PDAs come in a variety of forms, but the most popular are palm-sized computers made by Palm, Sony, Psion, HP and Compaq. These devices typically synchronize with workstations. Recent models have megabytes of memory and can carry thousands of address entries, documents, spreadsheets and even PowerPoint presentations. Some people have wireless connections to the Internet and use simplified browsers and e-mail clients on their hand-held computers.

I'm sure that readers are aware of the dangers posed by PDAs that contain confidential information. Users who synchronize their PDAs with corporate workstations almost certainly have confidential data in their pocket. Many people store their passwords for other systems on their PDA. These little computers can serve as inadvertent tunnels into secured networks because they are typically connected through PCs behind the firewall.

Security included with PDAs is weak and programmatic attacks are easy to create. For the Palm operating system (PalmOS), for example, the first Palm OS Trojan was discovered in August 2000: a supposed Nintendo Gameboy emulator wiped all applications on infected Palm PDAs. Then in March 2001, news reports indicated that any devices using the PalmOS have no effective security despite the password function. Apparently developer tools supplied by Palm make it very easy to write a back door conduit into the supposedly locked data.

In April 2002, Kaspersky Lab released Kaspersky Security for Palm OS, which it says is a full-scale defense system for handhelds and mobile devices operating on Palm OS. According to the company, the suite is comprised of two modules; one that controls access to a device using a reliable password structure on the system level and another that controls authorized access on the application level using encrypted data.

A few months ago, my old Palm PDA finally died and I bought a new Palm m515 unit. Adam Kennedy, one of my information assurance students at Norwich University, wrote an excellent term paper on protecting PDAs and mentioned another high-security product for the Palm OS. I looked into his suggestion and downloaded and installed PDA Defense from Asynchrony Solutions < http://www.pdadefense.com >. I think readers with their own Palm PDAs to protect will want to look into it as well as into Kaspersky’s product, and so will any network administrator whose users have Palm PDAs that plug into corporate systems.

(By the way, if you don’t think your users are plugging their PDAs into your corporate systems, you’d better do an audit.)

Because I have not seen Kaspersky’s product and cannot claim to have performed an evaluation of PDA Defense, please don’t take what follows as an endorsement. I’m just reporting what I’ve learned by using the latter product.

PDA Defense offers 64-bit, 128-bit or 512-bit Blowfish encryption for all data stored on the PDA. Records flagged as “private” can either be masked or hidden entirely at the user’s choice.
Password entry is masked to prevent shoulder-surfing; the RAM buffer is wiped immediately upon login and the password itself is stored as an MD5 one-way hash to make dictionary cracking more difficult.

The bit-wiping bomb defeats brute-force attacks by letting the user limit the number of attempts to unlock the device. When someone exceeds the maximum number of attempts, the bomb feature bit-wipes all RAM databases without a user prompt. Now, this does constitute a potential channel for a denial of service, but the user can restore the data from his or her PC if the device is recovered or replaced with a new unit. It is even possible to set a time-sensitive bit-wiping bomb that prevents unauthorized access to data if the PDA if it is lost or stolen by allowing the user to set a required time for synchronization with the PC; miss the deadline and all the data are wiped (this is the kind of feature one would want to be very careful with). The PDA is protected after a reset, requiring password entry for access; another option automatic locks the unit every time the power is turned off (e.g., three minutes after last use). While access is disabled, so are all data transfers such as HotSync and infrared links. It is possible to put the product into stealth mode so that it emulates the default security features and suppresses all signs of its presence unless the correct password is entered (thus potentially misleading an attacker into believing that they have in fact successfully taken control of the PDA even though they haven’t).

The enterprise version of the product (which I have not seen) apparently offers administrators great flexibility in applying encryption and security restrictions to selected applications and records as well as setting password global policies (e.g., length, complexity, longevity) and tailoring policies to individual users.

I hope that readers will look into PDA security products for their own little computers and protect their own data and their network security with equally powerful and convenient security.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.