"Performance Analysis and Enhancement in IPSec VPN to Reduce Connection Establishment Overhead and Transmission Delay: Part-1"

Vishal Sharma[1] and Manish Kalra
Jaipur National University, Jaipur
[1]Jagannath University, Jaipur

Abstract:

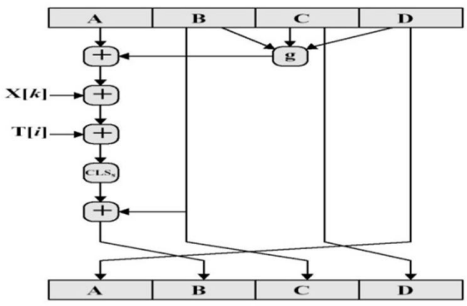
In this paper we are discussing various encryption and authentication algorithms and foreseeing the effect of these algorithms over network performance HMSC-MD5 and AES (authentication encryption) gives the optimum network performance parameter.

Key words: IPSec, Transmission, and algorithms

INRODUCTION

Virtual Private Network (VPN)

Beside Local Area Networks (LAN) or Wide Area Networks (WAN), networks can be generally cut into public and private. Examples for public networks are the internet or telephone networks. Private networks consisting of networked devices of restricted private organizations, mainly communicating among each other. The crossover between private and public network happens via gateway router. A configured firewall prevents attack from outside and restricted the user's access to the public network. The VPN concept blurs the boarders between public and private networks by offering the possibility to build up a safe, private network over public network(s) like the internet. A virtual private network is a method to simulate a private network in a public network. It is named "virtual", because of the virtual connections appearing to be within one private network – that means temporally connections that are not physical but consist of packages, transferred via public networking infrastructure (e.g. internet) without the notice of that by the user. Thus VPNs use the internet as a WAN connection. An advantage of this method for an organization can be the use of only relatively short dedicated connection from the own location to the next point of presence normally to the service provider. This connection could be a local leased line. The outcome of this is a lower –cost option for major organizations and scalability of the resources.VPN systems require an in depth understanding of public network security issues. The availability and performance of an organization`s wide-area VPN (over the Internet in particular) depends on factors largely outside of their control. Some VPN technologies from different vendors do not work well together due to immature standards. VPNs need to accommodate protocols other than IP and existing ("legacy") internal network technology. Different types of technologies are used to protect the data transmission. For data protection package tunneling and firewalls are used. VPN protocols also support authentication and encryption to keep the tunnels secure. VPN supports two types of tunneling, voluntary and compulsory tunneling. In voluntary tunneling, voluntary and compulsory tunneling. In voluntary tunneling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). In compulsory tunneling the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. Compulsory VPN tunneling authenticates client's associates them with specific VPN servers using logic built into the broker device. Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively moves control over the tunnels from clients to the ISP.



IPSec Overview: IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and it includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit. IPsec contains ESP (Encapsulating Security Payload) that provides confidentiality, authentication, and integrity. ESP provides all encryption services. IPsec also contains AH (Authentication Header) that provides authentication and integrity, which protect against data tampering and unauthorized retransmission of packets. The last

component it has IKE (Internet Key Exchange) that provides key management and security association management. IPsec has introduced the concept of SA (security association). A SA is a logical connection between two devices transferring data. A SA provides data protection for unidirectional traffic by using defined IPsec protocol.

IPSec Services

IPSec is designed to provide the following services at network layer.

- Access control
- Connectionless integrity
- Data Origin authentication
- Rejection of replayed packets
- Privacy/confidentiality

Of course the quality of these services depends upon the decision of the security administrator. IPSec is a tool, a powerful tool, but its effectiveness depends upon how it was implemented.

IPSec Authentication Header (AH)

IP Authentication Header (AH), a key protocol in the IPSec (Internet Security) architecture, is used to provide connectionless integrity and data origin authentication for IP datagram, and to provide protection against replays. This protection service against replay is an optional service to be selected by the receiver when a Security Association is established. AH provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is only partial in some cases. Figure 1.1 depicts the IPSec AH header format. The “Next header” field is of 8 bit size identifies the type of the next payload after the Authentication Header. The “Payload Length” field is of 8 bit size specifies the length of AH in 32-bit words (4-byte units), minus "2". The SPI (Security Parameter Index) field is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (AH), uniquely identifies the Security Association for this datagram. The “Sequence Number” field contains a monotonically increasing counter value and is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA. The “Authentication Data” field is a variable-length field containing an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data.

-Next	Payload	Reserved(32)
Header(8)	Length(8)	
Security Parameter Index(32)		
Sequence Number Field(32)		
Authentication Data		

Figure : IPSec Authentication Header Format

IPSec Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) is a key protocol in the IPsec (Internet Security) architecture. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality. Figure 1.2 depicts the ESP header format The IP Encapsulating Security Payload (ESP) seeks to provide confidentiality and integrity by encrypting data to be protected and placing the encrypted data in the data portion of the IP ESP. Depending on the user's security requirements, this mechanism may be used to encrypt either a transport-layer segment (e.g., TCP, UDP, ICMP, and IGMP) or an entire IP datagram. Encapsulating the protected data is necessary to provide confidentiality for the entire original datagram. ESP consists of an unencrypted header followed by encrypted data. The encrypted data includes both the protected ESP header fields and the protected user data, which is either an entire IP datagram or an upper-layer protocol frame (e.g., TCP or UDP). The set of services provided depends on options selected at the time of Security Association establishment and on the placement of the implementation. Confidentiality may be selected independent of all other services. However, use of confidentiality without integrity/authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service. Data origin authentication and connectionless integrity are joint services and are offered as an option in conjunction with (optional) confidentiality. The anti-replay service may be selected only if data origin authentication is selected, and its election is solely at the discretion of the receiver. Security association identifier - a pseudo-random value identifying the security association for this datagram. Sequence Number - it contains a monotonically increasing counter value and is mandatory and is always present even if the receiver does not elect to enable the anti-replay service for a specific SA. Payload Data - a variable-length field containing data described by the Next Header field. Padding - padding for encryption. Pad length - indicates the number of pad bytes immediately preceding it. Next header - identifies the type of data contained in the Payload Data field, e.g., an extension header in IPv6 or an upper layer protocol identifier. Authentication Data - a variable-

length field containing an Integrity Check Value (ICV) computed over the ESP packet minus the Authentication Data.

Security Parameter Index (32)		
Sequence Number Field (32)		
Payload Data (variable)		
Padding (0-255 bytes)		
	Pad Length (8)	Next Header(8)
Authentication Data (variable, Multiple of 32 bits)		

Figure : IPSec ESP Header Format

IPSec Technologies

IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity. In particular, IPSec uses:

- Diffie-Hellman key exchange for deriving key material between peers on a public network.
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks.
- Encryption algorithms, such as DES, 3DES for encrypting the data.
- Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication.
- Digital certificates signed by a certificate authority to act as digital ID cards.

IPSec Operation

The purpose of IPSec is to provide various services to traffic travelling between a source and destination. The destination/source maybe a router or a host. The services may be provided to all traffic or only to specific types of traffic [6].

There are different types of protection provided by IPSec and there are also different modes for IPSec to operate upon. IPSec may operate upon certain types of data while other data is transmitted on an unprotected path. In terms of packet construction and TCP/IP stack IPSec is implemented at the network layer. The diagram below shows the location of the IPSec protocol in the stack. The arrows show the path of a packet travelling from Host A to Host B. Notice that Host B implements IPSec as a separate layer, wherever Host A and the routers include IPSec as a part of the network layer. These are two different types of host implementation known as OS integrated or bump in the stack (BITS). There are drawbacks and advantages for both types of implementation; OS Integration can be difficult for external companies providing solutions to existing networks, however, OS integration can make use of services in an existing network layer. IPSec physically interacts with the stack by modifying, encapsulating or inserting data into the IP packet before it is passed to the data link layer on the way out and again modifying the packet before it is passed up to the network or transport layer.

Operating Modes of IPSec

IPSec defines two types of operating modes:

Transport Mode

In the transport mode of IPSec operation, authentication is provided directly between a client and a server workstation. IPSec Transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server.

Transport mode provides the protection of our data, also known as IP Payload, and consists of TCP/UDP header + Data, through an AH or ESP header. The payload is encapsulated by the IPSec headers and trailers. The original IP headers remain intact, except that the IP protocol field is changed to ESP (50) or AH (51), and the original protocol value is saved in the IPSec trailer to be restored when the packet is decrypted

.

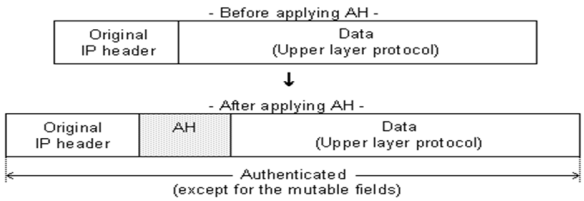


Figure : AH in Transport Mode

When AH is used in Transport mode the whole packet is authenticated but nothing is done to provide confidentiality.

Tunnel Mode

IPSec tunnel mode is the default mode. With tunnel mode, the entire original IP packet is protected by IPSec. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer).

In tunnel mode of IPSec operation a remote workstation authenticates itself to the corporate firewall.

In tunnel mode, the whole packet is processed including the IP header. Original IP source and destination addresses and other header components are protected by AH or ESP and a new IP header are inserted into the packet. The new IP source and destination addresses typically are those of the gateways. Based on the transformation method used, (AH or ESP), the whole packet is either authenticated, encrypted or both.

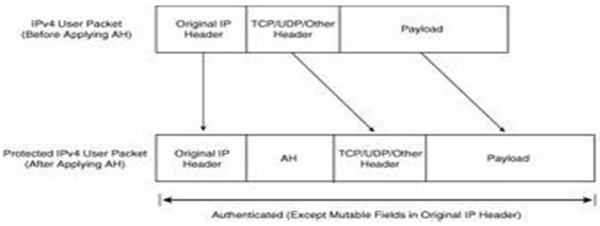


Figure : AH in Tunnel Mode

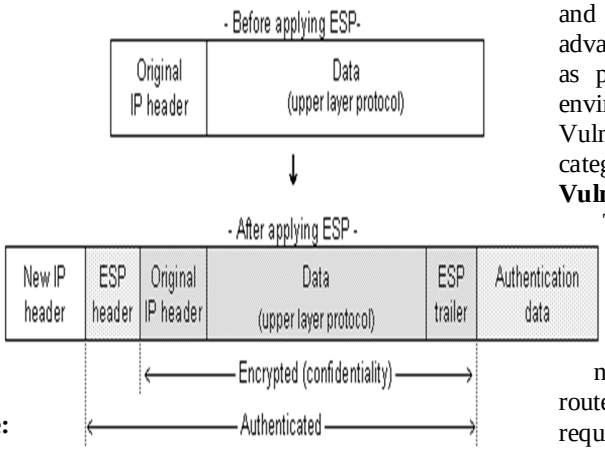


Figure:

ESP in Tunnel Mode

In Tunnel Mode, the whole packet is processed including the IP header, Original IP source and destination addresses and other header components are protected by AH or ESP and a new IP Header are inserted into the packet, the new IP source and destination addresses typically are those of the gateways. Based on the transformation method used. (AH or ESP) the whole packet is either authenticated, encrypted or both.

IPSec vs. other Layers Security

IPSec differs from security provided at other layers of TCP/ IP stack in following ways:

- ❖ Higher-level services protect single protocol
- ❖ Lower level services protect a single medium.

For example a pair of encryption boxes on the ends of a line makes wiretaps on that lone unless the attacker is capable of breaking the encryption. IPSec however, can protect any protocol, running above IP and any medium, which IP runs over It can protect a mixture of application protocols running over a complex combination of media

- ❖ IPSec can provide some security services in the background with no impact on user.
- ❖ Layer 4 security protocol (SSL). Develops something at user level without changing underlying OS. But layer3 means goal of IPSec is to develop something with in the so and not required changes to the application so can provide security to diverse range of application protocols.

The philosophy behind IPSec is that if only the OS need to chine, then by deploying an IPSec enhanced so all the application would automatically benefit from IPSec encryption and integrity protocol services.

Vulnerability of IPSec

IPSec protocols are an excellent step in the right direction for internet security If correctly implemented and configured the protocol could provide e- business and organization like defense with ability to tack advantage of speed and reach of internet without being as prone to the dangers of attack in an unplaced environment [7].

Vulnerabilities in IPSec can be broken into following categories:

Vulnerability in IPSec Protocols

There are numerous scenarios and speculation in which the protocol defined for operation of IPSec can be challenged.

Cut-and-Paste Attack

This attack will only be possible on two networks that use IPSec as a tunnel between the two routers that link the networks There is also a requirement that the attacker has access to a second machine in each of the two networks {8} The attack works by an attacker sniffing a legitimate encrypted packet from Host A to Host B Attacker also sniffs a planned packet sent from Host C to Host D Attacker copies encrypted data from Host A's packet into packet from Host C to D. Router B is tricked into decrypting Host A packer for Host B and sending it to Host D This exploit is not as straightforward as it may appear, as there are some other requirement relating to the sequence numbers used in IPSec packets and ensuring that Host A genuine packets don't reach Router B before the false packets do: IPSec includes various replay attack protection methods the would make this attack a little more difficult to unsuccessfully in real situation.

Encryption and Authentication algorithm in IPSec

Triple DES Encryption

The Data Encryption Standard(DES) was developed by an IBM team around 1974 {10} and adopted as a national standard in 1977 triple DES is a minor variation of this standard it is three times slower than

regular DES but can be billions of times more secure if used properly Triple DES enjoys much wider use than DES because DES is so easy to break with today rapidly advancing technology in 1988 the Electronic frontier foundation using a specially developed computer called the DES cracker managed to break DES in less than 3 days and this was done for under $ 250,000 The encryption chip that powered the DES cracker was capable of processing 88 billion keys per second In addition it has been shown that for a cost of one million dollars a dedicated hardware device can be built than can search all possible DES keys in about 3.5 hours This just serves to illustrate that any organization with moderate resources can break through DES with very little effort these days No sane security expert would consider singes to protect data {10} Triple DES was the answer to many of the shortcomings o9f DES Since it is based on the DES algorithm it is very easy to modify existing software to use Triple DES It also has the advantage of proven reliability and a longer key length that e3liminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES However even this more powerful version of DES may not be strong enough to protect data for very much longer The DES algorithm itself has become obsolete and is in need of replacement To this end the National Institute of standards and Technology (NIST) is holding a competition to develop the advanced Encryption standard (AES) as a replacement for DES Triple DES has been endorsed by NIST as temporary standard to be used until the AES is finished sometime in 2011.

The AES will be at least as strong as Triple DES and probably much faster Many security systems will probably use both Triple DES and AES for at least the next five years After that AES may supplant Triple DES as the default algorithm on most system if it lives up to its expectation Bui triple DES will be kept around for compatibility resounds for many years after that so the useful lifetime of Triple DES is far from over even with the AES near completion For the foreseeable future Triple DES is an excellent and reliable choice for the security needs of highly sensitive information.

Triple DES is simply another mode of DES operation {11} it takes three 64- bit keys for an overall key length of 192 bits In private Encrypt or you simply type in the entire 192-bit (234 character key rather than entering each of the tree keys individually7 The Triple DES DLL then breaks the user provided key into three sub keys padding the keys if necessary so they are each 64 bits long The procedure for encryption is exactly the same as regular DES but it is repeated three times Hence lithe name Triple DES the data is encrypted with the first key decrypted with the second key and finally encrypted again with the third key Consequently Triple DES runs tree times slower than standard DES but is much more secure if used properly The procedure for decryption something is the same as the procedure for encryption except it is executed in reverse Like DES data is encrypted and decrypted in 64 bit chunks Unfortunately there are some weak keys that one should be aware of if all three keys the first and second keys or the second and third keys are the same then the encryption procedure is essentially the same as standard DES This situation is to be avoided because it is the same as using a really slow version of regular DES note that although the input key for DES is 64 bits long the actual key used by DES is only 56 bits in length The least significant (right most bit in e4ach byte is a parity bit and should be set so that there are always an odd number of is in every byte These parity bits are ignored so only the seven most significant bits of each byte are used resulting in a key length of 56 bits this means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

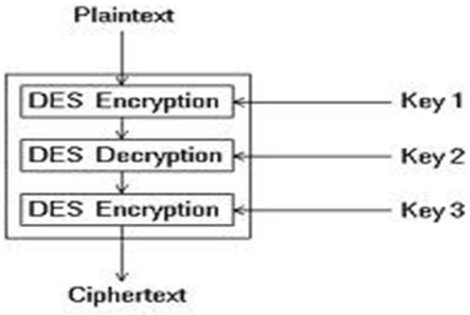


Figure : Triple Data Encryption Standard

Triple ECB (Electronic Code Book)

This variant of Triple DES woks exactly the same way as the ECB mode of DES Triple ECB is the type of encryption used by private encrypted. This is the most commonly used mode of operation. [2]

Triple CBC (Cipher Block Chaining)

This method is very similar to the standard DES CBC mode. As with Triple ECB the effective key length is 168- bits and keys are used in the same manner as described above but chaining features of CBC mode are also employed The first 64- bit key acts as the Initialization Vector to DES. Triple ECB is then executed for a single 64 bit block to be encrypted and the procedure is repeated. This method adds an extra layer of security to Triple DES and is therefore more secure than Triple ECB, although it is not used as widely as Triple ECB.

AES Algorithm Terminology

- Plaintext refers to the data to be encrypted Cipher text refers to the data after going

through the cipher as well as the data than will be going into the decipher

- The state is an intermediate form of the cipher or deciphers result usually displayed as a rectangular table of bytes with4 rows and 4 columns {14}

AES Algorithm Features

- Key lengths of 128, 192, and 256- bits are supported Each step in key size requires only two additional rounds The decipher is simply the inverse of the cipher.
- Figure 1.10 shows the Shift Rows transformation where the first row remains untouched, while the second third, and fourth rows perform a byte rotate by one two, and three bytes respectively.
- Figure 1.11 shows the Mix Columns transformation where each column is treated as a four term polynomial over GF(2) and multiplied by a(x)= {03}X3 + {01} X2 +{01}X+{02}.

AES Algorithm Implementations

- Optimized Software Implementation- The pure software implementation is bounded by the load/story behavior and byte arithmetic of the algorithm The encryption requires 774 cycles per block on a MIPS32 processor and the decryption requires837 cycles.
- AES Encryption primitives- This is the simplest form of Vocal's hardware acceleration The AES primitives extend the capabilities of the MIPS32 processor by taking advantage of MIPS Technologies Coextend capability to decreases the number of cycles to encrypt and 460 cycles to decrypt per block on the MIPS32 processor.
- AES Round Accelerator Algorithm- The Round Accelerator requires 1024 bytes of local memory, but increases the performance to 117 cycles per block to encrypt and 127 cycles per block to decrypt.
- AES 32- bit Block Accelerator Algorithm- The Block Accelerator is designed to be a good mid-scale solution. It used 2048 bytes of local memory The number of cycles to process a block on a MIPS32 CPU falls to 64 cycles for both encryption and decryption using this implementation.
- AES 32-bit Co- Processor Algorithm- The Co-Processor implementation uses 2048 bytes of memory to deliver performance of 45 cycles per block on the MIPS32.
- AES 64-bit Co-Processor Algorithm- The same amount of the memory is required for the 64-bit implementation, but the performance increases to just 25 eyeless per block on the MIPD32.

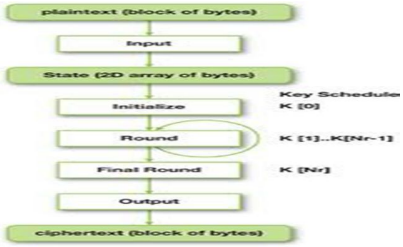


Figure : AES Algorithm Function

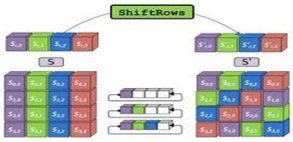


Figure : Shift Rows Transform

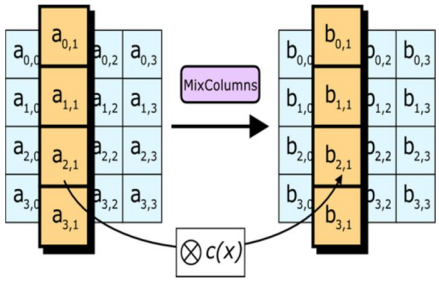


Figure : Mix Column Transfer

The encryption concept can be used in may application like the internet application to encrypt the password, visa canard number banks military communication networks, satellite channels and some other communication systems.

Blowfish Algorithm

Some of the Blowfish algorithm Specification can be summarized as {15},{16}:

1. Symmetric block cipher.
2. 64-bit Block
3. Variable-length key from 32-bits(4 Bytes) to 448 bits
4. Run at an acceptable clock speed.
5. Suitable and efficient for hardware.
6. Unpatented and no license is required.

The algorithm consists mainly of two parts the key expansion part and the data encryption part Key

expansion converts a key of at most 448-bits into 4168 bytes there is a p-array and four 32-bitS-boxes. The P-array contains 18 of 32-bit sub keys while each S- box contains 256 entries Data encryption occurs via a 16-round Festal network Each round consists of a key dependent permutation and a key and data dependent substitution All operation are Mors ad additions on 32-bit words. The only additional operations are four indexed array data lookups per round {16} The input is a 64-bit data elements, encryption may be illustrated as shown Figure 1.12.

The sub keys can be calculated by the following steps

1. Initialize the P-array and S-boxes
2. XOR P-array with the key bits(i.e., P1 XOR (first32 bits of key) P2 XOR (Second 32 bits of keys)
3. Use the above method to encrypt the all zero
4. This new Outpour is P1 and P2
5. Encrypt the new P1 and P2 with the modified key
6. This new output is now P3 and P4
7. Repeat 521 times in order to calculate new sub key for the P-array and the four S-boxes.

Blowfish uses four S-boxes each one has 256 entries, and each of the entries is 32- bits long as shown in Fig.2 Tocalculte the F- function use the first byte of the 32- bits of input to find an enter in the fast S-box the second byte to find an entry in the second S-box, and so on first dividing XL (left side of the 64- bit black of data to be encrypted) into four 8 bit quarters then calculate F(XL) as given by Eq. 1.

F (XL) = ((S1 [box]} + S2 {[box2]}+ XOR S3{[box3]}+ S4{[box4]}

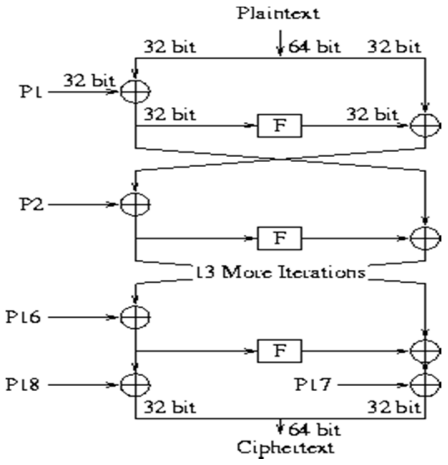


Figure: Data flow graph of Blowfish block cipher

How the Algorithm Works

Begin by initializing sub keys 1 through 18 followed by elements zero through 255 of the first S box, then elements zero through 255 of the second Sbox all the way to element 255 of the fourth S box with the factional part of Pi The most significant bit of the factional part of Pi become the nest significant bit of the first sub key Take the key which may be of any length up to 72 bytes, and repeat it as often as contents Then execute the Blowfish algorithm repeatedly with an initial input of a 64- byte block of all zeroes as plaintext input After each execution replace part of the sub keys or S boxes with the successive outputs of Blowfish in the same order as the digits of P in binary (or hexadecimal) form were placed in them after the first iteration replace sub keys1 and 2: after the tenth iteration replace the first two entries (0 and 1) in S- box and so on.

Encryption algorithm is the speed of execution. This speed is directly related to the size of the plaintext file sixe but it is not affected by varying the key length both encryption and decryption analyses where performed for deferent types of data

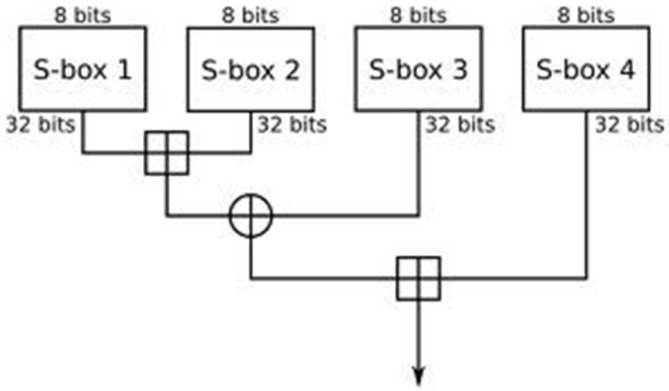
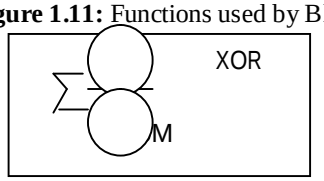


Figure 1.11: Functions used by Blowfish



MD5 (Message-Digest algorithm5)

In cryptography, MD5 is a widely used partially insecure cryptographic hash function with a 128-bit has value. As an internet standard{17} MD5 has been employed in a wide variety of security application and is also commonly used to check the integrity of files An MD5 hash is typically expressed as a 32 digit hexadecimal number.

Message Digest is a series of message digest algorithms designed by professor Ronald Ronald Rivets of MIT (Rivets, 1994). When analytic work indicated that MD5's Predecessor-MD4-was likely to be insecure, MD5 was designed in 1991 to be a secure replacement.

Algorithm

In the algorithm<<<<s denote a left bit rotation by s places, s varies for each operation and denotes addition modulo{2} MD5 processes a cartable-length message into a fixe length output of 128 bits The input message is broken up into chunks of 512 bit blocks (sixteen 32 bit little endian integers) the message is padded so that its length is divisible by 512 the padding works as follows first a single bit I is appended to the end of the message This followed by as many Zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512 The remaining bits are filled up with a64 bit integer representing the length of the original message in bits The main MD5 algorithm operates on a 128 M- bit state divided into four 32- bit works denoted ADV and D these are initialized to certain fixed constants The main algorithm then operates on each figure 1.14 one MD5 operation MD5 consists of 64 of these operation grouped in four founds of 16 operation F is a nonlinear function one function is used in each round M denotes a 32 bit block of the message input and K denotes a 32 bit constant different for each operation 512 bit message block in turn each black modifying the sate The processing of message black consists of four similar stages termed rounds each round is composed of 16 similar operation based on a non linear function F modular addition and left rotation. Round there are four possible functions F; a Different one is used in each round

F(X, Y, Z) =(X^Y) ^ (-X^Z)
G(X, Y, Z) =(X^Z) ^(Y^-Z)
H(X, Y, Z) =X*Y*Z
I (S, Y, Z) = Y*(X^-Z)

*, ^, ^, - denote the XOR, AND, OR and NOT operation respectively.

Secure Hash Algorithm(SHA-1)

The use of SHA-1 {FIPS-180-1} combined with HMAC [18] as a keyed authentication mechanism within the context of the Encapsulation security payload and the Authentication Header The goal of HMAC-SHA-1-96 is to ensure that the packet is authentic and cannot be modified in transit.

HMAC is a secret key authentication algorithm Data integrity and data origin authentication as provided by HMAC are dependent upon the scope of the distribution of the secret key if only the sauce and destination know the HMAC key this provides both data origin authentication and data integrity of packets sent between the two parties: if the HMAC is correct this proves that it must have been added by the sauce HMAC-SHA-1-96 is used within the context of ESP and AH, for further information on how the various pieces of ESP including the confidentiality mechanism—fit together to provide security services.

Security Considerations

The security provided by HMAC-SHA-1-96 is based upon the strength of HMAC, and to a lesser degree the strength of SHA-1 at the time of this writing there are no practical cryptographic attacks against HMAC-SHA-1-96 {18} STATES THAT FOR " minimally reasonable hash function" the " birthday attack" is impractical For a 64- byte block hash such as HMAC-SHA-1-96 AN attack involving the successful processing of 2**80 blocks would be infeasible unless it were discovered that the underlying hash had collisions after processing 2**30 blocks A hash with such weak collision resistance characteristic would generally be considered to be unusable.

It is also important to consider that while SHA-1 was never developed to be used as a keyed has algorithm HMAC had those criteria for the onset{18} also discusses the potential additional security which is provided by the truncation of the resulting hash Specification which include HMAC are strongly encouraged to prom this hash truncation As {18} provides a framework for incorporating various hash algorithms with HMAC it is possible to replace SHA-1 with other algorithms such as MD5 {18} contains a detailed discussion on the strengths and weaknesses of HMAC algorithms.

As is true with any cryptographic algorithm part of its strength lies in the correctness of the algorithm implementation the security of the key management mechanism and its implementation the strength of the associated secret key and upon the correctness of the implementation in all of the participating systems are contained in{20} Test vectors and example code to assist in verifying the correctness of HMAC-SHA-1-96 code.

Conclusion:

This work aims to reduce the security problems in sensitive data transfer across networks by providing secure protocols on implementing security services based on internet protocol security (IPSec) This paper present information that is independent of particular hardware platforms operation systems and applications other than providing real world examples to illustrate particular concepts authentication algorithms which are used in IPSec for network layer security services and find the optimal solution in them and how IPSec addresses these services It also describes alternatives to IPSec and discusses under what circumstances each alternative may be appropriate.

REFERENCES

1. W. Simpson: "IP in IP Tunneling" RFC 1853, October 1995.

2. Hamzeh K Pall, G Verthein, W , Taarud, J, Little W. and G Zorn: "Point-to-Point Tunneling Protocol (PPTP)" RFC 2637, July 1999,
3. S. kent and R. Atkinson: "IP Authentication Hearder", IETF RFC 2402, 1998
4. Elegancy and M M. Matalgeh "performance analysis of IPsec protocol; Encryption and Authentication" computer communication IEEE 2002,
5. Uyles Black: Internet Security Protocols Protecting IP traffic pearson Education Asia 1st Edition 2001
6. Daniel Clark: "Vulnerability of IPsec A discussion of possible weakness in IPsec implementation and protocol version 1.3" SANS institute 2002
7. Salary and Mate: "A Special Attack against IPsec ; A discussion of possible weakness in IPsec implementation and protocols Version 1.3" SANS institute 2002
8. C. Irvine T Levin E Spyropoulou and B Allen: "Security As a dimension of quality of service in Active service Environments" Computer Communication IEEE 2002
9. William C. barker: "Recommendation for the triple Data Encryption Algorithm (TDEA) Block Cipher" Computer Security and Technology Gaithersburg MD 20899-8930, May 2004
10. Hamalainen P. Hannikainen M. Hamalainen T. and Saarinen J. "Data encryption standard" Federal information processing standards (FIPS) publication 46-7, National institute of Standards and Technology (NIST) USA, 1999.
11. J Galvin, K. McCloghrie an J. Devin: "Date Encryption Algorithm- Modes of Operation", ANSI X3 106 American National Standards Institute, May 19, 1983.
12. J. Neuchâtel, E Barker, L Bass ham William Burr, Morris: "Working jams foci and Edward Runback Report on the Development of the Advanced Encryption Standard (AES)" National Institute of Standards and Technology, October 2000.
13. E. Bihar and A Shamir: "power analysis of the key scheduling of the ASE Candidates" sapid AES candidate Conference3 printed by the National Institute of standards and technology Gaithersburg, MD pp 115-121, march 22-23,1999
14. Kamahi N.A turkey al somatic and khalid al Zamia: "Performance evaluation of three encryption decryption algorithms proceeding of the 46th IEEE international Midwest symposium, Vol 1. No.2 pp 790-793, December 2003
15. B. Schneier "Description of a new variable Length Key 64-bit block cipher (Elbows) Proceedings of fast software Encryption security" Cambridge University press, pp 191-204, 1994
16. Rivest, R. "MD 5 Digest Algorithm" RFC-132, April 1992.
17. Krawczyk H Bear M and Canetti R, "HMAC; keyed – Hashing for message Authentication". RFC-2014 February,1997
18. Secure hash standard, [FIPS-180-1] NIST, FIPS PUB 180-1: secure hash standard, april, 1995.
19. Cheng P and R glenn: Test cases for HMAC_MD5 and HMAC-SHA-1rfc 2202, March 1997