

Re: Algorithm suggestions

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-09/msg00961.html>

- *From:* daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (David Wagner)
 - *Date:* Tue, 26 Sep 2006 23:43:05 +0000 (UTC)
-

Geoffrey Summerhayes wrote:

I'm looking for a relatively simple algorithm to add a second layer of protection to a transmitted packet.

The data to be encrypted is less than 256 bytes per packet, with a fair amount of similarity in the data, multiple senders, each can have their own key, the final packet is sent using SSL.

The main reason for the additional layer is to deter packet sniffing between the sender and the SSL device.

Why don't you just use SSL between the sender and the device?

This is not a "second layer of protection", if the packet is sent in the clear (unprotected by SSL) en route between the sender and the device. For that portion of the transmission, this will be the only layer of protection. I would be concerned about any suggestion that because this is a "second layer of protection", it doesn't have to be very good. That kind of attitude is dangerous.

What do you mean by "deter"? I don't think that "deterrence" is an effective strategy online.

I think we may need a little more detail on your security goals (what are you trying to achieve), your threat model (who is likely to attack the system, and what capabilities are they likely to have; to put it another way, who/what are you trying to defend against), and any economic/performance/other constraints that you may be facing. That may mean that you may have to think about those some more.

If you're considering taking "shortcuts", you'll need to be pretty darn confident that you've characterized the threat environment accurately and that you've understood the risks of the shortcut fully. And whenever you find yourself inclined to take "shortcuts", you have to be very careful that you're not just engaging in wishful thinking (as in, gee, my life would be nicer if there was a simple solution; this is simple and looks like a possible solution; if it doesn't work, my life is going to

Re: Algorithm suggestions

be unpleasant; therefore let's not look too closely at whether it really will be adequate or not).

.