Global Information Assurance Certification Paper

War dialing

Michael Gunn
October 5, 2002
GSEC v1.4, Option 1

Abstract

This paper will give the reader general information on war dialing, war dialing tools and general steps you can take to protect your network from unwanted intruders, that may try to gain access to your network via unauthorized or poorly managed modems.

Introduction

"Would you like to play a game, Doctor Falcon?" I'm sure some of us have heard this familiar line from the ever so popular 1983 movie War Games starring Matthew Broderick. In War Games, we get a clear demonstration of how easy it could be to penetrate complex network security measures (e.g. IP based security technologies) by a simple $20.00 modem. Although I'm sure that modems didn't cost $20.00 back in the 80's. ☺

"Unauthorized modems are one of the most overlooked security flaws in corporation today. Companies often have modem lines they don't even know are there."[2]

With the increasing attempts of hackers trying to gain access into our networks we have adopted the practice of performing vulnerability assessments within our organizations. In short a Vulnerability Assessment will give us an overall scorecard of our organizations network security posture by performing various security related tests on our network. Although vulnerability assessments are a great practice we must face the fact that deficiencies do exist. Port scanning and CGI assessments are not enough. There are more entry points into an organization network than just hacking the Internet. One popular entry point that hackers can use is the modem. Using War dialing tactics, a hacker may be able to locate vulnerable out of band entry points into your organization, and manipulate them to access your network. "War dialing (aka. **scanning** or **demon dialing**) is the practice of dialing all the phone numbers in a range in order to find those that will answer with a modem". [11]
In most countries, it is not a crime to dial phone numbers, as stated by Information Security Systems (ISS), "the legality of war dialing varies from place to place". [11] We must face the fact, regardless of how outdated analog modem technology may be, modems are still widely used in many organizations for equipment administration, remote connections etc. Therefore, War dialing is still a practice that many hackers can use to infiltrate our networks. In any organization, modems can be the single biggest hole that an administrator may

face. This is just one of the many reasons why you should include war dialing as part of your organizations vulnerability assessment, and have a modem policy in effect within your organization.

"…. most large companies are [probably] more vulnerable through poorly inventoried modem lines than via firewall-protected Internet gateways."[1]

War Dialing Brief

War dialing consist of dialing a block of numbers from a publicly switched telephone network (PSTN) (e.g. 456-1000 to 456-2000) in an attempt to locate carrier signals or other various tones that may reside in an organization Private Branch Exchange (PBX) or phone system.
Most commercial war dialers or telephone line scanner (PhoneSweep) applications will detect not only modems but also fax, voice, busy tones and anomalies that may be present in your organizations PBX system.

To give you a brief understating of how war dialing might be used for nefarious purposes by a Hacker we will use the following example:

Example 1:
Pat works for ACME XYZ Company and lives roughly one hour from work. Because of the long commute and pending deadlines that must be met, Pat decides to install remote control software (e.g. pcAnywhere [19]) on the desktop at work. Once the remote control software is installed, Pat connects the modem to a nearby fax line that is not being used. Not being a security savvy person, Pat does not configure a password for the remote control software's Host connection. Thus, leaving the "screen door" open for anyone to connect to the remotely controlled host system.

Coincidently, The Nefarious Hacker who has been trying to penetrate ACME XYZ Company via the Internet, decides to try a different route. So, The Nefarious Hacker starts a war dialing reconnaissance mission, and manages to dial ACME XYZ's entire phone range in six hours. After analyzing the war dialing logs, The Nefarious Hacker determines that one of the modems found, from the war dialing reconnaissance mission, is using remote control software. After a few connection attempts, using various remote control applications, The Nefarious Hacker finally connects to Pat's system that is connected to the network. Now, The Nefarious Hacker has access to ACME XYZ's network to do as they please.
See Figure 1 for visual on example1.

This is one possible way that a Hacker might try to gain access to your network by misconfigured or poorly managed modems in your organization.

As Example 1 shows, the information obtained by war dialing can be used in malicious ways. But, on the other side of the coin in conjunction as part of your organizations Vulnerability Assessment, it can also be used to thwart malicious attempts at obtaining access to your organization.

The findings that you gather from a war dialing assessment, can be used as a means to determine the following:

- Enumerate current modem status.
- Locate unsecured modems within your organization for the purpose of securing them.
- Inventory of devices on your PBX accessible by PSTN (e.g. Fax machines, modems etc).
- Locate phone lines on your PBX that are not being used.
- Locate rogue modems that may have been placed on your network for nefarious purposes.
- Locate misconfigured remote access servers.
- Locate inadequately secured remote access accounts.

Like any Vulnerability Assessment, to receive the full benefit of war dialing, we must perform war dialing assessments on a continuous cycle. This will enable you to perform trend analysis, which over time, can be used as a measure to indicate, “If we are getting better”.

Before performing a war dialing assessment in your organization there are some key points that you should adhere to:

- Get approval from upper management
- Involve and Notify all parties that may be affected
- War dial outside of regular business hours

Get approval from upper management
This will allow you to explain what the war dialing assessment will entail. It will also allow you to communicate your plans effectively in order to build a trust relationship, and communicate the necessity of performing the war dialing assessment. By having upper managements approval or buy in, this will indicate that they understand and support your goals. In the long run, having upper managements approval could also assist in creating a case to obtaining funds for necessary security related upgrades or changes that may be needed in the organization.

Involve and Notify all parties that may be affected
In case of outages, the necessary staff will be on hand to resolve the problem, there is nothing worse then coming into work in the morning and finding out that someone has killed your systems. This also gives the parties a chance to voice their opinions or concerns on issues that may arise before or during the war

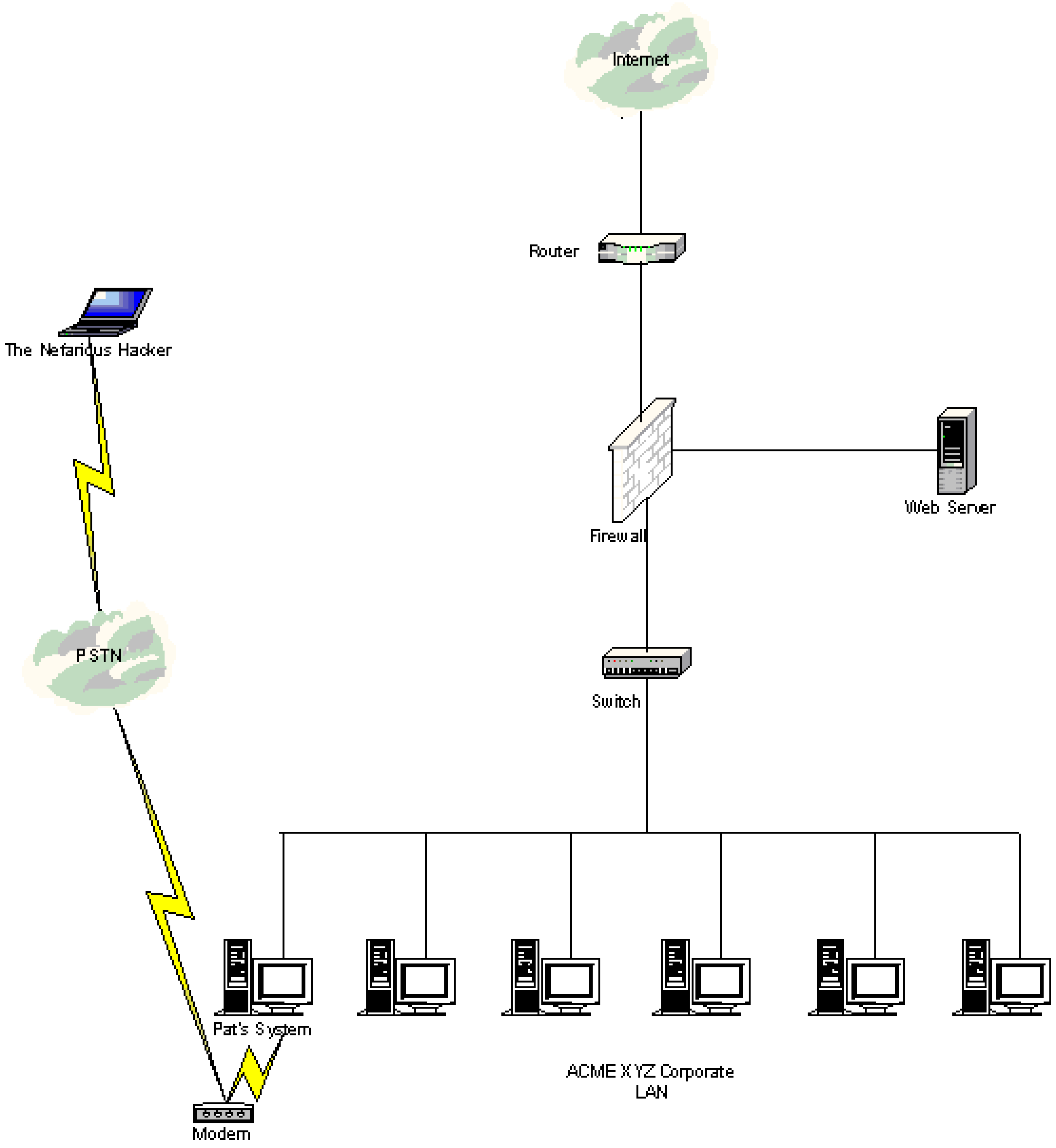
dialing assessment.

Implementing a change record policy, will allow coverage for all parties that may be affected by performing war dialing assessments. We must remember that managing security risks in an organization involves a collective effort by many parties.

War dial outside of regular business hours

Depending on the type of organization you work for it may be wise to war dial outside of regular business hours, as you would be less likely to disrupt employees, this would be especially true with most freeware war dial tools that do not have the capability to dial phone numbers randomly.

Figure 1 – Hacker Scenario



Modem Policy

Every organization should have and enforce modem policies and procedures within the workplace. An effective and realistic security policy is the key to effective and achievable security. [10]
Policies and procedures should be used as an organizational bible, in order to set guidelines which users should adhere to when performing actions in the workplace.
If modems are used in your organization then you should have a modem policy in your Information Security Manual. Your modem policy should clearly and precisely state its purpose, scope and outline the acceptable use policy that you intend to convey to your employees. But creating a policy is only one step in the right direction. In order to make the policy effective we must ensure that it is communicated to each employee.
A way to ensure that your policy is communicated to your employees effectively is to have each employee read, understand and obtain written affirmation of policy acceptance. Policies should be easily accessible by all employees by placing the information on an internal website.
When creating policies and procedures within your organization, you must remember, that these documents should be treated as living document that should be updated as the need arises.

As a guideline for creating Modem policies and Dial-In Access policies, you can visit the following web sites:
http://www.sandstorm.net/downloads/phonesweep/securitypolicy.pdf.
http://www.sans.org/newlook/resources/policies/policies.htm.

War Dialing Assessment Process

Generally there are three main phases when performing a war dialing assessment.

Phase I: Acquisition & Reconnaissance
Phase II: Identification and Assessment of Vulnerabilities
Phase III: Reporting

Phase I: Acquisition & Reconnaissance

Acquisition & Reconnaissance is a key phase in preparing for the war dialing assessment. It involves acquiring relevant information e.g. phone numbers needed to perform a war dialing assessment.

Depending on whether you are performing a blind war dialing assessment or if you are provided with the information, there are many resources that can be used for the acquisition & reconnaissance of an organizations PBX range(s). Some of these resources include:

- Phonebooks
- Business Cards
- Internet
- Help Desk
- InterNIC
- Dumpster Diving
- Social Engineering

Once we gather the necessary information (PBX ranges), we can continue with the actual war dialing assessment. The war dialing assessment can be performed with various tools (e.g. PhoneSweep, Telesweep Secure, Toneloc, THC-Scan etc). The time necessary to run the actual war dial assessment will vary depending on the following:

- Total phone numbers to dial
- Total number of modems available to scan
- Software capabilities
- Hardware capabilities

When the war dialing assessment is complete, the results will yield a snapshot and inventory of devices that exist in your organizations PBX. In essence, the war dialing reconnaissance phase is the equivalent to running a network port scan with nmap during a network vulnerability assessment.

Phase II: Identification and Assessment of Vulnerabilities

Phase II involves identifying and assessing the findings that you gathered from Phase I.

Identification and assessment of vulnerabilities are vital points that will help in assessing the adequacy of the security controls that the organization has in place pertaining to modems, and other out of band connections that may reside in your organization.

Some of the commercial tools such as PhoneSweep will allow you to further assess findings that you may have located in you assessment (e.g. test password strength on found accounts by “brute force” feature).

Phase III: Reporting

This final phase of war dialing will allow you to convey the findings to other parties in your organization (e.g. executives, telecom group, network administrators).
The reporting phase should include an Executive and Technical summary for the

different audiences that the report may be distributed to. Within the Executive and Technical summary you should list:

- Purpose of the assessment
- Timing and duration
- Tools
- Findings
- Recommendation

Purpose of the assessment
In this section you should explains why you are performing the war dialing assessment also, the scope of the war dialing assessment.

Timing and duration
This section explains when, and at what times, the assessment will take place.

Tools
This section will give an overview of the tools necessary to perform the war dialing assessment.

Findings
This section explains what was found during the war dialing assessment. Findings should be conveyed with a risk rating of HIGH, MEDIUM, or LOW depending on the risk factor that exist with the finding(s).

Recommendation
This explains what recommended "next steps" should be taken in order to resolve the issue(s) that were found during the war dialing assessment. Depending on the audience (management or technical personnel) you should emphasize recommendations accordingly.

Once you have presented the report to the necessary parties they should act upon your recommendations as soon as possible, in order to eliminate threat in your organization.

Benefits of War dialing

There are many benefits that can be gained by a war dialing assessment. Some of these benefits include:

- Locate insecure modems
- Locate insecure dial in accounts
- Inventory and lock down devices accessible by PSTN
- Create a base line for future war dialing assessments
- Test and locate out of band devices
- Identify holes and provide recommendations for repairing them
- Thwart backdoor break-ins

These benefits can especially be demonstrated in large organizations where your PBX may have 20,000 – 40,000 numbers. Inventorying this size phone system and keeping an active database of devices can be quite a considerable task for any administrator.

Ways to improve Modem Security

Here are a few points that can be used to improve modem security within your organization:

- Policy should be drafted and communicated effectively to employees.
- Manager approval should be granted for all new connections.
- Use encryption techniques.
- Modem firewall (e.g. Phonewall 20™ [20]) should be used on incoming lines – Device will route calls depending on "Authorized or Unauthorized" access list.
- Do not place a "Welcome" banner on the login screen.
- Remove banner information from login screen that may give hackers vital information pertaining to your system.
- Have a banner; warning that access to the system is monitored 24 hours a day and unauthorized users will be prosecuted to fullest extent of the law.
- Require a user name and/or strong password to gain entry to the system.
- Limit number of login attempts to three or less attempts before disconnecting the modem.
- Disable auto answer on modems where not needed.
- Enable event logging for all incoming connections.
- Enable callback option.
- Adherence to corporate policy pertaining to modem configuration
- As a general rule, do not attach modems to any servers except those whose purpose is to provide dial-in access. [6]

- If a vendor requires modem access make sure that the modem is only on when the vendor is accessing the system.
- Use a different range of phone numbers for out of band management devices (e.g. if your organizations phone system is using a range 444-6000, choose another range for your out of band management devices 567-7000).
- Change the remote dial access numbers periodically.

[17]

Some companies have even gone as far as prohibiting employees from installing modems on their desktop systems and "sacking" them for not obeying this policy.
Following these simple points will assist in securing your organization from malicious attacks.
[18]

War dialing Tools

In today's competitive market you can find many freeware and commercial based war dialing tools to assist you with the task of war dialing. Some well-known freeware tools are ToneLoc and THC-Scan. On the other side of the spectrum we have the commercial based tools such as Telesweep Secure and Sandstorm PhoneSweep. *See Appendix 1 for comparative table of war dialing tools.*

Toneloc (freeware)

- Short for Tone locator
- Created by Minor Threat and Mucho Maas
- DOS based but runs in Windows 95
- Dials numbers and saves the login session
- Can be configured to display the results of each number dialed in real time
- Blacklist feature to omit certain phone numbers from being dialed
- Displays details in a graphical map that represents information in colored patterns

[7] [8] [13]

THC-SCAN (freeware)

- The Hackers Choice Scanner
- Created by Van Hauser
- THC-Scan automatically detects the speed, data bits, parity and stop bits of discovered modems
- Recognizes subsequent dial tones
- ODBC databank support
- Works with DOS, Win95/98/NT and DOS emulators

  - Supports the usual Carrier and PBX Scanning mode plus a special manual mode for trying out PBXs and VMBs
  - Large palette of analyzing tools added

[14] [15]

SecureLogix Telesweep Secure (commercial)

  - Distributed Architecture
  - Unlimited Number Profiles
  - Supports Voice, Data, and Fax Detection
  - Dial-Up System Penetration
  - Dial-Up System Identification
  - Scan Difference Reports
  - Concurrent Profile Scans
  - Windows NT 4.0/2000 compatible
  - PPP Penetration
  - Remote Dialer Administration
  - Command Line Administration
  - Blacklist Import
  - Scan Progress Indicator

[16]

Sandstorm PhoneSweep (commercial)

- Referred to as a Telephone line scanner
- Capable of brute-force username/password guessing (penetration testing)
- Schedule stop and start sweep times
- Simple GUI
- Up to 20,000 numbers per profile, 16 modems, approximately 1,000 calls per hour
- Single call detect feature
- Supplied with a hardware license management device – dongle
- Produces detailed customizable reports
- Distributed Architecture
- Identify more than 470 different dialup systems

- Single call detect technology
- Runs under Windows 95 / 98 / NT4 / Windows 2000 Professional SP2 / Windows 2000 Server SP1 / XP
- Differential Reporting Capability

[14]

PhoneSweep Specification by Model

PhoneSweep Model	Modem Capacity	Phone Numbers per Profile	Approx Calls per Hour
Plus 16	16	* 20,000	1000
Plus 12	12	* 20,000	750
Plus 8	8	* 10,000	500
Plus	4	* 10,000	250
Basic	1	800	60

* More numbers can exist in a profile, but performance may suffer on all but high-end machines. [9]

All of the above-mentioned war dialing tools will get the job done but when choosing war dialing software you should consider the following:

- How many numbers do I need to dial?
- How often will I be performing the war dial assessment?
- What is the false positive rate?
- Is the software user friendly?
- Does the software contain documentation?
- What type of reporting am I looking for?
- What extension(s) can I use to export my findings?
- Can I trust the download site or does the software contain malicious code?
- Is technical support offered?
- What is the time frame offered to finish the assessment?
- Does the application have a scheduling feature?
- Does the application allow for differential reporting?

Quickly, you will find that the freeware tools (ToneLoc, THC-Scan) will get the job done, but do not give you as much flexibility as do the commercial tools (SecureLogix Telesweep Secure, Sandstorm PhoneSweep). In the long run, it all comes down to personal preference. If you are only looking for modems in your organization, then the freeware tools may just do the trick. If you need a more robust feature set then the commercial war dialer such as PhoneSweep will be the one for you. I found that in the long run the extra money we spent on PhoneSweep definitely paid off not only in reporting but also in cutting down the time to complete the war dial assessment task.

For more information on these war dialing tools listed above you can visit the following web sites:

http://www.textfiles.com/hacking/tl-user.txt
http://www.thehackerschoice.com/releases.php
http://applications.securelogix.com/index.htm#4

http://www.sandstorm.net/products/PhoneSweep/

Appendix 1

Application Features	Toneloc 1.10	THC-Scan 2.0	SecureLogix Telesweep Secure	Sandstorm PhoneSweep 4.02
GUI or DOS Based	DOS	DOS	GUI	GUI/DOS
System verification			X	X
Fax machine detection			X	X
Scheduling capable			X	X
Multi-modem scanning capability			X	X
Reporting capability Format	LOG, TXT	LOG, TXT	HTML, RTF, PS, CSV, PDF	HTML, RTF, XLS, ASCII
Differential reporting capability				X
Parallel Dialing			X	X
Automated reporting			X	X
Brute force penetration			X	X
PPP identification			X	X
Distributed Architecture			X	X
Technical Support			X	X

Note: X denotes that the feature is offered

What Next?

So, what happens when I locate rogue or insecure modems in my organization? This is a question that you may be faced with once you run a war dialing assessment in your organization. First and foremost, you should have a way of validating your findings to make sure that the device(s) in question do not belong in your organization. An easy way to determine this is by comparing your findings with that of your telecommunication team's database. Any unknown devices, anomalies or tones that are unknown by the telecommunications team should be assessed further. If your company does not have a telecommunications team or a proper database of modems and out of band devices that reside in your organization, this would be a great exercise that would allow you to build a database of these types of devices. Also, it will assist in creating a baseline for future war dialing assessments within your organization. We must always remember that any anomalies located in your organization should be handled with the utmost urgency, as timing could be a critical factor in preventing incidents that may arise.

Conclusion

Modems being a cause of network security breach may be a highly disputed subject in some administrator's eyes but we must all face the fact that all it takes is one poorly configured modem to breach your organizations network. Despite all the IP based security technologies that are being put in place to keep intruders out of your networks, and to keep a big brother like eye on employees unquenchable addiction to visit "non standard" web sites, more employees are turning to dialup Internet Service Providers (ISPs) in order to go unnoticed by network administrators. This dangerous and unauthorized practice will surely leave your network open to attack. War Dialing is a practice that can only help in the battle against unwanted intrusion into our networks. We must also remember, an ounce of prevention is worth a pound of cure.

References:

[1] Hacking Exposed: Network Security Secrets and Solutions. Second edition. McClure, Scambray & Kurtz. Osborne, 1999

[2] Information Week Magazine. August 1999

[3] KingPin. “War dialing Brief”. March 2000
URL: http://www.atstake.com/research/reports/acrobat/wardialing_brief.pdf

[4] Poulsen, Kevin “Dial “H” for Hacker”. June 30, 1999
URL: http://www.techtv.com/cybercrime/features/story/0,23008,2275510,00.html

[5] Gagne, Cathleen “Definitions” April 01, 2002
URL:
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci546705,00.html

[6] Allen, Julia H. The CERT guide to System and Network Security Practices. Pg.34 Reading: Addison Wesley, 2001

[7] Middleton, Bruce. Computer Security. Using the Hacker’s Toolbox
URL: http://www.securitymanagement.com/library/000689.html

[8] Edwards, Mark Joseph. Windows & .NET Magazine. The Handy Security Toolkit Revisited. October 1999
URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=7192

[9] Sandstorm Enterprises, PhoneSweep Product Specification. 1998 - 2000
URL: http://www.sandstorm.com/products/phonesweep/specs

[10] Northcutt, Stephen. SANS Security Essentials. Basic Security Policy. “Defining a Policy”. pg 2-4. 2001

[11] Information Security Systems, Advice/Countermeasures/Scanners, 2002
http://www.iss.net/security_center/advice/Countermeasures/Scanners/War_Dialers/default.htm

[12] Whatis.com. Whatis.com Terms. Apr 01, 2002
URL: http://whatis.techtarget.com/definition/0,289893,sid9_gci546705,00.html

[13] Information Security Systems. Advice/Countermeasures/Scanners. 2002
URL:
http://www.iss.net/security_center/advice/Countermeasures/Scanners/War_Dialers/ToneLoc/default.htm

[14] Geocrawler. “Comparison of THC-SCAN v2.0 with Sandstorm PhoneSweep 1.02.” December 29,1998
URL: http://www.geocrawler.com/archives/3/91/1998/12/0/199775/

[15] King, Nathan A. "Sweeping Changes for Modem Security". June 2000.
URL: http://www.infosecuritymag.com/jun2000/junpentesting.htm

[16] SecureLogix. TeleSweep Secure. 2001
URL: http://www.securelogix.com/telesweepsecure/features.htm

[17] Stephenson, Peter. Network Computing. Securing Remote Access. 2002
URL: http://www.networkcomputing.com/602/602work2.html

[18] Ranger, Steve. TechWeb. “Sun Sacks Employees For Modem Security Breaches”. March 18, 1998.
URL: http://www.techweb.com/wire/story/TWB19980318S0012

[19] Symantec. pcAnywhere. 2002
URL: http://www.symantec.com/pcanywhere/Consumer/

[20] Sentry Telecom Systems. Phonewall 20™. 2001 URL:
http://www.sentrytelecom.com/products/featuresbenefits.asp?b=3