

Remove all errors that are causing your PC to run slow

REMOVE NOW



Blog cien por ciento tecnológico Blog sobre Ciencia y Tecnología. Cultura Geek, Videojuegos, Internet y Webs 2.0, Empresas y noticias de actualidad.

[Autores](#) [Contacto](#) [Nosotros](#)

suscriptores



Recibe noticias en tu email:



Noticias Destacadas



Pinterest es una nueva, prometedora y sencilla red social



Estados Unidos quiere prohibir usar Google Glass al conducir



Xbox One: presentan nueva consola de Microsoft (oficial)



Lo que no se vió del nuevo Opening de los Simpsons



Google Chrome es el tercer navegador más

La 'irrompible' criptografía cuántica hackeada usando láseres

Publicado: October 4th, 2008 | Autor: nekrodomus | 3 Comentarios »

[Tweet](#) { 0 }

[Like](#)

[g+1](#) { 0 }

[Share](#)

[Share](#) { 0 }



Un estudiante de la Universidad Noruega de Ciencia llamado Vadim Makarov ha descubierto una vulnerabilidad en la que anteriormente se pensaba 'irrompible' encriptación cuántica que le ha permitido romper este tipo de encriptación sin ser detectado.

Para lograrlo usó una luz láser de alta intensidad para interceptar el flujo de datos encriptados. Si bien el tipo de cifrado suele variar frecuentemente para [asegurar](#) las transacciones, una vez que logras meterte en el sistema sin ser detectado el que una clave encriptada se rompa solo es cuestión de tiempo. Y esto es lo que

Makarov ha conseguido, "escuchar" las transacciones encriptadas sin ser detectado.

La criptografía cuántica es la criptografía que utiliza principios de la [mecánica cuántica](#) para garantizar la absoluta confidencialidad de la información transmitida. Las actuales técnicas de la criptografía cuántica permiten a dos personas [crear](#), de forma segura, una clave secreta compartida que puede ser usada como llave para cifrar y descifrar mensajes usando métodos de criptografía simétrica.

La criptografía cuántica como [idea](#) se propuso en la década del 70, pero no fue hasta 1984 cuando se publicó el primer protocolo.

Una de las propiedades más importantes de la criptografía cuántica es que si un tercero intenta hacer eavesdropping durante la creación de la clave secreta (por decirlo en terminos coloquiales fisgonear la creación de la clave), el proceso se altera detectándose al intruso antes de que se transmita la información privada. Esto es una consecuencia del principio de incertidumbre de Heisenberg, que nos dice que el proceso de medir en un sistema cuántico perturba dicho sistema.

Este tipo de criptografía se está comenzando a impulsar con el desarrollo de las redes de fibra óptica.

Según Makarov, el secreto está en la forma en que el remitente y el receptor comunican su clave secreta. Y es precisamente aquí donde se puede explotar la vulnerabilidad que han encontrado.

Su equipo ha demostrado que es posible permitir la transmisión de toda la información que va del remitente al receptor sin que se vea afectado el mensaje o la intrusión de un sea detectada. Al obtener la clave de encriptación el intruso es capaz de decodificar la transmisión sin ninguna dificultad y sin que lo detecten.

Fuentes: [tgdaily](#) | [Wikipedia](#)

Saludos desde lo más profundo de los bytes.

- Publicidad -

Posts Relacionados

- Los viejos ordenadores usando Linux, funcionan mejor que los nuevos usando Vista
- OpenIT: adiós al plástico irrompible de los productos
- Usando un iPhone para controlar un coche de RC
- Siente el placer usando Linux

Tags: [hacking](#), [Seguridad Informática](#)

Find us on Facebook

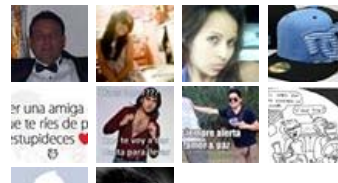


Geekets

[Like](#)
[Like](#)

You like this.

You and 5,673 others like Geekets. 5,673 people like Geekets.



GET YOUR SMOKEY ON

ONLY YOU CAN PREVENT WILDFIRES.

9 out of 10 wildfires are caused by humans.
9 out of 10 wildfires can be prevented.

[LEARN MORE](#)



Google™ Búsqueda personalizada

Tags

Archivo

Comentarios

- Android aplicaciones **Apple** blackberry
- Características de Smartphones Como
- Hacer Cultura Geek curiosidades Cámaras
- de Fotos **descargas gratis** España
- Facebook **Gadgets** Google HTC
- imagen iPad **iphone** iPhone 5 Lanzamientos
- de Smartphones Lanzamientos de Tablets
- Linux **Microsoft** Móviles Nintendo
- nokia noticias Noticias de Apple
- Noticias de Samsung Noticias de Tablets
- novedades Portátiles programas redes
- sociales Rumores de Apple Rumores de
- Smartphones **Samsung** Servicios Sistemas
- Operativos Móviles Software Sony
- videojuegos** Vídeos Windows windows 7



Geekets

[g+](#)

Seguir

+1

+ 305

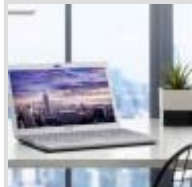
Blogroll

- Como crear una pagina web gratis
- Gigle
- Globbos
- Hoteles Benidorm
- Planeta Red
- Spam Loco

Categorías

- Accesorios Geeks
- Antivirus
- Cámaras Digitales
- Chicas Geek
- Ciencia
- Columnas
- Compra Venta
- Curiosidades Geeks

utilizado del mundo



Sony VAIO S y Sony VAIO Z con nuevo chip Ivy Bridge



Catch y BroadMap son compradas por Apple esta semana

Categoría: Noticias de Actualidad , Tecnología



Autor: **nekrodomus** Hace unos 30 años nací en Sevilla y aunque desde la infancia he estado rodeado de ordenadores no puede decirse que haya estado vinculados a ellos hasta que no empecé a estudiar una carrera superior. Por suerte para el mundo informático mis notas no fueron lo suficientemente buenas como para hacerme médico, por lo que hubo un giro en mis vocaciones y empecé a estudiar el título de Técnico Superior en Informática de Sistemas, después de lo cual pasé a estudiar la carrera de Ingeniería Técnica en Informática de Sistemas. Allí fue donde me peleé, junto con Enrique, con muchas asignaturas difíciles. Tras acabar la carrera, y casi sin darme cuenta, me vi trabajando en una consultora de informática de Madrid. Lugar en donde vivo actualmente y donde desarrollo labores de programador, diseñador gráfico.... Si te preguntas por lo que espero de este proyecto, pues comenzar en algo en lo debería de haberme puesto hace un tiempo. Siempre he estado interesado en los blogs y salvo algunos breves escauceos en este mundo, nunca me puse en serio a escribir, y es algo que quiero cambiar. Saludos, Carlos Jiménez

3 Comentarios

meneame.net says:

October 5, 2008 at 2:22 am

La 'irrompible' criptografía cuántica hackeada usando láseres...

Un estudiante de la Universidad Noruega llamado Vadim Makarov ha descubierto una vulnerabilidad en la que anteriormente se pensaba 'irrompible' encriptación cuántica que le ha permitido romper este tipo de encriptación sin ser detectado. Para lo...

Responder



Carelo says:

October 6, 2008 at 10:48 am

Bueno, esta noticia parece interesante de principio. Pero en el artículo solo explica un poco la criptografía cuántica, historia y principios de manera rápida. Pero resulta que no explica el cómo se hace para romperla, menciona un rayo laser, fibra óptica, pero no menciona cual es el principio con el que pueden medir un rayo de información sin afectarlo.

Responder



nekrodomus says:

October 6, 2008 at 10:56 am

Buenas Carelo, la mecánica cuántica nunca fue mi fuerte en la universidad y tampoco es que se expliquen muy bien en el post que me sirvió de fuente (en ingles)...

Responder

Responder entrada

Nombre (Requerido)

Correo (Requerido)

Página Web o Blog

Suscribirse vía email en esta discusión

Descargas

e-Reader

Editores Digitales

Empresas

Galerías Geeks

Hackers

Hardware

Humor Geek

Impresoras

Internet

Lanzamientos

Listados

Mensajería Instantánea

Motherboards

Móviles y Celulares

Navegadores

(browsers) Web

Notas de Geekets

Noticias de Actualidad

Ordenadores – Pc's

Otras

Películas Online

Phablets

plugins

Portátiles – Laptops

Programación y Código

Programas Gratuitos

publicidad en línea

Recursos

Robotica

Rumores

Sistemas Operativos

Smartphones

Smartwatches

Tablets

Tecnología

Televisión Online

Televisores

Terminales

Tutoriales Gratis

Video Juegos

Emuladores

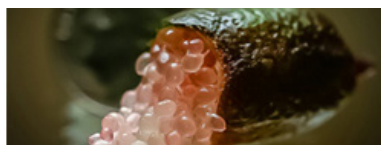
Juegos en línea

Juegos Móviles

Juegos PC

Videos de la Web

**Este producto
alimenticio
reduce
la obesidad**



Un padre pierde 7 kg de grasa CADA semana con este producto alimenticio. Los médicos dicen que se trata del "Santo Grial" del adelgazamiento... [\(LEER MÁS\)](#)



Geekets
Tendencius
Libros Gratis
Bitgame
Enceleb

Suburbios Utopicos
Misterekis
Portafolio Blog
Foro Universitario
Interlinkeo

Blog Bazaar
Sabor Universal
Literatura Libre
Globbos
Glovege



Geekets tiene las siguientes Políticas de Privacidad y pertenece a la red Blogurbania Blogs. Validado para XHTML 1.0 Transitional | CSS 3

 **Recomendado para Windows**

¡Sus Drivers no están actualizados!

Actualiza los Drivers de Windows en 3 sencillos pasos

Actualizar ahora



driverestore