

## Re: [fw-wiz] Username password VS hardware token plus PIN

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-02/0132.html>

---

**From:** David Lang ([david.lang\\_at\\_digitalinsight.com](mailto:david.lang_at_digitalinsight.com))

**Date:** 02/24/05

To: "Marcus J. Ranum" <[mjr@ranum.com](mailto:mjr@ranum.com)>

Date: Wed, 23 Feb 2005 22:23:21 -0800 (PST)

here's a box that's essentially a palm clone for about \$40 each in single unit quantities. not fancy, no color, etc but a well known platform with lots of good development tools (assuming it's not able to run off-the-shelf palm software)

[http://www.zexus.com.hk/products/products\\_all\\_PDA.htm](http://www.zexus.com.hk/products/products_all_PDA.htm)

David Lang

On Tue, 22 Feb 2005, Marcus J. Ranum wrote:

> *Date: Tue, 22 Feb 2005 12:56:36 -0500*  
> *From: Marcus J. Ranum <[mjr@ranum.com](mailto:mjr@ranum.com)>*  
> *To: Frank Knobbe <[frank@knobbe.us](mailto:frank@knobbe.us)>*  
> *Cc: MHawkins@TULLIB.COM, firewall-wizards@honor.icsalabs.com*  
> *Subject: Re: [fw-wiz] Username password VS hardware token plus PIN*  
>  
> *Frank Knobbe wrote:*  
>> *That's why I was never happy with SecureID tokens since the PIN is*  
>> *transmitted during logon and thus subject to interception by an*  
>> *attacker. I preferred tokens that require the PIN to unlock the token,*  
>> *but never transmit the PIN.*  
>  
> *This topic comes up SO MANY TIMES it's not even funny. I bet*  
> *if we looked through fw-wiz archives we could declare this to*  
> *be "Standard Ranum Rant #2978378" and instead of posting*  
> *this I could just say:*  
>  
> *#include <sys/rant/ranum/2978378.h>*  
>  
> *:) But anyhow....*  
>  
> *What amazes me is that organizations seem to think that having*  
> *authentication tokens is a) expensive and b) hard. If you look on*  
> *the websites for obsolete hardware clearing houses you can*

Firewall-Wizards: Re: [fw-wiz] Username password VS hardware token plus PIN

> *find vintage PDAs for next to nothing and I'm sure you can get them*  
> *in quantities. A lot of these PDAs are programmable with SDKs.*  
> *For example, a cursory query of BizRate shows that you can get*  
> *HP h2210 PDAs (they run windows mobile 2003!) for \$51.*  
> *It has a clock in it; it's a scheduler for crying out loud. Of course*  
> *Security Dynamics has patents on time-syching tokens so that's*  
> *not an option but you could cook up a number of cool variants*  
> *of the old Atalla authentication used in the Digital Pathways*  
> *SecureNetKey (there's compatible source in C for an implementation*  
> *in the firewall toolkit code. I know because I put it there)*  
> *Bizrate says you can get an Oregon Scientific PDA293 for \$9.99.*  
> *Did you read that? \$9.99. And you get free calendaring thrown*  
> *in and it probably can play games, which is more than your*  
> *Security Dynamics card will ever do! Franklin RF8120s are \$12.*  
> *Some of these things have voice recorders and all kinds of*  
> *fun stuff. If a company invested a tiny fraction of the cost of*  
> *fielding something like a Security Dynamics solution in*  
> *integrating some software they could probably have an*  
> *enterprise-wide authentication AND scheduling solution. Some*  
> *of these puppies have IRDa ports and you could integrate*  
> *them with building locks for the cost of a low-end PC and*  
> *some software hooked to a \$100 electronic lock striker*  
> *unit. "Point your token at the door and enter your PIN to open"*  
> *how cool is that? Or retrofit the sync cradle and use it as*  
> *a door control. Or use it to PGP-sign your documents.*  
> *Some of these things have built-in calorie counters! What's*  
> *not to like!? ;) "This document was PGP-signed by*  
> *Marcus Ranum, at 11:99 at XYZ GPS coordinates and*  
> *he had probably eaten too much when he wrote this."*  
>  
> *mjr.*  
>  
>  
> \_\_\_\_\_  
> *firewall-wizards mailing list*  
> *firewall-wizards@honor.icsalabs.com*  
> *<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>*  
>

--

There are two ways of constructing a software design. One way is to make it so simple that there  
-- C.A.R. Hoare

\_\_\_\_\_  
firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>