

# Re: Algorithm suggestions

---

*Source:* <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-09/msg00984.html>

---

- *From:* Unruh <[unruh-spam@xxxxxxxxxxxxxxxx](mailto:unruh-spam@xxxxxxxxxxxxxxxx)>
  - *Date:* 27 Sep 2006 18:43:38 GMT
- 

"Geoffrey Summerhayes" <[sumrnot@xxxxxxxxxxxx](mailto:sumrnot@xxxxxxxxxxxx)> writes:

David Wagner wrote:

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

The sender is a small terminal device that already has a lot of code on it. The SSL is a OEM add-on that is non-programmable.

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.

The main security threat is from the operator of the device, so there are numerous safeguards in place to stop quasi-legitimate data. Looking over the design, the largest packet is 64 bytes of data. I expect the number of packets passing between any device and the server to be around 100 per day at peak usage, so in theory at least, it could require some time to gather enough data to reverse engineer an encryption scheme. A major portion of the encrypted data is binary, so there's also the problem of recognizing the unencrypted data as correct.

If you're considering taking "shortcuts", you'll need to be pretty darn

## Re: Algorithm suggestions

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

I expect that every time someone invents a better lock, people start working on better lockpicks. I fully expect any system to be broken, I'd just prefer that the cost of their time and effort is more than their expected return.

Yes, but that depends on your knowing very very well what lockpicks are out there right now. For example the famous bic pen hack of the Kryptonite locks made them ( the pin type circular key locks) useless, but I am sure lots of people still believe that if it is Kryptonite it must be secure.

Ie, rolling your own shortcut could well be way on the wrong side of that cost benefit analysis simply because of your ignorance of what "lockpicks" are out there.

.