

Private Communication on a Shared Network

This factsheet explains why special measures need to be taken to protect some network transmissions, and discusses the two most common ways in which that protection is provided.

On most of JANET and the Internet, messages are transmitted as plain text. This means they can be read relatively easily by anyone with either a computer connected to the network or access to routers and other systems through which the messages pass. The effect is the same as sending greetings on a postcard, rather than in a sealed envelope, through the postal system. When sending sensitive information – for example using passwords to log in to remote systems or sending messages about people, examinations or finance – the risk of a message being read in transit may not be acceptable. There are a number of ways to improve the privacy of messages sent across a public network, most of which involve the use of encryption. It is important to remember that encrypted transmission can only protect a message while it is passing across the network. If the message is not stored securely on both the sending and receiving machines, or care is not taken while it is being written or read, the likelihood of it being read at those points is much greater than on the network between them.

There is no single standard for encryption on the Internet due to a number of technical, commercial and political factors. Since both parties to an encrypted communication must use the same method, negotiation is often required to agree on a method and version which both can use. Different versions and different nationalities of the same program may not work together because of legal restrictions. The most common methods can be divided into two types: some provide an encrypted 'tunnel' across the network through which a sequence of messages can be exchanged; others encrypt a single file, such as a document or e-mail message, before sending it across the network in the normal way.

Tunnelling

Tunnel protocols are most often used for interactive operations such as browsing a web site, reading e-mail or connecting to a remote terminal. There are four protocols in common use:

- Secure Sockets Layer (SSL, also known as TLS)
- Secure Shell (SSH)
- Point-to-Point Tunnelling Protocol (PPTP)
- Secure Internet Protocol (IPSEC)

SSL was designed by Netscape to allow encrypted communication between a web browser and server and is now supported by most popular browsers and servers. It is probably the most widely used encryption method, common on e-commerce sites to protect sensitive information such as passwords and credit card numbers as they are exchanged between buyer and merchant. SSL can support other applications including remote access to e-mail.

SSH was written as an encrypted replacement for the telnet system which allows remote machines to connect to servers as if they were local terminals. It can also be used as a tunnel for other protocols, for example to read mail from remote mailboxes or support remote graphical terminals. SSH is commonly

used on Unix servers, and clients and servers also exist for Windows and other operating systems. SSH version 1 servers have been attacked successfully, so version 2 of the protocol should be used.

PPTP is a protocol written by Microsoft to allow encrypted dial-up connections between Windows clients and servers. Concerns have been expressed about the security of the protocol and, although some of these have been addressed, the protocol is not recommended where a network is shared with other users.

It is possible to use the IPSEC protocol to establish point to point tunnels, known as Virtual Private Networks (VPNs). Draft standards are being developed by the Internet Engineering Task Force, but most products available now use proprietary hardware or software and are unlikely to be compatible with each other.

File Encryption

The most common file encryption system is Pretty Good Privacy (PGP), which allows a file or e-mail message to be encrypted for a particular recipient. The encrypted message can then be transferred using any normal method: e-mail, ftp, web, etc. Unlike the tunnelling protocols which work between two computers, file encryption systems work between two people. Messages can be kept in encrypted form on the sending and receiving computers and decrypted temporarily when the reader requires. PGP for e-mail and file transfer is available for many operating systems. Programs to encrypt files or discs for local storage are the subject of a Joint Information Systems Committee (JISC) paper, which can be found at: http://www.jisc.ac.uk/index.cfm?name=jcas_p

How Private is Private?

Encryption does not provide perfect protection against a third party reading the message. The mathematical algorithms used can be reversed if sufficient computer power and time is available. Most methods can be made stronger by using a longer encryption key (note that this does not apply to the current, flawed, implementation of PPTP). It has been estimated that SSL with a key length of 64 bits would require the resources of a corporation to decrypt. PGP uses a different measure of key length and here a key of at least 1536 bits is recommended. Both of these figures will increase in future as computers become more powerful.

Websites

Introduction to SSL:	http://www.windowsecurity.com/articles/Secure_Socket_Layer.html
SSH home page:	http://www.ssh.org/
PPTP:	http://msdn.microsoft.com/archive/en-us/dnarwebtool/html/understanding_pptp.asp
Problems with PPTP:	http://www.schneier.com/pptp.html
PGP collection of resources:	http://www.gla.ac.uk/scotmid/publications/pgp.html
What encryption can and cannot do:	http://www.schneier.com/essay-whycrypto.html

Books

The definitive book on cryptographic algorithms:

- Schneier, Bruce: *Applied Cryptography*, Wiley, 1995, ISBN 0471117099.

For more on the uses of cryptography:

- Kaufman and Perlmann: *Secure Networking: Cryptography, Protocols and Algorithms*, Prentice-Hall, 1995, ISBN 0130614661.

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

JANET® is a registered trademark of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of the trademark. JANET, the United Kingdom's education and research network, is funded by the Joint Information Systems Committee (JISC).