@stake
LØpht Research Labs

TBA

Wardialer for the Palm Computing® Platform

Palm Computing® Platform™

Kingpin
kingpin@atstake.com

Handbook for TBA

Kingpin
kingpin@atstake.com

Copyright

Disclaimer and Limitation of Liability

@Stake and L0pht Heavy Industries assume no responsibility for any damage or loss resulting from the use of this handbook.

@Stake and L0pht Heavy Industries assume no responsibility for any loss or claims by third parties which may arise through the use of this software. @Stake and L0pht Heavy Industries assume no responsibility for any damage or loss caused by deletion of data as a result of malfunction, dead battery, or repairs.

Cover Picture

Drawn by Nathan Saliwonchyk, Beanie Products,
http://www.sentex.net/~bracken/beanie.html.

Colored by Kingpin.

Contents

Introduction

TBA, the wardialer for the Palm Computing® Platform, is intended to make use of the portability of Palm™ devices while providing enough functionality to make the tool a viable option for security audits and telephony analysis. By taking advantage of the mobile platform and low cost of the Palm™ devices, one could:

- Provide on-site and in-the-field wardialing.
- Use multiple devices to shorten scan time.
- Hide the device for covert operation.
- Use a more dedicated platform to free up resources.

Wardialing, or scanning, consists of a computer which dials a given set of telephone numbers with a modem. Each phone number that answers with handshake tones and is successfully connected to is stored in a log. By searching a range of phone numbers for computers, one can find entry points into unprotected systems and backdoors into seemingly secure systems.

Brief Overview of Feature Set

TBA sets out to provide functionality to support a wide range of wardialing needs:

- **Activity Logging** to display all information related to the program operation and current scan.
- **Carrier Logging** to keep track of all successfully found computers.
- **Battery Voltage Display** for easy monitoring of the remaining battery life of the Palm™ device.
- **Prefix, Mask and Exclude Mask** specification.
- **Advanced Parameters** allow for fine-tuning of dial and exclude ranges.

- **Date and Time Selection** to start and/or end the scan at a given time.

- **Configuration Options** allow for user-specific preferences to be set related to the scan session, modem, or telephone line.

- **Datafile Manipulation Features** allow for summary, data extraction, status flag replacement, deletion and renaming.

- **Printing of Memo Pad Logs via Infrared** using PalmPrint, a third-party application.

System Requirements and Platform Compatibility

TBA has been tested using the following configurations:

- PalmPilot Personal™, PalmPilot Professional™, Palm III™ series, Palm V™, Palm Vx™, Palm VII™

- PalmOS® 2.0, PalmOS® 3.0, PalmOS® 3.1, PalmOS® 3.2, PalmOS® 3.3

- PalmModem® Accessory (also known as the PalmPilot™ Modem), Palm V™ Modem®

- (Optional) PalmModem® AC Adapter

TBA was developed using Metrowerks Codewarrior® for Palm Computing® Platform on Windows 98/NT 4.0.

TBA does not currently work with PalmOS® 3.5.

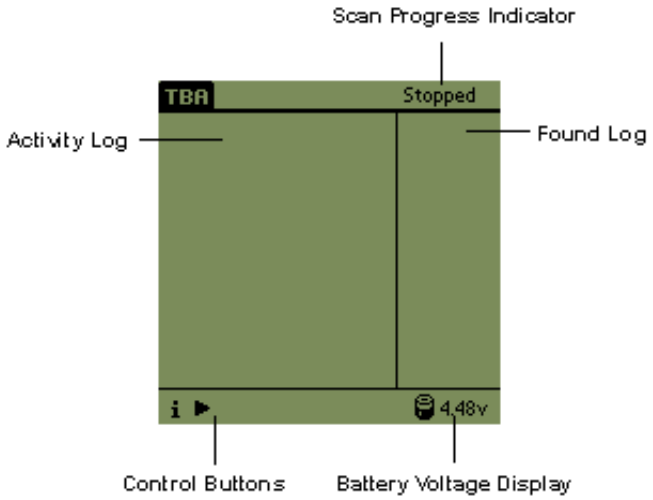
Chapter 1

Main Form

Tap the 

icon from the Palm™ Application Launcher to start TBA.

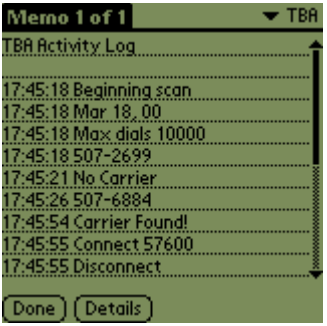
TBA opens with the Main Form, where all wardialing activity takes place.



Activity Log

The Activity Log displays the progress of the current scan and all messages related to program operation. Every dial attempt and result is displayed in this log. Each Activity Log entry is time-stamped with the current time.

All data written into the Activity Log is optionally copied to a Memo Pad memo named "TBA Activity Log" for storage and synchronization to a host PC. Copying to the Memo Pad, which is the default, can be disabled in the Scan Options form (See Scan Options, Chapter 2).



- **Beginning scan.** The wardialing session has commenced.
- **Max dials.** The maximum number of telephone numbers the current scan has to dial. This number is calculated based on the specified dial and exclude ranges (See Basic Parameters and Advanced Parameters, Chapter 3).
- **Scan paused.** The active scan has been paused.
- **Scan resumed.** The paused scan has been resumed.
- **Scan stopped.** The current scan has been stopped.
- **No Carrier.** The "Wait Delay" time has been reached and no connection was made (See Scan Options, Chapter 2). This is the most common response, because of a person answering the phone, other non-computer response, or no answer at all.
- **Busy.** The dialed telephone number is busy.
- **Carrier found!** TBA has successfully connected to a modem at the dialed number.
- **Connect 1200, 2400, 4800, 9600, 14400, 19200, 28800, 38400, 57600, Unknown.** Modem connection speed.
- **Disconnect.** Modem is disconnected after a successful connection.

- **No Dialtone.** The modem did not detect a valid telephone dialtone. TBA continues with the scan and counts the number of times this response happens.

- **No Dialtone Limit.** The "No Dialtone Limit" has been reached (See Scan Options, Chapter 2). TBA will stop the scan.

- **Prefix complete.** When all numbers in the specified range have been wardialed, the scan is complete.

- **No Modem.** TBA was not able to detect a valid Palm V™ Modem® or PalmModem® accessory attached to the Palm™ device's HotSync® port. This is often due to low batteries in the modem. If no modem can be found, the scan will stop.

- **Dial Error.** Dial command error response from the Palm V™ Modem® or PalmModem® accessory. This is most likely due to the dial string being too long for the modem's buffer or containing invalid characters (See Phone Setup and Modem Preferences, Chapter 2).

- **Battery low.** The scan is active and the battery voltage falls below the PalmOS® critically low threshold (See Battery Voltage Display, Chapter 1). TBA will stop the scan.

- **End Time Reached.** The specified time for the scan to end has been reached (See Basic Parameters, Chapter 3).

- **Waiting until <date, time>.** The TBA scan is pending until the specified start date and time have been reached (See Basic Parameters, Chapter 3). When the start date and time have been reached, the scan will begin.

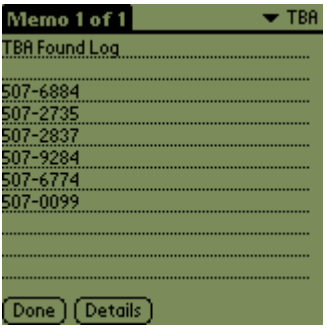
- **Cancelled.** The pending scan has been cancelled.

- **App exit.** The scan is active or paused and the user leaves the TBA application.

Found Log

The Found Log displays the list of carriers – the phone numbers of modems to which TBA was able to connect.

All data written into the Found Log is always copied to a Memo Pad memo named "TBA Found Log" for storage and synchronization to a host PC.



Scan Progress Indicator

This text indicator displays the current operating state of the TBA application.

- **Stopped.** Idle system state. Occurs when no scan is in progress, no scan is pending, and no activity is necessary.
- **Active.** When the scan is active and waiting in between dial attempts. The time to wait in between attempts is specified with the "Call Delay" parameter (See Scan Options, Chapter 2).
- **Dialing.** When the scan is active and the modem is in use.
- **Paused.** The active scan has been paused.
- **Pending.** A scan has been scheduled and TBA is waiting for the specified start date and time before beginning (See Basic Parameters, Chapter 3). During the Pending state, the Palm™ device will not go to sleep. This will deplete battery life during scans scheduled far in the future.

Battery Voltage Display

Displays the current battery voltage of the Palm™ device. When the battery reaches the low battery warning threshold, the scan will stop and PalmOS® will pop-up an alert. The low battery warning threshold is set specific to the type of battery chemistry used in the Palm™ device.

- For devices that use **Alkaline** batteries, such as the PalmPilot Personal™, PalmPilot Professional™, Palm III™ series, and Palm VII™, the threshold is normally set to 2.00V.

- For devices that use internal, rechargeable **Lithium Ion** batteries, such as the Palm V™, and Palm Vx™, the threshold is normally set to 3.76V.

Monitoring the remaining battery life of the Palm™ device makes it easy to know when the batteries need replacing or charging.

Control Buttons

The buttons control TBA actions with the same functionality as a VCR remote control.

Play. Will begin the scan (See Chapter 3, Begin The Hunt). If a scan is pending, this button will immediately begin the scan.

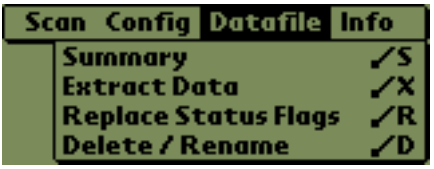
Stop. Will abort the current scan. If a scan is pending, this button will cancel the scan. If TBA is in the dialing state, hold the stylus on the Stop button until the scan stops. The delay is due to the modem being in use.

Pause. Will paused and resume the current scan. Useful when batteries need replacing.

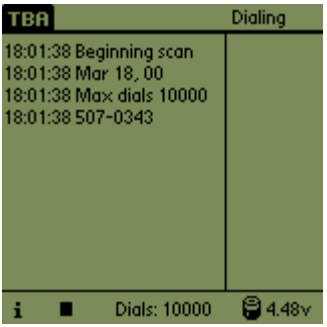
Depending on the current state of TBA, only the necessary buttons will be shown.

Menu Bar

Tapping the "Menu" silkscreen icon on the Palm™ device will bring up the TBA menu bar. All scanning, configuration options, datafile manipulation, printing, and about information can be accessed from the menus.



TBA In Action



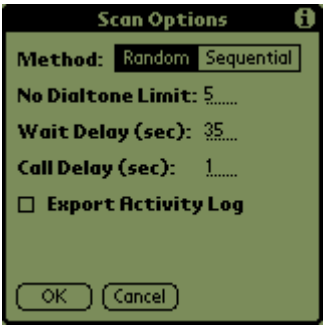
Chapter 2

Configuration Options

TBA has a number of user-specific preferences to be set related to the scan session, modem, or telephone line. This will allow for fine-tuning of a current scan depending on locale, telephone system, and other conditions.

All the preferences are stored on the Palm™ device and will be restored each time TBA is executed. This prevents the user from having to customize the options each time a wardialing session is started.

Scan Options



- **Method.** Configures the scan to dial the numbers in the specified range in either a **random** or **sequential** fashion.
  - **Random** will choose the next number to dial in a random order. No numbers will be repeated.
  - **Sequential** will increment the numbers in a linear fashion (i.e. 0000, 0001, 0002, …).
- **No Dialtone Limit.** The maximum number of "No Dialtone" modem responses which are allowed before the scan is aborted. Range = 0 – 255. Default = 5.

- **Wait Delay.** Length of time, in seconds, of each dial attempt. If a connection is successful within the time frame, a carrier has been found. Otherwise, TBA tries the next number. Be careful to set this delay long enough to support various types of modem handshakes, which vary in length of time. Range = 0 – 255. Default = 35.

- **Call Delay.** Length of time, in seconds, to delay between each dial attempt. Range = 0 – 255. Default = 1.

- **Export Activity Log.** Check the box to enable copying of the Activity Log to the "TBA Activity Log" Memo Pad memo. Default = checked.

Phone Setup

Commas represent 2-second pauses, commonly used to separate groups of numbers, such as when disabling call waiting or before entering a credit card.

"11" serves as a replacement for the "*" key for use with pulse dialing.

- **Dial Prefix.** Numbers that are dialed before the actual telephone number. For example, many offices require that you dial a "9" to gain access to an outside line. If long distance scanning is required, enter the area code in this field.

- **Disable call waiting.** If call waiting service is available on the

telephone line TBA is using, this string will prevent the telephone connection from being interrupted due to an incoming call.

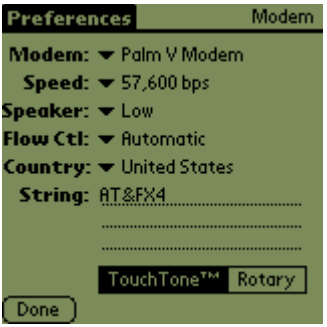
- **Use calling card.** Enables you to use a calling card when wardialing. Useful for when long distance scanning is necessary. Be aware that there often needs to be a delay before the calling card is entered.

To enable any of the options, tap the check box.

Modem Preferences

The Modem Preferences allow configuring settings directly related to the Palm V™ Modem® or PalmModem® accessory. Depending on the PalmOS® version, the Modem Preferences panel will appear differently.

When the Modem Preferences menu item is selected, TBA exits and automatically launches the built-in PalmOS® Preferences application. It is recommended that these preferences be configured at the initial execution of TBA, since the TBA application is exited and the current scan will stop.



The default preferences shown above are the most commonly used for the Palm V™ Modem®. Refer to the Palm V™ Organizer Handbook, Palm V™ Modem® Handbook, or PalmPilot™ Modem Handbook for specific information about the Modem Preferences.

Chapter 3

Begin The Hunt

The Begin The Hunt form is invoked by either the menu bar or tapping the Play button. This form serves to configure the individual wardialing session.

The **Basic Parameters**, shown on the form, allow for general scans to be setup. They consist of the most common features needed for a wardialing session. **Advanced Parameters** are necessary for more detailed specification of dial and exclude ranges.

Basic Parameters

- **Prefix.** The first 3 digits of the target telephone number. The prefix will stay the same throughout the scan session. Range = 000 – 999, Default = 000.

- **Mask.** Specified range of numbers to dial. For example, XXXX will scan 0000 – 9999, 12XX will scan 1200 – 1299. Default = XXXX.

- **Exclude Mask.** Specified range of numbers to be excluded from the scan. Must be a subset of the Mask. For example, Mask = XXXX and Exclude Mask = 12XX will scan 0000 – 9999 with the exception of 1200 – 1299. Default = XXXX, no numbers excluded.

- **Use Advanced Parameters.** Check the box to enable usage of Advanced Parameters. When the checkbox is selected, the Mask and Exclude Mask options disappear (See Advanced Parameters, Chapter 3).

- **Start Date.** Date for the scan to begin. Default = Today.

- **Start Time.** Time for the scan to begin. If no time is specified, the scan will begin immediately. Default = No time.

- **End Time.** Time for the scan to end. If the scan is not complete by the specified end time, the scan will stop. If no time is specified, the scan continue until complete. Default = No time.

Advanced Parameters

The Advanced Parameters are used for tighter control of the dial and exclude ranges. The command set is based on that of ToneLoc, a popular wardialing tool for the PC.

Advanced Parameters are defined within the "TBA Advanced Parameters" Memo Pad memo. TBA does not automatically create this memo - the user will need to create it if it is required.

- **R:xxxx-yyyy** to specify a range of numbers to dial.
- **D:xxxx-yyyy** to specify a range of numbers to be excluded from the scan.
- **D:xxxx** to exclude an individual number from the scan. Useful to avoid known telephone numbers within the scan, such as police and emergency lines.

Dial ranges must be specified before exclude ranges. Multiple commands, as shown above, are accepted in order to further configure the scan. The commands must be in the format above. Incorrect usage may cause unpredictable results.

Chapter 4

Datafile Manipulation

A Datafile is a PalmOS® database that is used to store all of the relevant scan information for a particular wardialing session.

The Datafile is created each time a new scan is started. The Datafile is named with "TBA" and the prefix that is being scanned (i.e. TBA000). If a Datafile of a particular name already exists, TBA will attempt to use that Datafile, preserving the status the already dialed phone numbers. This is useful for continuing a scan that was stopped. If a brand new scan is desired using the same prefix, you can choose to rename or delete the already existing Datafile (See Delete/Rename, Chapter 4).

TBA includes a number of manipulation functions to enable the user to:

- Generate an on-screen report of a selected Datafile.
- Extract specific data of a previous scan to a Memo Pad memo.
- Modify the data of a previous scans.
- Delete or rename Datafiles.

Datafile Structure

- **Prefix.**
- **Mask.** If Basic Parameters are used, the Mask is stored. Because the Advanced Parameters are stored in a Memo Pad memo, dialing and exclude ranges do not need to be stored.
- **Exclude Mask.** If Basic Parameters are used, the Exclude Mask is stored. Because the Advanced Parameters are stored in a Memo Pad memo, dialing and exclude ranges do not need to be stored.
- **Start Date.**

- **Start Time.**
- **End Time.**
- **Status Flags.** The current status of each phone number within the specified dial range. During the scan, the status becomes the result of the dial attempt for each dialed phone number. There are 14 possible Status Flag settings.
    - **Undialed.** The phone number has not yet been dialed for the current scan.
    - **Exclude.** The phone number has been specified to be excluded from the current scan.
    - **Timeout.** No connection was made and the "Wait Delay" has been reached (See Scan Options, Chapter 2). This is the most common wardial response, due to a human answering the phone, other non-computer response, or no answer at all.
    - **Busy.** The phone number returned a busy signal.
    - **Connect Unknown.** Successful connection at an unknown speed.
    - **Connect 1200.**
    - **Connect 2400.**
    - **Connect 4800.**
    - **Connect 9600.**
    - **Connect 14400.**
    - **Connect 19200.**

- **Connect 28800.**
- **Connect 38400.**
- **Connect 57600.**

Saving the Datafile

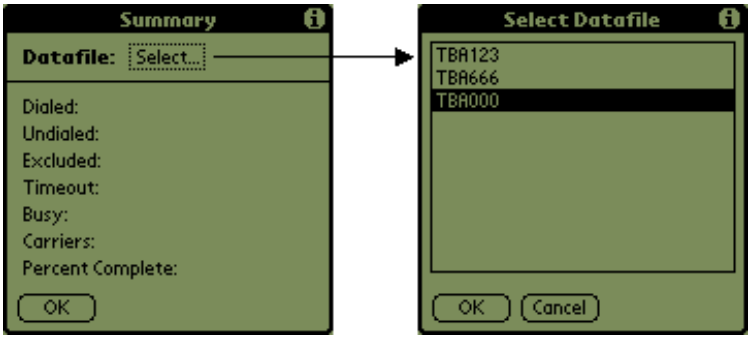
All Datafile saving is transparent to the user and handled by TBA in all situations.

- After every dial attempt during a scan session.
- When the current scan is paused.
- When the current scan is stopped.
- After changes to the Scan Options or Phone Setup have been entered.
- After any Datafile manipulation functions.

Saving the Datafile often will prevent most occurances of data loss and will preserve the data collected from the wardialing.

Summary

The Summary function will generate an on-screen report of a selected Datafile.

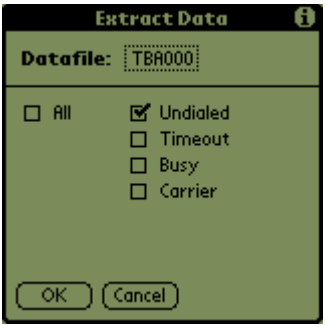


To select a Datafile, tap on the "Select…" trigger. The Select Datafile form will appear and the preferred Datafile can be chosen. Tap OK to accept or Cancel to return without selecting. If no Datafiles exist, tap OK to return.

When a Datafile has been selected, the fields will be filled in with the proper information.

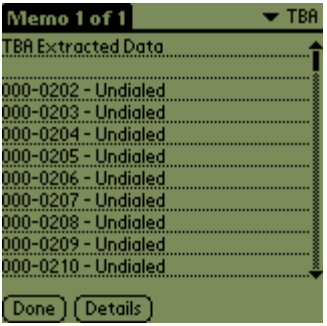
Extract Data

This function will create a Memo Pad memo entitled "TBA Extracted Data" and store the selected information extracted from the Datafile.

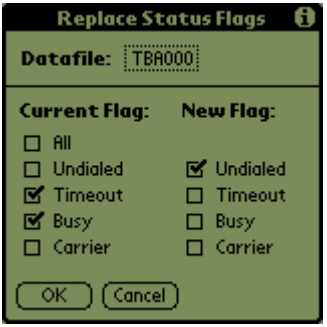


Extracting data is a processor-intensive operation and can take up to two minutes to complete. During this time, a "Working… Please wait…" message will be printed on the screen.

The Extract Data function is useful to generate a list of found carriers if the original Found Log is lost or destroyed. Selecting "All" will generate a streamlined Activity Log showing only the results of the scan, without the messages related to program operation.



Replace Status Flags



This function replaces particular status flags in a Datafile with another. For example, it could be used to replace all Busy numbers with Undialed, so those phone numbers can be redialed.

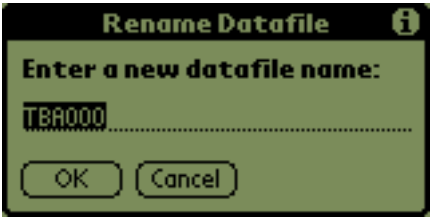
Delete / Rename

This function allows deletion or renaming of the selected Datafile. This is useful to erase old or obsolete scan information to free memory on the Palm™ device. Renaming a Datafile is useful if another scan

with the same prefix is desired. Since the name of the Datafile is based on the prefix, there may be a conflict (See Chapter 4, Datafile Manipulation).

Choose from the list of available Datafiles. Tap Cancel to return without performing any action. If no Datafiles exist, tap Cancel to return.

Tap Rename to rename the Datafile. Enter the desired name in the field. Names must not begin with a space and must not match any existing database name.



To accept the change, tap OK. Tap Cancel to return without making a change. The change will be reflected immediately in the Datafile list.

Tap Delete to purge the Datafile. You will be prompted with a confirmation dialog before the Datafile is deleted. The change will be reflected immediately in the Datafile list.

Chapter 5

Printing Memo Pad Logs

The Print Logs feature is designed for wireless printing of TBA Memo Pad memos with the use of an infrared-equipped (IR) printer.

Those users with access to a PC can simply synchronize their Palm™ device and print the desired Memo Pad memos from the Palm™ Desktop software. The infrared capability adds value to consultants and others that need report printing on-the-fly.

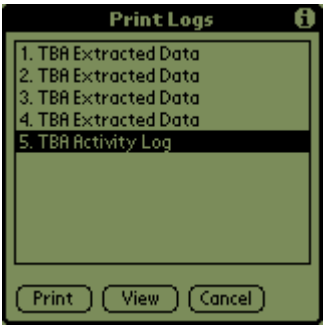
System Requirements

The Printing functionality is achieved with the server side of PalmPrint, a third-party application written by Stevens Creek Software. PalmPrint allows for direct IR and serial printing to a wide variety of printers.

Use of the infrared printing capability requires a Palm™ device with IR support running PalmOS® 3.0 or greater. PalmPrint supports the Palm III™ series, Palm V™, Palm Vx™, Palm VII™.

.

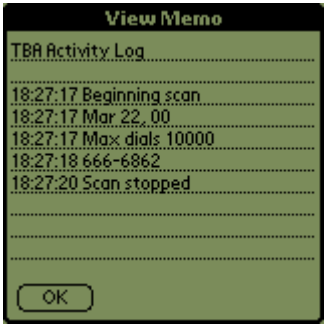
Usage



The list consists of all Memo Pad memos with "TBA" as part of the title. This is done to prevent non-TBA-specific memos from

appearing. To print other memos that are not related to TBA, simply use PalmPrint as a stand-alone application.

Choose from the list of available TBA Memo Pad log files. Tap View to look at the first page of the Memo Pad. This can be used to verify that the proper memo has been selected before it is printed.



Tap Print to begin the print session or Cancel to return without printing. If no Datafiles exist, tap Cancel to return. TBA will launch PalmPrint and print the selected log file based on the PalmPrint configuration.

If the PalmPrint application is not available on the Palm™ device, a dialog will notify the user and printing will not take place.

For more information on the specifics of PalmPrint, how to configure it, and its various uses outside of TBA, refer to the Stevens Creek Software web site, http://www.stevenscreek.com.

Appendix A

Additional Reading

1. Kingpin, "Wardialing Brief", March 2000, http://www. atstake.com.
2. L0pht Heavy Industries Palm™ Resource Web Page, http://www. L0pht.com/~kingpin/pilot.html.
3. Stevens Creek Software PalmPrint Web Page, http://www. stevenscreek.com/pilot/palmprint.shtml.
4. Palm, Inc. Web Page, http://www.palm.com.
5. Palm, Inc., "Palm V™ Organizer Handbook", 1999
6. Palm, Inc., "Palm V™ Modem® Handbook", 1998
7. 3Com Corporation, "PalmPilot™ Modem Handbook", 1997

AtStake, Inc.
One Kendall Square
Building 200
2nd Floor
Cambridge, Massachusetts 02139
United States of America

Web site
http://www.atstake.com