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

Grave fallo de diseño en PKI compromete las firmas digitales (11323 lectures)

Per **René Mérou**, ***H*** (http://h.says.it/)
Creado el 29/05/2006 11:07 modificado el 29/05/2006 11:07

> *Fernando Acero nos muestra en Kriptópolis[1] un fallo de seguridad en las firmas digitales con certificados X.509, como los expedidos por la Fábrica Nacional de Moneda y Timbre.*

Podéis encontrar la forma que ha encontrado de demostrar el fallo, bastante bien explicada en este artículo de Kriptópolis[2].

Si alguien puede firmar un documento con la firma de otra persona y esa firma es legalmente aceptada, supongo que os dais cuenta del peligro que todo ello significa.

Para mí que deberían anular la validez legal del sistema por un tiempo. Que ya sé que es algo muy difícil pero es que ésto es muy grave.

Gracias por pasarme la noticia ElectronD :)

Lista de enlaces de este artículo:

1. http://www.kriptopolis.org/
2. http://www.kriptopolis.org/node/2333

E-mail del autor: ochominutosdearco _ARROBA_ gmail.com
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=2304