

---

# REMOTE LOGIN

TORSTEINBØ  
NOVEMBER 2011

This document is part of the final evaluation for the course **Sicherheit in Applikationsprotokollen** at JKU. It covers the following application protocols for remote administration:

- Remote CLI:
  - Telnet
  - rlogin
  - SSH
- Remote Desktop:
  - VNC
  - Microsoft RDP
  - Citrix ICA
  - Other uses

A general overview will be given of each protocol with some extra details concerning the security.

A brief overview of KVM switches is included to give a historical context of the transition from command-line to GUI-based remote administration.

# REMOTE CLI

## TELNET

Developed in 1969, telnet enabled access to the command-line interface (CLI) of remote hosts. Telnet uses the client/server model, where the host you want to access remotely is configured as the server, allowing remote clients to control its CLI. The telnet protocol uses TCP and has port 23 defined as its standard by IANA.

On the 5<sup>th</sup> of March, 1973, the telnet standard was defined with the release of The Telnet Protocol Specification (RFC 854<sup>1</sup>) and the Telnet Option Specifications (RFC 855<sup>2</sup>). These documents are referred as STD 8, meaning that it was one of the first Internet Standards defined by the Internet Engineering Task Force (IETF) and that it is compatible with the TCP/IP stack.

When using the telnet protocol all information is transferred as plain-text in ASCII-format. The output on the CLI will therefore be presented identical on the client, as it would on a monitor directly connected to the host. All data exchange uses an 8-bit channel to transfer 7-bit ASCII data. Special telnet characters are denoted by setting the last bit (high bit) to 1.

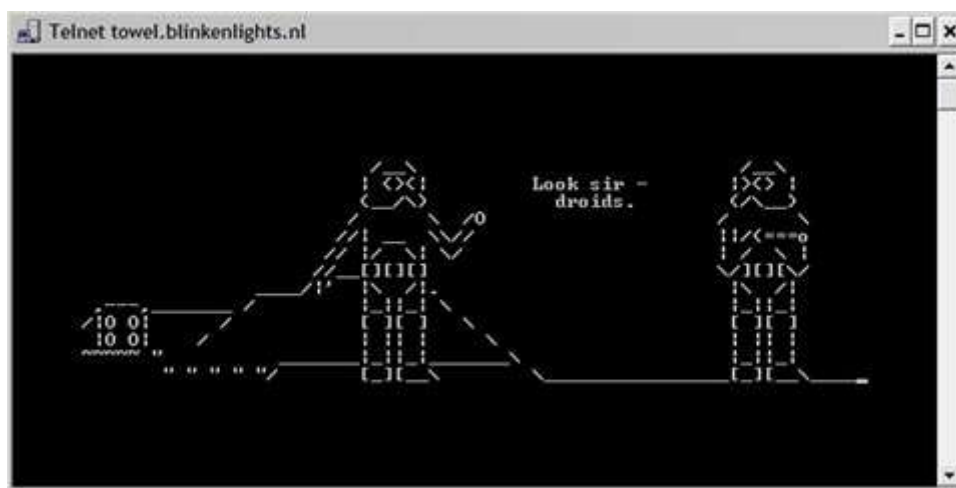


FIGURE 1: STAR WARS ASCIIIMATION -- TELNET://TOWEL.BLINKENLIGHTS.NL (PORT 23)<sup>3</sup>

## USE AND SECURITY

Today most network equipment and OS's ship with a telnet server built-in. Because the protocol offers no encryption or authentication it is usually disabled in its default form, and it is recommended to use alternatives such as Secure Shell (SSH). Even in situations where a Telnet server is available on a local network, it will in most be blocked by the firewall so that outsiders cannot gain access. If remote access should be needed, one possibility is to redirect traffic over a secure channel, such as a VPN or SSH tunnel.

While it is not common that vulnerabilities exists in the telnet service protocol, several exploits exists in the various telnet server and client services, allowing buffer overflow and similar attacks to take place.

<sup>1</sup> <http://tools.ietf.org/html/rfc854>

<sup>2</sup> <http://tools.ietf.org/html/rfc855>

<sup>3</sup> <http://www.telnet.org/hm/places.htm>

## RLOGIN

rlogin is a program provided on many UNIX systems as part of r-services<sup>4</sup> and allows establishing a terminal session on a remote host. Here is an excerpt from RFC 1282<sup>5</sup> that describes the elementary functionality of rlogin:

*The rlogin facility provides a remote-echoed, locally flow-controlled virtual terminal with proper flushing of output. It is widely used between UNIX hosts because it provides transport of more of the UNIX terminal environment semantics than does the Telnet protocol, and because on many UNIX hosts it can be configured not to require user entry of passwords when connections originate from trusted hosts.*

One feature of rlogin is that it passes the terminal type description from the local host computer to the remote host computer. The terminal type description allows terminal-aware programs, such as full-screen text editors, to operate properly across connections created with rlogin.

Apart from this, rlogin suffers most of the same security disadvantages as telnet, such as the fact that all communication, including passwords, is transmitted in clear-text.

The trusted hosts feature bypasses password authentication when an rlogin/rhosts-file is specified. This poses a great security risk as the files themselves are not very well secured, and in many cases can be found on the host's NFS share.

Because of these problems, rlogin is not in much use today and has mostly been replaced by the superior SSH protocol.

## SECURE SHELL (SSH)

In the early days of the internet, it became apparent that access to remote UNIX-like systems needed to be secure to combat password-sniffing and other security threats. The Finish researcher Tatu Ylönen designed the first version of the SSH protocol and released it as a tool during the summer of 1995. With the huge popularity of the tool; Ylönen decided to found SSH Communications Security during December the same year.

SSH is a network protocol that offers encryption and public key authentication. When a client connects to the SSH server, a secure channel is established between both endpoints. When properly authenticated, the client gains access to multiple services, including: Remote CLI, remote command execution, secure file transfer, packet forwarding/tunneling and many more.

The remote CLI, or *shell account* as it is often called, is perhaps the most popular feature and allows the replacement of older protocols such as Telnet and rlogin. Shell accounts are user accounts with access to the services of a kernel and is where SSH derives its name from.

### SSH-2

Today a revised version under the title SSH-2 has become the official standard. This version was developed by the Internet Engineering Task Force's (IETF) own SSH working group. Not only features, but also the security has been improved. SSH-2 sports the Diffie-Hellman key exchange and strong integrity checking via message authentication codes.

The most recent vulnerability is one that was discovered in 2008 that allowed the recovery of up to 32 bits when the encryption method used was CBC<sup>6</sup>.

---

<sup>4</sup> A collection of several remote administration tools: [http://www.itworld.com/nl/lnx\\_tip/01042002](http://www.itworld.com/nl/lnx_tip/01042002)

<sup>5</sup> <http://www.ietf.org/rfc/rfc1282.txt>

A popular use for SSH today is tunneling unsecure traffic over a secure SSH tunnel. The difference compared to a regular VPN is that SSH operates on the application layer, with the drawback that applications are required to redirect their communication through the tunnel by specifying a proxy configuration. This is not needed for VPN protocols such as IPsec since this technology works on the Internet layer and is practically invisible for the applications themselves.

## REMOTE DESKTOP

As server systems started requiring GUIs for doing configuration tasks, it became apparent that text-only access was insufficient. This meant finding a new way of doing remote administration.

### KVM (KEYBOARD, VIDEO, MOUSE) SWITCHES

Even though it is not an application protocol, it is worth to briefly mention KVM.

Originally KVM, or KV switches back in the early 80s, were used in server rooms for text consoles. Having an individual monitor and input devices per computer resulted in server rooms quickly filling up, so the solution became KV switches.

As soon as computers shipped with GUIs, it was natural to update the KV switches to account for this by adding mouse input. At the time (beginning of the 90s), having software do remote desktop would require quite a lot of processing power and bandwidth for rendering, compression, and data transfer. This wasn't available at this time, but was in development.

As the new millennium was nearing, hardware started to catch up, and Microsoft started pushing its own NT server system that came with its own remote desktop server software. Ironically, you could now remove all the excess hardware and cables that the KVM switches brought with them and replace them with a far more cost-effective and flexible tool.

### REMOTE FRAME BUFFER (RFB) AND VIRTUAL NETWORK COMPUTING (VNC)<sup>7</sup>

Remote frame buffer (RFB) was originally developed by Olivetti Research Laboratory. RFB is the underlying protocol used in VNC (also developed by Olivetti) and works at the frame buffer level of the windows system, which allows easy cross-platform compatibility. The drawback is that the data is sent per pixel, which can have quite a performance impact compared to other alternatives.

While originally intended for thin-clients RFB became incorporated into the VNC project, which later led to the open source release of both technologies. Today RealVNC is the official software package, developed by many of the original Olivetti researchers, but because of the open source nature, many alternatives exist, including more advanced commercial versions.

### SECURITY

From a security point of view VNC offered originally no security, but in newer versions of VNC clients this is of course built in. VNC works in stateless mode; this means that if you disconnect and then reconnect, the desktop will appear as it was left. Other protocols, such as Microsoft's RDP, will ask the user to login through the same account logon screen as found on local machines. Because of the stateless nature VNC credentials can also be kept separated from domain credentials.

When a connection is being established the security will be agreed upon. The server is responsible for selecting the security, and the selection can be extended by additional plugins. As standard, VNC ships with VNC Authentication, as well as TLS and certain application specific security protocols.

---

<sup>6</sup> [http://en.wikipedia.org/wiki/Secure\\_Shell](http://en.wikipedia.org/wiki/Secure_Shell)

<sup>7</sup> <http://www.realvnc.com/docs/rfbproto.pdf>

Some of these security protocols only encrypt the initial authentication and not the subsequent data exchange.

Apart from vulnerabilities in the various client and server installation, it seems popular to save the server passwords in the registry when running on Windows. This can then be retrieved, and if encrypted, an offline brute-force can be performed.

## MICROSOFT RDP (REMOTE DESKTOP PROTOCOL)<sup>8</sup>

RDP is Microsoft's proprietary remote desktop offering. The first version of RDP was version 4.0 and was introduced by Microsoft in 1998 as part of a special version of the Windows NT server OS. Although based on the ITU (International Telecommunication Union) T.120 series of protocols, RDP has been extended with a great range of features that is only supported by the official application itself. Still, an open alternative based on RDP 5.0 (released in 2000) called FreeRDP<sup>9</sup> is available for download.

Today the technology has grown quite advanced and boasts a broad feature set including:

- 32bit color
- Audio redirection to client system
- File redirection: making local files available on remote host
- Seamless window: Instead of streaming a whole remote desktop, you can stream a single application or window.
- RemoteFX: Virtualized GPU support where the remote computer gains access to the local GPU.

## SECURITY

RDP has two security modes: standard and enhanced. In standard mode the authentication is done with RSA public key cryptography and the encryption is negotiated to one of four levels: Low, Client Compatible, High, and FIPS Compliant. The server handles the configuration of the encryption level.

The levels are best described from Microsoft's own documentation<sup>10</sup>:

- *Low: All data sent from the client to the server is protected by encryption based on the maximum key strength supported by the client.*
- *Client Compatible: All data sent between the client and the server is protected by encryption based on the maximum key strength supported by the client.*
- *High: All data sent between the client and server is protected by encryption based on the server's maximum key strength.*
- *FIPS: All data sent between the client and server is protected using Federal Information Processing Standard 140-1 validated encryption methods.*

After authentication three symmetric session keys are generated. These are derived from random values generated by the client and the server. They are used in the following manner: client-to-server traffic encryption, server-to-client traffic encryption and in generating the MAC hash to insure data integrity.

Enhanced RDP security gives the option to use familiar security protocols such as TLS and Kerberos. This is then used instead of the security features specified as standard RDP security, and let's third

---

<sup>8</sup> [http://msdn.microsoft.com/en-us/library/cc240446\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc240446(v=PROT.10).aspx)

<sup>9</sup> <http://www.freerdp.com/>

<sup>10</sup> [http://msdn.microsoft.com/en-us/library/cc240770\(v=PROT.10\).aspx](http://msdn.microsoft.com/en-us/library/cc240770(v=PROT.10).aspx)

party developers work closely with security implementations they are more familiar with. The use of Network Level Authentication when using Microsoft's CredSSP as the External Security Protocol is also possible.

Even though the communication is secure, vulnerabilities to other parts of the protocol do pop up: as early as March this year Microsoft released a patch were an attacker could gain full access to a computer by exploiting the way RDP loads DLL-files.<sup>11</sup>

## CITRIX'S INDEPENDENT COMPUTING ARCHITECTURE (ICA)

While remote administration and management is an important usage of remote desktop technology, an even greater use is found in desktop virtualization. With the ICA protocol the user can connect directly to their desktop or applications hosted on a central server. This type of remote desktop service delivery makes it easier to manage enterprise IT in a central location and offers a greater flexibility and availability by letting the user connect to it from their own PC, thin-client or even web browser.

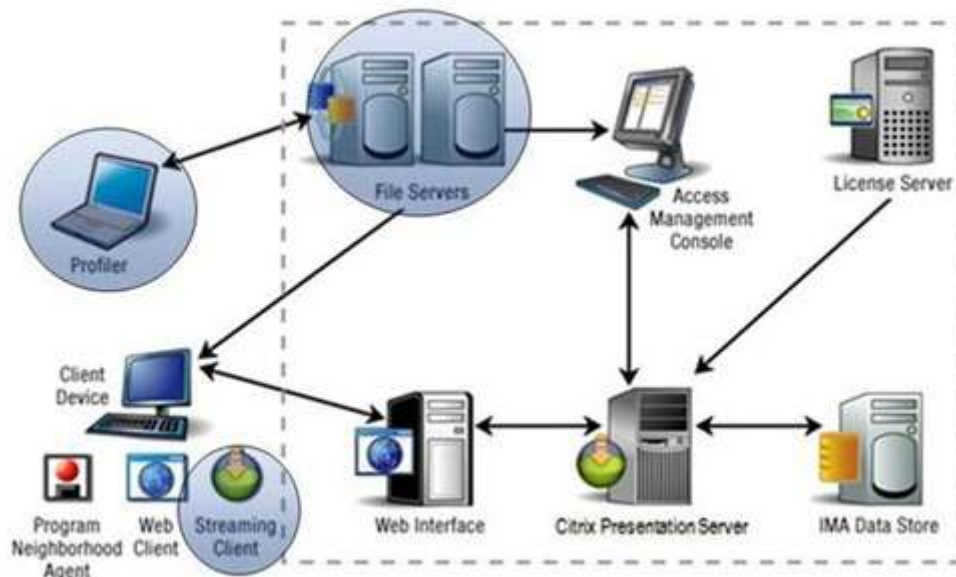


FIGURE 2: CITRIX INFRASTRUCTURE (SOURCE: CONGUIDE.COM)

As you can see in the figure above, the setup requires quite an infrastructure and is not targeted at individuals.

### SECURITY

All communications between the Access Gateway Plug-in and the Access Gateway are encrypted with SSL. The SSL protocol allows two computers to negotiate encryption ciphers to accomplish the symmetric encryption of data over a secure connection.

You can select the specific cipher that the Access Gateway uses for the symmetric data encryption on an SSL connection. Selecting a strong cipher reduces the possibility of malicious attack. For SSL connections RC4, 3DES, or AES encryption ciphers are available. The default setting is RC4 128-bit. The MD5 or SHA hash algorithm is negotiated between the client and the server.

<sup>11</sup> <http://technet.microsoft.com/en-us/security/bulletin/ms11-017>

The Access Gateway uses RSA for public key encryption in a secure connection. The encryption ciphers and hash algorithms that you can select for symmetric encryption are as follows:

- RC4 128-bit, MD5/SHA
- 3DES, SHA
- AES 128/256-bit, SHA

Similarly to Windows RDP, ICA also contains vulnerabilities in its various software packages and it is therefore crucial to keep up on the latest patches. Because the Citrix implementations often incorporate a Web Interface, additional attack vectors are created.

## OTHER REMOTE DESKTOP USES

### MICROSOFT VIRTUAL PC

When you create and use virtual machines you access them through a console. For Microsoft's Virtual PC this console is actually a remote desktop connection and takes advantage of much of the same technology as RDP.

### VMWARE VSPHERE

The vSphere platform combines both the world of virtual machine consoles with remote administration. The vSphere client connects to the vSphere cloud infrastructure and lets you access your virtualized servers remotely in the same fashion as out-of-band management implementations found on many physical servers. This means you can shutdown, restart and edit hardware settings without losing the connection to the server and can remotely administer it even when it is off.