December 1997
Volume 1, Issue 12

The Insider

Your Knowledgebase on Computer Security

Inside this Issue

Coming Up

Jan '98 **Forget Steroids - Eat more Rice!**
Beefing up the Security within Your Networks

Feb '98 **Who Watches The Watchers?**
Intrusion Detection Systems to Protect Your Network

Mar '98 **Spy Stuff**
Protecting your Mobile Data with Encryption

Apr '98 **DNA Tests**
Identifying your users with strong authentication

Back Issues

Back Issues are Available from http://www.bwa.net/about/insider.html or by contacting us.

Can't Wait for the Info?
Contact our Senior Security Consultant Now
041 4411 149

Technical Incursion Countermeasures Pty. Ltd.
ACN 080 068 891

Phone (08) 9429 8898
Fax (08) 9429 8800
Secure Fax (08) 9454 6042 (bus hrs)

1 Havelock Street
West Perth, WA, 6005
Australia

What is a Remote Access System?

A Remote Access System (RAS) is a system that enables you or your employees to access your LAN from a remote site. In addition the RAS enables the remote computer to act as if it was connected directly to the internal network.

Implementing a RAS can be done several ways. The traditional way was to purchase a several conventional modems and connect them to a terminal server. A new way to do it is to let the remote users use the Internet and create a Virtual Private Network (VPN) connected to your LAN.

Implementing a Remote Access System

Dial-Up RAS

By Dial-Up we mean that the remote users will dial to your physical location to connect to your LAN. A Dial-Up RAS relies on a modem pool of some kind to enable our remote users to connect. These modem pools may consist of several modems, a rack of modems, or a multiplexed ISDN line connecting to an ISDN RAS box (Ascend and Cisco are typical brands).

Prior to the multiplexed ISDN systems; providing a RAS required a large number of analog phone lines and a rotary system at the exchange so that callers had to only dial one number. This made having a RAS very expensive. Modern ISDN systems are still quite expensive, however, the cost is in the RAS box and so it is a capital cost, not an on-going cost. Also some ISDN RAS boxes (the Ascend in particular) can provide additional functions, eg. acting as screening router.

Virtual Private Networks

Virtual Private Networks are one of the current industry buzzwords. They are quite simple in concept, we have a conventional Internet session (say similar to a TELNET session), which is encrypted for privacy. Over that connection we push LAN packets. At each end the LAN packets are stripped out of the Internet connection. The result being that the remote system appears to be connected to the LAN.

The difficult part is ensuring that the data stays private. As is typical in the computing industry, there are a few different standards. Fortunately, the most common is the S/WAN standard and most of the larger firewall vendors support this.

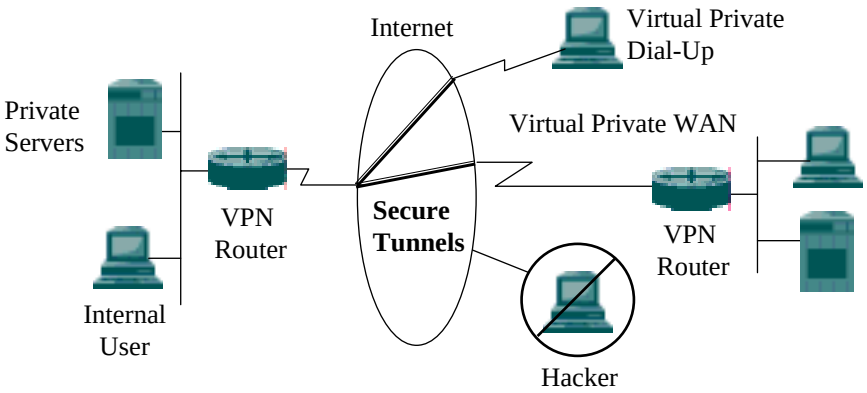
The major reason for installing a Virtual Private Network (VPN) is when your remote sites are far enough away to incur timed calls. Installing a VPN allows your remote sites to call a local ISP and from there connect through your firewall and into your local network. The connection is encrypted, commonly with 56bit DES (the maximum that can currently be exported from the US), and can carry almost any LAN protocol.

Vulnerabilities of a RAS

The first and most obvious one is that once an intruder has obtained a username and a password that works they will be able to access you internal network. They might also be able to access the Internet from your RAS and use your site as cover for other crimes they may commit. Gaining the username

is relatively simple, as it is normally also the e-mail address. Discovering the password is normally done by some brute-force method, either repeatedly attempting different passwords or by attempting to recover the password file from another machine.

The best solution to protect the RAS is to use a strong authentication system. Strong Authentication systems generally require something more than just a typed password, commonly a password calculator is used. We will go into this topic in more depth in the April edition.



A Simplified diagram of a VPN Network

Current Security Advisories

Vulnerability in GlimpseHTTP and WebGlimpse cgi-bin Packages.

Source: AUSCERT Mailing List

AUSCERT has received information that vulnerabilities exist in the GlimpseHTTP and WebGlimpse packages. Both of these packages provide a web interface which allows you to use Glimpse, an indexing and query system, to provide a search facility for your web site.

The cgi-bin programs in these packages perform insufficient argument checking. Due to this, intruders may be able to execute arbitrary commands with the privileges of the httpd process.

Up-to-date information regarding this vulnerability has been made available by the authors of GlimpseHTTP and WebGlimpse. It is available from:

http://glimpse.cs.arizona.edu/security.html

Remote users may be able to execute arbitrary commands with the privileges of the httpd process which answers HTTP requests. This may be used to compromise the http server and under certain configurations gain privileged access.

land.c - An new Denial of Service Attack

This attack totally freezes the Operating System and due to its method of attack, is able to pass through firewalls using packet filtering technologies. Here's how it works: send a spoofed packet with the SYN flag set from a host, on an open port (such as 113 or 139), setting as source the SAME host and port (ie: 10.0.0.1:139 to 10.0.0.1:139).

It is known to be effective against the following systems:

AIX 3, BSDI 2.1, HP External JetDirect Print Servers, HP-UX 10.20, MacOS 8.0, NetApp NFS server 4.3, NetBSD 1.2-1.2a, NeXTSTEP 3.0, NeXTSTEp 3.1, QNX 4.24, SunOS 4.1.4, Windows 95 (including service packs), Windows NT (including service packs), Cisco IOS 10.3(7), Cisco 2511, Cisco 753, Livingston Office Router (ISDN), NCD X Terminals, NCDWare v3.2.1

Systems known not to be vulnerable:

Ascend Pipeline 50 rev 5.0Ap13, Solaris 2.4-2.5.1-2.6, Novell 4.11, Linux 2.0.30-.32, IRIX 6.2-6.4, Digital UNIX 4.0. There may be more on both lists.

As in many of the current Denial of Service attacks, this attack is very difficult to trace and is the code required for it is publically known.

Security Forum

There is a new web-based resource for IT Managers and Network administrators. At

http://www.bwa.net/about/forum.html resides a On-line security forum, where you can post security queries, without receiving large quantities of junk mail or having to sift through 60 questionable opinions each day.

All information is rendered anonymous before being posted to the web page.

What is Technical Incursion Countermeasures?

Technical Incursion Countermeasures is the science of defending a facility from attempts to enter by technological means - as opposed to using a sledgehammer.

As a company, Technical Incursion Countermeasures (TICM for short) provide specialist consultation and devices to improve the security of your computer systems. TICM can be visualised as a System Integrator for security systems. We are able to provide almost any firewall and security device or software, ranging from disk encryption systems for laptops to E3 certified Firewalls and strong Authentication Systems. We also provide security auditing and training.