Ointment — A password recovery tool for Palm OS devices

Written by Joe Grand, August 13, 2001

Ointment exploits a particular design problem with the Palm OS backdoor debug mode and the use of weak obfuscated system passwords.

Ointment will emulate the serial link protocol and 'export' and 'reset' commands of the Palm OS Console Debug Mode, retrieve the encoded password block from the Unsaved Preferences database of the target device, and decode and display the resultant ASCII password. The target device must be running a Palm OS version less than 4.0.

Overview

The Palm OS Security application provides "system lockout" functionality in which the Palm device will not be operational until the correct password is entered. The password is also used to protect and hide records by the legitimate user by marking them as "Private". These mechanisms are meant to prevent an unauthorized user from reading data or running applications on the device.

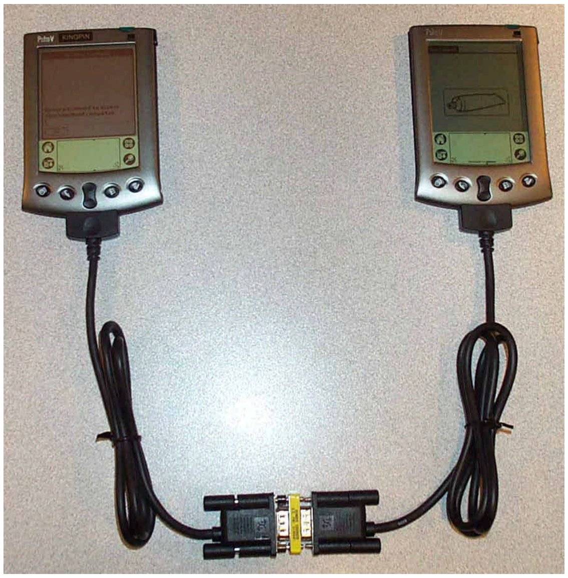
A backdoor exists in Palm OS which provides source- and assembly-level debugging of executables and the administration of databases existing on the physical device. Although this backdoor is documented for debugging purposes, it can be activated even if the Palm OS lockout functionality is enabled. This will allow an unauthorized user to perform a number of commands including, but not limited to, retrieving an encoded form of the system password, obtaining all database and record information on the device, and installing or deleting applications.

The system lockout mechanism is currently assumed by most users to be a sufficient protection feature of the Palm operating system. This is not the case and is a severe weaknesses for particular deployments of Palm OS devices.

In short, this tool will allow you to simply walk up to a Palm device that has been "locked", hook up a Palm-to-Palm cable (see Application Instructions), run Ointment, determine the system password, and log into the locked device (and access all of the user's private data).

Application Instructions

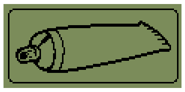
1. Connect the device running Ointment, Ointment, to the target device with the modified HotSync cable:

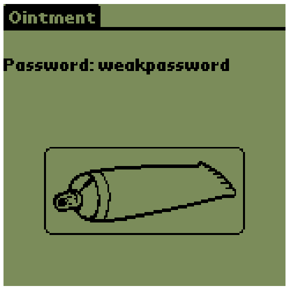


To connect the two Palm devices together, you will need to make a null modem cable to connect between the two using:

- Two Palm OS HotSync Cables, http://store.palm.com

- 9-pin Male-to-Male Null Modem Adapter

2. On the target device, enter **.2** (shortcut dot dot two) to enter console mode. If console mode is properly enabled, the text you just entered will be erased. The target device must be running a Palm OS version less than 4.0.
3. Tap the icon on the Ointment main form to begin,  . A status area will display the current state of the password retrieval process.
4. If successful, the target password will be decoded and displayed in the status area. The target device will automatically be soft-reset to disable the debug mode.



Ointment

Password: weakpassword