555-006-702
Issue 1
May 1993

HackerTracker for CAS for Windows

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, AT&T can assume no responsibility for any errors. Changes and corrections to the information contained in this document may be incorporated into future reissues.

Your Responsibility for Your System's Security

You are responsible for the security of your system. AT&T does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. AT&T will not be responsible for any charges that result from such unauthorized use. Product administration to prevent unauthorized use is your responsibility and your system administrator should read documents provided with this product to fully understand the features available that may reduce your risk of incurring charges.

Ordering Information

The ordering number for this document is 555-006-702 To order this document, call the AT&T Customer Information Center (CIC) at 1-800-432-6600 (in Canada, 1-800-255-1242). For more information about AT&T documents, refer to the Business Communications Systems Publications Catalog (555-000-010).

Trademarks

HackerTracker is a trademark of MOSCOM Corporation

Hayes is a registered trademark of Hayes Microcomputer Products, Inc.

Intel and SatisFAXtion are trademarks of Intel Corporation

MS-DOS is a registered trademark, Windows is a trademark of Microsoft Corporation

WinFax and WinFax PRO are trademarks of Delrina Technology, Inc.

HackerTracker™ for CAS for Windows™

HackerTracker is an easily installable enhancement to your call accounting software, designed to help you stop fraudulent use of telephone switches in your network.

How does “switch fraud” happen?

Switches with auto attendant or remote access lines are common targets of toll theft. One scenario is a hacker’s computer dialing into a switch and trying thousands of dial-out codes; codes that work are then used or sold. Like corporate secrets, there are many other ways to steal authorization codes — the unfortunate result is an astronomical phone bill for switch owners.

How can the HackerTracker System help?

- Stop the hacker. You can monitor switch facility or authorization code usage and receive alarms in time to shut down facilities before codes are broken.
- Reduce liabilities. You can monitor long distance calls by the hour and detect abuse early enough to change codes and keep damages to a minimum.
- Give peace of mind. You can do quick status checks from your PC to keep informed on how secure your switch is.

This guide helps you set up HackerTracker to work with your call accounting system and perform the functions described above.

Installation

1. From the CAS **Utilities** menu, select **Upgrades**.

2. Select the drive and insert the HackerTracker diskette. Choose **OK** and follow prompts to continue.

3. When complete, remove the diskette from the drive and proceed to *Setting Up*.

   You will notice the new HackerTracker icon: 

Setting Up

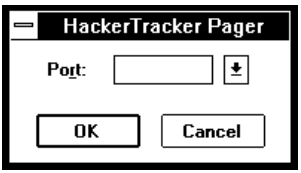
This section describes how to configure HackerTracker features. We suggest that you become familiar with your calling patterns (the Call Distribution and Facility Reports will help you to do so), then use HackerTracker to monitor possible problem areas:

- facilities dedicated to long-distance or remote access
- authorization codes susceptible to abuse
- dialed numbers to areas where you conduct little or no business, but have appeared on reports

To report alarms by pager, use any Hayes-compatible modem; to FAX alarms, use the Intel SatisFAXtion board and WinFax PRO (version 3.0) software. All devices must be already installed.

For a pager, select **HackerTracker Pager** from the **Configuration** menu.

When the dialog box appears, select its *port* and choose **OK**.

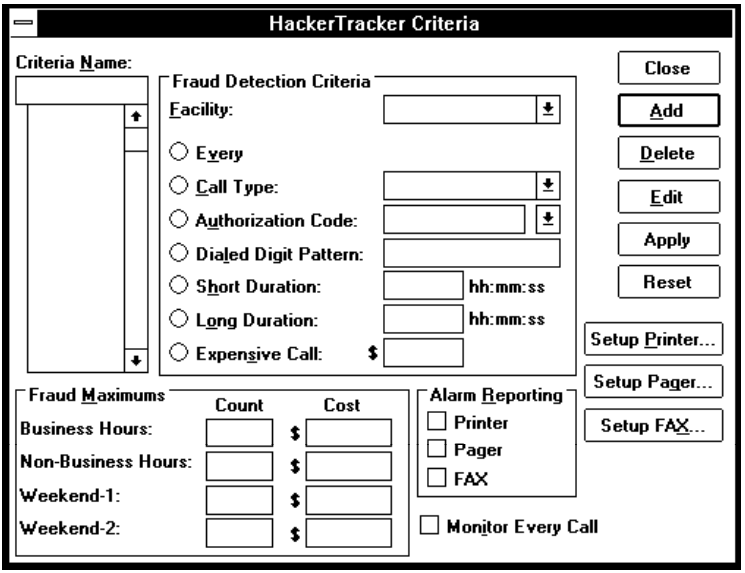


Alarm Criteria

You can set criteria for up to 20 alarm events — hourly count and cost limits on facility usage, call types, authorization codes (if reported by your switch), dialed numbers, long or expensive calls — and how to report them by printed message, FAX, or pager.

1. In a multi-site system, select the site to monitor (use **Site Selection**, under **Administration**).

2. From the **Administration** menu, select **HackerTracker Criteria**.



3. For a new entry, choose **ADD**; for changes or deletions, select a criteria name, then choose **EDIT** or **DELETE.**

4. For additions or edits, complete the dialog box.

To report alarms by printer, pager or FAX, first choose its setup button (see the procedures ahead) and return to complete the dialog box.

Criteria Name. The identifier (up to 7 characters) for this set of alarm conditions.

Fraud detection criteria. A *facility* (select a specific name or "(ALL)") and one item from the following list:

- — *every* (all calls using the named facility)
- — a *call type* from the selection list
- — an *authorization code* from the selection list (these are associated with extensions in the *Organization Table*) or a pattern that matches one or more existing codes (patterns are represented by digits and/or wild cards “?” = single digit or “%” = any number of digits).
- — a *dialed digit pattern* represented by digits and/or wild cards (include toll code, if any) — for example, **1809%** (Caribbean), **0115%** (Mexico, Central & South America), **0118%** (Asia and the Far East), **0119%** (Middle East & Indian Subcontinent).
- — calls under a *short duration* (in hours:minutes:seconds) or over a *long duration* (in hours:minutes:seconds) or *expensive call* (in dollars and cents).

Fraud maximums. The hourly *count* and *cost* limits during the *business* and *non-business hours, Saturdays* and *Sundays* set in your **Workweek** (under **Customization**). Exceeding any one of these limits triggers an alarm.

Alarm Reporting. Enable [X] or disable reporting alarms via the *printer, pager,* and/or *FAX* to be specified in step 5.

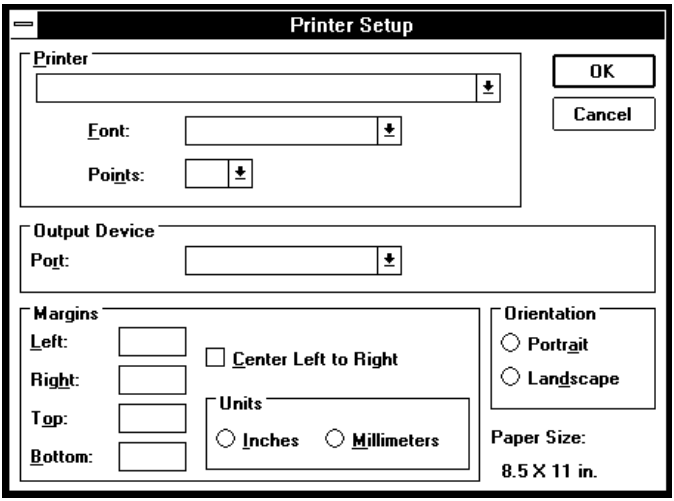
Monitor every call. Enable [X] or disable logging every call that matches the criteria (normally, only the call that trips the alarm is logged). This is useful when analyzing fraud patterns after an alarm, particularly if the criteria is *authorization code* or *short duration* .

5. When complete, choose **APPLY** (**RESET** cancels changes), then **CLOSE** to exit.

Do not shutdown CAS nor halt call rating after setup. HackerTracker can only work while CAS is rating calls.

Printer Setup

1. From the HackerTracker Criteria dialog box, choose **SETUP PRINTER**.



2. Complete the dialog box:

   Printer and Output Device. Select the *printer*, *font*, *point* size, and *port* from their list boxes.

   Margins. Set the spacing on the page:

   — Center Left to Right enables automatic left-right margin setup, resulting in a report centered on the page.

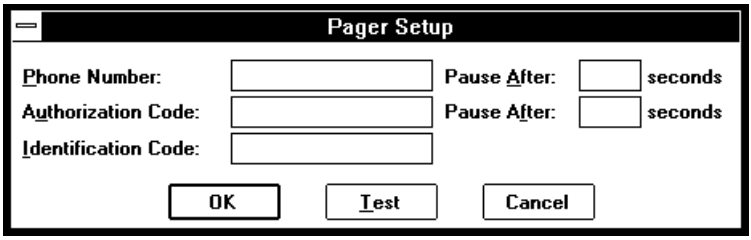
   — Left, Right, Top, Bottom sets margin *size* (in the specified unit = *inches* or *millimeters*).

   Orientation. Select *portrait* or *landscape* printing.

3. Choose **OK** to accept your entries (**CANCEL** discards them) and return to the HackerTracker Criteria dialog box.

Pager Setup

1. From the HackerTracker Criteria dialog box, choose **SETUP PAGER**.



2. Complete the dialog box:

   Phone Number and Pause after __ seconds. The *dialed pattern* to reach the pager or pager service, then the *pause* (in seconds) before dialing the authorization code (below).

   For the phone number, use the letters "T" (tone) or "P" (pulse), digits, and commas "," (pause) as required. For example, **T9,5551212** uses touch tone to dial 9, wait, then 555-1212.

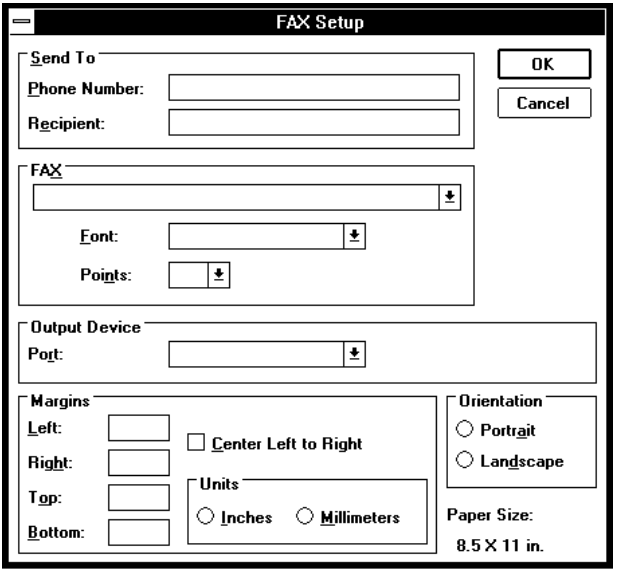
   Authorization Code and Pause after __ seconds. The *dialed code* you must provide to use the service, then the *pause* (in seconds) before dialing the identification code (below).

   Identification Code. The identification or notification number of the pager you want to reach.

3. Choose **OK** to accept your entries (**CANCEL** discards them) and return to the HackerTracker Criteria dialog box.

FAX Setup

1. From the HackerTracker Criteria dialog box, choose **SETUP FAX**.



2. Complete the dialog box:

   Send To. The *phone number pattern* to reach the FAX of interest and the name of the *recipient.*

   For the phone number, use the letters "T" (tone) or "P" (pulse), digits, and commas "," (pause) as required. For example, **T9,5551212** uses touch tone to dial 9, wait, then 555-1212.

   FAX and Output Device. Select the name of the FAX modem, *font*, *point* size, and the FAX modem's *port* from the list box.

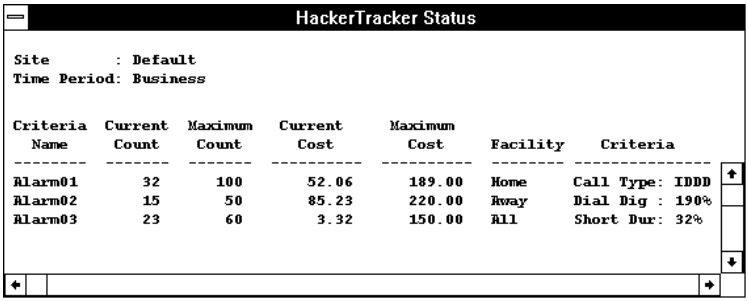
   Margins and Orientation. Select options as in the Printer Setup.

3. Choose **OK** to accept your entries (**CANCEL** discards them) and return to the HackerTracker Criteria dialog box.

Checking HackerTracker Status

After setting up your alarm criteria, you may check system status by selecting **HackerTracker Status** under the **Utilities** menu:

A window similar to the one below appears.



Every alarm criteria defined for the named site will be listed ("`Criteria Name`" = "`ALARM TYPE`" in an alarm message).

— The `Current` (hourly) `Count` and `Cost` show statistics on calls matching the named `Facility` and `Criteria`.

— `Maximum Count` and `Cost` correspond to the *fraud maximums* for the time period currently in effect.

Checking HackerTracker Alarms

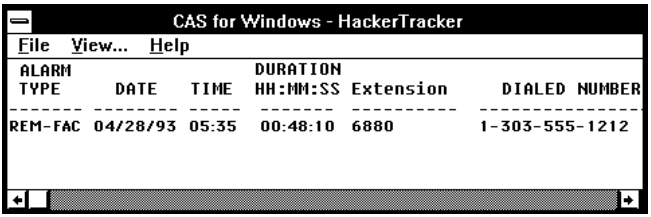
If one of the calls you are tracking trips the count or cost limit for its type, an alarm occurs:

- The HackerTracker normal icon changes into: 
- A detailed record of the call that tripped the alarm is logged.
- Copies of the call record are sent to the enabled devices.

Alarm-tracking statistics are reset to zero and monitoring resumes.

The HackerTracker log can keep up to 1000 records, listed from most recent to oldest. To investigate an alarm (or any time you wish to view the HackerTracker log), proceed as follows:

1. At the PC, select the HackerTracker (alarm or normal) icon or **View HackerTracker** from the **Listings** menu.



   a. If “Monitor every call” is disabled for the alarm type of interest, note the date and *time* and close the window. Proceed directly to step 2.

   b. If “Monitor every call” is enabled, all calls matching its criteria appear — an asterisk (*) marks calls that contributed, but did not trip the alarm.

      Select **View**, then the *alarm type* of interest. To obtain a printout, select **File**.

      Close the window and proceed directly to step 3.

2. Obtain the set of calls that contributed to the alarm:

   a. Open the **HackerTracker Status** window (see *Checking HackerTracker Status*). Note the specific *criteria* for the *alarm type* that you are investigating.

   b. Run a Selection Detail Report. Use as selection criteria:

      — Time range of 1 hour, ending at the time of the alarm

      — *Trunks* belonging to the facility tracked

      — The other alarm criteria used (except for *authorization codes* or *short duration*)

3. When the report prints, check it carefully looking for patterns that would indicate possible fraud.

4. If necessary, administer the switch to change facility restriction levels or shut down compromised facilities.

HackerTracker Tip

Use CAS reports as "passive" switch security monitors. For example, use **Schedule Reports** to set up the following:

Report Group: HackerTracker #1 (Frequency = daily)

Add report	Set criteria	
Selection Detail	Call type = IDDD	Date range = *today*
Selection Detail	Minimum cost = $10.00	Date range = *today*
Selection Detail	Min. duration = 0:30:00	Date range = *today*

Report Group: HackerTracker #2 (Frequency = weekly)

Add report	Set criteria
Selection Detail	Date range = *next Sat. & Sun.* (Weekend calls)