

Re: ssh with no encryption ?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-02/0281.html>

From: David Magda (dmagda+netnews@ee.ryerson.ca)

Date: 02/23/03

From: David Magda <dmagda+netnews@ee.ryerson.ca>

Date: 23 Feb 2003 11:35:25 -0500

those who know me have no need of my name <not-a-real-address@usa.net> writes:

[...]

> *but it's a problem in some cases, and the various ssh authors are*
> *trying to keep us safe, even from ourselves -- a pain, true, but if*
> *we really cared that could be changed (worst case yet another ssh*
> *project, best case they each put a safe cipher=none in, sort of*
> *middle case popularly maintained patches).*

[...]

If I want to shoot myself in the foot I should be able to. At least have a compile-time option (disabled by default) where it's possible to allow cipher=none.

There have been situations where I wanted to use ssh but without encryption. Mostly where rsh(1) has been disabled but ssh(1) has not and I want to login without passwords: of course one of the machines was a Sparc5 (80Mhz) and encryption really slowed things down (X11 forwarding).

Shouldn't policy be separated from mechanism?

--

David Magda <dmagda@ee.ryerson.ca>

Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new. -- Niccolo Machiavelli, *The Prince*, Chapter VI