trol panel and any Remote control panel that allows you access means that you can back up any attached storage devices to DAT (or whatever media you use). Backups can be restored to any computer, not just the one the data was backed up from.

2. Not activating Remote control panels. An unauthorized person could find unactivated control panels, enter an activator code, backup the hard drive to DAT, and then in the Network remote configuration, deactivate the control panel when finished. This would more or less restore the control panel to its virgin state. There is access to about five computers in this state.

3. Makes owner and hard drive names available on network. By using the Retrospect Remote server, a user can look at all of the owner names of any computer with the Remote control panel, even without knowing the security code. Because these owner names may not be the same as the machine names listed in the Chooser, they can be used to try the file sharing entrances explained above: owner name with blank password, owner name with machine name as password, vice versa, etc. Listings in the server's Network remote configuration that you do have access to will also allow you to see the name of the startup drive and any other attached drives. These names are also fodder for user name and password guessing.

Appletalk Remote Access (ARA)

Appletalk Remote Access allows a Macintosh to dial into an Appletalk network. It gives the user access to servers, email, printers, and any other network functions the same as if the user was in the office connected via Ethernet.

Where The Mistake is Made with ARA

A company has to go out of their way to allow ARA to access the network. At least one version of ARA allows users to save their passwords in the configuration file. You might be surprised at how many users prefer to save their password and take the chance rather than have to enter the password every time they log onto the network. That means that if you can get an ARA configuration document with the saved password, then you can access the network at will; the document already contains the user name and phone number, so all the secrets are out and nothing more is required. PowerBooks, as an example, are especially susceptible to the saved config file and the other methods described in this article for the simple reason that they are probably the most stolen computer in America by percentage.

Programs That Give You An Edge Over Nosey Parkers

I have found these two programs to be useful in monitoring security on my network.

Network Security Guard 3.1, http://www.mrmac.com/ for demo version. Lacks elegance and looks, but is effective. Does bulk password throwing at any shared drive on the network. Checks for the file sharing weaknesses mentioned above, uses dictionaries, lists files available, lists suspicious configurations available on a network. Saves everything in reports. Serious program for protecting yourself from attacks, but can also be used against you. When used it hogs all available processing power, so a dedicated Mac is good. You will want to run it during the day when computers are turned on and the network is at its most active.

Lookout! by Pace Bonner & Jeff Amfahr, PB Computing, distributed by Trik, Inc. at 800-466-TRIK, http://www.pbcomputing.com/. Part of the Nok Nok Package of AppleShare monitoring and control software. This control panel indicates in the Chooser next to the machine names whether guest access is enabled and what kind of filesharing is enabled. Makes checking each listing for guest access much faster, particularly on a large network.

CRAFT ACCESS TERMINAL

by Local Loop

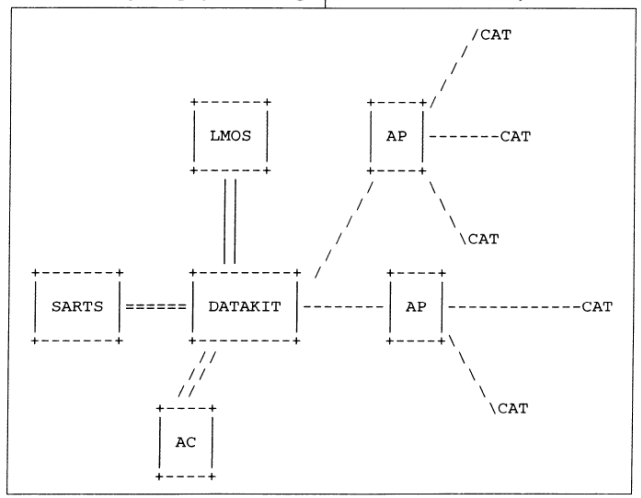
Aside from the butt sets, phone techs (linemen, splicers, etc.) also carry something known as CATs. Yellow handset lookalikes. They have been out for a while now and almost all of you have probably seen them. The regular TS-21 type handsets have almost faded as the CATs can do everything a TS type handset does and more! In this article I will briefly introduce the System, List the menus attained, and describe the sequence of events occurring when testing, etc. Here it goes.

CAS Test Site

Let's start with CAS (Craft Access System). CAS is a network of computers that provides the technician in the field direct access to the operating systems through hand-held computer terminals known as CATs. A tech can use CAT to perform various functions like dispatch, closeout, and testing, etc. Before CATs were introduced, dispatches and testing were done by calling into the dispatch office or the CO for various testing. This network of computers includes computer systems like LMOS HCFE (High Capacity Front End) and SARTS (lovingly called FARTS).

The CAS includes the AC (Administrative Computers) and the APs (Application Processors) which are directly linked by phone to CATs. Refer to the diagram below for the total picture:

The AC provides security, keeps a history of current jobs, handles disk storage functions and downloads information to the APs. The APs are usually located in the



COs, manage craft access dial-in lines (in other words, this is where the tech dials in using his CAT), software etc. Each AP can hold about 15 APM (Modules) and each of these APMs can have five dial-in lines accessed by a hunt group number sequence.

The connections between DATAKIT and the other host machines like APs and AC are synchronous. This network also supports LMOS/MLT (Mechanized Loop Test) for testing POTS (plain old telephone service).

The CAT, yellow in color, has a joystick below the terminal screen. See below:

```
        BACK
H        _       N
E       (_)      E
L                X
P                T
     REVIEW
```

In the above diagram (self explanatory), move as you wish.

Menus on the CAT

There are 14 main job screens or menus that can be accessed on the CAT. Here they are as follows:

LOOK AT LINE RECORD
From the Main Menu select:
1. work on current job
2. other test menu
3. look at line record

REARRANGE BULK LOAD
From the Main Menu select:
1. other
2. reorder bulk jobs
3. update sequence

RETURN INCOMPLETE
From the Main Menu select:
1. close or return
2. return incomplete
3. other

TROUBLE CLEARED IN CO
From the Main Menu select:
1. close or return
2. return menu options
3. return to CO

TEST OK
From the Main Menu select:
1. close or return
2. test ok

(Loyal telephone customers must agree that service is now OK.)

TROUBLE ISOLATED IN CO
From the Main Menu select:
1. close or return
2. return menu options
3. return to CO

(This is when the tech says, "I am sorry sir, further work will be required on your line."

PAIR CHANGE
From the Main Menu select:
1. close or return
2. return to menu options
3. return incomplete
4. pair change-CO work to be done

This is when Cable Pair Change is necessary to rectify the problem.

RETURN TO CABLE
From the Main Menu select:
1. close or return
2. return menu options
3. return to cable

LOCATE TWO SIDED FAULT
From the Main Menu select:
1. work on the current job
2. locate fault
3. verify fault
4. verify good pair
5. locate 2 sided fault

TONE ON LINE
From the Main Menu select:
1. work on current job
2. get tone or MDF
   DROP TONE WHEN DONE
   1. work on current job
   2. other test menu
   3. drop tone, locate, coin, or MDF

CHECK COMMITMENT DATE
From the Main Menu select:
1. close or return
2. no access

LOCATE ONE SIDED FAULT
From the Main Menu select:
1. work on current job
2. locate fault
3. verify fault
4. locate one-sided test

LINKED JOB

Go to review mode (move down and press joystick down), select dispatch. Techs use this to link other jobs together. They may select it or refuse.

USING CO SHOE TAG
From the Main Menu select:
1. work on current job
2. get tone or MDF
3. get MDF access
4. let MLT pick shoe

CAT - Sequence of Events when testing

1) Techs hook up the T and Ring on any block and use CAT to "receive new job" from the dispatch office. Techs dial into the CAS using a 4 digit passcode. The passcodes are sometimes written on the CAT (e.g., 4432 etc.)

The CAT's serial number and the 4 digit code are linked, so when the tech calls into the CAS APs, the serial number along with his XXXX code are matched.

So the next time you decide to steal a CAT, make sure it's on a Friday. This way, you can have fun with it on Saturday and Sunday. On Monday, when the tech informs the dispatch office, the passcode will die. However, the CAT will still keep giving you "bogus" menus. The CAT now is basically useless. The telephone company may trace you to the number the CAT is being used on. Since the CAT is officially useless, don't bother using it.

2) The circuit information for the circuit problem will already be prepared for the troubled circuit. The field tech, lineman, or whoever will then initiate the access request.

3) SARTS interface relays the circuit access and initiates the far-end to access in the same way as an access coming from a 52A TP (Test Position which is a stationary terminal that has access to SARTS). One major difference is that TSV (Test Status Verification) commonly known as monitoring lines, is not permitted on the CAT.

4) Once the circuit has been accessed and found idle, the tech may perform various tests.

5) The Far-end (like RTS - Remote Testing System - which is used with SMAS) performs the requested tests and sends the results back to the SARTS.

6) The SARTS sends results to DATAKIT and to AP.

7) AP sends the results to CAT display.

Some CAS Dial-ups

(718) 523-1177
(718) 657-4650
(718) 658-1666