

Re: Cryptocard database

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0089.html>

From: Kurt Seifried (*bt_at_seifried.org*)

Date: 02/17/05

To: "John Madden" <chiwawa999@yahoo.com>, <pen-test@securityfocus.com>

Date: Thu, 17 Feb 2005 14:50:28 -0700

> *Hi,*
>
> *Doing an internal pen-test for a company i came across*
> *a mysql db that contains the Cryptocard tokens*
> *database (root with no password)*
>
> *The most interesting table (duh !!!) is the*
> *"EncryptedKey". Obviously this is not good. I made the*
> *usual recommendation to secure the db but i was*
> *curious to know if any one had experience with*
> *Cryptocard tokens and what is uses to encrypt that*
> *field. I presume they use the PIN of each user...???*
>
> *The size of the field is 48 characters (3DES ?)*
>
> *I would appreciate any info*
>
> *Thank you*
>
> *John*

Cryptocard's (at least the older ones) have the ability to have their secret loaded from a machine (you have to buy a special cryptocard docking bay, the card itself has three metal contacts on it if memory serves). Thus let's say a user accidentally breaks, flushes or otherwise mangles their cryptocard (tough but I'm sure someone has done it) you can load a new card up with the same secret and be back in business. Additionally because of the way this technology works both sides (the client and the authentication system) have to have the shared secret (this is the whole point of these systems, you have a shared secret that is exchanged securely). The database is unlikely to be the user's pin numbers (which in any event would be mostly worthless) and is much more likely to be the actual shared secrets (VERY useful, just load one into a cryptocard or the software for palm/etc and be the CEO for a day). Hopefully this shared secret is encrypted as the table name implies.

Kurt Seifried, kurt@seifried.org

SecurityFocus Penetration: Re: Cryptocard database

A15B BEE5 B391 B9AD B0EF

AEBO AD63 0B4E AD56 E574

<http://seifried.org/security/>