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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.