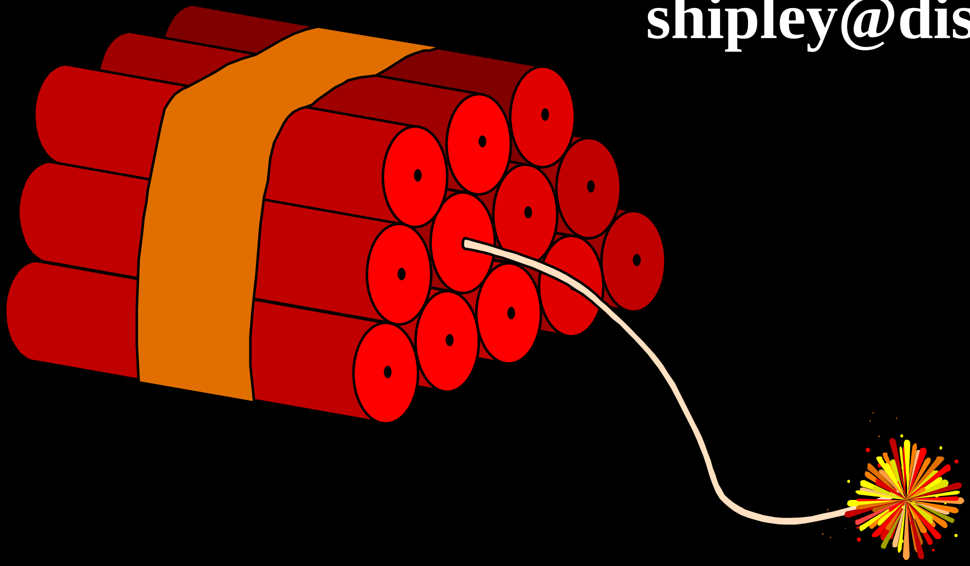
Wardialing

Peter Shipley
shipley@dis.org



Introduction

While it is common knowledge there are many security risks related to modem dialup access. There are relatively few (if any) published reference material on the subject.

So I figured I would change that.

What I Found

Things are worse then I expected.

Internet connectivity and modem connectivity are equally insecure.

Sysads do not care.

Non-IP based networks are more open

Areacodes Covered

I had posted to various security email lists asking if anyone is interested in scanning parts of their area for me, but did not receive any reasonable responses.

Thus the data is based from the San Francisco / Bay Area only

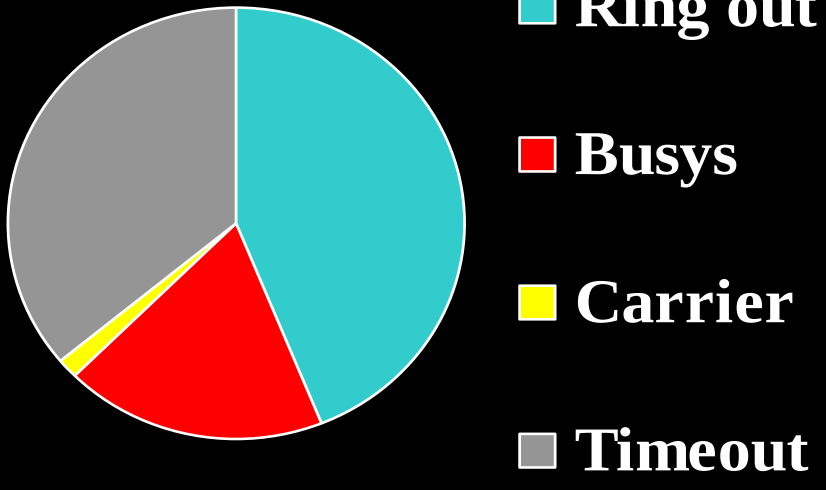
Areacodes Covered

- 408 - San Jose
- 415 - San Francisco *
- 650 - Sunnyvale / Palo Alto / Etc...
- 510 - Berkeley / Oakland *
- 707 - North-Western California
- 925 - Concord (East of Berkeley)

* majority of effort was made on these areas

Some Stats

- 1.01% Carrier
- 18.4% Busy
- 44.2% Ringouts
- 36.3% Timeouts



571 exchanges so far “scanned”

Modem Statistics

- A majority of dialups “greet” the user with a “welcome” message
- Less then 2% warn away possible intruders (no-trespassing)
- A majority of dialins overly identify themselves (OS version, Ownership, location)

Modem Statistics

On average an exchange has 94 modems

The highest percentage of modems in a exchange is 6.1% (top 10 range from 4.0% → 6.1%), the top is a UC Berkeley exchange

Modem Statistics

Of phones surveyed that answer with a modem:

30399	samples recorded in .fnd files
43976	samples recorded in .dat files

40012 / 46037 = .869

thus approximately:

87% communicate some type of data (as opposed to zero data eg: a modem with out a computer connected to it or a blind security mechanism)

Modem Statistics

Of phones surveyed that answer with a modem:

- 2% have warning or Unauthorized in their banners
- 1% identify with a domain name
- 2% Shiva LanRovers
- 3% annex terminal servers
- 0.4% ascend
- 0.2% Phone Switches (rolm|cbx|siem|audix)
- 0.4% Voice-Mail systems

Modem Statistics

22% of Shiva LanRovers have no “root” password

30% of Ascends answered with a “ascend%” prompt

“Lots” of Ciscos answered with a command prompt

25% of these were in “enable” mode.

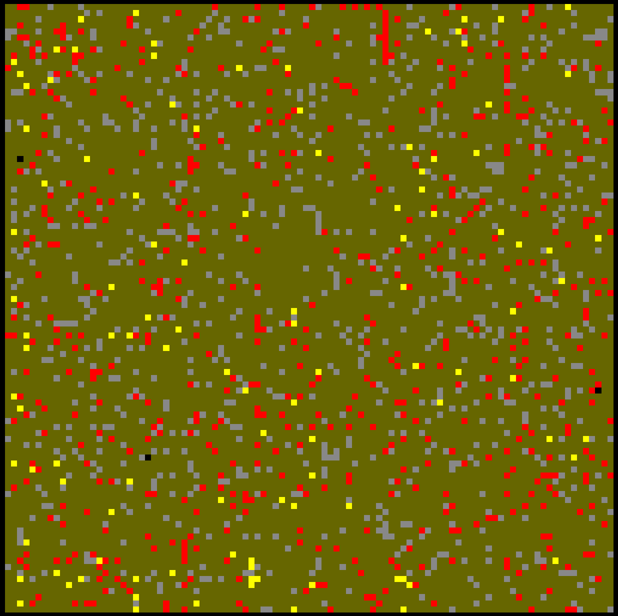
Modem Statistics

The Average baud rate is 20061

900	=	1	16800	=	63
1200	=	1592	19200	=	240
2400	=	1941	21600	=	248
4800	=	38	24000	=	144
7200	=	22	26400	=	558
9200	=	1	28800	=	2004
9600	=	1588	31200	=	1516
12000	=	78	33600	=	505
14400	=	5675	38400	=	3806

DATA

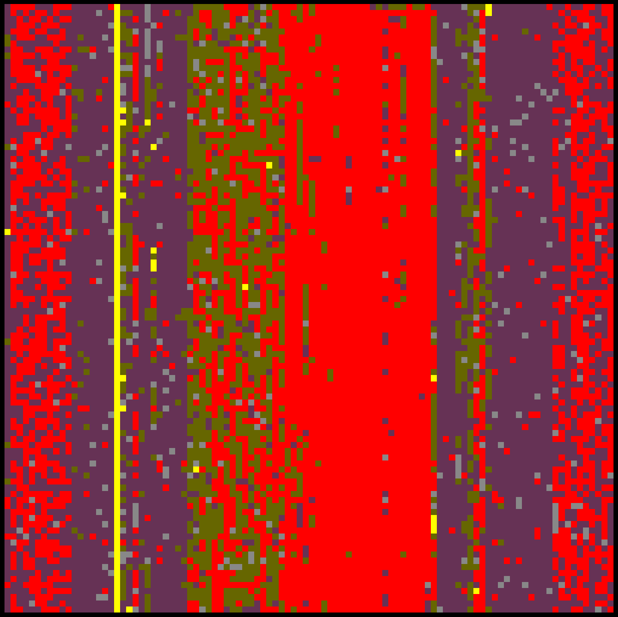
Residential exchanges have a more random distribution with less modems.



Modems = 109, Busies = 551, Timeouts = 846

DATA

- Business exchanges have a less random distribution with more modems.
- ISPs show up as yellow vertical lines or streaks.



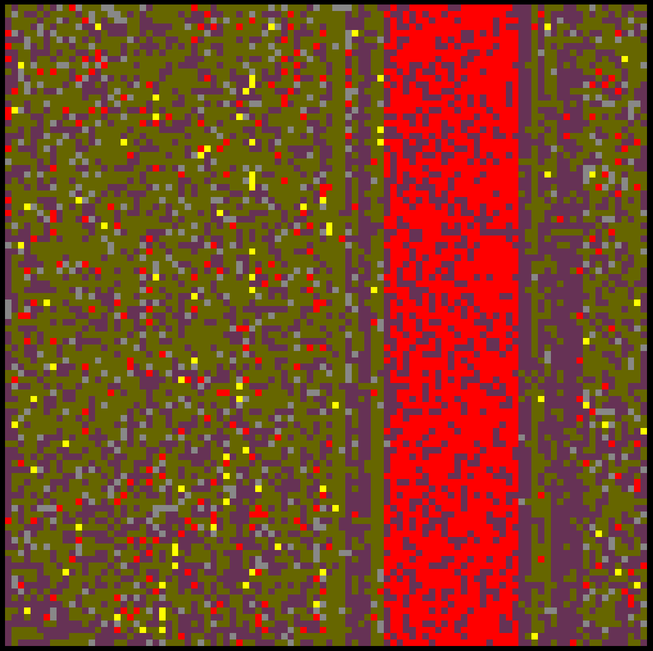
Modems = 123, Busies = 4170, Timeouts = 295

DATA

This is of the 510849 exchange.

The red band is a block of pagers

This particular exchange is mix of home, businesses and pagers

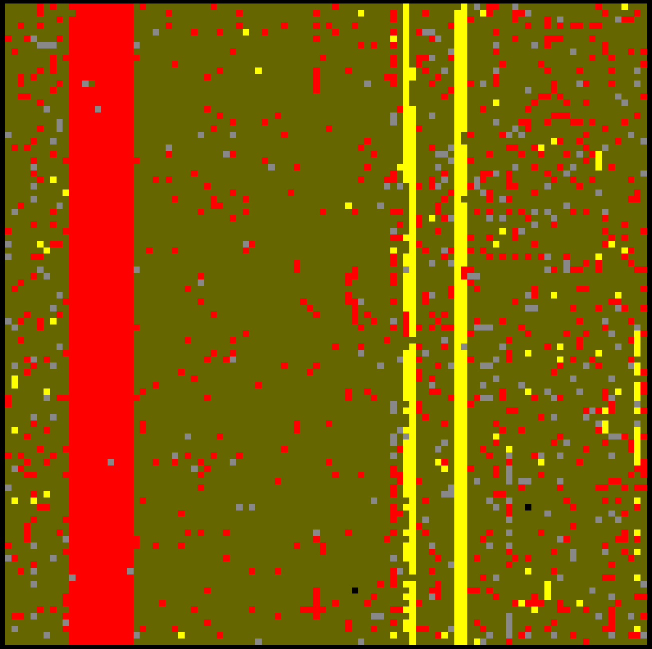


Modems = 87, Busies = 1734, Timeouts = 532

DATA

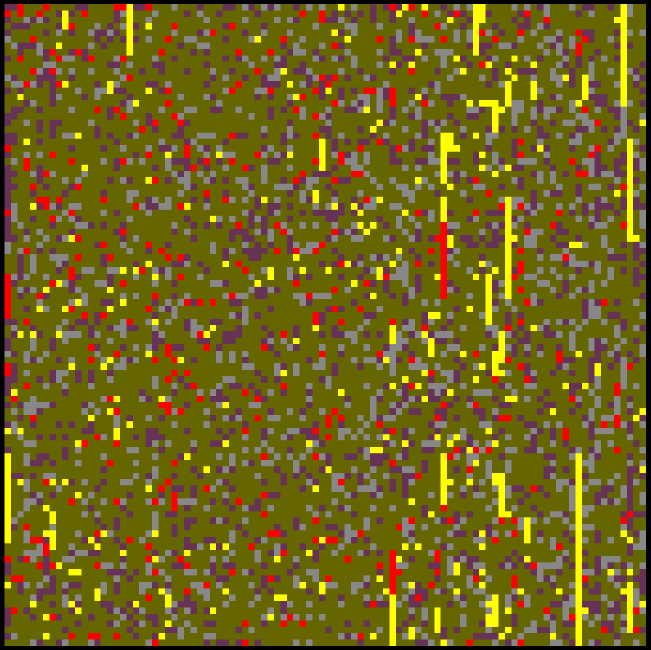
- This is of the 408459 exchange.

- Can you spot the Netcom dialup modem banks?

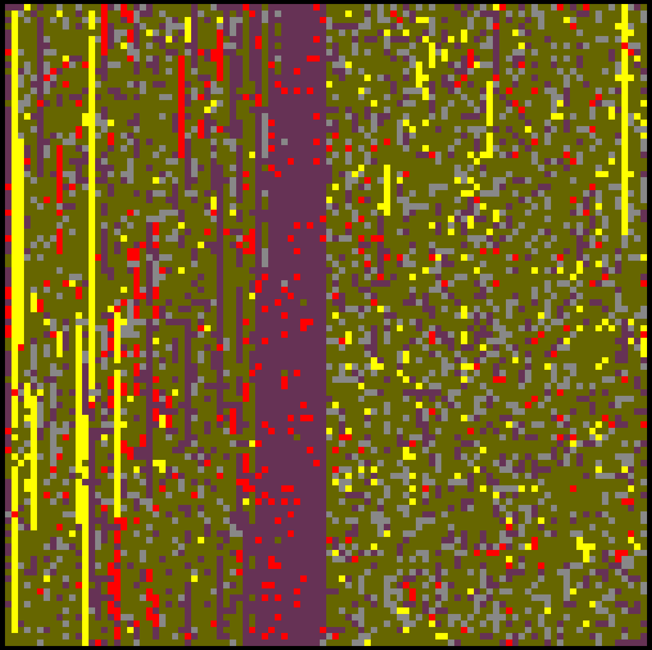


Modems = 141, Busies = 1697, Timeouts = 256

DATA



510642



510643

UC Berkeley had the most modems per exchange
Yet the most secure dialups

Things Discovered

- Firewall Router Consoles
- Environmental Controls
- Terminal Servers
- Unix Shells
- DOS Shells
- T-1 Multiplexors
- Oakland Fire Dispatch
- Cody’s Book Ordering Database

The list continues on……

Lease Line MUX

```
17:21:27 --------------------------[ Menu ]-------------------------- 09/16/97
ALARMS                             SYSTEM PARAMETERS
 DA  Display    SA  Set Ack         DP  Display
 ZA  Clr Cnts   SO  Set Rpts        SR  Set Port Baud   SP  Set

SHELF CONFIGURATION                LINE CARDS
 DC  Display                        DL  Display Table   DD  Disp Config
 SC  Set                            CL  Copy Config     SL  Set Config

MAP TABLE                          MAP MATRIX
 DT  Display    DN  Disp. Wrking    DM  Display
 ST  Edit       SN  Set Wrking      SM  Edit            CM  Copy

CLOCK SOURCE                       DIAGNOSTICS
 DS  Display    SS  Set             OL  Line Card       OD  T1-CSU

PASSWORDS                          PERFORMANCE
 LO  Logout     SW  Install         PM  FDL Monitor     SB  Set ERT Alarm
 DW  Display    EW  Erase           DH  Alarm History   ZH  Clr Alm History
------------------------------------------------------------------------------
```

Oakland Fire Dispatch

```
LI LOCATION ................ GRID.. NAT.  TAC TIME. TRUCKS ....................
 1 2272 TELEGRAPH AVENUE     3327   4P2         00:28  504
 2 1500 89 AVENUE            2722   17P2        00:20  505
 3 EB 580 SEMINARY ON TO KEL 521    3B    1     21:55  2566 2563 2560 2567 2561
                                                       2569 2513 2514 501 571
                                                       2577 S04 502 5662 5682
                                                       5690 2502 2565 2556
```

Oakland Fire Dispatch

```
                    - - - FIRE DISPATCH HELP SCREEN - - -
AHC - Display adjacent hazs cautns      TSP - Test station printer
CN  - Display caution notes for loc     UP  - Menu of user-written programs
CQ  - Display coverages and quarters    US  - Display Unit Status
CYC - Cycle Through Moveup Maps         UT  - Display unit times
DA  - Display CJ days activity          @   - Log off
EC  - Emergency contact information     #   - Telephone / pager directory
F   - Display fire actives              #T  - Truck status screen (1-9)
H   - Hazardous materials research      ?   - Display this help screen
INF - General info. file inquiry
M   - Display recommended moveups
MED - Display medical notes for addr
MO  - Memo system access
PC  - Display prior calls
PI  - Display prior incidents at loc
RUN - Display unit times and notes
SOP - Standard operating procedures
SR  - Display shift roster/schedule
T   - Display truck status screen #1
TIM - Display and reset timers
```

Passwords

It is a known fact that passwords people chose, in a corporate environment are typically easily guessable

Other Risks

10 hours to brute

Passwords

Given a small but optimized password dictionary of 432 words and a list of 12 common account names it is possible to brute force into a modem dialup in less then 10 hours!

This includes a five second delay enforced for bad passwords and redialing after every four tries.

How Bad is it?

On average I discover a "wide open" system four line (4) times a week.

Over half of the these "wide open" systems are terminal/dialup servers connected an internal LAN with out (apparent) Internet access.

How Insecure/Vulnerable are dialups?

Based on a *small* sample of current data

%75 are vulnerable to some form of attack (unprotected or "10 hour" password attack)

Note that this agrees with Dan Farmer's statistics in his internet security servey

http://www.trouble.org/survey

Observation: UC Berkeley has the most modems per exchange and observably the most secure

What to do

- Get a security audit and network risk assessment
- Plan ahead, write a security plan
- Test your firewall to see if it really does filter as advertised.
- Build and install a Intranet firewall

Software I Used

ToneLoc - written by Minor Threat and Mucho Maas.

Random Utilities - to read and process the data in the Unix environment

Hardware I Used

CPU:

- 8086 and 286 notebooks

Modems:

- ZyXEL 1496E+
- Courier V.Everything

Average dialing rate is 250 per hour

How much time has this taken?

The current data logs have 849671 minutes recorded

1214596 Minutes → 20243 hours → 843 days → 2.3 years

This is is machine time.

I have had up to three (3) system going at once. (Currently I have only two)

How much time has this taken?

I have been doing this for close to 1.5 years (data has been lost and discarded thus and I have not always had system running 24/7)

Other Software

- **Phonewall** - Sentry Telecom Systems Inc.

  Phonewall is a combination of hardware and software that monitors telecommunications trunks, and identify their content as voice, fax or data then allow or disallow particular types of traffic

Other Software

- **PhoneSweep** - Sandstorm

  PhoneSweep commercial wardialer support multiple modems, with the capability to identify remotely detected systems as well as generate reports and stuff.

Conclusions

- Your main risk is not always your internet front door.
- Firewalls do not provide real security
- Watch your back doors
- People are foolish

Wardialing

Peter Shipley

shipley@dis.org