

Re: One-sided authentication for small micros?

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/2005.html>

From: Andrew Swallow (am.swallow_at_eatspam.btinternet.com)

Date: 10/18/03

Date: Sat, 18 Oct 2003 13:36:06 +0000 (UTC)

"Matthue Gera" <zoomzoomzoom@xtra.co.nz> wrote in message
news:Vx3kb.182200\$JA5.4557184@news.xtra.co.nz...

> *Some thoughts on your problem.*

>

> *What about if you have a unique id in each slave.*

>

The simplest and most efficient hack for this system is to
buy similar equipment from a rival manufacturer.

A manufacturer whose equipment is fit for its purpose
and who does not maliciously sabotage his own
machines.

A full hack also involves black listing the supplier
and ensuring that even 10 years later the purchasing
department hang up when the salesman for nasty
manufacture rings. (The black list may not need
enforcing for that length of time, they have probably
gone bankrupt before then.)

A system based on secret information is hard
to maintain when the victim is the owner and
user of the machine. Reverse engineering
access will be granted.

The most used Standards are those that define
interfaces. This is because three groups win –
the makers of machine A, the makers of machine
B and the purchaser of both. Manufactures that
cheat their customers soon find that they have
none.

Andrew Swallow

p.s. The assumption has been taken that the
customer buys the master at the same time
as the first slave. The customer may already
have some slaves and wants a better controller.