

Re: Newbie packet verification/signing

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-01/2589.html>

From: Jeffrey Spoon (JeffreySpoon_at_hotmail.com)

Date: 01/29/05

Date: Sat, 29 Jan 2005 21:22:47 +0000

In message <mdcnev0dh8606438rpee71sqqugf0s75hf0@4ax.com>, Mack <macckone@a_nospamjunk123_ol.com> writes

>On Sat, 29 Jan 2005 15:46:13 +0000, Jeffrey Spoon

><JeffreySpoon@hotmail.com> wrote:

<Good stuff snipped>

>

>*I posted a protocol a while back (you can google for it). It did not address signature compromise and revokation. It used a single tiered model with a trusted public key signer. It did not address how the keys were signed (OOB). Its primary use is a command protocol with infrequent mostly one way communication.*

>

Thanks for the advice but I'm thinking this is quite serious overkill for what I'm doing. However I'll look into the things you have suggested and your protocol. Thanks

--

Jeffrey Spoon