An Analysis of Dial-Up Modems and Vulnerabilities

Peter Shipley, Simson L. Garfinkel

Abstract

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. There are, however, many documented examples of attackers gaining access to protected networks via unsecured dialup modems.

Security problems occur when the obvious is overlooked. With the growing attention upon securing high-speed Internet connections, web servers, VPNs, and firewalls, we believe that the problem of securing dial-up modems is significant yet largely ignored.

This paper formerly presents the results of the first large-scale survey of dialup modems. The survey dialed approximately 5.7 million telephone numbers in the 510, 415, 408, 650 and parts of the 707 area codes, and the subsequent analysis of the 46,192 responding modems that were detected.

Overall, the findings are troubling. The overall level of security observed in the field was far lower than was expected. Despite the emphasis on Internet connectivity, we found that modems connections are equally insecure and carry similar risks for large organizations. Many of the most vulnerable systems discovered had modems that were connected directly to application programs, rather than merely open dialups on IP-based networks.

Background

The 1983 movie WarGames, starring Matthew Broderick, introduced the world to the concept of telephone scanning. In the movie, a teenager named David Lightman writes a program that sequentially dials every telephone number in his city, listens for modems

[1] You may not publish these works in any hardcopy medium (magazines, newsletters, zines, etc.) without the authors express permission.

tones, and records what it finds. Although Lightman is looking for the dial-up modems of a nearby computer games company, what he actually stumbles upon is the dial-up modem for a top-secret US military computer. After penetrating the system, the teenager starts a nuclear war simulation game that almost inadvertently starts a real global thermonuclear war.

Since the debut of WarGames, telephone scanning has become a common tool in the computer underground for reconnaissance and target identification. More than a dozen telephone scanners can be downloaded from various websites on the Internet. Telephone scanning has also become a tool for security auditors, who dial blocks of phone numbers belonging to organizations for the purpose of inventorying dial-up systems and identifying vulnerable dial-up modems before outsiders find them. To assist with such scanning operations, at least three companies have developed and are now selling commercial telephone scanners.[i]

Numerous accounts in both the popular and the academic press have detailed security incidents that could be traced to an unsecured dial-up modem. One of the most dramatic incidents occurred in March 1997, when a youth in Worcester County, Massachusetts, discovered a modem connected to the controller of a fiber-optic communication system. The fiber optic system didn't ask for a username or password, but simply presented the youth with a series of commands that he could type. The youth proceeded to experiment with the system and succeeded in shutting down communications services for the Worcester County airport control tower and 600 nearby homes. Communications were disabled for many hours.[ii]

Although such stories make good copy and are effective tools for scaring higher-level management into purchasing the aforementioned security tools, anecdotal self-reports are ultimately not good tool for gauging threats or allocating scarce security dollars.

The majority of today's desktop computers are capable of acting as dial-up servers, either using built-in software[iii] or using third-party programs.[iv] Although most of these systems provide for access control using traditional usernames and passwords, many packages allow the systems to be configured for "open" access, granting access to all callers. Some remote access systems were distributed by their manufacturer with back-door or default accounts; rumor has it that these systems, when located in the field, can be easily compromised. Likewise, companies have deployed process control and remote monitoring systems that gain their security merely from the apparent secrecy of the access phone number, rather than any usernames or passwords.

But is the threat of unsecured dialups a significant threat, or are the media reports the only unsecured systems out there? In order to gauge the actual vulnerability of dial-up modems, Peter Shipley embarked on a self-project in April 1997 to obtain real numbers regarding the number of dial-up computer systems and the numbers of these systems that were not properly secured.

Methodology

At the beginning of the survey, Peter Shipley posted queries to various security mailing lists asking if anyone was interested in joining the project and scanning parts of their area. When no credible responses were received, Shipley decided to conduct the scan himself of the San Francisco Bay Area, where he lived.

When the project was initiated, the Bay Area consisted of four area codes: 408 (San Jose), 415 (San Francisco), 650 (Silicon Valley), and 510 (Berkeley), with the majority of the effort concentrated in the 415 and 510 area codes. A list of exchanges in each area code was obtained from Pacific Bell. No attempt was made to identify assigned from non-assigned phone numbers in each exchange. Instead, the decision was made to simply dial all phone numbers in each exchange, from -0000 through -9999. Likewise, no attempt was made to isolate "business" from "residential" telephone numbers.

Officials with local and federal law enforcement agencies were privately consulted with to determine the legality of proposed project. Unofficially, Shipley was advised that the proposed project would probably violate no laws as long as the telephone scanner were configured to merely capture system banners, rather than attempt to a break-in,

Business exchanges have a less random distribution with more modems.

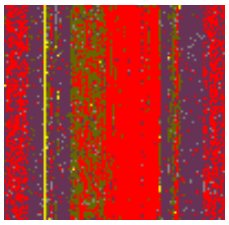

Figure #1: Distribution of dial-up modems in a business exchange

Telephone scanning was typically performed by between two and four laptops located in Berkeley, California. At one point, up to 12 modems were employed for telephone scanning. Each laptop ran a copy of the telephone scanning program "toneloc," a program written by Chris Lamprecht (a.k.a. "Minor Threat") that was modeled on the "WarGames" telephone scanner. The program was configured to dial all of the phone numbers within a 10,000 phone number telephone exchange, attempting one redial on all numbers that were busy. To minimize annoyance when dialing residential phone numbers, Toneloc was programmed to hang up after the remote phone had rung once. These calls were classified as a "ring out." (Dialup modems usually answer at the start of the first ring.) For each carrier found, Toneloc was programmed to send a control-E followed by two carriage returns to elicit a response from the remote system.

Telephone charges were kept low by the use of a special "flat-rate" telephone service offered by MCI, which provided for dialing throughout the Bay Area for $24/month per line.

Dialing was conducted from April 1997 through January 2000.

Initial Analysis

For each exchange dialed, Toneloc produces two files: a "DAT" file that is a map of the exchange, and a "FND" file that records a byte-by-byte transcript of the responses from the modem. A total of 572 exchanges were scanned, with modem carriers found in 523 of those exchanges. Approximately 900K (335,412 lines!) of modem banners and related information were captured. Once the scan was finished, the information in the "DAT" files was tabulated with a simple program written in C.

Approximately 5.7 million telephone lines were scanned in 572 exchanges. Modems were found in 523 of these exchanges. Businesses exchanges were found to have larger numbers of modems; those modems tended to be grouped in the exchange. Internet Service Providers were exceptionally easy to spot. Residential exchanges tended to have fewer modems and those modems were distributed randomly..

Residential exchanges have a more random distribution with less modems.

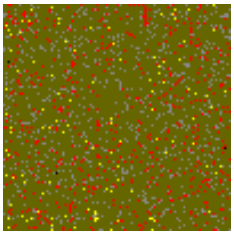

Figure #2: Distribution of dial-up modems in a residential exchange

Telephone exchanges were found to have 94 modems on average, or approximately 1%. The top 10 exchanges had percentages ranging from 4.0% to 6.1%, a modem penetration rate at an exchange associated with the University of California at Berkeley.

Approximately 87% of modems answered with some kind of banner; the remaining 13% transmitted no data, apparently waiting for some kind of challenge-response. (Modems dedicated to Microsoft Windows NT Remote Access Service, for example, will not transmit any data until they see an initial PPP packet from the initiating modem.)

Security practitioners frequently compare unsecured modems to unlocked "back doors" through with an intruder can gain unauthorized access. If this simile is correct, then this scan found an astounding number of unlocked doors:

- Security practitioners recommend that dialup modems should convey as little identifying information as possible, so as to make it harder for attackers to probe for valid usernames and passwords or to exploit known vulnerabilities. Nevertheless, the majority of dialup modems analyzed in the sample greeted the caller with a "welcome" message that identified the operating system version, the owner of the modem, the modem's location, or all three. Less than 2% of the systems had banners designed to warn away possible intruders.

- To evaluate the prevalence of systems with unchanged default passwords, logins with the "root" account were attempted on a sample[v] of the discovered Shiva LanRovers. On approximately one quarter of these systems, no password was set for the "root" account and access was immediately granted, thus permitting full login and reconfiguration access. As Shiva LanRovers accounted for approximately 3% of the answering systems, this statistic implies that there are more than 1100 dialup modems in the San Francisco Bay Area that allow administrative access to anyone who attempts to log in with the user "root" --- no password required!

  (Background: For several years, Shiva LanRovers were supplied by the vendor with two administrative accounts --- "admin" and "root". However, due to an error on the part of the vendor, only the "admin" account was documented. The "root" account was thus an undocumented back door allowing any caller to obtain full administrative access to any Shiva LanRover system simply by typing "root" at the login prompt. The existence of the Shiva LanRover "root" back door was publicized as early May 1996 on the "firewalls" mailing list.[2])

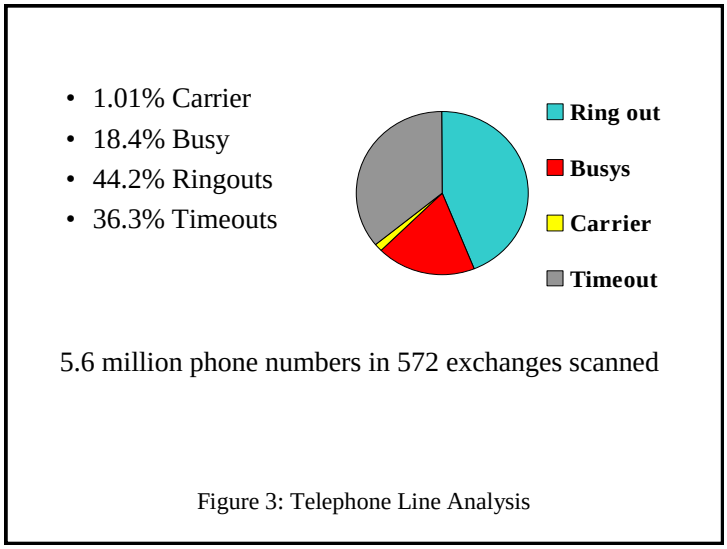

Figure 3: Telephone Line Analysis

- Of the Ascend remote access devices that were discovered, approximately 30% answered with the "ascend%" prompt, indicating that no username or password was required before a dial-up user could use the Ascend server to connect to other machines on the organization's networks.

- The majority of modems that were connected to Cisco routers were found to be in the command prompt mode, rather than demanding a "Username:" to log-in. Of these systems, approximately 25% were in the "enable," or privileged mode.

The vulnerability rates found in this survey were roughly on par with those observed by Dan Farmer in his December 1996 survey of 2200 computing systems on the Internet.[3]

---

[2] Keanini, Tim, Amy, "Re: 'Back door' via Modems," firewalls@GreatCircle.COM mailing list, May 1st, 1996. Archived at http://lists.gnac.net/firewalls/mhonarc/firewalls.199605/msg00012.html.

[3] Farmer, Dan. "Shall We Dust Moscow? Security Survey of Key Internet Hosts & Various Semi-Relevant Reflections." December 18th, 1996. http://www.fish.com/survey/

The fact that Farmer's survey was done at the beginning of the corporate push to e-commerce, and these modem results were done when dialup modems were considered a "mature" technology indicates that remote communications access points present long-term security problems, irrespective as to the communications medium.

On average, "wide open" systems were discovered by each scanning modem at least four times each week, or a little more than once every two days. At least half of these systems were dialup servers connected to an internal IP networks without apparent Internet access. The fact that these networks had no external access indicates that they were behind some kind of firewall system, presumably to provide additional security. The fact that the dialup systems had no usernames or passwords required for access indicates that the security that was desired by not connection to the Internet was somewhat inconsequential.

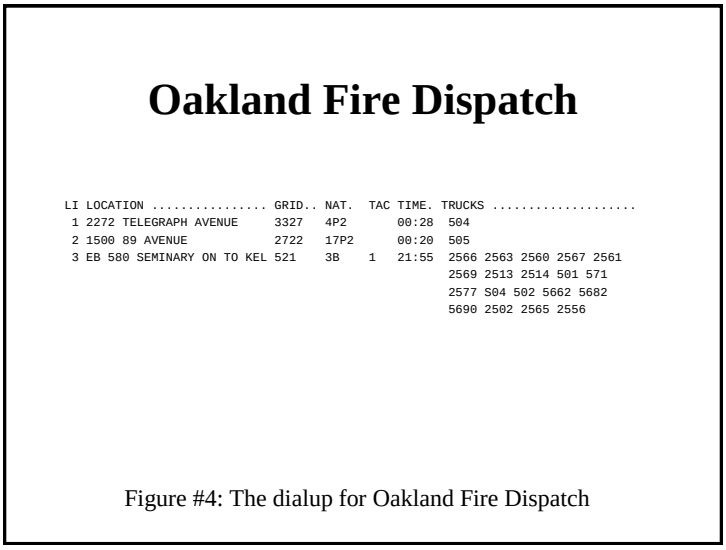

Figure #4: The dialup for Oakland Fire Dispatch

During the data collection, periodic analysis was performed by inspection. The results were unsettling: many dial-up modems were found that were not secured by usernames and passwords and that allowed access to confidential systems. On at least two occasions,[vi,vii] journalists (including one of the authors) wrote about these intermediate results. Among the discoveries were:

- A dialup that allowed unrestricted access to the Oakland Fire Department's dispatch system (Figure #4 & #5)
- A dialup that allowed unrestricted access to a lease line control system..
- A dialup to a popular bookstore that allowed access to customer order information, including credit card numbers and books ordered.
- A dialup on a computer at a pediatric care practice in Berkeley, Calif., that allowed unrestricted access to medical billing records.
- Several unrestricted dialups on remote access servers that were connected to internal networks of financial organizations.
- A dialup for a system that controlled a high-voltage power transmission line.

Secondary Analysis

One year into the scan of the San Francisco Bay Area, Simson Garfinkel and ten other computer security professionals formed the software development firm Sandstorm Enterprises. Sandstorm's first project was to develop and market a commercial telephone scanner. Initial customer requirements for this scanner included multi-modem operation (to replace multiple computers running multiple copies of Toneloc), the ability to identify remote systems, and the ability to test multiple username/password combinations against the remote systems. This commercial telephone scanner was called PhoneSweep.

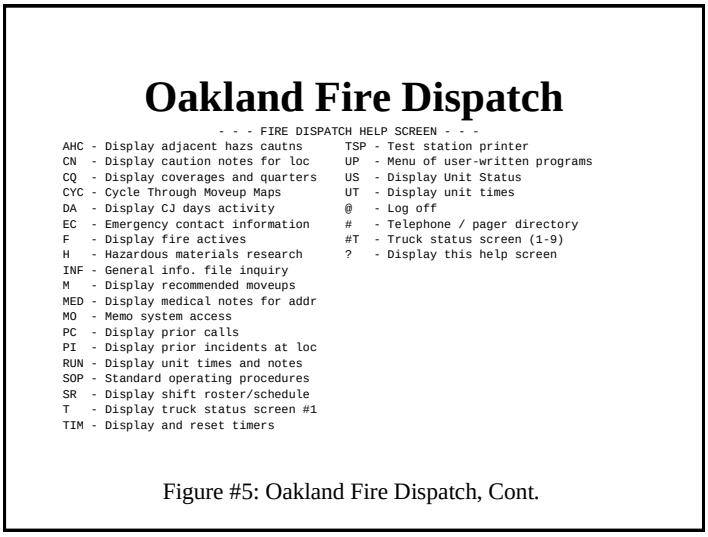

Figure #5: Oakland Fire Dispatch, Cont.

As part of a joint research agreement, Shipley provided Sandstorm with the intermediate results of his scanning. Sandstorm created a telephone scanner simulator that allowed the PhoneSweep recognition engine to analyze Shipley's raw data and characterize the results. At first, only a small percentage of the 41,243 answering modems could be identified. The responses from the remaining unidentified systems were sorted and stored on HTML pages, with approximately 500 systems per page. These files were then visually inspected for identifying characteristics, such as vendor names, version numbers, or unique login sequences. The new identification strings were added to the PhoneSweep identification engine and the process was repeated.

Finding identification strings in a sea of unstructured data is demanding work. There is also the problem of diminishing returns: at the beginning of the process, each new identification string can match hundreds of remote systems. But as the most popular systems are identified, successive identification string only identify a few dozens, or even just a handful of the remote systems in the corpus.

Crafting the identification strings was also hampered by the fact that many remote systems do not identify their name and version number in their banners. For example, the BayNetworks BayStack 450 Switch (24 port) places the character sequence "BayStack 450-24T" in its banner, making the system readily easy to identify. But the Electrotek Concepts Power Quality Network remote access system identifies itself only as "PQNode." These banners simply could not be identified without the use of Internet search engines such as Google, HotBot and AltaVista.

The initial version of PhoneSweep could identify less than a hundred different remote systems. Drawing largely on the Shipley corpus, PhoneSweep version 2.0 released in

June 2000 could identify 250 systems. Continued analysis through April 2001 lead the to the discovery of an additional 50 identification strings, for a total of 300 remote systems identified by PhoneSweep version 3.0.

Currently, the recognition system can identify 21,643 (54.6%) of the responding modems in the Shipley corpus. Another 13,968 (35.24%) responded with a text message did not allow sufficient vendor identification, and are characterized as "unidentified text protocol." Finally, 4,053 (10.23%) systems responded with an unintelligible binary protocol. Identifications for the remaining systems are presented in Table 2.

Table 2: Identified Systems

System Identification	#	%
>> unidentified binary protocol <<	4053	10.23%
>> unidentified text protocol <<	13968	35.24%
3Com Multiprotocol Communications Server	7	0.02%
3Com SuperStack II Remote Access System 1500	6	0.02%
3Com Total Control HiPer ARC Platform	24	0.06%
3Com Total Control Platform	1	0.00%
ACCULINK Access Controller	14	0.04%
AHC System	414	1.04%
AMS Pick64+ 2.3	1	0.00%
AT&T 386 UNIX	21	0.05%
AUDIX Voice Messaging System	2	0.01%
AccessBuilder 4000	44	0.11%
Advanced PICK O/S	5	0.01%
Advanced PICK O/S v.6.1	1	0.00%
Alphanumeric paging system	18	0.05%
Annex Remote Access Server	854	2.15%
Ascend MAX Terminal Server	8	0.02%
Ascend MAX200 Terminal Server	30	0.08%
Ascend Pipeline Terminal Server	156	0.39%
Ascend Terminal Server	49	0.12%
Autonet dialup port	88	0.22%
BITCOM Host	8	0.02%
BLAST	5	0.01%
BSD/OS (UNIX)	18	0.05%
BayNetworks System	71	0.18%
Brite Voice System	1	0.00%
Building Automation System w/o password	71	0.18%
CRC Netpath 100 Frame Relay	2	0.01%
CRC Netpath 64 Frame Relay	8	0.02%
Chase Research IOLAN Terminal Server	1	0.00%
Cisco	1365	3.44%
Cisco 3640 Router	22	0.06%
Cisco Catalyst or Router	3	0.01%
Cisco Terminal Server (no authentication required)	35	0.09%
Citrix ICA WinFrame	303	0.76%
Cognitronics Announcer	5	0.01%
Computer Process Controls System	3	0.01%
Computerm VMC (Virtual Mainframe Channel) 8100 channel extension system	1	0.00%
Computone Intelliserver Terminal Server	38	0.10%
Concentric.net Dialup	13	0.03%
Convergent Technologies CTIX (UNIX)	1	0.00%
Cubix WorldDesk	9	0.02%
DECserver 200 Terminal Server	13	0.03%
DECserver System	10	0.03%
DIALOG network dialup	212	0.53%
DRS/NX 6000 (UNIX)	2	0.01%
DUNSNET dialup port (Dun & Bradstreet)	31	0.08%
DYNIX System (UNIX)	4	0.01%
DYNIX System V.2.1.2 (UNIX)	7	0.02%
Data General AOS/VS System	16	0.04%
Data General System MV/5500	5	0.01%
Data General's DG/UX (UNIX)	6	0.02%
DataSMART System	1	0.00%
DataSMART T3 SMDSU	2	0.01%
Defender 5000	32	0.08%

Defender Security Server	14	0.04%
Dell UNIX System V	2	0.01%
Digital OpenVMS Alpha	5	0.01%
Digital OpenVMS VAX	2	0.01%
Digital Research Concurrent DOS system	2	0.01%
Digital Speech Systems TMX Series voice mail system	3	0.01%
Digital Speech Systems TMX-12/500 voice mail system	2	0.01%
Digital Speech Systems UniVoice 100 voice mail system	2	0.01%
Digital Ultrix (UNIX)	11	0.03%
Digital VAX/VMS	23	0.06%
Digital VMS System	132	0.33%
Digital VaxCluster (VMS)	1	0.00%
Electrotek Concepts Power Quality Network	1	0.00%
Emulex ConnectPlus LT Remote Access Server	1	0.00%
Excalibur BBS	8	0.02%
FirstClass BBS	140	0.35%
FreeBSD (UNIX)	10	0.03%
GCM System	30	0.08%
Gandalf Starmaster network	3	0.01%
General Automation Power95 control system (PICK Environment)	2	0.01%
General Automation ZEBRA	2	0.01%
Generic IBM system, possibly mainframe	34	0.09%
HP Remote Assistant	22	0.06%
HP System	12	0.03%
HP-UX (UNIX)	26	0.07%
HP9000 Console Prompt	7	0.02%
Hermes II Macintosh BBS	1	0.00%
Hewlett-Packard MPE/XL System	56	0.14%
Hewlett-Packard MPE/iX System	16	0.04%
Homecare Management System	1	0.00%
IBM 3174 Control Unit Emulator, ver. 7.03	1	0.00%
IBM 3708	24	0.06%
IBM 5251 Terminal	7	0.02%
IBM AIX (UNIX)	186	0.47%
IBM PhoneMail	5	0.01%
IBM System/32	11	0.03%
IBM System/88	5	0.01%
Infonet DialXpress	1	0.00%
Inter-Tel IMX 1224/2460 Key Telephone System	1	0.00%
InterLynx/400	5	0.01%
InterSystems MSM-PC/PLUS	4	0.01%
Lansource WINport	3	0.01%
Lantronix	6	0.02%
Libra Systems Corp. Quarry Master 2 Plus	1	0.00%
Lighthouse Power Switch	1	0.00%
Linux System (UNIX)	68	0.17%
Lucent PortMaster PM3	3221	8.13%
MANAKON Telemanagement Console	10	0.03%
MAXIMUS BBS, version 3.01	1	0.00%
MEGAHOST BBS	1	0.00%
MUMPS-systems 3.0.6 for a IBM/PC platform	1	0.00%
MUMPS-systems for a IBM/PC platform	1	0.00%
MediaGate EdgeCommander	1	0.00%
Mentor PRO integrated database environment	4	0.01%
MichTron BBS	1	0.00%
Microware OS-9	16	0.04%
NCR 386/486 UNIX	9	0.02%
NLynx Interlynx/400	2	0.01%
NeXTSTEP / NXFax System (UNIX)	4	0.01%
NeXTSTEP System (UNIX)	1	0.00%
NetWare CONNECT Service Selector	395	1.00%
Netlink OmniLinx Switch	73	0.18%
Network Access SW (Digital VAX cluster terminal server)	9	0.02%
Newbridge 3600 MainStreet	3	0.01%
Newbridge 3624 MainStreet	1	0.00%
Northern Telecom SL-1	74	0.19%
Novell Internet Access Server (NAIS) v.4.1.0	16	0.04%
Octel System	2	0.01%
Octel Voice Processing System	67	0.17%
Open M for MS-DOS	7	0.02%
PC Anywhere	1077	2.72%
PCBoard BBS	32	0.08%
PPP	395	1.00%
PPP (MajorTCP/IP by Vircom Inc	12	0.03%
PROMIS II System	5	0.01%

Pentium SCO Unix (UNIX)	6	0.02%
Perle 394 Remove Controller	4	0.01%
Perle Model 3i PC Dial-up Server	6	0.02%
Perle equipment (unknown model number)	5	0.01%
Picker IQ System	1	0.00%
Portmaster1 Terminal Server	9	0.02%
Possible Alarm System	19	0.05%
Possible Bulletin Board System (BBS)	65	0.16%
Possible Cisco 2500 without password	1	0.00%
Possible Cisco router without password	1	0.00%
Possible MS-DOS Command Prompt	12	0.03%
Possible PICK Environment	16	0.04%
Possible Telephone PBX	2	0.01%
Possible X.25 PAD	14	0.04%
Premier ESP Key Telephone System	3	0.01%
Premisys IMACS/800 Digital Telephone Switch	1	0.00%
ProBoard BBS	1	0.00%
Procomm	1	0.00%
Procomm Plus	12	0.03%
Procomm Plus for Windows	8	0.02%
Procomm System	48	0.12%
QNX Realtime OS	39	0.10%
QuickMail	19	0.05%
R91 Enhanced PICK	9	0.02%
ROLM CBX	29	0.07%
ROLM PhoneMail	33	0.08%
Red Hat Linux (UNIX)	26	0.07%
Remote2 Host	29	0.07%
Renex System	1	0.00%
Renex TMS-3	5	0.01%
SAGE System	7	0.02%
SCO Open Desktop (UNIX)	9	0.02%
SCO Open Server Enterprise (UNIX)	15	0.04%
SCO OpenServer (UNIX)	175	0.44%
SCO System (UNIX)	60	0.15%
SCO UNIX System V/386	125	0.32%
SOTAS Circuitsentry	3	0.01%
Schindler Elevator Corp. Lobby Monitor	1	0.00%
Searchlight BBS	2	0.01%
Searchlight BBS (TeleGrafix Communications, Inc.)	4	0.01%
SecurID Prompt	225	0.57%
Secure Sentinel	56	0.14%
Sentinel 2000 access control system	3	0.01%
Shiva LanRover	1306	3.29%
Siemens Rolm System	1	0.00%
Siemens/Rolm CBX 8004 PBX	10	0.03%
Siemens/Rolm CBX 9004 PBX	1	0.00%
Sun Solaris (UNIX)	77	0.19%
SunOS (UNIX)	4	0.01%
Sunsoft INTERACTIVE UNIX System V.4 (UNIX)	14	0.04%
	4	0.01%
TELENET dialup port	1105	2.79%
TRIAD System	2	0.01%
Telco Systems Inc. Route-24	6	0.02%
Telco Systems Inc. System	6	0.02%
TeleFinder BBS	15	0.04%
Telebit ACS	44	0.11%
Telebit NetBlazer	122	0.31%
Telebit NetBlazer (possibly unconfigured)	3	0.01%
Telebit NetBlazer version 3.0	1	0.00%
Telrad Digital Key BX PBX	4	0.01%
Tenon MachTen (UNIX for Mac)	1	0.00%
TimePlex SYNCHRONY Enterprise Router	2	0.01%
TriBBS	4	0.01%
Triad Systems System	9	0.02%
UNIX System	86	0.22%
US Robotics Courier Fax Dial Security Session	3	0.01%
US Robotics V.Everything Dial Security Session	15	0.04%
UUPC (UUCP client software) for MS-DOS v. 5.00	1	0.00%
Ultimate PLUS	13	0.03%
UnixWare	4	0.01%
Unknown BBS	2	0.01%
Unknown BBS with first name prompt	10	0.03%
Unknown BBS with full name prompt	3	0.01%
Unknown BBS with name prompt	5	0.01%
Unknown Premisys System	36	0.09%
Unknown building control system	20	0.05%

Unknown with !login prompt (probably UNIX)	201	0.51%
Unknown with PASSWORD prompt	123	0.31%
Unknown with account name: prompt	1	0.00%
Unknown with login : prompt	3	0.01%
Unknown with login. prompt	284	0.72%
Unknown with login: prompt	5	0.01%
Unknown with login: prompt (probably UNIX)	2983	7.53%
Unknown with login> prompt	7	0.02%
Unknown with logon please: prompt	17	0.04%
Unknown with logon: prompt	171	0.43%
Unknown with name: prompt	551	1.39%
Unknown with passwd: prompt	5	0.01%
Unknown with password : prompt	25	0.06%
Unknown with password:	1398	3.53%
Unknown with password> prompt	69	0.17%
Unknown with sign on: prompt	6	0.02%
Unknown with sign-on: prompt	68	0.17%
Unknown with user id/account name prompt	4	0.01%
Unknown with user name: prompt	30	0.08%
Unknown with user number: prompt	1	0.00%
Unknown with userid prompt	133	0.34%
Unknown with username prompt	178	0.45%
Unknown with username: prompt	194	0.49%
Unknown, sending ANSI escape codes	538	1.36%
VAIS FirstLine Voice Scripts	1	0.00%
Virtual Advanced BBS	4	0.01%
WESCOM II Branch System	4	0.01%
WESCOM Phone System	1	0.00%
WILDCAT! BBS	46	0.12%
Wang VS	5	0.01%
WebFlow System	3	0.01%
Wellfleet System	2	0.01%
Western Telematic PollCat III PBX data recorder	12	0.03%
Western Telematic PollCat PBX data recorder	3	0.01%
Wildcat! BBS for Win95/NT	27	0.07%
Worldgroup BBS	19	0.05%
XETA System	6	0.02%
Xylogic Annex Remote Access Server	7	0.02%
Xylogics Annex Remote Access Server	2	0.01%
Xylogics System	7	0.02%
Xyplex System	2	0.01%
Xyplex Terminal Server	8	0.02%
Yale ASCII Terminal connected to IBM Mainframe, ver. 2.1	5	0.01%
Total systems identified by PhoneSweep 3.0:	39637	100%

Conclusions and Recommendations

In this age of high-speed Internet connections, firewalls, VPNs, and other networking technology, it is easy to overlook the threat caused by unsecured dialup modems. Dialup modems are, after all, a technology that is more than 20 years old. Yet this survey indicates that dialup modems still represent a real and present danger for many organizations.

Organizations need to understand that their main risk may not be their Internet connection. Moreover, conventional Internet firewalls do not provide protection for dialup modems. Even so-called "telephone firewalls[4]" cannot provide protection for lone dial-up lines that are directly provided by a local telephone company.

As the costs of telephone scanning are exceedingly low (the laptops in this survey ran DOS and were equipped with 8086 and 80286 microprocessors), it is unreasonable to assume that potentially hostile parties are not conducting their own scans of metropolitan telephone exchanges. Large-scale surveys such as this one can be invaluable for specific organizations. Alternatively, they could be used by terrorists or foreign governments as for planning a large-scale information warfare attack against businesses or local governments.

[4] Two telephone firewalls on the market are the Sentry Telecom Systems Phonewall and the SecureLogix Telewall. Both of these products are situated between an organization's PBX and the public telephone system and have the ability to block inbound modem connections to unauthorized telephone lines.

About the Authors:

Peter Shipley
[shipley@dis.org] is a security consultant from the San Francisco's Bay Area. Mr. Shipley has been doing security for near fifteen years and one of the few that is well known and respected in both the professional world as well as the underground/hacker community. He has extensive experience in system and network security as well as programming and project design as well as design the first automated Internet scanner in 1987.

Mr. Shipley's specialties are penetration testing, computer risk assessment; secure systems design and security training. Mr. Shipley also performs post-intrusion analysis as well as expert witness testimony.

Simson Garfinkel
[simsong@sandstorm.net] is Chief Technology Officer and co-founder of Sandstorm Enterprises, which develops aggressive tools for security auditing.

[i] Three commercial telephone scanners are PhoneSweep, by Sandstorm Enterprises, http://www.sandstorm.net/phonesweep; TeleSweep Secure, by SecureLogix Corporation, http://telesweepsecure.securelogix.com/; and Xiscan by Xinetica Ltd, http://www.xiscan.com/.
[ii] Garfinkel, Simson L. "Advanced Telephone Auditing with PhoneSweep: A better alternative to underground "war dialers", *Matrix News*, 8(12), December 1998
[iii] For example, the desktop versions of Microsoft Windows NT and Windows 2000 provide facilities for controlling a single dial-up modem.
[iv] Symantec's pcANYWHERE and Compaq's Carbon Copy are both popular programs for providing remote access to Windows desktop computers.
[v] 162
[vi] Littman, Jonathan, "Hacker shocker: Project reveals breaches galore," ZDNN, September 18, 1997.
[vii] Garfinkel, Simson L. "Cold calls uncover vulnerable computers," San Jose Mercury News, February 5, 1998.

