Outsourcing and the Increased Dangers of 'Dial Up' Access

Paul Jenkinson

Outsourcing and the Increased Dangers of 'Dial Up'Access

Paul Jenkinson
15-09-01 version1

The Outsourcing Scenario

The amount of businesses today actively using outside IT service providers to support the many elements of their IT infrastructures is increasing a rapidly. From WAN / LAN management to helpdesk provision, more and more, businesses are justifying the use outsourced service provision with the need to have greater control over IT expenditure. Aside of managing expenditure, advocates of outsourcing argue that well constructed contractual service level agreements (SLA's) with a service provider will yield improved operation and performance across an IT infrastructure.

Often the simple management notion is 'let us concentrate on our core business, and allow specialists to take care of our IT'

Telecommunications provider NTL recently announced it was going to outsource its IT operations, including billing, customer care and helpdesk to IBM. Their IT director, Chris Reveley, stated "We want to focus on what is core to NTL. The back office isn't core business. We want to concentrate on the cables telephony and interactive TV. "*Computing" magazine, June 2001.*

IT outsourcing is becoming increasingly popular. The recent Holway Report into the UK IT services industry found spending on outsourcing last year grew by 15% compared with 5% the previous year. Also the value of outsourcing deals doubled between 1999 and 2000 from £713 million to £1.8 billion.

The main advantages of outsourcing are clear. Firstly, it allows a business to fix the price of supporting its IT, and secondly it alleviates the requirement to employ and maintain a large body of IT support staff in house.

However from an IT security perspective an outsourced environment can create many issues. Identifying such issues and maintaining the security of an organizations IT infrastructure has to be considered along with outsourcing, and not after it. All too often this is not the case, and the objective this paper is to highlight how the current trend of outsourcing support services can dangerously augment the already well-known issues surrounding dial up access to a corporate network.

The dangers of 'Dial Up'

Any large modern business today which takes security of its network seriously will be aiming for, or proclaim to have "security in depth." Typically its network perimeter defenses may consist of multiple firewalls complimented by comprehensive

intrusion detect systems, external mail scanning and good psychical security throughout its buildings. The threat of an attacker, however proficient, hacking in and through such defenses in most environments would be slim. But like any good burglar, a hacker will always try a back door before even attempting the front door, and in terms of modern data networks that back is very often a small and inexpensive item of hardware called 'The Dial Up Modem'. Once compromised any other array of expensive security measures can be worthless.

Any analogue modem connected to a PC or server, which is then connect on an internal LAN, can become a very noticeable backdoor to an intruder with the correct hacking tools. The fact is a network is only as secure as it's weakest point, and all to often this is a poorly configured modem.

If an analogue modem is connected to a PC or server it may only be meant for a well trusted system administrator to gain access from home in an emergency, but what is it's configuration, does it dial back and is it password protected?
A business may have well documented control procedures for altering a firewall ruleset, yet do they have a security policy in place for modem usage, defining a basic configuration standard. Its not uncommon for a business to have somewhere on its network one, or maybe many modems that anyone anywhere can dial into without authentication. Such an invite into a foreign network is a hacker's dream.

One could argue this is a slight exaggeration of course. Although, even with the barrier of authentication in place, gaining unauthorized access via such a modem is only a question utilizing the correct hacking tools (alternatively known as network security tools if undertaking penetration testing!). I will shortly highlight two such freeware tools easily available on the Internet. Additionally I will compare the freeware programs with two commercial security products.

At this point you may ask 'but how does outsourcing increase the already established vulnerabilities of modem access to a network?' particularly when most service providers would never agree to maintain a service level agreement (SLA) over the limited speed of just a dial up connection.

However consider this situation…….

An organization is busy implementing a program of outsourcing IT support functions to various service providers. In order to get the services underway, contractual agreement needs to be reached with each individual service provider, and an integral part of each agreed SLA is that a secondary/back up network connection must be available. With the primary connection being a leased line connected through a DMZ (De-militarized Zone) onto the main firewall, the service provider requests that some resilience against any failure of this connection to be in place. Whilst the companies IT Security team advocate using a VPN (Virtual Private Network) solution of connecting through an encrypted tunnel across the internet, the companies firewall is not currently configured/licensed to receive VPN clients. Whilst the in house firewall administrators advise management to re-configuring the firewall to provide VPN access, management disagree. Cost analysis shows

management that the extra training for their firewall administrators, the upgrading of the firewall software, the testing time on the firewall and logistics of distributing the VPN client software to different organizations laptops is prohibitive. When compared to utilizing existing modem connectivity to the network management become convinced that costs associated with a VPN solution will diminish some of their initial projections on the cost benefits to be gained by outsourcing. Additionally, management view the time required to set VPN access compared with 'no-delay' advantages of using the existing modems as key to keeping their outsourcing ambitions on schedule.

So in this situation multiple service providers would have dial up connectivity to a network and its key servers and thus the vulnerability to war dialing should be seriously considered by such an organization.

A war dialer is a software tool used to scan a range of phone numbers with the aim to successfully make connections with computer modems. The program automatically dials a defined range of phone numbers and logs those numbers that are successfully connecting to modems.
Most underground war dialers, like ToneLoc and THC-Scan *(supplied by www.thehackerschoice.com),* are freeware, downloadable directly from the Internet. Most are driven via a command line interface, like DOS, and thus are eminently configurable to search and find corporate PBX's as well as individual modems. So providing you have medium specification internet ready PC, a phone line and the patience to study the product instructions you are ready to hunt out that back door onto a private network. It's really that easy.

For example using ToneLoc you can issue a single command string like this:

```
C:\ToneLoc SCANRS /M0208454-1XXX /H:6:00 /x:5XX /x:8XX
```

This will initiate a scan of all numbers from 0208454-1000 to 0208454-1999 for five hours maximum, saving the dialed numbers to SCANRS.DAT, excluding the ranges 1500-1599 and 1800-1899. When the scan is complete the resulting data produced will include:

- The start and finish times of the scan
- The maximum number of possible numbers, based on any masks eg: 0208454-1xxx
- The number of numbers dialled
- Number of responses for Carriers(**modems**),Tones, Voices, Busy's & Ringouts
- The average number of dials per hour
- The numbers of all carriers found (most important)

Another utility provided with ToneLoc can be used convert all the carrier information logged in the scans dat file into a readable text file. Within this file will be responses from the various carriers detected. By adjusting the scanning modems configuration

settings (eg: the parity and character stripping of the captured responses) over the course of a few scans you can reliably get results which will show cleanly answering modems:

```
12-Jul-101 23:59:07 902085653047 C: CONNECT 2400/ARQ/LAPM/V42BIS

AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.

IMPORTANT NOTICE:  THIS PRIVATE SYSTEM IS RESTRICTED TO AUTHORIZED USERS
ONLY. CONNECTION TO THIS SYSTEM BY UNAUTHORIZED USERS IS ILLEGAL AND WILL
BE PROSECUTED TO THE FULL EXTENT OF THE LAW.

login:
login:
login:

USRobotics Courier HST Dual Standard V.34+ Fax Dial Security Session
Serial Number 0109550000432193

Password (Ctrl-C to cancel)?
Invalid Password!
```

Despite it's usability Toneloc isn't the newest program around (last released 1994). The previously mentioned THC-Scan (released Dec 1998) is basically a more recent enhancement of Toneloc's functionality. Unlike Toneloc this freeware program will actually auto-detect a modems speed, data bits, parity and stop bit settings adding to the efficiency and quality of a scan. More importantly it is compatible with another freeware offering from THC called 'THC Login Hacker'. Using this program it is possible to perform full brute force penetration attack on identified modem login prompt, such as those above.

Basically, THC Login Hacker is password cracker for penetrating terminal logins via dictionary or brute force hacking, configurable for telnet and dialup connections. Like any password cracker it does this by using a huge process of elimination and trying millions password permutations based on predefined criteria. Brute force hacking will run through combinations of characters, using a predetermined search length, until it finds the combination accepted by the device, while a dictionary search searches each word from a dictionary for the correct password.

Whilst this sounds all too easy, just war dialing itself is illegal in many leading first world countries like the US and the UK. So unless you like the prospect of imprisonment or can adequately disguise your landline's location, penetration attacks are particularly not advisable. However, if you browse the user guides from both Toneloc and THC-Scan they both give advice on covering your tracks, which includes piggy backing local PBX's. Ultimately this can allow an attacker to keep his or her original number fairly anonymous behind the PBX. If local telecommunication company did detect some suspicious number dialing, which is not an easy task when numbers are dialled randomly by default, the call traces would go back to the local PBX and be lost, or so a hacker hopes!

Commercially war diallers are referred to as phone scanners. These programs are not the tools of hackers, mainly due to their price, and are widely used by security professionals to monitor a large corporate network's vulnerability to war dialing. The two most popular products on the market at present are TeleSweep Secure® from the SecureLogix Corporation and PhoneSweep™ from Sandstorm Enterprise, Inc. Both products provide much richer functionality than the freeware diallers. Apart from easy to use windows interfaces, they both have the ability to dial faster from multiple lines simultaneously which can provide large network coverage in a fraction of the time of a war dialler, such as THC-Scan. For freeware diallers to undertake the same activity multiple copies of the program would need to be run probably on multiple devices. Another advantage of commercial scanners is their ability to collate scan data into one database from which reports can be run to documented findings and produce a user friendly audit history of scan results.

PhoneSweep™, first introduced in 1998, claims to have been "the first commercial telephone scanner" according to its web site www.sanstorm.net. Also the product is advertised as supporting multi-modem scanning with either 4, 8, 12 or 16 modems, and supports the detection of over 300 dial up systems or devices. Not only can PhoneSweep™ detect modems, but equally as important, it is able find PC's or servers running remote management software like Carbon Copy™, pcANYWHERE™, Windows NT RAS and Shiva LanRover. The software will generate reports detailing which services it discovered and on which dial-up numbers. Scan results can be stored in an embedded SQL database from where the program can compile data into detailed reports. Once dial up devices are detected both PhoneSweep™ and TeleSweep Secure® can use generic of customized brute force password guessing. Additionally, PPP identification and hybrid analogue/data scanning for ISDN modems is a possibility with PhoneSweep™.

To add to the products credibility the web site even provides this link GSA# GS-35F-0360J where PhoneSweep™ is listed on the US Government's GSA Schedule.

So, particularly in an outsourced environment where modem usage may be high, using either of the two commercial phone scanners mentioned above will provide the best mechanism to audit, remove and re-configure vulnerable modem's or dial in PC's / Servers.

However, regardless of how often an organizations security team phone scan their own network there is never any guarantee that someone will not try to install another rogue modem or remote access program the next day. Despite this, strong policies on modem usage, remote authentication and the provision of RAS services can help. In detail an organization should ensure:

- A common configuration standard on all dial up devices in terms of make, model and strong authentication (e.g. using something like RSA's SercureID™ token authentication on each modem)

- A modem usage policy to describe when, where and why any modem is to be used (e.g. use one modem pool to provide a known area from which to restrict access)
- Managers, administrators, employees or service providers are directly responsible to maintain the configuration standards on dial up devices under their charge and control (i.e. regularly change) telephone numbers used for modems
- Strict penalties for anyone found not be following the modem usage policy or dial up configuration standard
- A signed security agreement for each service provider connecting to the network via a dial up to ensure regular reports on who is using the access, from where and with what privileges, what psychical security must be present at a foreign office, and rights of the customer being supported to impose unscheduled site audits
- Any dial up server is positioned on a DMZ network connect onto a firewall protecting the internal network so that all connections can authenticated against the firewall (e.g. Check Point Firewall-1 supports RSA Secure ID authentication as standard)

Good policies, procedures and regular internal phone scans are all very well but a more sophisticated and obviously more technical measures is to attempt 'war dialing intrusion detection'.

One basic, inexpensive method used to proactively detect war-dialing activity is to use a workstation based 'war dial trap'. The global telecommunications company AT&T® from their web site offer advice on creating such a trap.

In summary, you need to dedicate a workstation solely is dedicated to identifying incoming war dialing activity. A sure sign of war dialing activity is calls to unused numbers in an organization. Therefore logically if you set up a PC with an attached modem on such a number, making sure it is stand-alone from your network, the PC can then be dedicated to just 24-7 monitoring of that phone line. The modem configuration below can be used to give real-time alerts by:

- configuring the modem to answer all incoming calls
- answer call
- hang up call
- log details to a file
- generate an alarm (possibly a page to the security manager)
- reset the answer incoming calls

To enable most modems to perform this looping activity some sort of scripting communications software using Perl or C/C++ would be required. It is also important assign the trap PC a low, unused number in an organizations telephone number space. Some war dialers scan numbers sequentially and randomly for better scan performance and using low number will give an early alert of activity. A

possible enhancement of this trap PC technique to add an event correlation feature to the script being used. Any initial call to the modem may well be a wrong number, but if an additional call is detected soon after the probability of an attack is higher. The correlation code would contain logic to scrutinize such dialing trends to recognize intrusion activity to a high degree of confidence, before issuing an alert.

All this said creating trap PC is not full proof. As with any intrusion detection system there is always a chance of false positives. But combined with the strong policies and configurations described earlier an organization's susceptibility to 'dial up device compromise can be greatly reduced.

Conclusion

Gladly many businesses have taken the threat of unguarded dial up access seriously for a few years now.

Back in 1998 Sun Microsystems sacked a series of employees just for having modems on their desks! Sounds harsh but when your consider the value of data on corporate network like Sun's, (source code, marketing details, financials) you understand why modems are massive cause of concern. At the time Suns network security manager, Mark Graff, went on record as saying "If a senior manager finds an employee with a modem on their desk they are gone the next day"

Famously also in late nineties, Peter Shipley, a security consultant from California USA, undertook a project to war dialing masses of phone lines in the San Francisco / Bay Area and published his findings. His intention of raising public awareness of the threats posed by unprotected dial up access were most definitely achieved when it was he reported that 1% of all phone lines answered with a modem. Institutions like the Fire Department and local hospitals were found to have modems with no password protection.

If such an exercise was undertaken again tomorrow, it is fair to say the results wouldn't be as shocking. In general, organizations are wiser and have better tools to combat the threat of war dialing. Although, with the growing popularity in today's world to outsource many different IT support tasks, it is all to easy to allow poorly configured dial up access as means to a financial end. Security professionals today must be more and more aware of this and do everything in their power to convince management that 'security should always the primary consideration before allowing any remote access to any private network'.

References

Samuels, Mark, "Outsourcing is in, says Holway" Computing magazine, June 2001, pages 44-45.

http://www.att.com/isc/docs/war_dial_detection.pdf *(September 5, 2001)*

http://www.sandstorm.net/phonesweep/

http://www.sandstorm.net/phonesweep/faq.shtml

http://www.sandstorm.net/phonesweep/specifications.shtml

http://www.sandstorm.net/phonesweep/sysids.shtml (September 5, 2001)

http://telesweepsecure.securelogix.com/
http://telesweepsecure.securelogix.com/security.htm
http://telesweepsecure.securelogix.com/solution.htm?solutionid=42 (September 1, 2001)

Peter Shipley, "Remote Access" http://networkcommand.com/docs/ras2.html (September 4, 2001)

Kingpin@atstake.com, "War Dialing Brief"
http://www.atstake.com/research/reports/wardialing_brief.pdf (September 1, 2001)

http://networkice.com/advice/countermeasures/scanners/war_dialers/default.htm
(September 4, 2001)

Minor Threat & Mucho Maas, ToneLoc v1.10 User Manual, October 1994 pages 1-17

Marcus Goncalves & Steven Brown, Check Point Firewall-1 Administration Guide, 2000, pages 107-114