This file is part of the documentation for the Linux FreeS/WAN project.
See the documentation index or project home page for more information.

Glossary for the Linux FreeS/WAN project

Entries are in alphabetical order. Some entries are only one line or one paragraph long. Others run to several paragraphs. I have tried to put the essential information in the first paragraph so you can skip the other paragraphs if that seems appropriate.

Jump to a letter in the glossary

numeric A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Other glossaries

Other glossaries which overlap this one include:

- glossary portion of the Cryptography FAQ
- an extensive crytographic glossary on Terry Ritter's page.
- The NSA's glossary of computer security on the SANS Institute site.
- an Internet Draft Crypto Glossary
- the IETF provide a glossary of Internet terms as RFC 1983
- a small glossary for Internet Security at PC magazine
- The glossary from Richard Smith's book Internet Cryptography

More general glossary or dictionary information:

- Free Online Dictionary of Computing (FOLDOC)
  - North America
  - Europe
  - Japan

  There are many more mirrors of this dictionary.
- CRC dictionary of Computer Science
- The Jargon File, the definitive resource for hacker slang and folklore
  - North America
  - Holland
  - home page

  There are also many mirrors of this. See the home page for a list.
- A general technology glossary
- An online dictionary resource page with pointers to many dictionaries for many languages
- A search engine that accesses several hundred online dictionaries
- O'Reilly Dictionary of PC Hardware and Data Communications Terms

Definitions

3DES (Triple DES)
: Using three DES encryptions on a single data block, with at least two different keys, to get higher security than is available from a single DES pass. The three-key version of 3DES is the default encryption algorithm for Linux FreeS/WAN.

  IPSEC always does 3DES with three different keys, as required by RFC 2451. For an explanation of the two-key variant, see two key triple DES. Both use an EDE encrypt-decrypt-encrpyt sequence of operations.

  Single DES is insecure.

  Double DES is ineffective. Using two 56-bit keys, one might expect an attacker to have to do 2^{112} work to break it. In fact, only 2^{57} work is required with a meet-in-the-middle attack, though a large amount of memory is also required. Triple DES is vulnerable to a similar attack, but that just reduces the work factor from the 2^{168} one might expect to 2^{112}. That provides adequate protection against brute force attacks, and no better attack is known.

  3DES can be somewhat slow compared to other ciphers. It requires three DES encryptions per block. DES was designed for hardware implementation and includes some operations which are difficult in software. However, the speed we get is quite acceptable for many uses. See benchmarks below for details.

Active attack
: An attack in which the attacker does not merely eavesdrop (see passive attack) but takes action to change, delete, reroute, add, forge or divert data. Perhaps the best-known active attack is man-in-the-middle. In general, authentication is a useful defense against active attacks.

AES
: The Advanced Encryption Standard, a new block cipher standard to replace DES being developed by NIST, the US National Institute of Standards and Technology. DES used 64-bit blocks and a 56-bit key. AES ciphers use a 128-bit block and are required to support 128, 192 and 256-bit keys. Some of them support other sizes as well. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks.

  Fifteen proposals meeting NIST's basic criteria were submitted in 1998 and subjected to intense discussion and analysis, "round one" evaluation. In August 1999, NIST narrowed the field to five "round two" candidates:
  - Mars from IBM
  - RC6 from RSA
  - Rijndael from two Belgian researchers
  - Serpent, a British-Norwegian-Israeli research collaboration
  - Twofish from the consulting firm Counterpane

  We expect IPSEC will eventually use the AES winner, and we expect to see a winner (or more than one; there is an ongoing discussion on that point) declared in the summer of 2000.

  Adding one or more AES ciphers to Linux FreeS/WAN would be useful undertaking, and considerable freely available code exists to start from. One complication is that our code is built for a 64-bit block cipher and AES uses a 128-bit block. Volunteers via the mailing list would be

welcome.

For more information, see the NIST AES home page or the Block Cipher Lounge AES page. For code and benchmarks see Brian Gladman's page .

AH
The IPSEC Authentication Header, added after the IP header. For details, see our IPSEC Overview document and/or RFC 2402.

Alice and Bob
A and B, the standard example users in writing on cryptography and coding theory. Carol and Dave join them for protocols which require more players.

Bruce Schneier extends these with many others such as Eve the Eavesdropper and Victor the Verifier. His extensions seem to be in the process of becoming standard as well. See page 23 of Applied Cryptography

Alice and Bob have an amusing biography on the web.

ARPA
see DARPA

ASIO
Australian Security Intelligence Organisation.

Asymmetric cryptography
See public key cryptography.

Authentication
Ensuring that a message originated from the expected sender and has not been altered on route. IPSEC uses authentication in two places:

- authenticating the players in IKE's Diffie-Hellman key exchanges to prevent man-in-the-middle attacks. This can be done in a number of ways. The methods supported by FreeS/WAN are discussed in our configuration document.
- authenticating packets on an established SA, either with a separate authentication header or with the optional authentication in the ESP protocol. In either case, packet authentication uses a hashed message athentication code technique.

Outside IPSEC, passwords are perhaps the most common authentication mechanism. Their function is essentially to authenticate the person's identity to the system. Passwords are generally only as secure as the network they travel over. If you send a cleartext password over a tapped phone line or over a network with a packet sniffer on it, the security provided by that password becomes zero. Sending an encrypted password is no better; the attacker merely records it and reuses it at his convenience. This is called a replay attack.

A common solution to this problem is a challenge-response system. This defeats simple eavesdropping and replay attacks. Of course an attacker might still try to break the cryptographic algorithm used, or the random number generator.

Automatic keying
A mode in which keys are automatically generated at connection establisment and new keys automaically created periodically thereafter. Contrast with manual keying in which a single stored key is used.

IPSEC uses the Diffie-Hellman key exchange protocol to create keys. An authentication mechansim is required for this. The methods supported by FreeS/WAN are discussed in our configuration document.

Having an attacker break the authentication is emphatically not a good idea. An attacker that breaks authentication, and manages to subvert some other network entities (DNS, routers or gateways), can use a man-in-the middle attack to break the security of your IPSEC connections.

However, having an attacker break the authentication in automatic keying is not quite as bad as losing the key in manual keying.

- An attacker who reads /etc/ipsec.conf and gets the keys for a manually keyed connection can, without further effort, read all messages encrypted with those keys, including any old messages he may have archived.
- Automatic keying has a property called perfect forward secrecy. An attacker who breaks the authentication gets none of the automatically generated keys and cannot immediately read any messages. He has to mount a successful man-in-the-middle attack in real time before he can read anything. He cannot read old archived messages at all and will not be able to read any future messages not caught by man-in-the-middle tricks.

That said, the secrets used for authentication, stored in ipsec.secrets(5), should still be protected as tightly as cryptographic keys.

Bay Networks

A vendor of routers, hubs and related products, now a subsidiary of Northern Telecom. Interoperation between their IPSEC products and Linux FreeS/WAN was problematic at last report; see our compatibility document.

benchmarks

Our default block cipher, triple DES, is slower than many alternate ciphers that might be used. Speeds achieved, however, seem adequate for many purposes. For example, the assembler code from the LIBDES library we use encrypts 1.6 megabytes per second on a Pentium 200, according to the test program supplied with the library.

The University of Wales at Aberystwyth has done quite detailed tests and put their results on the web.

Even a 486 can handle a T1 line, according to this mailing list message:

```
Subject: Re: linux-ipsec: IPSec Masquerade
   Date: Fri, 15 Jan 1999 11:13:22 -0500
   From: Michael Richardson

. . . A 486/66 has been clocked by Phil Karn to do
10Mb/s encryption.. that uses all the CPU, so half that to get some CPU,
and you have 5Mb/s. 1/3 that for 3DES and you get 1.6Mb/s....
```

From an Internet Draft *The ESP Triple DES Transform*:

```
Phil Karn has tuned DES-EDE3-CBC software to achieve 6.22 Mbps with a
133 MHz Pentium.  Other DES speed estimates may be found at
[Schneier95, page 279].  Your milage may vary.
```

If you want to measure the loads FreeS/WAN puts on a system, note that tools such as top or measurements such as load average are more-or-less useless for this. They are not designed to measure something that does most of its work inside the kernel.

BIND
: **B**erkeley **I**nternet **N**ame **D**aemon, a widely used implementation of DNS (Domain Name Service). See our bibliography for a useful reference. See the BIND home page for more information and the latest version.

Birthday attack
: A cryptographic attack based on the mathematics exemplified by the birthday paradox. This math turns up whenever the question of two cryptographic operations producing the same result becomes an issue:
  - collisions in message digest functions.
  - identical output blocks from a block cipher
  - repetition of a challenge in a challenge-response system

  Resisting such attacks is part of the motivation for:
  - hash algorithms such as SHA and RIPEMD-160 giving a 160-bit result rather than the 128 bits of MD4, MD5 and RIPEMD-128.
  - AES block ciphers using a 128-bit block instead of the 64-bit block of most current ciphers
  - IPSEC using a 32-bit counter for packets sent on an automatically keyed SA and requiring that the connection always be rekeyed before the counter overflows.

Birthday paradox
: Not really a paradox, just a rather counter-intuitive mathematical fact. In a group of 23 people, the chance of a least one pair having the same birthday is over 50%.

  The second person has 1 chance in 365 (ignoring leap years) of matching the first. If they don't match, the third person's chances of matching one of them are 2/365. The 4th, 3/365, and so on. The total of these chances grows more quickly than one might guess.

Block cipher
: A symmetric cipher which operates on fixed-size blocks of plaintext, giving a block of ciphertext for each. Contrast with stream cipher. Block ciphers can be used in various modes when multiple block are to be encrypted.

  DES is among the the best known and widely used block ciphers, but is now obsolete. Its 56-bit key size makes it highly insecure today. Triple DES is the default transform for Linux FreeS/WAN because it is the only cipher which is both required in the RFCs and apparently secure.

  The current generation of block ciphers -- such as Blowfish, CAST-128 and IDEA -- all use 64-bit blocks and 128-bit keys. The next generation, AES, uses 128-bit blocks and supports key sizes up to 256 bits.

  The Block Cipher Lounge web site has more information.

Blowfish
: A block cipher using 64-bit blocks and keys of up to 448 bits, designed by Bruce Schneier and used in several products.

  This is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN.

Brute force attack (exhaustive search)
: Breaking a cipher by trying all possible keys. This is always possible in theory (except against a one-time pad), but it becomes practical only if the key size is inadequate. For an important

example, see our document on the insecurity of DES with its 56-bit key. For an analysis of key sizes required to resist plausible brute force attacks, see this paper.

Longer keys protect against brute force attacks. Each extra bit in the key doubles the number of possible keys and therefore doubles the work a brute force attack must do. A large enough key defeats **any** brute force attack.

For example, the EFF's DES Cracker searches a 56-bit key space in an average of a few days. Let us assume an attacker that can find a 64-bit key (256 times harder) by brute force search in a second (a few hundred thousand times faster). For a 96-bit key, that attacker needs 2^{32} seconds, just over a century. Against a 128-bit key, he needs 2^{32} centuries or about 400,000,000,000 years. Your data is then obviously secure against brute force attacks. Even if our estimate of the attacker's speed is off by a factor of a million, it still takes him 400,000 years to crack a message.

This is why

- single DES is now considered dangerously insecure
- any cipher we add to Linux FreeS/WAN will have *at least* a 90-bit key
- all of the current generation of block ciphers use a 128-bit or longer key
- AES ciphers support keysizes 128, 192 and 256 bits

Cautions:
Inadequate keylength always indicates a weak cipher but it is important to note that *adequate keylength does not necessarily indicate a strong cipher*. There are many attacks other than brute force, and adequate keylength *only* guarantees resistance to brute force. Any cipher, whatever its key size, will be weak if design or implementation flaws allow other attacks.

Also, *once you have adequate keylength* (somewhere around 90 or 100 bits), *adding more key bits make no practical difference*, even against brute force. Consider our 128-bit example above that takes 400 billion years to break by brute force. Do we care if an extra 16 bits of key put that into the quadrillions? No. What about 16 fewer bits reducing it to the 112-bit security level of Triple DES, which our example attacker could break in just over a billion years? No again, unless we're being really paranoid about safety margins.

There may be reasons of convenience in the design of the cipher to support larger keys. For example Blowfish allows up to 448 bits and RC4 up to 2048, but beyond 100-odd bits it makes no difference to practical security.

Bureau of Export Administration
see BXA

BXA
The US Commerce Department's **B**ureau of **E**xport **A**dministration which administers the EAR Export Administration Regulations controling the export of, among other things, cryptography.

CA
Certification **A**uthority, an entity in a public key infrastructure that can certify keys by signing them. Usually CAs form a hierarchy. The top of this hierarchy is called the root CA.

See Web of Trust for an alternate model.

CAST-128
A block cipher using 64-bit blocks and 128-bit keys, described in RFC 2144 and used in products such as Entrust and recent versions of PGP.

This is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN.

CAST-256
Entrust's candidate cipher for the AES standard, largely based on the CAST-128 design.

CBC mode
Cipher Block Chaining mode, a method of using a block cipher in which for each block except the first, the result of the previous encryption is XORed into the new block before it is encrypted. CBC is the mode used in IPSEC.

An initialisation vector (IV) must be provided. It is XORed into the first block before encryption. The IV need not be secret but should be different for each message and unpredictable.

Certification Authority
see CA

Cipher Modes
Different ways of using a block cipher when encrypting multiple blocks.

Four standard modes were defined for DES in FIPS 81. They can actually be applied with any block cipher.

ECB	Electronic CodeBook	encrypt each block independently
CBC	Cipher Block Chaining	XOR previous block ciphertext into new block plaintext before encrypting new block
CFB	Cipher FeedBack	
OFB	Output FeedBack	

IPSEC uses CBC mode since this is only marginally slower than ECB and is more secure. In ECB mode the same plaintext always encrypts to the same ciphertext, unless the key is changed. In CBC mode, this does not occur.

Various other modes are also possible, but none of them are used in IPSEC.

Challenge-response authentication
An authentication system in which one player generates a random number, encrypts it and sends the result as a challenge. The other player decrypts and sends back the result. If the result is correct, that proves to the first player that the second player knew the appropriate secret, required for the decryption.

Variations on this technique exist using public key or symmetric cryptography. Some provide two-way authentication, assuring each player of the other's identity.

Because the random number is different each time, this defeats simple eavesdropping and replay attacks. Of course an attacker might still try to break the cryptographic algorithm used, or the random number generator.

Ciphertext
The encrypted output of a cipher, as opposed to the unencrypted plaintext input.

Cisco
A vendor of routers, hubs and related products. Their IPSEC products interoperate with Linux FreeS/WAN; see our compatibility document.

Conventional cryptography
See symmetric cryptography

Collision resistance
The property of a message digest algorithm which makes it hard for an attacker to find or construct two inputs which hash to the same output.

Copyleft
see GNU General Public License

CSE
Communications Security Establishment, the Canadian organisation for signals intelligence.

DARPA (sometimes just ARPA)
The US government's **D**efense **A**dvanced **R**esearch **P**rojects **A**gency. Projects they have funded over the years have included the Arpanet which evolved into the Internet, the TCP/IP protocol suite (as a replacement for the original Arpanet suite), the Berkeley 4.x BSD Unix projects, and Secure DNS.

For current information, see their web site.

Denial of service (DOS) attack
An attack that aims at denying some service to legitimate users of a system, rather than providing a service to the attacker.

- One variant is a flooding attack, overwhelming the system with too many packets, to much email, or whatever.
- A closely related variant is a resource exhaustion attack. For example, consider a "TCP SYN flood" attack. Setting up a TCP connection involves a three-packet exchange:
  - Initiator: Connection please (SYN)
  - Responder: OK (ACK)
  - Initiator: OK here too

  If the attacker puts bogus source information in the first packet, such that the second is never delivered, the responder may wait a long time for the third to come back. If responder has already allocated memory for the connection data structures, and if many of these bogus packets arrive, the responder may run out of memory.
- Another variant is to feed the system undigestible data, hoping to make it sick. For example, IP packets are limited in size to 64K bytes and a fragment carries information on where it starts within that 64K and how long it is. The "ping of death" delivers fragments that say, for example, that they start at 60K and are 20K long. Attempting to re-assemble thse without checking for overflow can be fatal.

The two example attacks discussed were both quite effective when first discovered, capable of crashing or disabling many operating systems. They were also well-publicised, and today far fewer systems are vulnerable to them.

DES
The **D**ata **E**ncryption **S**tandard, a block cipher with 64-bit blocks and a 56-bit key. Probably the most widely used symmetric cipher ever devised. DES has been a US government standard for their own use (only for unclassified data), and for some regulated industries such as banking, since the late 70's.

DES is seriously insecure against current attacks.

Linux FreeS/WAN includes DES since the RFCs require it, but our default configuration refuses to negotiate a connection using it. **We strongly recommend that single DES not be used.**

See also 3DES and DESX, stronger ciphers based on DES.

DESX

An improved DES suggested by Ron Rivest of RSA Data Security. It XORs extra key material into the text before and after applying the DES cipher.

This is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN. DESX would be the easiest additional transform to add; there would be very little code to write. It would be much faster than 3DES and almost certainly more secure than DES. However, since it is not in the RFCs other IPSEC implementations cannot be expected to have it.

DH

see Diffie-Hellman

Diffie-Hellman (DH) key exchange protocol

A protocol that allows two parties without any initial shared secret to create one in a manner immune to eavesdropping. Once they have done this, they can communicate privately by using that shared secret as a key for a block cipher or as the basis for key exchange.

The protocol is secure against all passive attacks, but it is not at all resistant to active man-in-the-middle attacks. If a third party can impersonate Bob to Alice and vice versa, then no useful secret can be created. Authentication is a prerequisite for safe Diffie-Hellman key exchange.

IPSEC can use any of several authentication mechanisims. Those supported by FreeS/WAN are discussed in our configuration document.

Digital signature

Take a message digest of a document and encrypt it with your private key for some public key cryptosystem. I can decrypt with your public key and verify that the result matches the digest I calculate. This proves that the encrypted digest was created with your private key.

Such an encrypted message digest can be treated as a signature since it cannot be created without *both* the document *and* the private key which only you should possess. The legal issues are complex, but several countries are moving in the direction of legal recognition for digital signatures.

DNS

Domain **N**ame **S**ervice, a distributed database through which names are associated with numeric addresses and other information in the Internet Protocol Suite. See also BIND, the Berkeley Internet Name Daemon which implements DNS services and Secure DNS. See our bibliography for a useful reference on both.

DOS attack

see Denial Of Service attack

EAR

The US government's **E**xport **A**dministration **R**egulations, administered by the Bureau of Export Administration. These have replaced the earlier ITAR regulations as the controls on export of cryptography.

ECB mode

Electronic **C**ode**B**ook mode, the simplest way to use a block cipher. See Cipher Modes.

EDE

The sequence of operations normally used in either the three-key variant of triple DES used in IPSEC or the two-key variant used in some other systems.

The sequence is:

- Encrypt with key1
- Decrypt with key2
- Encrypt with key3

For the two-key version, key1=key3.

The "advantage" of this EDE order of operations is that it makes it simple to interoperate with older devices offering only single DES. Set key1=key2=key3 and you have the worst of both worlds, the overhead of triple DES with the security of single DES. Since single DES is insecure, this is a rather dubious "advantage".

The EDE two-key variant can also interoperate with the EDE three-key variant used in IPSEC; just set k1=k3.

Entrust
: A Canadian company offering enterprise PKI products using CAST-128 symmetric crypto, RSA public key and X.509 directories.

EFF
: Electronic Frontier Foundation, an advocacy group for civil rights in cyberspace.

Encryption
: Techniques for converting a readable message (plaintext) into apparently random material (ciphertext) which cannot be read if intercepted. A key is required to read the message.

Major variants include symmetric encryption in which sender and receiver use the same secret key and public key methods in which the sender uses one of a matched pair of keys and the receiver uses the other. Many current systems, including IPSEC, are hybrids combining the two techniques.

ESP
: **E**ncapsulated **S**ecurity **P**ayload, the IPSEC protocol which provides encryption. It can also provide authentication service and may be used with null encryption (which we do not recommend). For details see our IPSEC Overview document and/or RFC 2406.

Extruded subnet
: A situation in which something IP sees as one network is actually in two or more places.

For example, the Internet may route all traffic for a particular company to that firm's corporate gateway. It then becomes the company's problem to get packets to various machines on their subnets in various departments. They may decide to treat a branch office like a subnet, giving it IP addresses "on" their corporate net. This becomes an extruded subnet.

Packets bound for it are delivered to the corporate gateway, since as far as the outside world is concerned, that subnet is part of the corporate network. However, instead of going onto the corporate LAN (as they would for, say, the accounting department) they are then encapsulated and sent back onto the Internet for delivery to the branch office.

For information on doing this with Linux FreeS/WAN, look in our Configuration file.

Exhaustive search
: See brute force attack.

FIPS

Federal **I**nformation **P**rocessing **S**tandard, the US government's standards for products it buys. These are issued by NIST. Among other things, DES and SHA are defined in FIPS documents. NIST have a FIPS home page.

Free Software Foundation (FSF)

An organisation to promote free software, free in the sense of these quotes from their web pages

> "Free software" is a matter of liberty, not price. To understand the concept, you should think of "free speech", not "free beer."
>
> "Free software" refers to the users' freedom to run, copy, distribute, study, change and improve the software.

See also GNU, GNU General Public License, and the FSF site.

FreeSWAN

see Linux FreeS/WAN

FSF

see Free software Foundation

GCHQ

Government Communications Headquarters, the British organisation for signals intelligence.

GILC

Global Internet Liberty Campaign, an international organisation advocating, among other things, free availability of b cryptography. They have a campaign to remove cryptographic software from the Wassenaar Arrangement.

Global Internet Liberty Campaign

see GILC.

Global Trust Register

An attempt to create something like a root CA for PGP by publishing both as a book and on the web the fingerprints of a set of verified keys for well-known users and organisations.

GMP

The **G**NU **M**ulti-**P**recision library code, used in Linux FreeS/WAN by Pluto for public key calculations.

GNU

GNU's **N**ot **U**nix, the Free Software Foundation's project aimed at creating a free system with at least the capabilities of Unix. Linux uses GNU utilities extensively.

GPG

see GNU Privacy Guard

GNU General Public License (GPL, copyleft)

The license developed by the Free Software Foundation under which Linux, Linux FreeS/WAN and many other pieces of software are distributed. The license allows anyone to redistribute and modify the code, but forbids anyone from distributing executables without providing access to source code. For more details see the file COPYING included with GPLed source distributions, including ours, or the GNU site's GPL page.

GNU Privacy Guard

An open source implementation of Open PGP as defined in RFC 2440.

GPL

see GNU General Public License.

Hash

see message digest

Hashed Message Authentication Code (HMAC)

using keyed message digest functions to authenticate a message. This differs from other uses of these functions:

- In normal usage, the hash function's internal variable are initialised in some standard way. Anyone can reproduce the hash to check that the message has not been altered.
- For HMAC usage, you initialise the internal variables from the key. Only someone with the key can reproduce the hash. A successful check of the hash indicates not only that the message is unchanged but also that the creator knew the key.

The exact techniques used in IPSEC are defined in RFC 2104. They are referred to as HMAC-MD5-96 and HMAC-SHA-96 because they output only 96 bits of the hash. This makes some attacks on the hash functions harder.

HMAC
see Hashed Message Authentication Code

HMAC-MD5-96
see Hashed Message Authentication Code

HMAC-SHA-96
see Hashed Message Authentication Code

Hybrid cryptosystem
A system using both public key and symmetric cipher techniques. This works well. Public key methods provide key management and digital signature facilities which are not readily available using symmetric ciphers. The symmetric cipher, however, can do the bulk of the encryption work much more efficiently than public key methods.

IAB
Internet Architecture Board.

ICMP
Internet **C**ontrol **M**essage **P**rotocol. This is used for various IP-connected devices to manage the network.

IDEA
International **D**ata **E**ncrypion **A**lgorithm, developed in Europe as an alternative to exportable American ciphers such as DES which were too weak for serious use. IDEA is a block cipher using 64-bit blocks and 128-bit keys, and is used in products such as PGP.

IDEA is not required by the IPSEC RFCs and not currently used in Linux FreeS/WAN.

IDEA is patented and, with strictly limited exceptions for personal use, using it requires a license from Ascom.

IESG
Internet Engineering Steering Group.

IETF
Internet Engineering Task Force, the umbrella organisation whose various working groups make most of the technical decisions for the Internet. The IETF IPSEC working group wrote the RFCs we are implementing.

IKE
Internet **K**ey **E**xchange, based on the Diffie-Hellman key exchange protocol. IKE is implemented in Linux FreeS/WAN by the Pluto daemon.

Initialisation Vector (IV)
Some cipher modes, including the CBC mode which IPSEC uses, require some extra data at the beginning. This data is called the initialisation vector. It need not be secret, but should be different for each message. Its function is to prevent messages which begin with the same text from encrypting to the same ciphertext. That might give an analyst an opening, so it is best prevented.

IP
Internet **P**rotocol.

IP masquerade

A method of allowing multiple machines to communicate over the Internet when only one IP address is available for their use. See the Linux masquerade resource page for details.

The client machines are set up with reserved non-routable IP addresses defined in RFC 1918. The masquerading gateway, the machine with the actual link to the Internet, rewrites packet headers so that all packets going onto the Internet appear to come from one IP address, that of its Internet interface. It then gets all the replies, does some table lookups and more header rewriting, and delivers the replies to the appropriate client machines.

To use masquerade with Linux FreeS/WAN, you must set leftfirewall=yes and/or rightfirewall=yes in the connection description in /etc/ipsec.conf.

IPng
"IP the Next Generation", see IPv6.

IPv4
The current version of the Internet protocol suite.

IPv6 (IPng)
Version six of the Internet protocol suite, currently being developed. It will replace the current version four. IPv6 has IPSEC as a mandatory component.

See this web site for more details.

IPSEC
Internet **P**rotocol **SEC**urity, security functions (authentication and encryption) implemented at the IP level of the protocol stack. It is optional for IPv4 and mandatory for IPv6.

This is the standard Linux FreeS/WAN is implementing. For more details, see our IPSEC Overview. For the standards, see RFCs listed in our RFCs document.

ISAKMP
Internet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol, defined in RFC 2408.

ITAR
International **T**raffic in **A**rms **R**egulations, US regulations administered by the State Department which until recently limited export of, among other things, cryptographic technology and software. ITAR still exists, but the limits on cryptography have now been transferred to the Export Administration Regulations under the Commerce Department's Bureau of Export Administration.

IV
see Initialisation vector

Keyed message digest
See HMAC.

Key length
see brute force attack

KLIPS
Kernel **IP** **S**ecurity, the Linux FreeS/WAN project's changes to the Linux kernel to support the IPSEC protocols.

LDAP
Lightweight **D**irectory **A**ccess **P**rotocol, defined in RFCs 1777 and 1778, a method of accessing information stored in directories. LDAP is used by several PKI implementations, often with X.501 directories and X.509 certificates. It may also be used by IPSEC to obtain key certifications from those PKIs. This is not yet implemented in Linux FreeS/WAN.

LIBDES
A publicly available library of DES code, written by Eric Young, which Linux FreeS/WAN uses in both KLIPS and Pluto.

Linux
A freely available Unix-like operating system based on a kernel originally written for the Intel 386 architecture by (then) student Linus Torvalds. Once his 32-bit kernel was available, the GNU utilities made it a usable system and contributions from many others led to explosive growth.

Today Linux is a complete Unix replacement available for several CPU architectures -- Intel, DEC/Compaq Alpha, Power PC, both 32-bit SPARC and the 64-bit UltraSPARC, SrongARM, . . . -- with support for multiple CPUs on some architectures.

Linux FreeS/WAN is intended to run on all CPUs supported by Linux and is currently (February 1999) known to work on Intel, Alpha and StrongARM. See our compatibility document for details.

Linux FreeS/WAN
Our implementation of the IPSEC protocols, intended to be freely redistributable source code with a GNU GPL license and no constraints under US or other export laws. Linux FreeS/WAN is intended to interoperate with other IPSEC implementations. The name is partly taken, with permission, from the S/WAN multi-vendor IPSEC compatability effort. Linux FreeS/WAN has two major components, KLIPS (KerneL IPSEC Support) and the Pluto daemon which manages the whole thing.

See our IPSEC Overview for more detail. For the code see our primary distribution site or one of the mirror sites on this list.

Mailing list
The Linux FreeS/WAN project has an open public email list for bug reports and software development discussions. The list address is **linux-ipsec@clinet.fi**. To subscribe, send mail to majordomo@clinet.fi with a one-line message body "subscribe linux-ipsec". For more information, send majordomo the one-line message "help".

NOTE: **US citizens or residents are asked not to post code to the list, not even one-line bug fixes.** The project cannot accept code which might entangle it in US export restrictions.

For more detail, see our document on this and other mailing lists.

Man-in-the-middle attack
An active attack in which the attacker impersonates each of the legitimate players in a protocol to the other.

For example, if Alice and Bob are negotiating a key via the Diffie-Hellman key agreement, and are not using authentication to be certain they are talking to each other, then an attacker able to insert himself in the communication path can deceive both players.

Call the attacker Mallory. For Bob, he pretends to be Alice. For Alice, he pretends to be Bob. Two keys are then negotiated, Alice-to-Mallory and Bob-to-Mallory. Alice and Bob each think the key they have is Alice-to-Bob.

A message from Alice to Bob then goes to Mallory who decrypts it, reads it and/or saves a copy, re-encrypts using the Bob-to-Mallory key and sends it along to Bob. Bob decrypts successfully and sends a reply which Mallory decrypts, reads, re-encrypts and forwards to Alice.

To make this attack effective, Mallory must

- subvert some part of the network in some way that lets him carry out the deception
  possible targets: DNS, router, Alice or Bob's machine, mail server, ...
- beat any authentication mechanism Alice and Bob use
  strong authentication defeats the attack entirely; this is why IKE requires authentication
- work in real time, delivering messages without noticable delay
  not hard if Alice and Bob are using email; quite difficult in some situations.

If he manages it, however, it is devastating. He not only gets to read all the messages; he can alter messages, inject his own, forge anything he likes, . . . In fact, he controls the communication completely.

Manual keying

An IPSEC mode in which the keys are provided by the administrator. In FreeS/WAN, they are stored in /etc/ipsec.conf. The alternative, automatic keying, is preferred in most cases.

MD4

Message Digest Algorithm Four from Ron Rivest of RSA. MD4 was widely used a few years ago, but is now considered obsolete. It has been replaced by its descendants MD5 and SHA.

MD5

Message Digest Algorithm Five from Ron Rivest of RSA, an improved variant of his MD4. Like MD4, it produces a 128-bit hash. For details see RFC 1321.

MD5 is one of two message digest algorithms available in IPSEC. The other is SHA. SHA produces a longer hash and is therefore more resistant to birthday attacks, but this is not a concern for IPSEC. The HMAC method used in IPSEC is secure even if the underlying hash is not particularly strong against this attack.

Meet-in-the-middle attack

A divide-and-conquer attack which breaks a cipher into two parts, works against each separately, and compares results. Probably the best known example is an attack on double DES. This applies in principle to any pair of block ciphers, e.g. to an encryption system using, say, CAST-128 and Blowfish, but we will describe it for double DES.

Double DES encryption and decryption can be written:

```
C = E(k2,E(k1,P))
P = D(k1,D(k2,C))
```

Where C is ciphertext, P is plaintext, E is encryption, D is decryption, k1 is one key, and k2 is the other key. If we know a P, C pair, we can try and find the keys with a brute force attack, trying all possible k1, k2 pairs. Since each key is 56 bits, there are 2^{112} such pairs and this attack is painfully inefficient.

The meet-in-the middle attack re-writes the equations to calculate a middle value M:

```
M = E(k1,P)
M = D(k2,C)
```

Now we can try some large number of D(k2,C) decryptions with various values of k2 and store

the results in a table. Then start doing E(k1,P) encryptions, checking each result to see if it is in the table.

With enough table space, this breaks double DES with 2^{57} work. The memory requirements of such attacks can be prohibitive, but there is a whole body of research literature on methods of reducing them.

Message Digest Algorithm
: An algorithm which takes a message as input and produces a hash or digest of it, a fixed-length set of bits which depend on the message contents in some highly complex manner. Design criteria include making it extremely difficult for anyone to counterfeit a digest or to change a message without altering its digest. One essential property is collision resistance. The main applications are in message authentication and digital signature schemes. Widely used algorithms include MD5 and SHA. In IPSEC, message digests are used for HMAC authentication of packets.

MTU
: **M**aximum **T**ransmission **U**nit, the largest size of packet that can be sent over a link. This is determined by the underlying network, but must be taken account of at the IP level.

IP packets, which can be up to 64K bytes each, must be packaged into lower-level packets of the appropriate size for the underlying network(s) and re-assembled on the other end. When a packet must pass over multiple networks, each with its own MTU, and many of the MTUs are unknown to the sender, this becomes a fairly complex problem. See path MTU discovery for details.

Often the MTU is a few hundred bytes on serial links and 1500-odd on Ethernet. There are, however, serial link protocols which use a larger MTU to avoid packet packet fragmentation at the ethernet/serial boundary, and newer (especially gigabit) Ethernet networks sometimes support much larger packets because these are more efficient in some applications.

NAI
: Network Associates, a conglomerate formed from PGP Inc., TIS, Macaffee Anti-virus products and several others. Among other things, they offer an IPSEC-based VPN.

NAT
: **N**etwork **A**ddress **T**ranslation.

NIST
: The US National Institute of Standards and Technology, responsible for FIPS standards including DES and its replacement, AES.

Nonce
: A random value used in an authentication protocol.

Non-routable IP address
: An IP address not normally allowed in the "to" or "from" IP address field header of IP packets.

Almost invariably, the phrase "non-routable address" means one of the addresses reserved by RFC 1918 for private networks:

- 10.anything
- 172.x.anything with 16 <= x <= 31
- 192.168.anything

These addresses are commonly used on private networks, e.g. behind a Linux machines doing IP masquerade. Machines within the private network can address each other with these addresses. All packets going outside that network, however, have these addresses replaced before they reach the Internet.

If any packets using these addresses do leak out, they do not go far. Most routers automatically discard all such packets.

Various other addresses -- the 127.0.0.0/8 block reserved for local use, 0.0.0.0, various broadcast and network addresses -- cannot be routed over the Internet, but are not normally included in the meaning when the phrase "non-routable address" is used.

NSA

The US National Security Agency, the American organisation for signals intelligence, the protection of US government messages and the interception and analysis of other messages. For details, see Bamford's "The Puzzle Palace".

Some history of NSA documents were declassified in response to a FOIA (Freedom of Information Act) request.

Oakley

A key determination protocol, defined in RFC 2412.

One time pad

A cipher in which the key is:

- as long as the total set of messages to be enciphered
- absolutely random
- never re-used

Given those three conditions, it can easily be proved that the cipher is perfectly secure, in the sense that an attacker with intercepted message in hand has no better chance of guessing the message than an attacker who only knows the message length. No such proof exists for any other cipher.

There are, however, several problems with this "perfect" cipher.

- It is wildly impractical for many applications. Key management is difficult or impossible.
- It is *extremely* fragile. Small changes which violate the conditions listed above do not just weaken the cipher a bit; quite often they destroy its security completely.
  - Re-using the pad weakens it to the point where it can be broken with pencil and paper. With a computer, the attack is trivially easy.
  - Using computer-generated pseudo-random numbers instead of a really random pad completely invalidates the security proof. Depending on random number generator used, this may also give an extremely weak cipher.
- If an attacker knows the plaintext and has an intercepted message, he can discover the pad. This does not matter if the attacker is just a passive eavesdropper. It gives him no plaintext he didn't already know and we don't care that he learns a pad which we'll never re-use. However, knowing the pad lets an active attacker perform a man-in-the-middle attack, replacing your message with whatever he chooses.

Outrageous marketing claims about the "unbreakable" security of various products which somewhat resemble one-time pads are common. They are a sure sign of cryptographic snake oil.

See also the one time pad FAQ.

Opportunistic encryption

A situation in which any two IPSEC-aware machines can secure their communications, without a pre-shared secret and without a common PKI. This is a long-term goal of the Linux FreeS/WAN

project which we expect to acheive using Secure DNS.

P1363 standard
: An IEEE standard for public key cryptography.

Passive attack
: An attack in which the attacker only eavesdrops and attempts to analyse intercepted messages, as opposed to an active attack in which he diverts messages or generates his own.

Path MTU discovery
: The process of discovering the largest packet size which all links on a path can handle without fragmentation -- that is, without any router having to break the packet up into smaller pieces to match the MTU of its outgoing link.

This is done as follows:

- originator sends the largest packets allowed by MTU of the first link, setting the DF (don't fragment) bit in the packet header
- any router which cannot send the packet on (outgoing MTU is too small for it, and DF prevents fragmenting it to match) sends back an ICMP packet reporting the problem
- originator looks at ICMP message and tries a smaller size
- eventually, you settle on a size that can pass all routers
- thereafter, originator just sends that size and no-one has to fragment

Since this requires co-operation of many systems, and since the next packet may travel a different path, this is one of the trickier areas of IP programming. Bugs that have shown up over the years have included:

- malformed ICMP messages
- hosts that ignore or mishandle these ICMP messages
- firewalls blocking the ICMP messages so host does not see them

Since IPSEC adds a header, it increases packet size and may require fragmentation even where incoming and outgoing MTU are equal.

Perfect forward secrecy (PFS)
: A property of systems such as Diffie-Hellman key exchange which use a long-term key (the shared secret in IKE) and generate short-term keys as required. If an attacker who acquires the long-term key *provably* can

- *neither* read previous messages which he may have archived
- *nor* read future messages without performing additional successful attacks

then the system has PFS. The attacker needs the short-term keys in order to read the trafiic and merely having the long-term key does not allow him to infer those. Of course, it may allow him to conduct another attack (such as man-in-the-middle) which gives him some short-term keys, but he does not automatically get them just by acquiring the long-term key.

PFS
: see Perfect Forward Secrecy

PGP
: **P**retty **G**ood **P**rivacy, a personal encryption system for email based on public key technology, written by Phil Zimmerman.

The 2.xx versions of PGP used the RSA public key algorithm and used IDEA as the symmetric cipher. These versions are described in RFC 1991 and in Garfinkel's book. They are freely available. There is a US version and an International version . The differences are questions of licensing; the two are fully compatible.

Since version 5, the products from PGP Inc. have used Diffie-Hellman public key methods and IDEA or CAST-128 symmetric encryption. These can verify signatures from the 2.xx versions, but cannot exchange encryted messages with them. Some 5.x and 6.x products are free for

personal use. Information on all products and downloads of the free ones are available from PGP Inc. The free versions are also on the US and International sites listed above.

An IETF working group has issued RFC 2440 for an "Open PGP" standard, similar to the 5.x versions. PGP Inc. staff were among the authors. A free Gnu Privacy Guard based on that standard is now available.

PGP Inc.
A company founded by Zimmerman, the author of PGP, now a division of NAI. See the corporate website.

Their PGP 6.5 product includes PGPnet, an IPSEC client for Macintosh or for Windows 95/98/NT.

Photuris
Another key negotiation protocol, an alternative to IKE, described in RFCs 2522 and 2523.

PPTP
Point-to-**P**oint **T**unneling **P**rotocol.

PKI
Public **K**ey **I**nfrastructure, the things an organisation or community needs to set up in order to make public key cryptographic technology a standard part of their operating procedures.

There are several PKI products on the market. Typically they use a hierarchy of Certification Authorities (CAs). Often they use LDAP access to X.509 directories to implement this.

See Web of Trust for a different sort of infrastructure.

PKIX
PKI e**X**change, an IETF standard that allows PKIs to talk to each other.

This is required, for example, when users of a corporate PKI need to communicate with people at client, supplier or government organisations, any of which may have a different PKI in place. I should be able to talk to you securely whenever:

- your organisation and mine each have a PKI in place
- you and I are each set up to use those PKIs
- the two PKIs speak PKIX
- the configuration allows the conversation

At time of writing (March 1999), this is not yet widely implemented but is under quite active development by several groups.

Plaintext
The unencrypted input to a cipher, as opposed to the encrypted ciphertext output.

Pluto
The Linux FreeS/WAN daemon which handles key exchange via the IKE protocol, connection negotiation, and other higher-level tasks. Pluto calls the KLIPS kernel code as required. For details, see the manual page ipsec_pluto(8).

Public Key Cryptography
In public key cryptography, keys are created in matched pairs. Encrypt with one half of a pair and only the matching other half can decrypt it. This contrasts with symmetric or secret key cryptography in which a single key known to both parties is used for both encryption and decryption.

One half of each pair, called the public key, is made public. The other half, called the private key, is kept secret. Messages can then be sent by anyone who knows the public key to the holder of the private key. Encrypt with the public key and you know only someone with the matching private key can decrypt.

Public key techniques can be used to create digital signatures and to deal with key management issues, perhaps the hardest part of effective deployment of symmetric ciphers. The resulting hybrid cryptosystems use public key methods to manage keys for symmetric ciphers.

Many organisations are currently creating PKIs, public key infrastructures to make these benefits widely available.

Public Key Infrastructure
see PKI

Random
A remarkably tricky term, far too much so for me to attempt a definition here. Quite a few cryptosystems have been broken via attacks on weak random number generators, even when the rest of the system was sound.

See RFC 1750 for the theory. It will be available locally if you have downloaded our RFC bundle (which is described here). Or read it on the net.

See the manual pages for ipsec_ranbits(8) and random(4) for details of what we use.

There has recently been discussion on several mailing lists of the limitations of Linux /dev/random and of whether we are using it correctly. Those discussions are archived on the /dev/random support page.

Raptor
A firewall product for Windows NT offerring IPSEC-based VPN services. Linux FreeS/WAN interoperates with Raptor; see our Compatibility document for details. Raptor have recently merged with Axent.

RC4
Rivest **C**ipher four, designed by Ron Rivest of RSA and widely used. Believed highly secure with adequate key length, but often implemented with inadequate key length to comply with export restrictions.

RC6
Rivest **C**ipher six, RSA's AES candidate cipher.

Replay attack
An attack in which the attacker records data and later replays it in an attempt to deceive the recipient.

RFC
Request **F**or **C**omments, an Internet document. Some RFCs are just informative. Others are standards.

Our list of IPSEC and other security-related RFCs is here, along with information on methods of obtaining them.

RIPEMD
A message digest algorithm. The current version is RIPEMD-160 which gives a 160-bit hash.

Root CA
The top level Certification Authority in a hierachy of such authorities.

Routable IP address
Most IP addresses can be used as "to" and "from" addresses in packet headers. These are the routable addresses; we expect routing to be possible for them. If we send a packet to one of them, we expect (in most cases; there are various complications) that it will be delivered if the address is in use and will cause an ICMP error packet to come back to us if not.

There are also several classes on non-routable IP addresses.

RSA algorithm
Rivest **S**hamir **A**dleman public key encryption method, named for its three inventors. Patented (expires in Sept. 2000) with licenses available from RSA Data Security. Widely used.

RSA Data Security
A company founded by the inventors of the RSA public key algorithm.

SA
Security Association, the channel negotiated by the higher levels of an IPSEC implementation and used by the lower. SAs are unidirectional; you need a pair of them for two-way communication.

An SA is defined by three things -- the destination, the protocol (AH orESP) and the SPI, security parameters index. It is used to index other things such as session keys and intialisation vectors.

For more detail, see our IPSEC Overview and/or RFC 2401.

Secure DNS
A version of the DNS or Domain Name Service enhanced with authentication services. This is being designed by the IETF DNS security working group. The BIND 8.2 implementation is available for download. Another site has more information.

IPSEC can use this plus Diffie-Hellman key exchange to bootstrap itself. This would allow opportunistic encryption. Any pair of machines which could authenticate each other via DNS could communicate securely, without either a pre-existing shared secret or a shared PKI.

Linux FreeS/WAN will support this in a future release.

Secret key cryptography
See symmetric cryptography

Security Association
see SA

Sequence number
A number added to a packet or message which indicates its position in a sequence of packets or messages. This provides some security against replay attacks.

For automatic keying mode, the IPSEC RFCs require that the sender generate sequence numbers for each packet, but leave it optional whether the receiver does anything with them.

SHA
Secure **H**ash **A**lgorithm, a message digest algorithm developed by the NSA for use in the Digital Signature standard, FIPS number 186 from NIST. SHA is an improved variant of MD4 producing a 160-bit hash.

SHA is one of two message digest algorithms available in IPSEC. The other is MD5. Some people do not trust SHA because it was developed by the NSA. There is, as far as we know, no cryptographic evidence that SHA is untrustworthy, but this does not prevent that view from being strongly held.

Signals intelligence (SIGINT)
: Activities of government agencies from various nations aimed at protecting their own communications and reading those of others. Cryptography, cryptanalysis, wiretapping, interception and monitoring of various sorts of signals. The players include the American NSA, British GCHQ and Canadian CSE.

SKIP
: **S**imple **K**ey management for **I**nternet **P**rotocols, an alternative to IKE developed by Sun and being marketed by their Internet Commerce Group.

Snake oil
: Bogus cryptography. See the Snake Oil FAQ or this paper by Schneier.

SPI
: **S**ecurity **P**arameter **I**ndex, an index used within IPSEC to keep connections distinct. A Security Association (SA) is defined by destination, protocol and SPI. Without the SPI, two connections to the same gateway using the same protocol could not be distinguished.

  For more detail, see our IPSEC Overview and/or RFC 2401.

SSH
: Secure **SH**ell, an encrypting replacement for the insecure Berkeley commands whose names begin with "r" for "remote": rsh, rlogin, etc. Web site.

SSH Communications Security
: A company founded by the authors of SSH. Offices are in Finland and California. They have a toolkit for developers of IPSEC applications.

SSL
: Secure Sockets Layer, a set of encryption and authentication services for web browsers, developed by Netscape. Widely used in Internet commerce. Also known as TLS.

SSLeay
: A free implementation of SSL by Eric Young (eay) and others. Developed in Australia; not subject to US export controls.

Stream cipher
: A symmetric cipher which produces a stream of output which can be combined (often using XOR or bytewise addition) with the plaintext to produce ciphertext. Contrasts with block cipher.

  IPSEC does not use stream ciphers. Their main application is link-level encryption, for example of voice, video or data streams on a wire or a radio signal.

subnet
: A group of IP addresses which are logically one network, typically (but not always) assigned to a group of physically connected machines. The range of addresses in a subnet is described using a subnet mask. See next entry.

subnet mask
: A method of indicating the addresses included in a subnet. Here are two equivalent examples:
  - 101.101.101.0/24
  - 101.101.101.0 with mask 255.255.255.0

  The '24' is shorthand for a mask with the top 24 bits one and the rest zero. This is exactly the same as 255.255.255.0 which has three all-ones bytes and one all-zeros byte.

These indicate that, for this range of addresses, the top 24 bits are to be treated as naming a network (often referred to as "the 101.101.101.0/24 subnet") while most combinations of the low 8 bits can be used to designate machines on that network. Two addresses are reserved; 101.101.101.0 refers to the subnet rather than a specific machine while 101.101.101.255 is a broadcast address. 1 to 254 are available for machines.

It is common to find subnets arranged in a hierarchy. For example, a large company might have a /16 subnet and allocate /24 subnets within that to departments. An ISP might have a large subnet and allocate /26 subnets (64 addresses, 62 usable) to business customers and /29 subnets (8 addresses, 6 usable) to residential clients.

S/WAN

Secure Wide Area Network, a project involving RSA Data Security and a number of other companies. The goal is to ensure that all their IPSEC implementations will interoperate so that their customers can communicate with each other securely.

Symmetric cryptography

Symmetric cryptography, also referred to as conventional or secret key cryptography, relies on a *shared secret key*, identical for sender and receiver. Sender encrypts with that key, receiver decrypts with it. The idea is that an eavesdropper without the key be unable to read the messages. There are two main types of symmetric cipher, block ciphers and stream ciphers.

Symmetric cryptography contrasts with public key or asymmetric systems where the two players use different keys.

The great difficulty in symmetric cryptography is, of course, key management. Sender and receiver *must* have identical keys and those keys *must* be kept secret from everyone else. Not too much of a problem if only two people are involved and they can conveniently meet privately or employ a trusted courier. Quite a problem, though, in other circumstances.

It gets much worse if there are many people. An application might be written to use only one key for communication among 100 people, for example, but there would be serious problems. Do you actually trust all of them that much? Do they trust each other that much? Should they? What is at risk if that key is compromised? How are you going to distribute that key to everyone without risking its secrecy? What do you do when one of them leaves the company? Will you even know?

On the other hand, if you need unique keys for every possible connection between a group of 100, then each user must have 99 keys. You need either 99*100/2 = 4950 *secure* key exchanges between users or a central authority that *securely* distributes 100 key packets, each with a different set of 99 keys.

Either of these is possible, though tricky, for 100 users. Either becomes an administrative nightmare for larger numbers. Moreover, keys *must* be changed regularly, so the problem of key distribution comes up again and again. If you use the same key for many messages then an attacker has more text to work with in an attempt to crack that key. Moreover, one successful crack will give him or her the text of all those messages.

In short, the *hardest part of conventional cryptography is key management*. Today the standard solution is to build a hybrid system using public key techniques to manage keys.

TIS

Trusted Information Systems, a firewall vendor now part of NAI. Their Gauntlet product offers IPSEC VPN services. TIS implemented the first version of Secure DNS on a DARPA contract.

TLS

Transport Layer Security, a newer name for SSL.

Traffic analysis

Deducing useful intelligence from patterns of message traffic, without breaking codes or reading the messages. In one case during World War II, the British knew an attack was coming because all German radio traffic stopped. The "radio silence" order, intended to preserve security, actually gave the game away.

In an industrial espionage situation, one might deduce something interesting just by knowing that company A and company B were talking, especially if one were able to tell which departments were involved, or if one already knew that A was looking for acquisitions and B was seeking funds for expansion.

IPSEC itself does not defend against this, but carefully thought out systems using IPSEC can do so. In particular, one might want to encrypt more traffic than was strictly necessary, route things in odd ways, or even encrypt dummy packets, to confuse the analyst.

Transport mode

An IPSEC application in which the IPSEC gateway is the destination of the protected packets, a machine acts as its own gateway. Contrast with tunnel mode.

Triple DES

see 3DES

Tunnel mode

An IPSEC application in which an IPSEC gateway provides protection for packets to and from other systems. Contrast with transport mode.

Two-key Triple DES

A variant of triple DES or 3DES in which only two keys are used. As in the three-key version, the order of operations is EDE or encrypt-decrypt-encrypt, but in the two-key variant the first and third keys are the same.

3DES with three keys has 3*56 = 168 bits of key but has only 112-bit strength against a meet-in-the-middle attack, so it is possible that the two key version is just as strong. Last I looked, this was an open question in the research literature.

RFC 2451 defines triple DES for IPSEC as the three-key variant. The two-key variant should not be used and is not implemented directly in Linux FreeS/WAN. It cannot be used in automatically keyed mode without major fiddles in the source code. For manually keyed connections, you could make Linux FreeS/WAN talk to a two-key implementation by setting two keys the same in /etc/ipsec.conf.

Virtual Interface

A Linux feature which allows one physical network interface to have two or more IP addresses. See the *Linux Network Administrator's Guide* in book form or on the web for details.

Virtual Private Network

see VPN

VPN

Virtual Private Network, a network which can safely be used as if it were private, even though some of its communication uses insecure connections. All traffic on those connections is encrypted.

IPSEC is not the only technique available for building VPNs, but it is the only method defined by RFCs and supported by many vendors. VPNs are by no means the only thing you can do with IPSEC, but they may be the most important application for many users.

VPNC
Virtual Private Network Consortium, an association of vendors of VPN products.

Wassenaar Arrangement
An international agreement restricting export of munitions and other tools of war. Unfortunately, cryptographic software is also restricted under the current version of the agreement.

Web of Trust
PGP's method of certifying keys. Any user can sign a key; you decide which signatures or combinations of signatures to accept as certification. This contrasts with the hierarchy of CAs (Certification Authorities) used in many PKIs (Public Key Infrastructures).

See Global Trust Register for an interesting addition to the web of trust.

X.509
A standard from the ITU (International Telecommunication Union), for hierarchical directories with authentication services, used in many PKI implementations.

Use of X.509 services, via the LDAP protocol, for certification of keys is allowed but not required by the IPSEC RFCs. It is not yet implemented in Linux FreeS/WAN.

Xedia
A vendor of router and Internet access products. Their QVPN products interoperate with Linux FreeS/WAN; see our compatibility document.

Click below to go to:
- Document index file
- Table of Contents
- Beginning of this file
- FreeS/WAN home page