

Re: RSA SecureID on Solaris

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2002-04/0018.html>

From: Crist J. Clark (crist.clark@attbi.com)

Date: 04/09/02

Date: Mon, 8 Apr 2002 22:55:19 -0700

From: "Crist J. Clark" <crist.clark@attbi.com>

To: "Jonathan A. Zdziarski" <jonathan@networkdweebs.com>

On Mon, Apr 08, 2002 at 10:53:25AM -0400, Jonathan A. Zdziarski wrote:
[snip]

> *The number on the back is merely a serial number; the encryption seeds
> associated with that number are locked in a vault at RSA (and on your
> floppy)*

And on your ACE server, a computer hooked up to a network. =|

Also consider the "soft tokens." Software you run on a notebook, PDA,
or other portable electronic device. These can be easily copied.

> *so unless someone gets hold of one there's zero chance of
> someone guessing the code from the serial number. RSA doesn't release
> much about their algorithm (at least they didn't when we were using it),
> but it appears to be either a one-way hash function or a one-time pad.*

It's basically a hash. You seem to know you load short keys (seeds)
onto the server. You don't load big one-time pad files for each
token.

> *Since the tokens expire, I'd lean towards one-time pad unless the
> expiration is merely a marketing tool.*

Bingo!

But actually expiration dates on any authentication material is a Good
Thing(tm). Cards always slip through the cracks. A user loses a token
without realizing it. There is still only a finite window of
vulnerability. Five years from now a baddie who finds the lost token
can't slip through your legacy authentication mechanism that the
administrators don't pay attention to but is kept running for that one
marketing VP who can't figure out how to use the latest-and-greatest
system everyone else is using.

> *When configuring SecurID on our systems for shells, we used password +*

SecurityFocus SUN: Re: RSA SecureID on Solaris

- > *securid + pin just to make it more secure. You ought to be fine with*
- > *just securid + pin for your everyday security, though if someone was to*
- > *launch a focused attack, it's much easier to steal someone's pin than it*
- > *is their password, which is why we used both. Dusting the user's*
- > *numeric pad on their keyboard or watching them through a camera would*
- > *make it fairly easy to get someone's PIN.*

It's even easier to just look at the little Post-It Note the user put on the back of the token with both the password and PIN written on it. ;)

--

Crist J. Clark

| ciclark@alum.mit.edu

| ciclark@jhu.edu

| <http://people.freebsd.org/~cjc/>

| cjc@freebsd.org

- ***Previous message:*** Tony Lorimer: "RE: Good news: /dev/random from Sun for Solaris 8"
- ***In reply to:*** Jonathan A. Zdziarski: "RE: RSA SecureID on Solaris"
- ***Next in thread:*** Jonathan A. Zdziarski: "RE: RSA SecureID on Solaris"
- ***Next in thread:*** Doug Hughes: "Re: RSA SecureID on Solaris"
- ***Reply:*** Jonathan A. Zdziarski: "RE: RSA SecureID on Solaris"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]