Global Information Assurance Certification Paper

Security Vulnerabilities in the Palm OS® version 3.x
July 24, 2001
Laura Thomas

PDAs using the Palm OS® are becoming more popular by the day; sales are up quarter after quarter. Is the data on your Palm device at risk? Yes, it is. Take a moment and think about the data on your Palm device you do not want to be public knowledge: credit card numbers, PINs, banking information, passwords, client lists, sales strategies, competitive information. "But I have a password set for power on, and I use private records," you say. Unfortunately, these precautions do not mean your data is secure. It is true that someone must be in physical possession of your Palm device to do most of the things discussed in this article. By their very nature Palm devices are easily stolen or misplaced, allowing them to fall into malicious, mischievous, or simply curious hands.

This article will examine the security features standard with the Palm OS® version 3.x, their vulnerabilities, and some alternative security software which help remedy these vulnerabilities. The classic ideals of information security apply to a Palm device as well as to a network. The key to any good security strategy is defense in depth. A good perimeter (in this case a robust locking system at boot) and encryption of data on the Palm device protected by another strong password make up an adequate defense for most individuals. Devices running Palm OS® v4.0 do not share all of these vulnerabilities. To check the version of the Palm OS® you are running go to the System program group, push the menu button, choose info and choose version from the options on the bottom of the screen. Your Palm OS® version should be listed at the top of the display.

Survey
An informal survey I conducted via email showed that most people (17/22) were aware of the security features included in the Palm OS® . The complete text of the survey, along with a summary of the results, is included at the end of this document. However, only a small number (6/22) actually used the security features on their Palm device. Only two users had additional Palm OS® security software. It is apparent that there is a lack of easily available information about security for these devices.

The primary reason given for not using the included security features was slower access to data. As quick access to data is a significant reason for use of a Palm device, this was a problem. In response to the question "Do you use the security features that come with your Palm OS® device? Why or why not?", one respondent stated "No, they seem complex and putzy, I don't have a lot of time to dink around." The respondents also indicated that they didn't keep any "important" or "confidential" data on their Palm devices. An important aspect of any security system is ensuring that people actually use it. If it is too much of effort to use security tools, people will disable or circumvent security features, leaving the door unlocked for those with malicious intent.

When asked if they thought data was safe on their Palm devices, respondents were less than sure. Eight believed their data was safe, ten said it was not, and four gave conditional answers. The overwhelming feeling was the data was as safe as the device was physically. As long as the respondents were in possession of their Palm device, they felt their data was safe. However, they were in big trouble if they lost physical control of the device. Many people cited uncertainty about security as a reason for not keeping anything "important" on their device.

What are you going to secure and why?

The device

There are two aspects to securing the Palm device itself: physical security and using a power-on password. Maintaining the physical security of your devices includes not leaving it on the airplane, sitting on a conference room table, or even leaving it unattended at your desk. Using a power-on password secures access to all data on your Palm device. A significant advantage to locking the whole device, if you use a well secured password, is that everything on the device is secure. Unfortunately, using the Palm OS® out of the box, no power-on password is well secured. The details of this vulnerability are discussed below. If someone gets past your power-on password, they have full access to all data on the device. Additionally, the need to enter a password every time you turn your Palm device on can be a hassle, especially if your Graffiti skills are weak. This increases the probability that you will cease to use this line of defense. One line of defense is better than none, but a Palm device is not an exception to the crucial need for defense in depth.

Some records

Securing only a portion of the records on your Palm device allows easy access to unimportant less private, such as shopping lists. Out of the box, the Palm OS® provides private records for this purpose. As discussed below, there are serious vulnerabilities in the implementation of private records. There are also third-party Palm OS® applications available which allow you to store certain kinds of data in encrypted form protected by a separate password. These are far more secure than the provided Palm OS® hidden record system.

All records

Securing all records on the device, either in the Palm OS® hidden record system or a third-party software, does not make much sense. This method requires extra steps to access every record. Fast access to data is the one of the main reasons people use Palm devices. If a user must complete extra steps to get to any information, they will no doubt stop using either the device or the security features. Software that can encrypt all of the information on your Palm device does exist, and it should be considered by those with high-level security concerns.

Palm OS® out of the box: Good Ideas, big vulnerabilities.

Palm does provide some limited security right out of the box. This consists of a single password for use at power on and to make some records private. The password is set in the Security application under the System menu. While these elements are better than no protection, there are serious vulnerabilities regarding password security and

encryption in the Palm OS® .

Private records are a significant part of the security features included in the Palm OS® . Unfortunately private records are not truly secure. They are protected by the standard Palm OS® passwording scheme. This scheme is easy to compromise with physical access to the Palm device, a synchronization device and a computer. Simply synchronizing the Palm device to any computer immediately compromises all data stored in private records. For example, all of the memos for a particular user are stored in one file in the Palm OS® directory on the PC: \Palm\<user>\Memopad\memopad.dat. This file can be easily read in a text editor. The same is true for entries in the other standard Palm OS® applications. For this reason alone, the private record system should be avoided for all but the most unimportant of data.

Another concern with the private records system is one of usability. Any 3.x version of the Palm OS® offers the ability to hide all private records. The problem with this ability is the records are completely hidden. As such, you may forget that you have hidden a specific entry and be unable to find it. Additionally, all private records are either hidden or visible. It is not possible to reveal only one private record. In version 3.5 or later of the Palm OS® , private records may be hidden or masked. As with earlier versions, hidden records are completely invisible. Masked records, however, show a grayed line with a padlock symbol where the record would appear. Tapping on this grayed line allows you to enter your password to reveal the record. Very few users are aware that unmasking one private record unmasks all private records in all applications. Once any record is unhidden or unmasked, all records are unhidden or unmasked until you return to the security application to hide or mask them again. The inconvenience and lack of intuitiveness of private records forces many users away from the meager security features provided them by the Palm OS®.

Both the private records feature and the power-on password can be easily compromised. In March of 2001, @stake released an advisory stating that "a backdoor exists in Palm OS® which provides source- and assembly-level debugging of executables and the administration of databases existing on the physical device."[1] This allows an unauthorized user to gain access to all data, including the system password, and to install or remove programs on the device.[2] This vulnerability is caused by a documented feature included in every installation of the Palm OS® . There are shortcuts built in to the Palm OS® which can be used at power on to enter either the console or debug modes. This is possible even when the device is locked. These shortcuts are used by developers for debugging purposes. All that is needed to compromise a device is the development kit, a computer, and a HotSync cable. The development kit is downloadable from the Palm site. Instructions on how to use the shortcut can be found on page 82 of the Palm OS® Programming Tools Development Guide. Software tools which close this back door are discussed below.

The handling of the password itself is another major weakness in the Palm OS® . The password is stored unencrypted in the Unsaved Preferences database on the device. It

is also transmitted in a weakly encrypted form when the Palm OS® is synchronized with the computer. While the password is encrypted during this transmission, the encryption consists of a very weak hash which is always padded to 32 bytes. This encryption can be quickly decoded by XOR'ing the encrypted password against a known block.[3] The password can also be deleted using a single system call.

The ease of deleting the password with a single system call is the basis of NoSecurity, written by Remo Hofer. This program does one thing: remove your Palm OS® system password. It leaves all of the records that were hidden by that password unlocked and unprotected. Mr. Hofer states that he wrote the program for three reasons: to be used by those who forgot their password, to demonstrate the weakness of the Palm OS® security and as an exercise in coding.[4] This piece of software works exactly as advertised, which is a terrifying thought to those protecting confidential data with the inherent Palm OS® security. However, this tool is also very handy for those in an IT environment where users forget their passwords and have important documents marked as private. Deleting the system password renders all hidden records visible.

Third-party software

Fortunately, there are a great many third-party software packages available for the Palm OS® to increase security. These applications fall into two basic categories: those which lock the device at power on/off and programs that hold secure data. The latter category is quite large as there are applications for every sort of data you can imagine. A sampling of some of the more popular programs of both types are discussed here.

Locking Software

Easylock, and its companion program ShortFix, are written by Daniel Seifert. ShortFix should be considered a must for every security conscious Palm OS® user, as it closes the debug/console mode vulnerability in the Palm OS® . This application removes the two shortcuts from the Palm device that allow access to the debug and console mode, until the next hard reset. Closing this gap is essential in protecting your Palm device. You need not use EasyLock to use ShortFix.[5]

EasyLock is an alternative way to use the Palm OS® security features. It gives you an option instead of entering a Graffiti password when you turn your Palm device on. You choose a button or combination of two buttons from the 12 available on most Palm devices to be hit within a designated number of seconds. If these buttons are not hit within the time limit, the device is locked using the standard Palm OS® locking mechanism. When using this it is critical that, the standard password locking mechanism was made more secure by the use of the companion program ShortFix.[6]

OnlyMe by Tranzoa is another Palm OS® locking application, but it does not rely on the Palm OS® security. OnlyMe was designed to be moderately safe, easy to use, and automatic. It automatically locks the device when it is powered off. When in a locked state, the software does not allow beaming or synchronization. Additionally, it blinds the password on entry, preventing someone else from viewing your password as you

enter it. OnlyMe also returns you to the place you last left when the device was powered off.[7] OnlyMe has a wide variety of options for passwords, and quick logon features similar to those provided by EasyLock. OnlyMe considers the quick log-on features a security risk, however.

An additional feature of OnlyMe is Cracker Time Lock™ which makes brute forcing the password. It does so by locking out the device for increasing durations after each five failed logon attempts. The Tranzoa site provides fairly extensive information about security on the Palm OS® and some general security information including guidelines for password selection and encryption.[8]

PDADefense , formerly PDABomb, is another security package for the Palm OS®. They also make versions for other handheld operating systems. PDADefense is currently available in two editions, with two more to be released in August of 2001. The Standard Edition stores an MD5 hash of the password rather than the password itself, and all information on the device is protected using 64-bit Blowfish encryption.[9] The Professional version uses 128-bit or 512-bit Blowfish encryption for all data and includes several extra features. An example of these features is the Bomb feature which protects versus brute force attacks by bit-wiping all the RAM databases on the device after a predetermined number of attacks.[10] Both versions also secure the device from HotSync and IR communication while locked and create the decryption key each time the password is entered. The key is not stored on the device.

Secure Databases

Another type of security available for the Palm OS® is that of a secure database, a single application to hold all of your private information. These applications typically encrypt the data both on the device and when it is synchronized to the computer. By storing all your private information in one place, you maintain fast and easy access to your public data while still providing an additional layer of defense for sensitive information.

Keyring for PalmOS, formerly gnukeyring, is a freeware application for the storage of passwords and other sensitive information. Each record (referred to as a key) has a public name, an account name, a password, and freeform notes. This allows you to store login information or other important data. One handy feature of Keyring is the random password generator which allows you to set password length and the types of characters, numbers, and letters used in password. The authors do warn that the base of this is the PalmOS random number generator, which may be predictable. [11]

eWallet is available on more than one platform, including a version designed for your desktop. It is designed to keep credit cards, calling cards, pin numbers, and account information in a single place. eWallet has templates for many different types of information from credit cards to locker combinations. It uses RC4 encryption to keep your data secure on your Palm. The decryption key is created from your password, thereby not storing the key on your Palm device. [12]

Conclusion: Is your Palm a safe place to keep data?

Your Palm device is only as safe as you make it. Out of the box, even with the security features provided, the Palm OS® version 3.x is essentially wide open for anyone to access your sensitive data. Fortunately, with additional software your Palm device can be made much safer. At a minimum, every user should use ShortFix to close the debug/console mode vulnerability. A more secure choice would be to not use the Palm OS® security features at all, choosing instead an outside software package, such as PDA Defense or OnlyMe as a first layer of defense. Security features and software must be easy to use or people will not use them. It is up to every user or company to determine the correct level of security is for their Palm devices.

An additional way to improve security on your Palm device is to be cautious what data is stored on it. Keep only data to which you need immediate access on your Palm device. Then select a software package such as GNU Keyring or eWallet to encrypt and protect sensitive data on the device behind a second password. This allows you to quickly get at most of your data while providing an additional layer of defense for your confidential data. When choosing security software, there are two key issues. Ensure that the encryption used to protect your data is strong. Is the data still encrypted after it has been synchronized to a PC? If not, your data can still be easily compromised.

Sensitive data stored on your Palm device can be protected. Unfortunately, the security features provided with the Palm OS® version 3.x will not be sufficient. You will need to consider defense in depth and third-party software to bring adequate security to your Palm device.

Works Cited

Asynchrony.com. "PDA Defense, Professional." 25 July 2001. URL: http://www.pdabomb.com/professional.asp (25 July 2001).

Asynchrony.com. "PDA Defense, Standard." 25 July 2001. URL: http://www.pdabomb.com/standard.asp (25 July 2001).

Hofer, Remos. "No Security." 12 October 2000. URL: http://www.geocities.com/nucifera.geo/nosecurity.htm (25 July 2001).

Ilium Software. "Ilium Software's eWallet." 25 July 2001. URL: http://www.iliumsoft.com/walletp.htm (25 July 2001).

Kingpin. "Palm OS Password Lockout Bypass." a030101-1. 1 March 2001. URL: http://www.@stake.com/research/advisories/2001/a030101-1.txt (25 July 2001).

Kingpin. "PalmOS Password Retrieval and Decoding." A092600-1. August 2000. URL: http://www.atstake.com/research/advisories/2000/a092600-1.txt (25 July 2001.

Pool, Martin. "Keyring for PalmOS: introduction." 25 February 2001. URL: http://gnukeyring.sourceforge.net/ (25 July 2001).

Robinson, Alex. "PalmSource 2000 Session 708 Talk." 14 February 2001. URL: http://www.tranzoa.com/onlyme/palmsource2000talk.htm (25 July 2001).

Siefert, Daniel. "EasyLock." 22 July 2001. URL: http://www.dseifert.com/easylock/index.html (25 July 2001).

Siefert, Daniel. "ShortFix - Increase Security On Your Palm." 22 July 2001. URL: http://www.dseifert.com/ShortFix/ (25 July 2001).

Tranzoa Company. "OnlyMe." 2 June 2001. URL: http://www.tranzoa.com/onlyme/onlyme.htm

(25 July 2001).

Appendix A
The survey was sent via email to people I knew with Palm devices. They then passed it on to other Palm users they knew. In total I got about 30 responses, some telling me they did not have a Palm OS® based device. There were 22 responses from people with Palm OS® based devices. The questions follow, then the tabulated answers and any comments made about each question.

1) Are you aware of the security tools that come with Palm OS? (including private documents and password checking at power on)

Yes 17
No 6

• Yes, I am aware of them but don't use them out of laziness. Per our discussion earlier, I choose not to use the private document because they are not "private" when stored on a PC
• Not really, I know there is a password system and a way to hide records. Other than that. I know squat.
• Yes I am aware of most of these.
• I knew the Palm has some sort of password feature, but have never used it.
• Have a PalmV - yes, I am aware of the security tools that come with the unit
• Yes. I use private documents in several applications, and password checking.
• Yes - I used the password check
• I know they're there...but I've never explored or used them.

2) Do you store any private/confidential data on your Palm OS® based device? (credit card numbers, passwords, PIN, customer data etc)

Yes 12
No 11

• just non-critical passwords like AvantGo, and website I don't visit very often.
• Yes - I used the palm pilot to store confidential numbers but did not label them
• Some few
• Yes, I do. They are password protected.
• Yes, but in a program the requires a password to access it and that stores the data in an encrypted format.
• Very little, and what's there is hidden -- Security by Obscurity. I can be more specific if you like.
• Limited, such as frequent flier numbers for the airline programs I am in.
• Yes, some credit card information for closed accounts.
no. would like to.
• Yes, I store some passwords and PINs.

3) Do you use the security features that come with your Palm OS® device? Why or why not?

Yes 6
No 16
• SOME
• I use a program called Teal Lock to keep my Palm locked.
yes, only the password at power on and swiping the screen top -to-bottom to lock and turn off.
• No - Too tedious and I don't consider the information that important
• Not aware of them
• No. Because I use it for quick reference like dates, calculator, jot Bugme notes.
• NO. Because I have not taken the time to see how they work.
• Yes, I do. Although I know they are not infallible, I feel that the only time my privacy could be compromised is if my Palm was lost or stolen. Then I would know to cancel cards, etc. I doubt someone could pick the Palm up from my desk and quickly circumvent security.
• Yes. Limited security against theft.
• Do not use the security features - no private info and do not connect to a PC or network
• NO. I DON'T KNOW WHAT THEY ARE
• Did not know about them
• No have not needed to use them
• Because from what I've read about the Palm's default password protection, any idiot who gets the development kit available from palm.com, for a free download, can bypass the Palm OS password.
• No, at present I avoid placing sensitive information on the Palm or when that is unavoidable, I encrypt/conceal it. Part of the advantage of a PDA is swift convenient access to information, and until I need to keep data that requires protection, I will avoid doing so.
• No, I have not taken the time to learn this and also do not thik it is necessary for the uses I make on my Palm. Also I do not want to be bothered with passwords every time I pick it up to reference the Palm.
• No, they seem complex and putzy, I don't have alot of time to dink around.
• no. no need or education.
• Not regularly. Laziness?
• No. The data that I keep on there is not that important.
• No - I don't store any private/confidential data on it.

4) Do you feel your data is safe on your Palm device?
Yes 8
No 10
Partially 4
• No - That's why I don't store any sensitive info on it.
• No safer than the device itself (IE, if I have the device in my pocket, it's safe enough). The device is worth more than the data I store on it.
• As long as it remains in my possession, I feel comfortable about it. If it were lost or stolen, I would be in some difficulty.
• Yep, it's always with me.

• Yes, as long as I keep my Palm in my control
• Only because I'm careful with the physical device. Few data storage technologies are safe once the hardware is out of your posession.
• No - particulary because someone could easily take palm from desk
• Should be safe - but then again do not store data or connect
• As safe as it would be in my wallet. That is the level of security I give the Palm. • As long as it is under my control, I consider the data safe.
• I though my data was secure but I 'lost' a note file containing confidential information during a reconciliation procedure with my pc so now I'm rather more cautious.
• yes, only limited data is on there anyway
• Yes, safe enough. What're the chances I'll lose my Palm combined with someone overcoming Teal Lock? I believe the risk is reasonable.

5) Do you use any other security software on your Palm OS® based device? If so what do you use?

Yes 2
No 21

• Yes, Teal Lock
• Yes, eWallet. I'm considering a program called PDABomb, but I store very little sensitive data on my Palm OS device, so I'm not sure how protective I need to be right now.

6) Have you heard of any threats to the integrity of your data on your Palm OS® device? (viruses, known vulnerabilities etc)

Yes 7
No 15

• No, but I suspect that the lifeless bastards who do that sort of thing have come up with something.
• Yes (viruses).
• No. Occasional concern about inadverent IR contact. Some BP folks have had a surprise when their laptops connected to others on airplanes. Haven't heard of the issue with Palms.
• Some viruses, it's my understanding that they enter through hackmaster. But, I could be wrong.
• I do worry about viruses on the Palm and it has on occassion locked up so I had to start from the begining as I lost all of teh data stored. An excellent feature is the IR port. But some people have asked how secure this might be as a means of transferrign data.
• Yes, I am poorly educated about the specifics, however. Most of what I've heard still refers to email issues, and I do not use my palm for email.
• Yes, both viruses and the easy ability to hack the password via the developer's kit.
• Have not been made aware of threats to the integrity of the data other than if I forget my password, then I lose all information on the unit.
• I have heard that viruses are not impossible. It concerns me, but everything on

my Palm is backed up. I do very little sharing of files with others.

[1] Kingpin. "Palm OS Password Lockout Bypass." a030101-1. 1 March 2001. URL: http://www.@stake.com/research/advisories/2001/a030101-1.txt (25 July 2001).
[2] Kingpin. "Palm OS Password Lockout Bypass." a030101-1. 1 March 2001. URL: http://www.@stake.com/research/advisories/2001/a030101-1.txt (25 July 2001).
[3] Kingpin. "PalmOS Password Retrieval and Decoding." A092600-1. August 2000. URL: http://www.atstake.com/research/advisories/2000/a092600-1.txt (25 July 2001.
[4] Hofer, Remos. "No Security." 12 October 2000. URL: http://www.geocities.com/nucifera.geo/nosecurity.htm (25 July 2001).
[5] Siefert, Daniel. "ShortFix - Increase Security On Your Palm." 22 July 2001. URL: http://www.dseifert.com/ShortFix/ (25 July 2001).
[6] Siefert, Daniel. "EasyLock." 22 July 2001. URL: http://www.dseifert.com/easylock/index.html (25 July 2001).
[7] Robinson, Alex. "PalmSource 2000 Session 708 Talk." 14 February 2001. URL: http://www.tranzoa.com/onlyme/palmsource2000talk.htm (25 July 2001).
[8] Tranzoa Company. "OnlyMe." 2 June 2001. URL: http://www.tranzoa.com/onlyme/onlyme.htm (25 July 2001).
[9] Asynchrony.com. "PDA Defense, Standard." 25 July 2001. URL: http://www.pdabomb.com/standard.asp (25 July 2001).
[10] Asynchrony.com. "PDA Defense, Professional." 25 July 2001. URL: http://www.pdabomb.com/professional.asp (25 July 2001).
[11] Pool, Martin. "Keyring for PalmOS: introduction." 25 February 2001. URL: http://gnukeyring.sourceforge.net/ (25 July 2001).
[12] Ilium Software. "Ilium Software's eWallet." 25 July 2001. URL: http://www.iliumsoft.com/walletp.htm (25 July 2001).