, implantar una dictadura global?

FUENTE: NOTICIASDOT.COM

Estados Unidos no quiere que la ONU controle Internet

Estados Unidos manifiesta su oposición a la creación de una agencia de Naciones Unidas que controle Internet.

Agencias -Estados Unidos espera poder evitar en la próxima cumbre mundial sobre la sociedad de la información, que tendrá lugar en Ginebra (Suiza), la creación de una agencia de Naciones Unidas que controle internet, argumentando que un organismo de ese tipo impediría la libertad de expresión en la red de redes, según explicaron fuentes oficiales norteamericanas.

Esta cumbre mundial sobre la sociedad de la información (SMSI, por sus siglas en inglés) reunirá a 62 jefes de Estado y de Gobierno entre el 10 y el 12 de diciembre en Ginebra.

Estados Unidos tiene previsto no apoyar la proposición senegalesa de un fondo de solidaridad para financiar proyectos tecnológicos en los países en vías de desarrollo, según precisó David Gross, coordinador del Departamento de Estado para las comunicaciones internacionales y la política de información.

De todas formas ahora hay una alternativa a la internet, y es FREENET, una red totalmente anónima. Y supongo seguirán surgiendo subredes, formando nuevas comunidades de internautas que pretenden conservar su privacidad y libertad.

FUENTE: http://www.lasindias.com/articulos_2/tecnologia_noviembre_2.html

Freenet: la nueva frontera

Por Javier Lorente

Tal vez la expresión "protocolo de enrutamiento" o las siglas NGR no le digan nada. Pero la presentación de NGR, el protocolo de enrutamiento para Freenet supone un importante paso en el desarrollo de redes que garanticen la completa privacidad, independencia y seguridad del individuo. Desde sus inicios en 1999, Freenet, el proyecto de una red libre distribuida, se ha convertido en una de las batallas claves para garantizar las libertades civiles en el nuevo siglo.

La implantación de Internet en todo el mundo despertó el interés de muchas personas que veían en la red una nueva forma de comunicación en la que podían difundir contenidos que apenas eran tenidos en cuenta por los medios habituales. Durante los dos o tres primeros años, se convirtió en un extenso campo de pruebas al que cualquier persona podía acceder: tan sólo se necesitaba un ordenador y una conexión. Sin embargo, la afluencia de público cada vez mayor llamó la atención de diversos grupos empresariales que comenzaron a comprar a golpe de talonario sus nuevos derechos sobre la red y que alteraron las relaciones paritarias que se habían establecido. La situación había cambiado: la información comenzaba a ser controlada de nuevo por los poderosos consorcios de comunicación.

En el principio fue Napster

En mayo de 1999 Shawn Fanning y Sean Parker revolucionaron la Red al poner en marcha su proyecto Napster Inc., un servicio de intercambio de ficheros desarrollado a partir de los modelos de programas de comunicación IRC y de los buscadores de contenidos que en aquel momento comenzaban a aparecer. Sin embargo, a diferencia de ellos, se basaba en la comunicación directa entre ordenadores: los usuarios almacenaban y descargaban los contenidos que les interesaban en sus propios discos duros, sin recurrir a ningún servidor. La nueva arquitectura, denominada peer to peer (P2P), fue aceptada de inmediato y propició la implantación de un formato de codificación para archivos musicales, el MP3, que se ha convertido en la actualidad en uno de los estándares más empleados.

Lo que después ocurrió es de sobra conocido: el uso masivo de este servicio llevó a las compañías discográficas a temer por su futuro y, en lugar de adaptarse a la nueva situación, tal como han hecho muchos músicos, comenzaron a emprender acciones legales ese mismo año a través de la RIAA, que culminaron con el juicio y la posterior sentencia que condenaba a Napster al cierre. El caso habría quedado en un simple pleito entre compañías si los representantes de Metallica no hubiesen entregado en los juzgados un listado con las IP y los nombres de 335.000 usuarios que habían intercambiado archivos musicales del grupo. A partir de ese momento, la responsabilidad penal recaía tanto en los suministradores del servicio como en sus clientes.

La revolución de las redes P2P

Aunque la tecnología P2P se consideró en un principio válida sólo para redes de trabajo pequeñas que funcionasen a modo de intranets, el éxito de Napster, Gnutella, Kazaa o Emule demuestra todo lo contrario. Sin embargo, las implicaciones de este nuevo modo de conexión son mucho más importantes de lo que pudiera parecer a primera vista, ya que el almacenamiento de los contenidos no requiere un servidor al uso, sino simplemente una carpeta situada en el disco duro de un ordenador personal a la que pueda accederse desde cualquier punto de la Red. De este modo, cualquier usuario gestiona directamente la información que desea publicar, sin depender de ninguna empresa de servicios y, lo que es mejor, sin correr el riesgo de que alguien desee bloquear el acceso al servidor donde los aloja por considerarlos molestos, inadecuados o peligrosos. El P2P, por su propia naturaleza, subvierte las restricciones inherentes a Internet.

El nacimiento de Freenet

En 1999, el mismo año en que aparecía Napster como red de intercambio libre, un estudiante de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Edimburgo, Ian Clarke, presentaba su trabajo de final de carrera, A distributed decentralised information storage and retrieval system (Un sistema de almacenamiento y recuperación de información distribuido y descentralizado), en el que describía un algoritmo que, ejecutado en un grupo de ordenadores interconectados, permite gestionar grandes cantidades de información sin que fuese necesario un control centralizado y garantiza un uso anónimo de los ficheros, así como su duplicación dinámica y la transferencia de su localización según la demanda. No era más que un prototipo: las simulaciones realizadas hasta el momento, escritas en Java, habían dado buenos resultados, pero no podía asegurarse su eficacia en un entorno tan extenso y complejo como la World Wide Web.

Tras licenciarse, Clarke comenzó a simultanear su trabajo en la empresa británica Logica UK con el desarrollo de su proyecto. En poco más de un año, las simulaciones sobrepasaban los 200.000 nodos y la construcción de la red estaba cada vez más cerca. El interés por los resultados crecía: desde el año 2000, las reuniones anuales del Intel Developer Forum han seguido los progresos de Clarke, quien finalmente, junto con su equipo, ha conseguido desarrollar un protocolo de enrutamiento (NGR) que asegura la plena estabilidad de la red.

La arquitectura de Freenet

El sistema se basa en el modelo descentralizado de Gnutella, en el que cada ordenador se convierte en un nodo que funciona como cliente y servidor al mismo tiempo. De este modo, mientras el usuario busca información en otros nodos, el suyo ofrece la que desea compartir. Este modelo de organización permite una mayor capacidad de cómputo, ya que se basa en un procesamiento en paralelo, una propagación por inundación, una búsqueda mucho más rápida en comparación con los motores actuales que, con excepción de Google, no suelen rebasar un 20% del total de sitios existentes y, en la medida en que no depende de ningún nodo principal, una gran estabilidad ante posibles caídas del sistema.

Sin embargo, Gnutella cuenta también con dos inconvenientes: en la medida en que la información fluye libremente por esa red, el mantenimiento de los índices de contenidos exige un esfuerzo mayor y aumenta el peligro de que los archivos sean interceptados y se localice el ordenador de donde proceden. Freenet solventa esos dos problemas mediante la incorporación de un robusto sistema de encriptación que garantiza el anonimato completoasí como de un algoritmo de búsqueda que determina los archivos más visitados y genera rutas adicionales para evitar una sobrecarga de la red. Para ello, se ha dispuesto que cada nodo ofrezca el índice de contenidos más completo posible, tanto de los archivos públicos que almacena en su disco duro como de los que pueden encontrarse en los demás ordenadores conectados.

Por otra parte, el mecanismo de duplicación de ficheros está diseñado de manera que, ante una avería o un ataque a un nodo, la información que se halle contenida en éste sea copiada en otros nodos para evitar su desaparición, lo cual hace de Freenet un medio completamente autónomo que se adapta y se organiza sin cesar según el número de ordenadores conectados en ese preciso momento.

Las implicaciones políticas de Freenet

A diferencia de muchas otras tecnologías, Freenet fue desarrollado bajo una premisa política concreta: el derecho de toda persona a compartir información sin correr ningún riesgo. A finales de los años noventa se vislumbraron algunos de los riesgos que planteaba Internet. El desmantelamiento de algunos sitios que distribuían contenidos perseguidos por las leyes internacionales o que servían de tapadera o enlace de diversas organizaciones criminales hizo que las autoridades de diversos países comenzaran a pensar en la posibilidad de crear leyes que castigaran los usos y comunicaciones electrónicas que entrañasen algún peligro para sus ciudadanos o para la estabilidad de sus propias instituciones. Algunos, como Arabia Saudí, la República Popular China o España, bloquearon en mayor o menor medida los servidores DNS que podían albergar informaciones ilegales. Otros, como Estados Unidos, desarrollaron sofisticados sistemas de control como Echelon o Carnivore con los que se podía espiar y registrar cualquier mensaje transmitido a través de medios electrónicos.

Pese a que estas medidas han dado ciertos resultados, éstos han sido bastante discretos, pues las redes criminales o terroristas son mucho más difusas y complejas de lo que se preveía, y aunque los atentados del 11 de septiembre de 2001 han puesto en evidencia que el espionaje e inteligencia de señales, sigint, por muy competente que sea, no asegura la desarticulación de estos grupos, todavía se considera que el uso de la criptografía en la Red supone un peligro muy grave para todos los ciudadanos.

La garantía de privacidad en todas las comunicaciones es una de las reivindicaciones más importantes de nuestra época, ya que asegura no sólo la libertad de pensamiento, sino también la de acción. Freenet, al no depender de ningún servidor, se ha convertido en una de las armas más poderosas para que los disidentes de países que restringen el acceso a Internet mediante el bloqueo de DNS puedan comunicarse y denunciar los atropellos contra las libertades que sufren continuamente, ya que no sólo les permite conectarse de manera anónima, sino que les garantiza la permanencia de sus contenidos a pesar de la desconexión o destrucción de los nodos que empleasen.

Un reflejo de nuestro mundo, no una utopía

El uso favorable o no de Freenet no es una cuestión que preocupe demasiado a Clarke y a sus compañeros de proyecto. Cualquier tecnología, por sí misma, no es buena ni mala y sus efectos dependen obviamente del uso que se le dé. Las redes de comunicaciones son una parte de nuestra organización social y, en consecuencia, su mayor o menor bondad dependerá de cómo se organice la sociedad. No obstante, Freenet, por sus propias características, ofrece una cierta resistencia a ser manipulada: la dispersión de los contenidos y la encriptación no sólo evitan la interceptación y destrucción de los mensajes, sino también la apropiación de la red por parte de colectivos, empresas o instituciones, ya que no hay manera de asegurar los derechos por los contenidos ni tampoco la identidad de los usuarios. Su uso comercial es inviable y no podrá ser colonizada como Internet.

Esta vocación acomercial no la convierte en un medio marginal. Aunque por el momento la mayor parte de los contenidos que se encuentran en Freenet podrían tildarse de alternativos o minoritarios, no se trata de una red underground. La programación en Java garantiza que los programas de transmisión de comunicaciones puedan funcionar en cualquier plataforma, sea Windows, Linux, Unix o Apple, y su instalación no requiere ningún tipo de conocimiento informático especializado. Tan sólo basta con descargar el archivo adecuado a cada sistema, descomprimirlo y comenzar a navegar (aunque no es recomendable el uso de Internet Explorer, por sus fallos de seguridad). De este modo, cualquiera puede gestionar la información de la manera que crea más conveniente. El objetivo de Clarke y sus compañeros es volver, en cierto modo, a los orígenes de Internet y reinventar las relaciones entre usuarios para alcanzar la realización plena de la nueva sociedad de la información. Pocas veces en la historia hemos tenido la oportunidad de dar marcha atrás y enmendar nuestros pasos. Ahora podemos hacerlo.

Está mal que lo diga pero, en "La Verdadera Matrix I" el último artículo, el de Jean Dixon, lo dice bien claro (recomiendo su lectura)… y esta noticia no hace más que corroborar esa información. Cuesta creerlo pero es VERDAD. No hay peor ciego que el que no quier ver.

FUENTE: HISPASEC.COM

Fallos en un software de voto electrónico ponen en duda las victorias republicanas en EEUU

La Electronic Frontier Foundation y la mayoría de universidades de los Estados Unidos se han unido para denunciar las prácticas fraudulentas de una importante empresa de votación electrónica, Diebold Elections Systems. Un hacker entró en el sistema de la compañía y copió 15.000 documentos confidenciales, que puso a disposición del público. En ellos se demuestra que el "software" de Diebold, usado en las elecciones que dieron la victoria a Bush y Schwazeneger, tenía agujeros que permitían cambiar los votos.

En marzo, alguien se introdujo en los servidores de la compañía norteamericana de sistemas de votación electrónica, Diebold Elections Systems, y copió 1,8 gigabits de datos, la mayoría correo electrónico desde 1999 y documentos internos. Diebold suministra máquinas de votación electrónica a 37 estados y tiene repartidas más de 50.000 terminales por el país. Los documentos demostraban que la empresa conocía los graves errores de seguridad en sus programas, que podían provocar fraude, como la posibilidad de cambiar votos sin dejar rastro o la instalación de programas no certificados por las autoridades electorales.

En agosto, el hacker envió los documentos a diversos activistas, que los publicaron en sus "weblogs". Pronto, otras webs replicaron el contenido, la mayoría en universidades estadounidenses, desde Hardvard hasta el Bronx, pero también Australia, Canadá o Italia. Diebold les mandó avisos legales para que retirasen los documentos, amparándose en la ley de derechos de autor Digital Millenium Copyright Act (DMCA).

Capitaneados por el grupo de estudiantes "Why War?", del Swarthmore College de Pennsylvania, los activistas iniciaron entonces una campaña de desobediencia civil electrónica, negándose a retirar el material.

Según los estudiantes, "no podemos permitir la supresión de evidencias que prueban que una máquina Diebold registró 16.022 votos negativos para Al Gore en Florida, durante las elecciones presidenciales del 2000. Tampoco que el CEO de esta compañía ha dado 9.965 dólares a Bush y el partido republicano desde el 2001. Ni que Diebold se esté preparando para contar los votos de las presidenciales del próximo año. Están usando la ley del "copyright" para suprimir una información que necesita ser hecha pública".

Diebold envió también un aviso legal al proveedor Online Policy Group, para que uno de sus usuarios, el San Francisco Indymedia, retirase enlaces hacia los documentos. Este ISP, sin ánimo de lucro, está ligado a la Electronic Frontier Foundation (EFF), que salió en su defensa. La EFF y la Stanford Law School han pedido una orden judicial para que Diebold deje de enviar amenazas. Según los abogados de la EFF, "las exigencias abusivas del "copyright" no pueden silenciar el debate público sobre la seguridad del voto electrónico. Estos documentos son del dominio público, por su importancia en este debate. Además, defendemos el derecho de los usuarios a enlazar con información que es crítica". Diebold ha hecho pocas declaraciones sobre el tema: que sus amenazas no significan que los documentos sean auténticos y que algunos pueden haber sido alterados, después de robados. Un ex-trabajador de la compañía ha desvelado, por su parte, que Diebold instaló, el año pasado, tres programas no certificados en 22.000 máquinas, vendidas al estado de Georgia por 56 millones.

Las consecuencias no se han hecho esperar: Marc Carrel, de la secretaría de estado de California, ha anunciado que retrasará la certificación de los productos de Diebold para las elecciones de 2004, hasta que no se haga una investigación. Según Carrel, Diebold instaló programas sin certificar en 4.000 máquinas de voto electrónico del condado de Alameda, usadas en las elecciones que dieron la victoria a Arnold Schwazeneger. Otro condado californiano, San Diego, se encuentra en estos momentos negociando la compra de 10.000 máquinas Diebold.

En Maryland, los demócratas han pedido una auditoría independiente a las máquinas Diebold que su estado acaba de comprar. Los demócratas no se fían de los informes de la auditora Science Application International Corp (SAIC): en julio, un estudio de dos universidades avisaba a las autoridades de Maryland de serias debilidades en el sistema de voto de Diebold. Se pidieron explicaciones a SAIC, quien replicó que los científicos no entendían el sistema. En Europa, se ha creado una plataforma para exigir la fiabilidad del voto electrónico.

Me hicieron llegar vía e-mail esta información que aunque no tenga que ver con la parte de tecnología, software, ó el tipo de noticias que normamente publico, merece difundirse.

Y como se lo dije a mi amigo Juan, quien me envió la noticia, se los digo a todos:

"No se puede luchar por la libertad, la verdad y la privacidad en la red, y dar la espalda a una realidad tan injusta como esta. Creo que todo va de la mano, pero primero está el ser humano, luego el ciberespacio, la tecnología y lo demás, esto lo tengo bien claro".

Entre todos podemos apoyar a los Indios Mapuches y evitar esta injusticia.

FUENTE: http://puntodoc.com/informes/informes.php?cod=534

La resistencia

La marca de ropa italiana Benetton se hizo famosa en el mundo entero por sus transgresores avisos publicitarios. Muchos de esos avisos, tienen un fuerte mensaje humanitario. Pero detrás del impacto publicitario de Benetton están sus negocios millonarios. Puntodoc fue hasta una de las estancias de la familia Benetton en la Patagonia; la estancia "Leleque" de casi un millón de hectáreas.

Leleque es un pequeño caserío a medio camino entre El Maitén y Esquel, cerca de la Ruta 40. Hay una estación de tren por donde el tren ya no pasa... Todo el recorrido de la vía y el pueblo de Leleque, están dentro de la estancia. Su dueña es la Compañía de Tierras del Sud Argentino, que hoy pertenece al grupo italiano Benetton. A simple vista, Leleque parece un pueblo fantasma pero aún vive gente. Candelaria Curiñanco es la habitante más antigua del lugar. Pero hoy, para buscar agua del arroyo, tiene que saltar el alambrado de la estancia.

Una lucha plagada de desventahas

Durante los últimos tres siglos, la historia de la comunidad mapuche está signada por injusticias y engaños. "Nuestra gente estuvo mucho tiempo sometida, muy sumisa; acá hubieron terratenientes que llegaban a tener hasta calabozos en sus estancias. Y no estoy hablando de algo de hace 100 años atrás, estoy hablando de hace dos décadas", cuenta Mauro Millán artesano mapuche y activo defensor de su comunidad.

Los mapuches nunca tuvieron en cuenta los títulos de propiedad. Estos fueron impuestos por el hombre blanco a punta de fusil y los modificó cuando quiso y a su antojo.

La historia de Abelardo Sepúlveda muestra que la Conquista del Desierto no ha terminado. Sólo que en la actualidad, detrás del fusil, un juez certifica la legalidad de la usurpación.

Abelardo es mapuche y nos cuenta que de las 625 hectáreas que le pertenecen a su abuelo, hoy sólo le quedan 300. Pero hace un tiempo, el intendente de la zona le informó que en realidad, sólo le pertenecen 40 hectáreas. Según Abelardo, "el hermano del intendente nos quiere usurpar el campo. Dicen que tienen papeles, pero son papeles truchos que han deformado en Catastros".

La tierra que habitan los mapuches es codiciada por sus riquezas. Pero en estos parajes ya nadie acepta cambiar oro por espejitos. Por eso los desalojos también son una constante en la vida de los mapuches.

Doña Carmen Jones, es nieta de Julio Marinao, quien a principios del siglo pasado, vivía en un campo denominado 'Lote 134' de la comunidad de Vuelta del Río. En este campo, cuando Doña Carmen tenía 11 años, vivió su primer desalojo.

Cuando se producen los desalojos, los mapuches no tienen donde ir.

Rogelio Fermín, el hijo de Doña Carmen, reconstruyó la historia de su madre y para eso, volvió con Puntodoc a los lugares donde su familia sobrevivió a los desalojos. En un cerro, perdido en la cordillera, Doña Carmen encontró una cueva donde se protegió de la policía.

Los relatos de desalojos violentos parecen pertenecer al pasado, pero estas situaciones siguen ocurriendo en la actualidad.

El 15 de marzo pasado un funcionario judicial y 20 policías se presentaron en la casa de Doña Cármen. Le dijeron unas pocas palabras conocidas: 'venimos a desalojarlos'. Y cuando Rogelio, el hijo de Fermín, pidió que le muestren la orden de desalojo, la respuesta fue demoler su casa y arriar a sus animales.

Doña Segunda es una mapuche que vive en la Comunidad Vuelta del Río y el día del desalojo, fue a la casa de los Fermín para hacer resistencia.

Los mapuches de la comunidad, a pié o a caballo, fueron a la casa de Fermín y como pudieron, defendieron su tierra. Saben que gente poderosa quiere quedarse con ella.

Finalmente, ese día consiguieron parar el desalojo.

Pero la semana pasada, la justicia provincial ratificó la orden de desalojo. Para Doña Cármen y Rogelio eso significa que tendrán que volver a los cerros.

Pero los cerros tienen un dueño poderoso y los mapuches saben que no serán bien recibidos. "Es todo de Benetton. Los cerros también pertenecen a Benetton. Estamos rodeados por alambre de Benetton", cuenta Rogelio Fermín.

La Compañía

El grupo Benneton, con 6.000 tiendas de ropa en 120 países, factura más de dos mil millones de dólares al año. Pero la ropa no es todo... También diversificó sus inversiones en la industria alimentaria, autopistas, telecomunicaciones y campos. Asi fue como Benetton llegó a la Patagonia.

Hoy, tiene 280 mil cabezas de ganado ovino. En estas estancias del sur del país, obtiene el 20% de la lana que requiere su empresa. Y además, obtiene importantes ventajas con la mano de obra barata.

Hace ya muchos años, las tierras patagónicas eran habitadas por mapuches, pero en 1896 el Gobierno Nacional, presidido por José Evaristo Uriburu, "concesionó tierras para colonizar" a la Compañía de Tierras Sud Argentina. La conseción fue realizada sin tener en cuenta a los mapuches.

En el año 1991, por 80 millones de dólares, Benetton se quedó con las 900 mil hectáreas de la Compañía de Tierras Sud Argentina.

Pero esta vez, los mapuches no solo fueron ignorados sino que también fueron denunciados. La compañía italiana Benetton denunció por usurpación a la familia mapuche de Atilio y Rosa Curiñanco.

Hoy, a la espera del juicio oral, Atilio y Rosa están procesados y si se los declara culpables, se transformarán en delincuentes.

En este links, hay más información sobre el caso:

http://old.clarin.com/diario/2003/12/02/s-03401.htm

Será hasta la próxima.

Saludos.

Kbza

Kbza37@yahoo.com