Global Information Assurance Certification Paper

Secure (and free) IP tunneling using Zebedee

Overview

The need to transfer data securely over the internet has become increasingly important in a world where hackers and snoops are lurking around every corner. There are many products which offer this security including VPN's, ssl, and SSH, among others. While these products are robust and work very well, some are expensive and others are difficult to implement.

One simple and free way to send encrypted data across the internet (or between any TCP/IP connection) is by using Zebedee. Zebedee is "a simple program to establish an encrypted, compressed "tunnel" for TCP/IP or UDP data transfer between two systems" (Zebedee).

Its main goals, as stated on its website, are as follows:

- Provide full client and server functionality under both UNIX and Windows 95/98/NT.
- Be easy to install, use and maintain with little or no configuration required.
- Have a small footprint, low wire protocol overhead and give significant traffic reduction by the use of compression.
- Use only algorithms that are either unpatented or for which the patent has expired.
- Be entirely free for commercial or non-commercial use and distributed under the term of the GNU General Public License.

What's In a Name

Zebedee is named for it's three main components:

- **Z**lib compression
- **B**lowfish encryption and
- **D**iffie-Hellman key agreement.

Zlib is **"**a free, general-purpose, legally unencumbered -- that is, not covered by any patents -- lossless data-compression library for use on virtually any computer hardware and operating system" (zlib).

"Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use" (Counterpane Internet Security)

Blowfish encryption is considered to be faster than DES and it is thought by many to be a superior algorithm.

The Diffie-Hellman key agreement is a standard which "describes a method…whereby two parties, without any prior arrangements, can agree upon a secret key that is known only to them (and, in particular, is not known to an eavesdropper listening to the dialogue by which the parties agree on the key). This secret key can then be used, for example, to encrypt further communications between the parties" (RSA Security).

Installing and Configuring VNC and Zebedee

This paper will explain how to set up Zebedee to encrypt data across a VNC (Virtual Network Computing) connection.

VNC is a freeware program that allows a user to view and use a computer remotely as if they were sitting in front of it.

Both Zebedee and VNC use a Host/Client schema. The first thing that needs to be done is to install both VNC and Zebedee. They can be downloaded from the following sites:

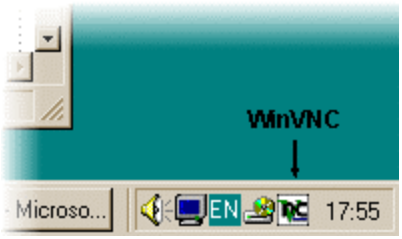
Zebedee:	http://www.winton.org.uk/zebedee/index.html
VNC:	http://www.uk.research.att.com/vnc/

In this tutorial, we will be using Windows NT 4.0 as our operating system.

The first item of business is to install VNC viewer on the host (server) machine. After extracting the downloaded zip file, double click on 'setup.exe' in the 'vnc_x86_win32\winvnc' folder. The installation wizard will now start. The wizard may tell you that you need to close any running versions of VNC. Make sure this is done and click 'OK.' At the welcome window, click 'Next.' Then, read the license agreement and click 'Yes.' Next, choose the directory to which you want VNC installed, click 'Next', choose which program group you want created, and click 'Next' again.

Now we need to install VNC as a service. To do this, we need to go to the VNC program group created by the installer. By default, the program group is in the following location: Start Menu -> Programs -> VNC -> Administrative Tools. First, click on the "Install Default Registry Settings" icon. This ensures proper screen refreshes with certain applications. Next, click on the "Install VNC Service" icon. This will install VNC as a service on an NT 4 machine (Service Pack 3 or higher). You will then be asked to set a password for VNC. Do this and click 'OK.' VNC has now been installed on the host machine.

When the VNC server is running, the icon in the graphic below will be displayed in your task bar.



To install VNC on the client machine, follow the instructions above for the host machine. However, do not install VNC as a service.

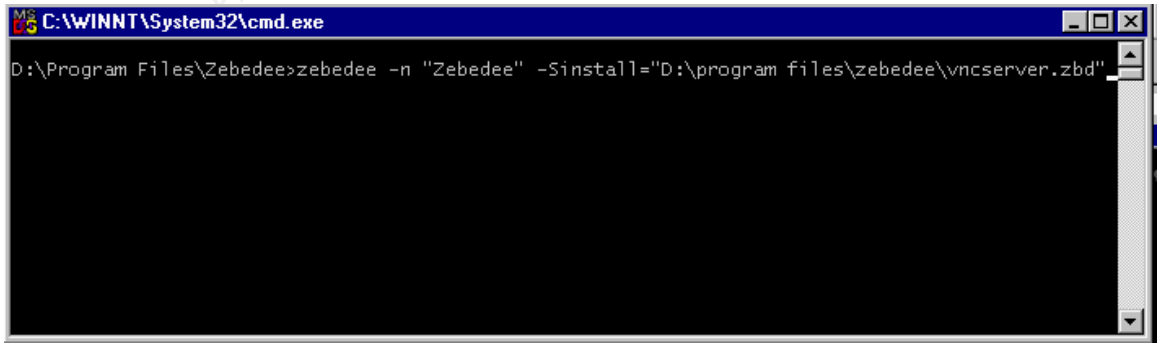
Zebedee is downloaded in zip format and uses and install wizard for a simple installation.

Before setting up Zebedee and VNC to work together, we must make one change in the Windows registry. VNC, by default, does not allow Loopback connections (connecting to the machine you are using). However, this needs to be enabled when using Zebedee. The following instructions are taken directly from the Zebedee website:

> Saving the following snippet (without any leading spaces) in file a and then importing it into **regedit** will do the trick:
>
> ```
> REGEDIT4
>
> [HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3]
> "AllowLoopback"=dword:00000001
>
> [HKEY_LOCAL_MACHINE\SOFTWARE\ORL\WinVNC3\Default]
> "AllowLoopback"=dword:00000001
> ```

Once Zebedee is installed, the first thing we need to do is configure the host. The easiest way start Zebedee and keep it running is to install it as a service. Zebedee is command-line based, so we will be using a DOS prompt to type in the commands. In a DOS window, go the directory where Zebedee is installed. Then, type in the following command:

```
zebedee -n "Zebedee Client Service" -Sinstall=c:\zebedee\vncserver.zbd
```

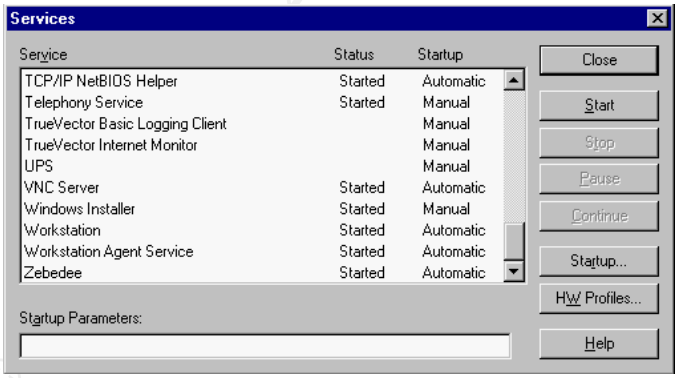


This line assumes that you have Zebedee installed in the D:\program files\ directory. This will install Zebedee as a service with name "Zebedee." The -Sinstall="D:\program files\zebedee\vncserver.zbd" option installs the service using the configuration file vncserver.zbd. The configuration file, which is included with the Zebedee installation, is printed below:

```
#
# Zebedee server sample config file for tunnelling VNC traffic
#

verbosity 1             # basic messages only

keygenlevel 2           # Generate maximum strength private keys

server true             # Yes, it's a server!
detached true           # Convert to daemon if possible

# Set up allowed redirection ports

redirect 5900-5950      # Redirect VNC server ports
redirect telnet         # Allow telnet too for initial server start

compression zlib:9      # Allow maximum zlib compression
keylength 256           # Allow key length up to 256 bits
```

The configuration is fairly self-explanatory. VNC, by default uses a tcp port between 5900-5950. The line "`redirect 5900-5950`" line specifies that these ports will be used in a secure connection using Zebedee.

After the service is installed, it can now be viewed in the services control panel.



Once the host computer is configured, we can now move to the client machine. First, install Zebedee on the client machine. Now we can initiate a secure connection to the host from the client. We will again be using a zebedee configuration file. The file we will be using is included with the zebedee installation. It is called vncviewer.zbd. Here are the contents of the file:

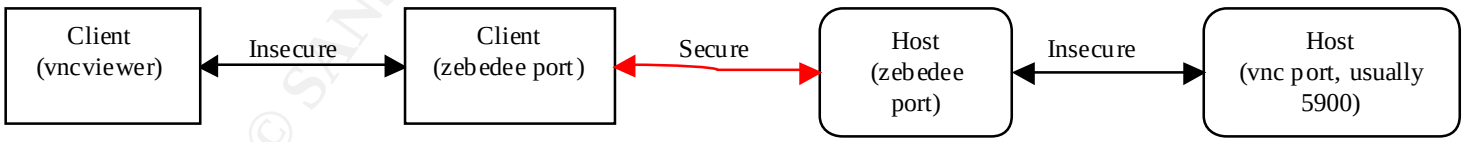
```
#
# Zebedee configuration file to start up a tunnelled VNC session
#
```

```
# Usage: zebedee -f vncviewer.zbd remote-host:vnc-port
#

verbosity 1 # Basic messages only

server false      # It's a client
detached true     # Detach from terminal

message "Starting VNC viewer"

# On Windows systems you might use the following:

command '"d:\Program Files\ORL\VNC\vncviewer.exe" localhost:%d'

# On UNIX systems you might use the following:

# command 'vncviewer localhost:%d'

compression zlib:9      # Request normal Zlib compression
```

The configuration file is very straight forward. In the line `command '"d:\Program Files\ORL\VNC\vncviewer.exe" localhost:%d'` we are telling Zebedee to execute vncviewer.exe (the client program included with VNC). The localhost:%d tells the vncviewer which port we wish to connect to. The "%d" in the string is automatically replaced with the local port number that Zebedee will be using to securely connect to the host.

While it may seem counter-intuitive to tell vncviewer to connect to the localhost (the client computer), this is actually correct. When we execute zebedee, it sets up a secure connection between a high port number (%d) on the client machine and a high port number on the host machine. So by telling vncviewer to connect to the localhost:%d, we are telling it to use the secure connection. On the host side, by running the zebedee service and having it redirect the vnc ports (5900-5950 in this case), any connection that attempts to use the vnc ports will be redirected to a higher port which has been reserved for the secure connection.

Below is a diagram of the connection.

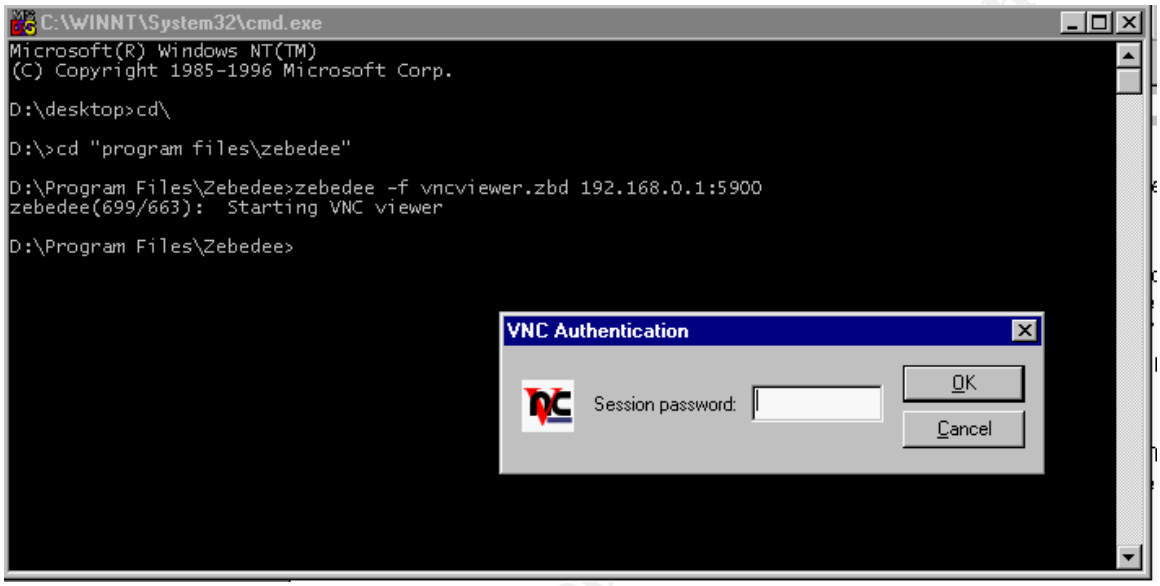


Now, we can open a DOS prompt and start the connection. At the DOS prompt, go to the directory where Zebedee is installed. Then, type in the following command:

```
zebedee.exe -f vncviewer.zbd host.ip.address:5900
```

Substitute host.ip.address with the ip address of the host system. The 5900 should correspond to the port the VNC host is serving.

In the DOS window, you should see the message "Starting VNC viewer." A window will then open up, asking for the VNC password.



After the password is entered, the vncviewer will display the host computer's screen.

We have now created a secure session between the client and host computer. Any data that is exchanged in this session between the host and client computer is encrypted.

Identity Checking

In its default configuration, Zebedee simply creates a secure connection between two points. This however, does not guarantee that the data is being sent to the place that you think it is being sent. These security attacks are called "man-in-the-middle" attacks. To avoid this problem, you can use a fixed private key. Zebedee then can "…generate a key "fingerprint" by hashing together the modulus, generator and public key value" (Zebedee). Instructions on how to implement identity checking can be found on the Zebedee manual (website printed on works cited page).

Nathan Rinsema
Version 1.2d

Works Cited

AT&T. "WinVNC - The Windows NT VNC server."
URL: http://www.uk.research.att.com/vnc/winvnc.html (June 26, 2001).

Counterpane Internet Security. "The Blowfish Encryption Algorithm."
URL: http://www.counterpane.com/blowfish.html (May 3, 2001).

Fourmilab North America. "Speak Freely: Blowfish Encryption."
URL: http://www.fourmilab.to/speakfree/windows/doc/blowfish.html (May 17, 2001).

RSA Security. "PKCS #3: Diffie-Hellman Key-Agreement Standard."
URL: ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-3.doc (May 3, 2001).

Zebedee. "Zebedee — a simple, free, secure TCP and UDP tunnel program."
URL: http://www.winton.org.uk/zebedee/manual.html (May 3, 2001).

zlib HomeSite. "zlib."
URL: http://www.gzip.org/zlib/ (May 3, 2001).