Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

¿Es SSH lo suficientemente seguro? (8872 lectures)

Per **Celso González**, ***PerroVerd*** (http://mitago.net)

Creado el 28/08/2001 00:48 modificado el 28/08/2001 00:48

> Un equipo de la Universidad de Berkeley opina que no. En un estudio realizado opinan que ssh tiene dos problemas fundamentales: primero es fácil averiguar el tamaño de los datos encriptados ya que se encripta usando un limite de 8 bytes, y segundo en modo interactivo se puede aprender de las pulsaciones del usuario ...

Cuando se usa SSH en modo interactivo sucede lo siguiente: cada vez que se pulsa una tecla se realiza un envío de un paquete IP, a través de estos envíos se puede sacar una secuencia temporizada de las pulsaciones de un usuario.

La idea es la siguiente si yo escribo "se" en el teclado tardaré menos tiempo que si escribo "st" (las teclas estan más separadas y escribo con 2 dedos) aplicando un modelo estadistico se puede llegar a aproximar bastante lo que se está escribiendo

Es más han desarrollado un programa denominado **Herbivore** que se encarga de realizar este trabajo (no he podido encontrar ninguna referencia al programa salvo las que se indican en el estudio)

El texto completo del estudio, en formato PDF y en inglés, lo podeis encontrar aquí[1]

Lista de enlaces de este artículo:

1. http://paris.cs.berkeley.edu/~dawnsong/papers/ssh-timing.pdf

---

E-mail del autor: celso _ARROBA_ mitago.net

Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=823