Security and Firewall Issues

SIR International User Conference New York 2005

David Baxter SIR

Introduction

This presentation will cover some of the ways you can use the Internet and protect yourself at the same time.

You may want to maintain a database from at home or on the road, or you may want to capture data from multi center trials through the Internet.

This paper is about networking and security issues and things you need to know if you want to get access to your database through a network but keep your data and computer secure.

What did we do before the Internet?

Fax/Telex/Voice protocols worked over the phone system. If you had a modem at A and one at B then you could connect the two.

Now days you can email web browse, transfer files, listen to video and audio broadcasts – even log on to your computer at work from the other side of the world. There are thousands of ways to use the Internet. Several of these can be used with sir:

TELNET: lets you logon to a computer and enter commands via a console window – for example, you can run batch jobs or data entry (using the terminal version of SIRForms (SIRFormsc). Dave Doulton's simple but effective SIRAPI creation sirdbmse is designed for use with telnet.

FTP: Lets you transfer files. As you may have seen from Tom's demonstration yesterday, you could build a remote database control system using FTP.

Then there's the SIRSQL Server, which lets you connect to a database remotely using ODBC.

HTTP and its CGI let you run programs remotely via a web browser. You can use SIRWEB.ISA or SIRWEB.CGI to build SIR applications to extract or update data through the web.

This all means we can continue to run things when we are at home or on the other side of the world. Data capture can be done live on multi-centre studies.

Things are much easier for us now.

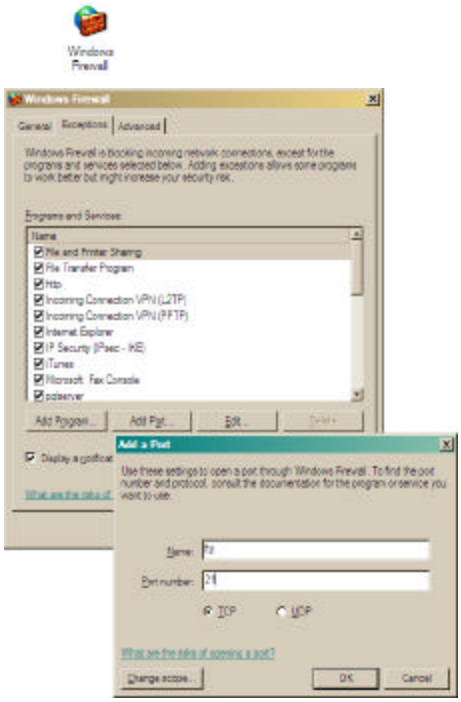
Issues

How do you get access to a computer or database on an internal network from another computer on a different internal network?

Gateways, Firewalls, Port mapping (or port forwarding)

The gateway connects one or more computers on an internal network to the Internet. A gateway will consist of a connection to the internet (e.g. a modem), sometimes an integrated device for diverting messages to the appropriate computer (hub/switch/router) and also sometimes there will be a built in firewall. Most modern broadband modems are a gateway with integrated switch and firewall.

WindowsXP service pack 2 has its own firewall as do other modern OSs.



If you want to get FTP say, to work from your home computer, through to your desk at work then you need to set your firewall to forward messages from a port, say 3021, to your work computer's port 21 (standard). This essentially unblocks port 3021 in your gateway's firewall.

You may have to unblock port 21 in your computer's local firewall.

You will also need to start the ftp server on your work computer. On WindowsXP professional this is done via Internet Information Services (and that may need to be installed through Windows Control Panel, Add or Remove Programs, Add Windows Components),

Once this is done, you will need to find your Gateway's address as it is known on the Internet. The quick way to do this is go to http://www.whatismyip.com/ and it will tell you.

Your IP is 215.224.31.12

Back at home you can start ftp and connect to this address and using the port you mapped to 21:

ftp> open 215.224.31.12 3021
Connected to 215.224.31.12.
220 Microsoft FTP Service
User (215.224.31.12:(none)): david
331 Password required for david.
Password:
230-Welcome to the sir ftp site.
230 User david logged in.

If you need to open several computers in your internal network to ftp then you map different incoming ports to port 21 on each of the machines. You then need to remember which port goes where.

To get Telnet access you need to open port 23, for HTTP (web) it's 80 and for SIRSQLs it's 3050. (These are the default ports for these protocols but you can set up the servers to use others).

Security

TELNET and FTP operate through the same password system as the rest of the operating system. If you are opening the computer to FTP or TELNET it is important not to have easily guessable passwords. You can tighten the security by not allowing certain users to have ftp access.

The SIRSQLs server runs with the permissions of the process owner. The passwords given to the server by incoming connections are not used for system security purposes (but to identify individual users when more than one user is connected). If you were opening the SIRSQLs port then you would want to ensure that all databases that the user that starts the server has access to have appropriate database password protection.

HTTP servers will sometimes allow you to set the user whose permissions are used to run CGI programs. The default is a user who has little rights beyond being able to execute programs in the CGI directory. You could use ISS to make you login before you can execute programs in a particular directory. Apache does this through suEXEC (http://httpd.apache.org/docs/suexec.html).
If you are using the sirweb.cgi or sirweb.isa programs then you can also code some security in PQL by using the CGIVARSV functions to identify the user (and ask for a password) before executing the bulk of the program. See CGIMENU.LOGIN in the CGIMENU example.

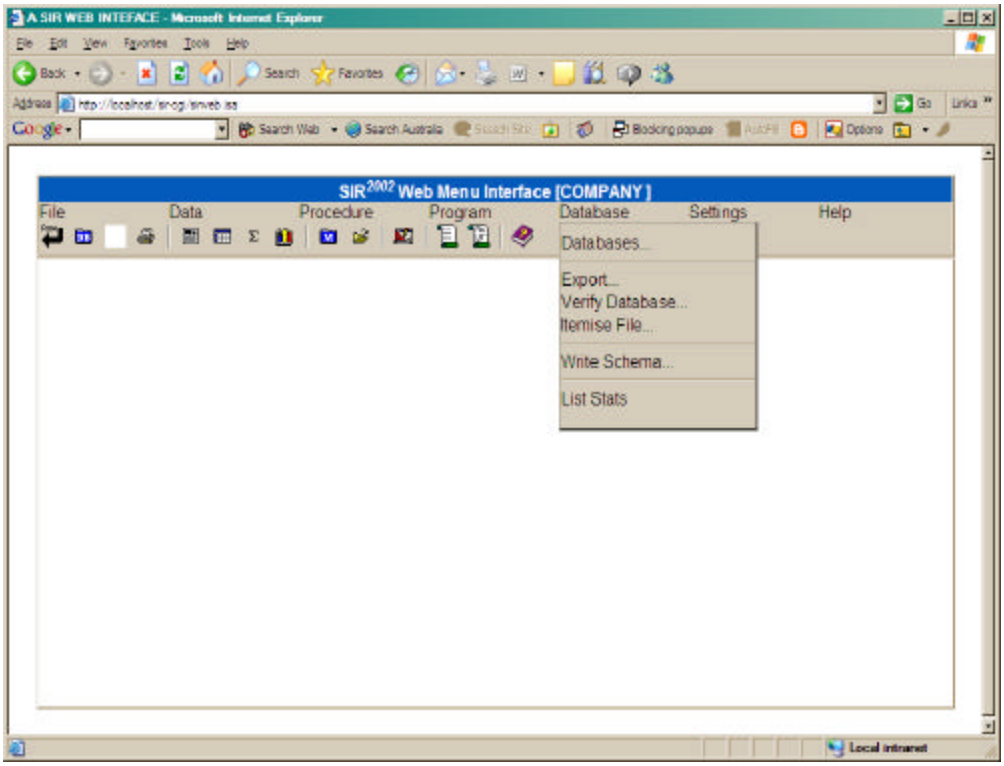
SSL
Secure Sockets Layer is a protocol that encrypts data transferred through the connection using a unique private key. This is to stop information being intercepted as it is being transferred between the server and client.

CGIMENU
This example application demonstrates the need for security. When properly installed this sirweb.isa application can be used to control sir database and other files remotely via a web interface – it can also be used to maintain its own source code as you can edit and run procfile members with this system. This example will only work on windows http servers (as sirweb.isa is only available on windows).
Install IIS
Don't map anything to port 80 on this machine from the gateway.
Unzip CGIMENU.zip into c:\inetpub\wwwroot\
Configure the sir-cgi directory to be read and execute
Set the user to basic authorization or integrated windows (the later won't work from non-windows clients).
Start your Internet browser and go to
http://localhost/sir-cgi/sirweb.isa?sirapp=sysproc.cgimenu.run

You will be prompted for a login from the server – use your windows login and password on the server machine. Then there is another prompt, this time from the sir code for a name and a password. The password is APPLE05.

With this interface you can delete files easily:

```
program
pql escape "cmd /c del c:\Inetpub\wwwroot\sir-cgi\test.txt"
end program
```



Summary

Good Internet system can make your work easier. Default security can make it hard to set these things up. An Internet application is not something that you want to set up quickly and easily as it probably means the security is lacking.