

IPV6 vs. SSL

comparing Apples with Oranges

Reto E. Haeni
r.haeni@cpi.seas.gwu.edu

The George Washington University
Cyberspace Policy Institute
2033 K Str. Suite 340 N
Washington DC 20006

Washington DC, January 1997

Index

1 Abstract	3
2 Introduction	4
3 Overview on IPv6	4
3.1 Header	4
3.2 Addressing	6
3.3 Routing	7
3.4 Security	7
3.4.1 IPv6 Authentication Header	7
3.4.2 IPv6 Encapsulating Security Header	7
3.5 Transition	8
4 IP Security in comparison to SSL	9
4.1 Architecture	9
4.2 Typical use	10
4.3 Key exchange	10
4.4 Used Ciphers	11
4.5 Authentication	12
4.6 Encryption	12
4.7 Traffic Analysis	13
5 Conclusions	14
6 References	15

1 Abstract

IPv6, also called IPng, is the next generation of IP protocol following IPv4. Its design exists as a proposed standard, and multiple organizations are researching its implementation in different operating systems and have such IPv6 running.

IPv6 uses the actual security specifications of IP secure, which can also used with IPv4. If IPv6 and SSL (Secure Sockets Layer) are not located on the same level, I compared them to each other. The results are:

- IPv6 is located on the network layer while SSL is a Transport layer protocol. IPv6 can use its security capabilities for all packets passing to its layer, while SSL provides authentication and confidentiality only to the HTTP, NNTP and SMTP protocols.
- While SSL is used for host-to-host or mostly host-to-server services, IPv6 can be used for host-to-host, host-to-subnet and subnet-to-subnet authentication or encryption. In my point of view, IPv6 security will mostly be activated on a subnet-to-subnet basis while the local traffic on the LAN will not be encrypted, as encryption requires additional processing time.
- Key exchange mechanisms are not yet defined for IPv6 but are absolutely necessary if its security mechanisms shall be used on a regular basis. Due to the large number of hosts a manual key exchange in large networks is very difficult.
- Both protocols (IPv6 and SSL) are open and are not restricted to certain ciphers. However, both protocols use DES CBC as standard algorithm. This cipher is relatively weak for today's standards as it can be broken with relative small effort (see section 4.4). For a next generation protocol, the standard cipher should be more secure as it will be used in the future. Therefore I propose to use 3DES (triple DES) as the standard cipher.
- Due to its location at the Network layer, IPv6 can provide authentication and confidentiality (by using the tunnel mode ESP) to the whole IP packet and not only to the payload. This capability prevents a large number of network attacks such as host masquerading and IP spoofing.
- None of the protocols have the capability to prevent traffic analysis, although the routing header of IPv6 could be used to make traffic analysis attempts more difficult.

While IPv6 provides stronger authentication and confidentiality in all cases over SSL, Secure Sockets Layer will still be used in spontaneous (potentially) secure transactions on the World Wide Web by its Web Browser applications such as Netscape Navigator. These applications make it possible to create a potential secure transmissions over an unsecure network with moderate expenditure.

The reader should keep in mind that 100% secure transmissions over an unsecure network are not possible. Every security protocol is only as strong as its implementation. While SSL is used in popular applications like Netscape and security leaks were discovered, IPv6 is only implemented in test applications for the different operating systems. It will show its strengths and weaknesses when implementations are widely available and used.

2 Introduction

Security is an important issue for today's communication. With the increasing factor in networking and the Internet in particular, the need for authentication and encryption is climbing rapidly. Many commercial and government (not to mention defense) organizations are no longer willing to send their sensitive information and communications unencrypted over an insecure network. In addition, the Internet is running out of IP addresses. As the Internet continues to grow exponentially, the 32 bit addressing scheme will run out of addresses in a short time. Certainly, a 32 bit addressing space contains a lot of possible addresses. But with the partition of this space into A,B,C and D addresses, we are already short of C addresses, which represent the most needed network size. During a relatively short period, we can work around this problem with subnetting larger classes, however a solution to this problem will soon be required.

IPv6 (IP version 6), also known as IPng (IP next generation) is a proposed standard and most features are already implemented and IPv6 packets are being tested on the Internet by different organizations. In IPv6, the proposed standards for IPsec (IP secure) will be implemented. IPsec is not restricted to IPv6 but can also be implemented in IPv4 (actual IP version). In this paper I will give a brief overview of the features of IPv6 and discuss the security specifications of IPsec, which throughout this paper I will refer to as the security features of IPv6. In the later sections of the paper, I compare the security specifications of IPv6 to one of today's available security protocols, SSL (Secure Sockets Layer). I am aware, that I am comparing "apples with oranges". The two protocols are located on different layers and work in different ways. Both protocols have the goal to provide authentication and confidentiality of the data. Therefore my focus will not be which one of them is "better" but if IPv6 has strong enough security and if SSL has still a place in a world where everyone is using IPv6.

3 Overview on IPv6

These pages provide a practical overview of the proposed standard of IPv6. For more specific information please refer to the IPng Web pages at

<http://playground.sun.com/pub/ipng/html/ipng-main.html>

You will find links to different Request For Comments (RFCs) where the specific sections are explained in detail.

3.1 Header

Although the address space of IPv6 is significant larger than in version 4 (see next section), the header is only twice as large. This is the result of dropping a number of header Fields in IPv6 to reduce the processing cost of packet handling and keeping the bandwidth requirements as low as possible.

The header of IPv6 contains the following fields [5]:

Version	Priority	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Version

4- bit field, contains version number of Internet Protocol (6)

Priority

4-bit field. Enables a source to determine the delivery priority of the packet. The following priority values are recommended:

- 0 - uncharacterized traffic
- 1 - filler traffic such as netnews
- 2 - unattended data transfer such as e-mail
- 3 - reserved
- 4 - attended bulk transfer such as FTP
- 5 - reserved
- 6 - interactive traffic such as telnet
- 7 - internet control traffic such as SNMP

Values 8 to 15 are used to specify the priority of non back off traffic such as videos. The lowest priority (8) should be used for traffic that the user is most willing to lose (such as high fidelity videos) and the highest priority (15) should be used for the traffic that the user is least willing to lose (such as low fidelity voice).

Flow Label

24-bit field. A flow would be a sequence of packets where either the sender or the receiver has the need for special handling by the routers. Real time video represents an application in which a Flow label would most likely be used.

Payload Length

16 bit field. Defines the length of the packet following the header. IPv6 requires that the links can handle packets with 576 bytes. This means that the payload for normal packets can be as large as 536 bytes (576 minus 40 bytes for header) regardless of the environment. However, IPv6 can carry payloads as large as 65,535 bytes. IPv6 supports fragmentation to transport large packets over limited links. If larger packets have to be sent than the link

has the capability to carry, the link may use the Fragment header (8 bytes) to split up the packet. This packet will be reassembled at the destination.

Another option defined by the Hop by Hop Header is the Jumbo Payload option, which can be used if packets have to be larger than 65,535 bytes

Next Header

8 bit field. Identifies the type of header which follows immediately the IPv6 header. For example, this can be a TCP, Routing or Fragmentation header and the combinations of them. With the exception of the Hop by Hop header, which carries optional information about the packet, the entry in this header is not processed by the intermediate nodes along the path.

Hop Limits

8 bit field. Decrement by one by every node that processes the packet. If the Hop Limit is zero, the packet is discarded.

Source Address

128 bit address of the packet sender.

Destination Address

128 bit address of the recipient. If a Routing Header is present, the Destination Address is not the ultimate recipient.

3.2 Addressing

IPv6 has three type of addresses:

unicast *identify a single interface*

anycast *identify a set of interfaces. Packet will be delivered to one member of the set*

multicast *identify a group of interfaces. Packet will be delivered to all interfaces in group*

To avoid the experience that an exponentially growing Internet has had with IPv4 - that is, a 32 bit address results in routing problems and an inadequate amount of addresses - IPv6 has a 128 bit address field. To verify if this number of addresses is large enough, I made a calculation referring to the surface of the earth [7]. IPv6 can in theory address 2^{128} interfaces or set of interfaces. In the practical implementation, this number will be much smaller as an appropriate addressing scheme will be used. an example of such a scheme could be (the actual address scheme is not yet defined):

<provider><organization ><network><interface>

Therefore, the usable addressing space will be significantly smaller than 2^{128} . Huitema [8] concluded that IPv6 addresses could address between $8 \cdot 10^{17}$ and $2 \cdot 10^{33}$ nodes. Using the lowest estimation, 1,564 addresses would be available for every square meter of the planet Earth's surface (assuming that the surface of the earth is 511,263,971,197,990 square meters). This should provide enough addresses into the more distant future when in addition to computers TV sets, maybe even toasters will be addressable.

3.3 Routing

Routing of IPv6 does not differ much from IPv4 routing except that the addresses are 128 bit long. Therefore all of IPv4's routing algorithms will work with IPv6. IPv6 also includes routing extensions which support powerful new routing possibilities. This includes [7]:

- Provider Selection based on policy, performance etc
- Host mobility (routing to current location)
- Auto Readdressing (route to new address)

The Routing header (defined in the "Next Header" field) is used to list one or more intermediate nodes, where the packet has to follow the link. This function is very similar to the Source Route in IPv4.

3.4 Security

This section gives a brief description of IPv6 security. IPv6 security will be addressed more specifically in the section in which I compare it to SSL. IPv6 Authentication and Encapsulating can be used separately or in combination.

3.4.1 IPv6 Authentication Header

The Authentication Header is a mechanism which provides authentication and integrity. This does not include confidentiality, as the IPv6 datagrams are not encrypted. IPv6 does support many different authentication techniques and algorithms. The keyed MD5 algorithm is the proposed standard to help prevent compatibility problems within the Internet. This mechanism helps to eliminate a large amount of network attacks such as IP spoofing or host masquerade. As IP is located at the Internet layer, it helps to provide host authentication (origin authentication). Although the export restrictions of the US are out of the topic of this paper, authentication should be exportable because it only provides authentication and integrity, not confidentiality.

3.4.2 IPv6 Encapsulating Security Header

The second security extension Header, the IPv6 Encapsulation Security Header, provides integrity and confidentiality to IPv6 datagrams. Like the authentication, the Encapsulating Security Header is also cipher independent. To get interoperability within the Internet, the DES CBC algorithm is being used as the standard algorithm. The ESP uses Tunnel mode where the whole IP packet is encrypted and a new unencrypted IP header is allocated; and Transport mode where only the payload is encrypted as options.

3.5 Transition

IPv6 is designed so that IPv6 and IPv4 hosts and router can interoperate. The goal is to make the transition of the Internet to IPv6 with as little disruption as possible. The IPv6 transition mechanisms provide the following features [7]:

- Incremental upgrade and deployment. New IPv6 hosts and routers can be installed (or upgraded) one by one
- Minimal upgrade dependencies. The only prerequisite is that the DNS (Default Name Server) is upgraded first.
- Easy addressing. When hosts or routers are upgraded from IPv4 to IPv6, the existing addressing plan does not need to be changed. The host or router may continue to use the existing address.
- Low start up cost. Little or no preparation work is needed to upgrade existing systems to IPv6. Mechanisms used by the IPv6 transition mechanisms are:
 - ◆ IPv6 addressing structure embeds IPv4 addresses and encodes other information used by the transition mechanisms.
 - ◆ Technique of encapsulating IPv6 packets within IPv4 headers to carry the packets over segments where the routers have not yet been upgraded to IPv6.
 - ◆ Header translation technique allows the eventual introduction of routing topologies that route only IPv6 traffic.

These mechanisms guaranty that IPv6 hosts and routers can interoperate with IPv4 hosts and routers anywhere until the time when IPv6 is installed in all places.

I believe that the transition time for the Internet will be very short as we are running out of address space with the IPv4 protocol. The most likely topology will be that the local area networks (LANs) will use IPv4 until they are upgraded host by host. The DNS and the router which connects the LAN to the Internet will be upgraded as soon as the appropriate IPv6 protocol is ready to use. This would be the easiest way to get the advantages of IPv6 in the Internet environment quickly and to provide the local network management enough time to upgrade their network.

4 IP Security in comparison to SSL

In this chapter, I compare the security specifications of IPv6 versus SSL (Secure Sockets Layer). When using SSL, I am referring to SSL Version 3 (Internet Draft March 1996). I do not compare IPv6 to the implemented version of SSL V2 in Netscape, as SSL can be used in general by different applications and not only by Netscapes Web browser.

4.1 Architecture

While IPv6 is located at the Network Layer, SSL is a Transport layer protocol. With this, a major difference appears. IPv6 handles everything above the network layer equally. In other words, IPv6 has no notion of the transport protocol (TCP, UDP) or their port numbers. It can also work with non transport protocols like ICMP. All the packets are handled similarly and therefore are authenticated or encrypted without regard to what they contain.

SSL is a session layer protocol, that works with reliable transport protocols only (such as TCP). SSL has a specific port number assigned that is dependent on the application protocol where SSL is located in the next lower layer. Until now, there are three port numbers assigned by the IANA (The Internet Numbers Authority) and therefore can be used with SSL. These are:

- HTTP
- NNTP
- SMTP

Principally, SSL doesn't need to have separate ports allocation. If the existing protocol supports some form of negotiation, then you can add SSL negotiation into that protocol. However, this is not a standard but is used in a few applications based on the free SSL version.

With its location on a lower layer, IPv6 provides more security as all information from the layers above are encrypted. Therefore information such as port numbers are not available to traffic analysis attempts and provide some more security.

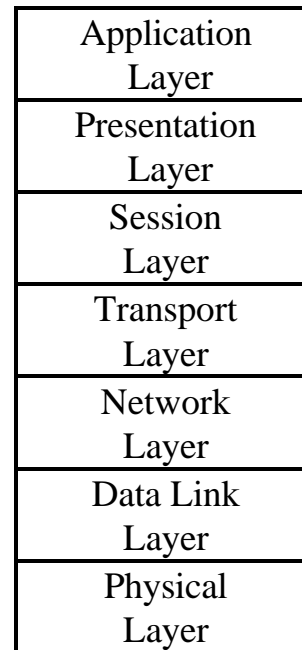


Figure 1:
OSI Layer
Architecture

4.2 Typical use

Both mechanisms (IPv6 and SSL) do roughly the same thing from a user standpoint. Both provide data confidentiality and authentication. From the network point of view, IPv6 can be used in three different ways, while SSL only provides security from Host-to-Host.

The three cases where the security features of IPv6 can be used are:

- Host to Host
- Host to Subnet
- Subnet to Subnet

In all three cases, encryption, authentication or the combination of both can be used. This makes it possible that not only encryption between two hosts can be used but that inside a corporation network, the traffic can go unencrypted (and therefore with less delay and computation resources used) and that the router encrypts all traffic at IP level at the point where the traffic leaves the local network and goes over the Internet (Subnet to Subnet).

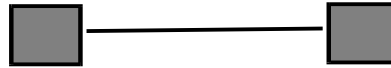


Figure 2:
Host to Host

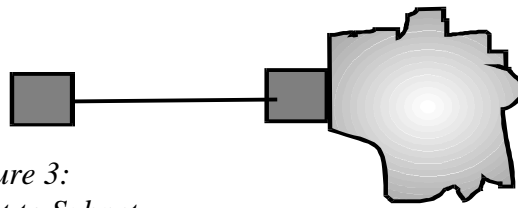


Figure 3:
Host to Subnet

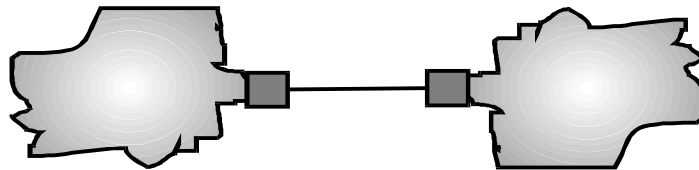


Figure 4:
Subnet to Subnet

In my point of view, this is the most likely case in which the security mechanisms of IPv6 will be used. This demands that the network is designed properly and clear gateways to the "outside world" are defined. In addition to this, both sides must support the same version of IP (v4 or v6).

SSL provides only the possibility of confidentiality and authenticity between two hosts or typically between a host and a server. A Host to Subnet or Subnet to Subnet application is not reasonable as SSL provides its features only for defined ports and therefore not for all protocols as described in the last section.

4.3 Key exchange

Despite the lack of a key exchange mechanism for IPv6 until now, all the keys have to be distributed manually. In large networks, this can be an almost impossible task. However, there will be developed protocol and cryptographic techniques that will support the key management requirements of IPv6. The Internet Key Management Protocol (IKMP) will be specified as an application layer protocol. It will be independent of the security protocol of the layers below it. It will support public key based techniques and eventual support of Key Distribution Centers such as

used by Kerberos. However, the IKMP should be submitted by March 1997 to IESG for consideration as a Draft Standard.

SSL has built in key exchange capabilities. It supports Server key exchange messages as well as Client key exchange messages. It is able to provide a (presumably) secure communication where the server does not have to have knowledge a priori of the clients public key. The client can have a limited set of server public keys which are trusted by the client (approved by an authority). After the request to make a secure connection, the client encrypts its public key with the use of the servers public key. The server decrypts the client's public key by using his own private key. From this point, the secure connection by using both keys can be established. This mechanism has the limitation that the Server cannot authenticate the Clients identity as it gets the Clients public key without being able to identify it. The Client on the other hand can be sure about the Servers identity as the Server can only decrypt the Clients public key if it has his own private key corresponding to the trusted public key used by the client.

With this capability of key exchange, SSL can be used for spontaneous secure communications between a Server and a Client. This case is often used in potential secure WWW Internet connections where passwords or credit card numbers have to cross the Internet.

4.4 Used Ciphers

IPv6 as well as SSLv3 are cipher independent. This has the advantage that while ciphers are changing and cipher attacks get more successful for small keylength, the protocol can be set up to use another, more sophisticated encryption algorithm. However, both protocols have defined algorithms. These are:

IPv6	
Authentication	Hash size byte
Keyed MD5	16
Encryption	Key Bits
DES CBC	56

SSL	
	Hash size byte
MD 5	16
SHA	20
Encryption	Key Bits
Fortezza	96
IDEA CBC	128
RC2 CBC 40	40
RC4 40	40
RC4 128	128
DES40 CBC	40
DES CBC	56
3DES EDE CBD	168

Both protocols have as default DES CBC with a 56 bit key (SSL in the US version according to the actual export restrictions). IPv6 chose the DES CBC cipher mainly for compatibility reasons. They also realized that this cipher is potentially weak and vulnerable to attacks. Weiner has shown that it's possible to design a DES cracking computer that can crack one key every 3.5 hours by spending \$1 million for this computer. In the mean time, the price for a similar computer is

decreasing rapidly and therefore DES CBC does not really provide confidentiality on a strong basis.

In my opinion, IPv6 should not choose DES CBC as a default as at the time the protocol will be used, the cipher will not provide much more confidentiality as sending plaintext. Instead of DES CBC, triple DES (3DES) should be chosen, as this cipher offers significantly more confidentiality and should be able to resist attacks in the near future.

4.5 Authentication

Both protocols rely on basically the same default authentication algorithm. While SSL uses MD5, IPv6 has proposed keyed MD5. Both algorithms have a 128 bit has length. Although basically the same algorithms are used, the authentication of IPv6 is more resistible to attack who can find two chosen texts with a common MD5 hash value [7].

The main difference between the two authentication possibilities lies on the different levels on which they work. As SSL works on the transport layer, it can only authenticate these packets. IPv6 is located on the network layer and therefore its authentication is much more valuable. This can be used to eliminate a significant amount of network attacks. This includes host masquerading and IP spoofing techniques which have gained more importance in the last months. IPv6 authentication provides authentication to the source and destination address as well as to the upper layer protocols, while SSL is only capable to provide authentication to the transport layer and above.

4.6 Encryption

As both protocols use the same possible encryption algorithms, I focus on the accordingly to the layer where the protocols are defined. While SSL only has the option to encrypt the whole (HTTP, NNTP or SMTP) packet on it's layer, IPv6 has two possibilities to provide confidentiality.

Tunnel mode ESP (Encapsulating Security Payload)

In this mode, the original IP datagram (including header) is encrypted. This entire ESP frame is placed within a new datagram having an unencrypted IP header. All additional unencrypted information as routing header are placed between the IP header and the encapsulated security payload. The receiver strips off the cleartext IP header and decrypts the ESP.

Transport mode ESP (Encapsulating Security Payload)

In this mode, only the payload is encrypted. The IP header and the IP options are unencrypted and are used for routing the packet. The receiver decrypts the ESP and uses the unencrypted header as IP header further if necessary.

The transport mode ESP provides approximately the same capabilities as the SSL protocol except that it provides its services to all packets and not only to defined port addresses like SSL.

The tunnel mode ESP can be used that in the LAN, all traffic goes unencrypted and the gateway to the Internet (IPv6 capable router) encrypts the IP packets using the tunnel mode to route the

packets to the gateway of the next corporate LAN. This capability makes it possible that the original source and destination address is not readable for someone who tries to get information on the content of the packets or makes attempts at traffic analysis. The original source and destination address (including all other IP header information) are encrypted and this datagram is encapsulated by a new IPv6 header which contains the source and destination address of the two routers. The router at the destination LAN strips off the unencrypted IPv6 header and decrypts the packet. The header of the decrypted packet is then used to route the packet to the recipient.

4.7 Traffic Analysis

Neither SSL or IPv6 does provide any possibility to prevent traffic analysis. However, I had the idea to use the Routing Header in IPv6 to prevent from a large amount of traffic analysis attacks.

I believe that the Routing Header information could be set up so that the list of intermediate nodes changes when the system setting provide a list of alternative routing paths. An error condition could arise similar to the definition in the fragmentation header, if not all packets are received to complete reassembly of the message within 60 seconds (a long time but I think this is a reasonable waiting for users concerned about traffic analysis).

This would prevent (or at least make the attempt more difficult) Traffic analysis in the case that not only one routing path between the two hosts exists. I could imagine that this would be used from one corporation router to the other if the links in between are using the Internet.

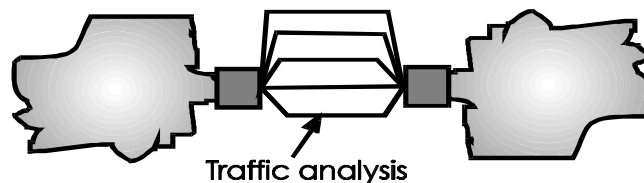
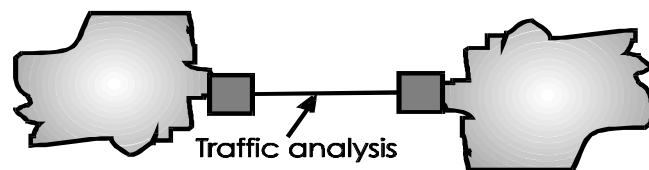


Figure 5:
Alternative routing path to make traffic analysis more difficult.

I proposed this to the IPsec working group but did not receive an enthusiastic reaction. The fact that a lot of attacks cannot be defended at the IP layer seems to make it reasonable enough not to implement some mechanisms at this layer. At IP layer the intermediate routers must be able to look at the packet header to route the packets. Therefore the source and destination address must be cleartext and is available for traffic analysis which is also true for the packet size. A more successful implementation would be at the link layer, as one can encrypt all the bits (including addresses). Therefore no information would be available for traffic analysis, particularly if a stream cipher would be used that keeps the link occupied although no "real" information is transmitted.

5 Conclusions

The security specifications are clear enough to conclude that the IPv6 protocol has enough security capabilities to provide better authentication and confidentiality than SSL in general. This is based mainly on the fact that IPv6 is located at the Network layer while SSL is placed at the Transport layer. Therefore, IP can provide its services to all information (packets) above the Network Layer while SSL's standard provides only authentication and confidentiality to protocols using defined port numbers. Therefore IPv6 is universally usable without being limited to the type of payload.

One of the most important mechanisms, the key exchange, is still not defined for the IPv6 protocol. It is vital that this will be an universal standard and will probably be located at the application level, so that it can provide key exchange services to all layers below. However, as long as no such mechanism exists, IPv6 security can be used only on a very limited basis as manual key exchange is not realistic in large networks and particularly not on the Internet.

While IPv6 has its advantages in all discussed fields over SSL (except key exchange which is not yet defined for IPv6), SSL will have, at least in the near future, still its place in a world where everyone runs IPv6 with its security features enabled. I see the most plausible place for SSL to be in spontaneous Internet transactions (like encrypted credit card numbers) as a probably secure transmission can be made without prior knowledge of the private key of the client. Therefore, SSL will still have its applications in Web browsers.

In general, every security specification is only as secure as its implementation in the final product. While Netscape uses its SSL version 2 in the Netscape Navigator browser, IPv6 is implemented only by multiple organizations in research projects. Therefore, I cannot make any predictions about the IPv6 implementations and their security but it is quite possible that IPv6 will have security holes in the implementation like SSL had (and still has) in its implementation in Netscape.

The reader should keep in his mind that IPv6 offers a high standard for probably secure transmissions over network but no protocol or application can guarantee a 100% secure way for transmitting information over networks.

6 References

- [1] R. Atkinson, Security Architecture for the Internet Protocol , RFC 1825 , August 1995.
- [2] R. Atkinson, IP Authentication Header , RFC 1826 , August 1995.
- [3] R. Atkinson, IP Encapsulating Security Payload (ESP) , RFC 1827 , August 1995.
- [4] S. Bradner, A. Mankin, The Recommendation for the IP Next Generation Protocol, RFC 1752, January 1995
- [5] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 1883, December 1995
- [6] A. Freier P. Karlton P. Kocher, The SSL Protocol Version 3.0, Internet Draft, Netscape Communications Corporation, 03/04/96
- [7] Robert M. Hinden, IP Next Generation Overview,
<http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html>, May 14 1995
- [8] C. Huitema, The H Ratio for Address Assignment Efficiency, RFC 1715, November 1994
- [9] P. Karn, P. Metzger, W. Simpson, The ESP DES-CBC Transform , RFC 1829 , August 1995.
- [10] P. Metzger, W. Simpson, IP Authentication using Keyed MD5 , RFC 1828, August 1995.
- [11] Adam Shostack, An Overview of SSL, May 1995
<http://www.homeport.org/~adam/ssl.html>
- [12] M.J. Wiener, Efficient DES Key Search, Carleton University, Ottawa, August 20 1993,
http://www.cert-kr.or.kr/doc/des_key_search.ps.asc.html