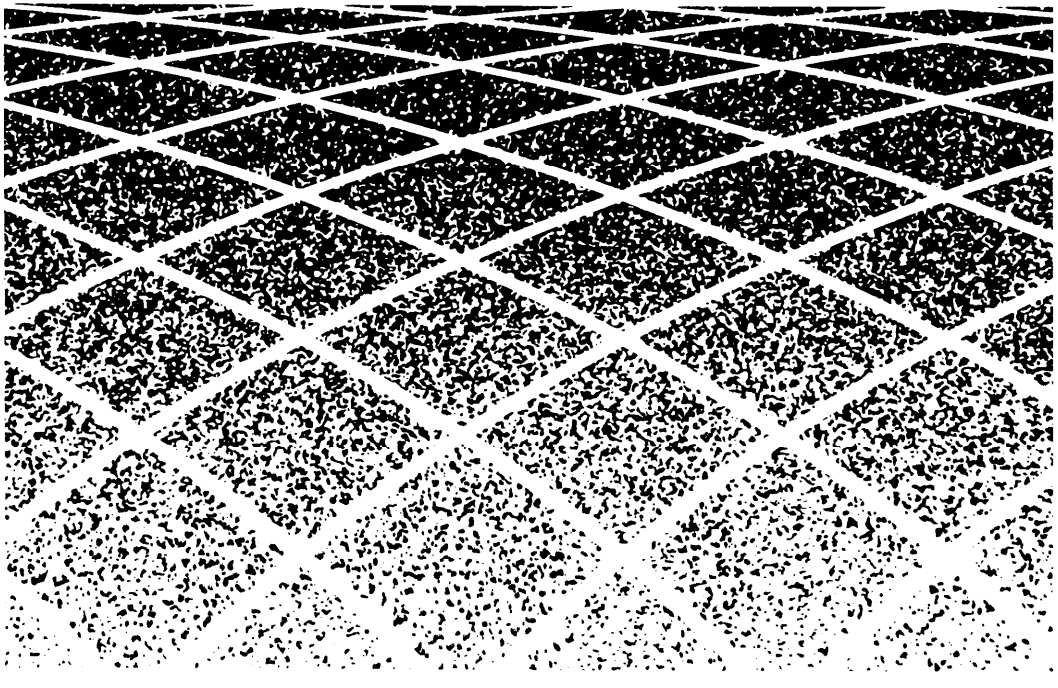
AT&T

HackerTracker™ for Integrated Solution CAS

User's Guide



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 all documents provided with this product to fully understand the features available that may reduce your risk of incurring charges.

Trademarks

HackerTracker is a trademark of MOSCOM Corporation
Integrated Solution CAS and AUDIX Voice Power are trademarks of AT&T

Support Telephone Numbers

AT&T provides atoll-free customer help between 8AM and 5 PM. In the U. S., call the AT&T National Technical Support Center (NTSC) at 1-800-628-2888 if you need assistance when installing, programming, or using your system.

Ordering Information

The ordering number for this document is 585-247-122. 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).

HackerTracker for Integrated Solution CAS

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

How does “switch fraud” happen?

Switches with auto attendant, voice mail, 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 HackerTracker help?

- Stop the hacker. You can monitor facilities or authorization code usage, and receive alarms in time to shut down facilities before codes are broken.
- Reduce liabilities after a security breach. 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 setup daily reports to keep you informed on how secure your switch is.

This guide helps you set up HackerTracker to work with Integrated Solution CAS and perform the functions described above.

Overview

HackerTracker is designed as an active and a passive tool for reporting “suspicious” call activity:

- Its active role consists of monitoring calls soon after the switch sends them to CAS and generating an alarm if one of the calls you are tracking trips the count or cost limit for its type. You can select up to 20 alarm criteria to track calls.
- Its passive role consists of generating four daily Selection Detail Reports for international, Caribbean, lengthy, and expensive calls and one weekly report for weekend calls. You can change selection criteria as future needs are defined.

What criteria should you set for alarms?

You can monitor calls by area code, call type, authorization code, and/or by facility. As you become familiar with your calling patterns, decide what calls to track (use the Area Code and City/State Summaries and the Trunk Group Busy Hour Reports to help you).

For example, if your switch uses authorization codes, track those that have been compromised or are susceptible to abuse. If you conduct little or no business on areas that appear on reports, monitor these area codes. If international calls area problem, look for call type IDDD (see the tips shown later in this guide). If you have facilities dedicated to long-distance or remote access, track them.

Next, set hourly count and cost limits for calls matching the criteria during business and non-business hours and on weekends. Reaching either limit generates an alarm.

Upon an alarm, a message is sent to the CAS printer and to a log; AUDIX Voice Power is notified to place a message into a mail box.

To investigate an alarm condition, generate a Selection Detail Report for the past hour. Then, if necessary, administer the switch to change facility restriction levels or shut down its trunk group.

Installation

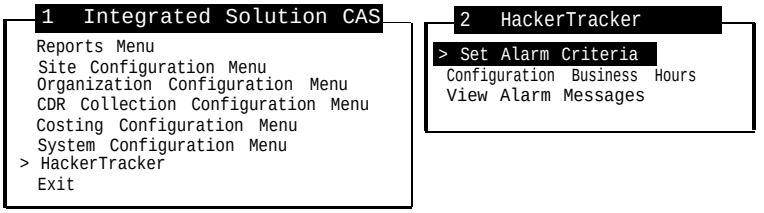
1. From the Integrated Solution CAS menu, select **System Configuration Menu,** then, **Install Update.**

2. Load the HackerTracker diskette in the drive and follow screen instructions to continue.

   NOTE:
   Be prepared to provide the `root` password.

3. When complete, exit, then re-enter CAS.

   `HackerTracker` appears as an Integrated Solution CAS menu option (see below). Proceed to *Setting Up.*



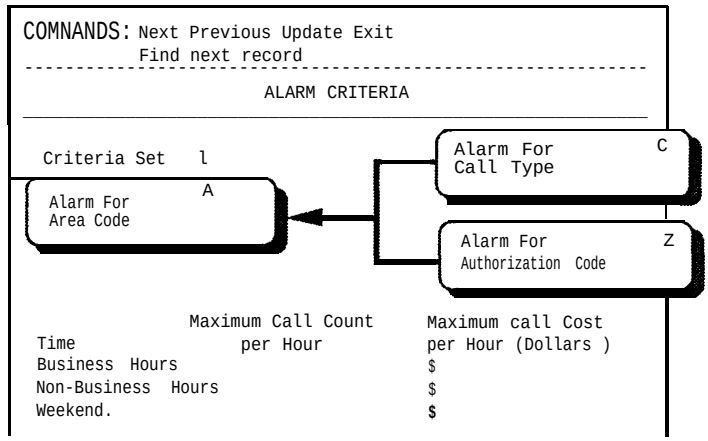
Setting Up

1. From CAS main menu, select **HackerTracker,** then **Set Alarm Criteria.**

   A screen similar to the one shown on the next page appears on display.

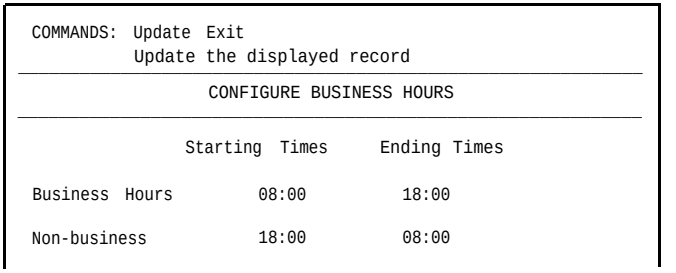
2. Press <U>pdate to set values as in the list that follows.

3. When complete, press <ESC>, then <E>xit.



- `Alarm For.` The calls to track on the named facility (below):
  - — The <A>rea code named in the associated field.
  - — The <C>all type named in the associated field.
  - — The authori<Z>ation code named in the associated field. Used only with switches that report *authorization codes.*
  - — <E>verything.
  - — <N>othing (to disable this criteria set).
- `Facility.` A facility from the Telephone System Configuration that you wish to monitor or a blank (all facilities).
- `Maximum Call Count` (and `Cost) per Hour.` Alarm-triggering limits (count = 0 to 9999; cost= `0` to `32000` dollars) for these time periods:
  - — `Business` (and `Non-business) Hours.` The hours, Monday to Friday, defined by the `Configure Business Hours` option.
  - — `Weekend.` Saturdays and Sundays.

4. From the HackerTracker menu, select **Configure Business Hours.** A screen similar to the one below appears on display.



5. Press <U>pdate to enter the *starting times* of the Business and Non-business hours as *hours:min,* in a 24-hour format. Enter the same time on both fields to set the entire day as business hours.

   When complete, press <ESC>.

6. To end the procedure, press <E>xit.

HackerTracker Tips

Create new call type names for use as alarm criteria by (1) adding the names as new facilities in the Telephone System Configuration of Integrated Solution CAS, then (2) using Dialed Digit Processing (DDP) to associate them to dialed patterns.

For example, you may flag calls to specific world zones and/or countries that are not part of your usual calling patterns:

DDP Search for	Set call type	Comments
0115%	S-AM	Mexico, Central & South America
01158%	VNZLA	Venezuela
0118%	ASIA	Asia and Far East
011880%	BGLSH	Bangladesh
0119%	MEAST	Middle East & Indian Subcontinent
01192%	PAKIS	Pakistan

HackerTracker Reports

HackerTracker has enhanced the CAS Schedule Reports feature as follows:

- Five new reports with report codes SR26 through SR30 are preset as Selection Reports with the default values in Table 1 (below).
- The additional reports brings the total Schedule Reports to 150, and the number of Selection Reports to 30.

Consult your CAS documentation if you wish to change the schedule, selection criteria, and output for these new reports.

Table 1. HackerTracker Scheduled Reports

Schd. Rpt.#	Rpt. Code	Report Name	Freq.	Run Time	Selection Criteria
146	SR26	INTERNATIONAL CALLS	D (daily)	06:00 AM	Call type= IDDDD Date=today
147	SR27	EXPENSIVE CALLS	D (daily)	06:15 AM	Cost ≥ $10.00 Date=today
148	SR28	LENGTHY CALLS	D (daily)	06:30 AM	Duration ≥ 0:30:00 Date = today
149	SR29	CARIBBEAN CALLS	D (daily)	06:45 AM	Dial no. = 809% Date = today
150	SR30	WEEKEND CALLS	W (Mondays)	07:00 AM	Date = next Saturday and Sunday

NOTES:

— Reports are set to run using output method= append and output device = report *n*. out (where *n* = schedule report number). To retrieve these reports, use the CAS View Reports function.

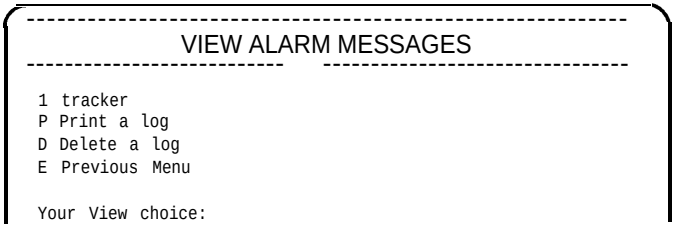
— Date ranges remain unchanged until reports run; at that point, dates are moved ahead by the frequency (that is, one day or one week),

Accessing Alarm Messages

HackerTracker can store up to 500 messages in its alarm log files. These files are accessed and maintained very much like the CAS view logs and reports functions.

The log `'tracker"` contains the most recent alarm messages. Should the file grow larger than 50K, the system creates up to 3 file extensions (`"tracker. 1"` to `"tracker. 3")` with newer data displacing older data into the next extension. The oldest data from `"tracker. 3"` is written over.

1. From the main menu, Select **HackerTracker,** then **View Alarm Messages.** A screen similar to the one below appears on display.

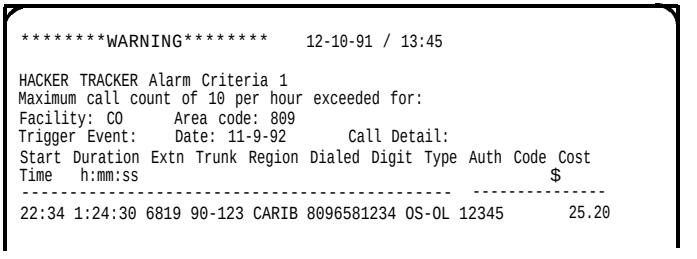


```
VIEW ALARM MESSAGES

1 tracker
P Print a log
D Delete a log
E Previous Menu

Your View choice:
```

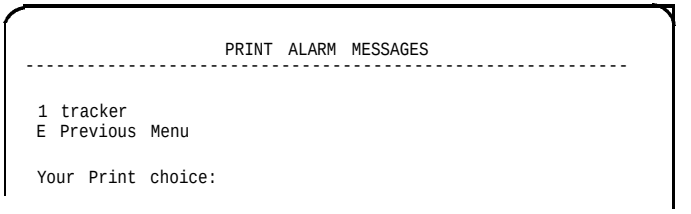
2. To display the alarm messages contained in a log, enter the log's menu number. A sample alarm message appears below.



```
********WARNING********    12-10-91 / 13:45

HACKER TRACKER Alarm Criteria 1
Maximum call count of 10 per hour exceeded for:
Facility: CO      Area code: 809
Trigger Event:    Date: 11-9-92       Call Detail:
Start  Duration Extn Trunk Region Dialed Digit Type  Auth Code Cost
Time    h:mm:ss                                              $
-------------------------------------------  ---------------
22:34 1:24:30 6819 90-123 CARIB 8096581234 OS-OL 12345       25.20
```

3. a. To print a log's contents, enter **P ;** to delete the entire log's contents, enter **D.** A screen similar to the one below appears on display.



b. To proceed with printing or deleting a log, enter its menu number and follow further screen instructions.

AUDIX Voice Power Alarms

Upon an alarm, HackerTracker sends the following message code to the AUDIX Voice Power application:

`ht_cr_` ***n*** (where *n* corresponds to alarm criteria *n* = 1 to 20)

The AUDIXI application uses this code to place a prerecorded voice message into a mailbox and/or place a pager call. We suggest the following voice recording:

> "HackerTracker has alarmed on criteria ***n.*** Potential fraud has occurred. Please retrieve the alarm message from the CAS application and determine the specific conditions which generated the alarm. "

Messages, mailbox selection, and/or pager functions are configurable within the AUDIX application. For assistance, refer to its documentation or call your technical support organization.