2007-11-24

SECURITY ISSUES OF THE INTERNET

Sobhan, M. Abdus

Daffodil International University

http://hdl.handle.net/20.500.11948/751

Downloaded from http://dspace.library.daffodilvarsity.edu.bd, Copyright Daffodil International University Library
SECURITY ISSUES OF THE INTERNET

M. Abdus Sobhan  
School of Engineering and Computer Science  
Independent University of Bangladesh (IUB), Dhaka  
E-mail: asobhan@secs.iub.edu.bd

Abstract: This paper presents an overview of the security issues of the Internet. It reviews the security issues and challenges of both the IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) protocol stacks, currently in use. The weaknesses giving birth of the security challenges are mentioned. Security improvements of the Internet use in the newly defined IPv6 are discussed. Security issues arising of the IPv4-IPv6 dual stack protocols are also included in the discussion. Some security-related functionality of the new IPv6 protocols are reviewed. It is seen that the security of the Internet is not a current concern only; it existed before, and will continue to exist in the future. As we know, nowadays, security requirements have become more critical because, small, medium and big enterprises all are using the Internet and the Internet-like infrastructure for their day-to-day businesses. As business incurs money involving profit and loss, so we may say that a continuous war will be on between the Internet-based system managers and the rivals including malicious attackers. It is recommended that the network/system administrators should remain aware of the new flaws using the Internet and immediately get the patches to keep the system secure. Incidentally, our discussion is confined to the technical aspects of security issues of the Internet. The challenges to the financial, social and ethical aspects of the Internet security could not be included due to limitation of paper size.

Keywords: Security Issues, Internet, IPv4, IPv6, IPsec, Authentication, Mobility

1. Introduction

The IPv4 is the de facto standard for Internet connectivity. With IPv4, there have been a variety of misuses and exploits on end and intermediate systems due to protocol design as well as implementation problems resulting in substantial loss of revenues. As a consequence, IPv4 has been supplemented by the IPsec (Secure Internet Protocol) protocols to provide for security needs at the network layer. In the IPv6 [1], the IPsec is made a part of its basic design. The IPsec helps serve the data privacy and integrity needs of the data in transit across the Internet in addition to providing authenticity of the data’s origin. The network security definitions of the International Telecommunications Union (ITU) [2]) have the following requirements:

- **Privacy:** (the protection of the association of the identity of users and the activities performed by them);
- **Data confidentiality:** (the protection against unauthorized access to data contents);
- **Authentication:** (proof that the claimed identity of an entity is true);
- **Integrity:** (that data have not been altered in an unauthorized manner); and
- **Availability:** (no denial of authorized access).

In the network layer, the IPsec provides the first four of the above requirements. As IPsec is embedded in IPv6, therefore it is compatible with the ITU definition. In the rest of the paper, we attempt to describe some security issues of the Internet.

Organization of the paper is as follows: A general introduction is furnished in the present section one. Challenges to Internet security are covered in section two. A brief overview of the security issues of IPv4 is furnished in section three. An overview of IPv6 is provided in section four followed by section five dealing with the improvements of Internet security in IPv6. Some important security-related features of IPv6 appear in section six. The conclusion is drawn in section seven.

2. Challenges to Internet Security

As Internet-based communications gain an ever-increasing foothold in our lives, the need for security has become paramount. The field of security includes concepts of authentication, confidentiality, integrity, availability, access control and non-repudiation. These security requirements are critical for enterprises which use the Internet or Internet-like infrastructure for their day-to-day business. In the Internet, users may enjoy a high level of anonymity if desired. To an
evil Internet user wishing to breach the security, have, then to exploit the following weak points:
- The standards used for basic Internet protocols are public, thus attackers know much more about how the Internet works than they would if a closed network were used.
- The level of technical sophistication required to carry out attacks is falling [3].
- Modern systems are very complex and operate at several layers. Complexity of modern systems makes comprehensive testing an extremely difficult problem, and thus production systems almost inevitably have flaws.
- The Internet development speed is huge, as result much of the software is developed only with its main functionality in mind, with less thought being given to the security aspects. IPv4 was not designed with security in mind.
- The code mobility provides opportunities for the development of viruses and worms. These are autonomous agents that, once released, can reproduce. The resulting combinatorial explosion allows the attacker’s wishes to be carried out on a very large scale.

These attacks manifest themselves as identity impersonation (referred to as spoofing), loss of privacy, loss of data integrity (e.g. credit card transaction details being modified in transit), communications monitoring, and denial-of-service. Such attacks are the result of discovering exploits that emerge from the flaws in the basic protocol design.

Defenses available to Internet-based systems managers include:
- the strict enforcement of a comprehensive security policy,
- avoidance of insecure technologies and protocols wherever possible,
- use of the best available and most secure technologies, and to
- keep up-to-date with events in the world of security, especially in order to patch systems when a new exploit is discovered.

Just as attackers quickly share information about new flaws using the Internet, system administrators can be warned almost immediately and patches disseminated quickly.

3. IPv4 Security Issues

In the present section, we discuss some of the limitations of IPv4’s security issues. During the IPv4 development, it was assumed that the security should be provided by the end nodes [4]. As for example, if an application such as e-mail requires encryption services, it should be the responsibility at the end nodes to provide such services. Today, the original Internet continues to be completely transparent and no security framework provides for resilient against threats such as:

- **Denial of service attacks (DOS):** in this kind of attack certain services are flooded with a large amount of illegitimate requests that render the targeted system unreachable by legitimate users. An example of DOS attack that results from an architectural vulnerability of IPv4 is the broadcast flooding attack or Smurf attack [5]
- **Malicious code distribution:** viruses and worms can use compromised hosts to infect remote systems. IPv4’s small address space can facilitate malicious code distribution [5].
- **Man-in-the-middle attacks:** IPv4’s lack of proper authentication mechanisms may facilitate men-in-the-middle attacks. Additionally, ARP poisoning (see below) and ICMP redirects can also be used to perpetrate this type of attacks [5] [6].
- **Fragmentation attacks:** this type of attacks exploits the way certain operating systems handle large IPv4 packets. An example of this type of attack is the ping of death attack. In a ping of death attack the target system is flooded with fragmented ICMP ping packets. With each fragment, the size of the reassembled ping packet grows beyond the packet size limit of IPv4 - therefore, crashing the target system [5].
- **Port scanning and other reconnaissance attacks:** in this type of attacks a whole section of a network is scanned to find potential targets with open services. Unfortunately, IPv4’s address space is so small that scanning a whole class C network can take a little more than 4 minutes [7].
- **ARP poisoning and ICMP redirect:** in IPv4 networks, the Address Resolution Protocol (ARP) is responsible for mapping a host’s IP address with its physical or MAC address. This information is stored by each host in a special memory location known as the ARP table. Each time a connection with an unknown host is needed, an ARP request is sent out on the network. Then, either the unknown host responds broadcasting its own IP address or a router does it with the appropriate information. ARP poisoning occurs when forged ARP responses are broadcasted with incorrect mapping.
information that could force packets to be sent to the wrong destination. A similar approach is used by ICMP redirect attacks [5]. However, many techniques have been developed to overcome some of the IPv4 security limitations. For instance, although Network Address Translation (NAT) and Network Address Port Translation (NAPT) were introduced to facilitate the re-use and preservation of a rapidly depleting IPv4 address space, these techniques can provide also for certain level of protection against some of the aforementioned threats [8]. Also, the introduction of IPsec facilitated the use of encryption-based communication, although its implementation is optional and continues to be the sole responsibility of the end nodes. Before, we attempt to discuss the security features of IPv6, let the reader have brief overview of IPv6 protocol as presented in the next section.

4. An Overview of IPv6
IPv6 is the new suite of protocols having a good number of features [9-10]. The following are some of its features.

a. **Wider bit-range and larger address space:** IPv6 is 128-bit wide addressing scheme whereas IPv6 is only 32-bit wide. IPv4 address space is $2^{32}$ whereas that of IPv6 is $2^{128}$, i.e. IPv6 provides $2^{96}$ times larger IP addresses in total. To have a feeling of the largeness of IPv6, it is seen that IPv4 has 4,294,967,296 numbers of addresses whereas that for IPv6 is $3.4028236692093846346337460743177 \times 10^{38}$.

b. **Addressing hierarchy:** In IPv6 there are three major types of addresses: unicast, multicast, and anycast addresses. Unicast addresses are assigned to a single IPv6 node. Multicast addresses are assigned to multiples nodes within a single multicast group. Packets sent to a multicast address must be delivered to all members of the same multicast group. On the other hand, anycast addresses are assigned to groups of nodes, which do not have to be delivered packets to all its group members - it is sufficient that one node receives the packets. IPv6 has the routing infrastructure that provides more efficient and smaller routing tables.

c. **Stateless and stateful address configuration:** IPv6 allows hosts to acquire IP addresses either in a stateless or autonomous way or through a controlled mechanism such as DHCPv6.

d. **Quality of service (QoS):** the IPv6 packet header contains fields that facilitate support for QoS for both differentiated (DiffServ) and integrated (IntServ) services.

e. **Better performance:** IPv6 provides for significant improvements such as better handling of packet fragmentation, hierarchical addressing, and provisions for header chaining that reduce routing table size and processing time.

f. **Built-in security:** Although IPsec is also available for IPv4 implementations, it is not mandated but optional. Support for IPsec is embedded in IPv6 implementations.

g. **Extensibility:** Although an IPv6 address is four times larger than an IPv4 address in bit-length, the new IPv6 header is just twice the size of the IPv4 header (i.e. IPv4’s header size is 20 bytes and that of IPv6 is 40 bytes). IPv6 header does not include any optional fields, also does not include a checksum either. Optional fields can be added as extension headers up to the size of the IPv6 packet. This feature does not only provide for better extensibility but also for reducing the time a router process IPv6 header options, increasing the network overall performance.

h. **Mobility:** IPv6 provides mechanisms that allow mobile nodes to change their locations and addresses without loosing the existing connections through which those nodes are communicating. This service is supported at the Internet level and therefore is fully transparent to upper-layer protocols. IPv6 has many other interesting features, but we discuss in the following section the important and pressing security issues only.

5. Security Improvements in IPv6
As noticed in [10], we may say that IPv6 is not necessarily more secure than IPv4. In fact, IPv6 approach to security is marginally better than IPv4 but not radically new [11]. Port scanning is one of the best known reconnaissance techniques used by the “black-hats”. Port scanning allows them to listen to specific services (ports) that could be associated to well-known vulnerabilities [12]. Most IPv4 segments are Class C, with 8 bits allocated for host addressing. Thus, in IPv4 networks, port scanning is a relatively simple task. Scanning a typical IPv4 subnet, at a rate of one host per second, translates into:

$$2^4 \text{ hosts} \times \frac{1 \text{ second}}{1 \text{ host}} \times \frac{1 \text{ minute}}{60 \text{ seconds}} = 4.267 \text{ minutes}$$

In IPv6 networks, the landscape is radically different. IPv6 subnets use 64 bits for allocating...
host addresses. Consequently, a typical IPv6 subnet requires:
\[
\int \frac{2^{32}}{1 \text{ host}} \times \frac{1 \text{ second}}{31,556,000 \text{ seconds}} = 584,942,417,355 \text{ years}
\]
Thus, scanning such a large address space is almost an impossible task [10]. However, it is not absolutely impossible [4]. The important security features of IPv6 are discussed in the following sections.

5.1 IPsec
As mentioned above, IPv4 also offers IPsec support. However, IPv4’s support for IPsec is optional. By contrast, the RFC4301 mandates for IPv6 to use IPsec in all nodes [10, 13].

IPsec consists of a set of cryptographic protocols that provide for securing data communication and key exchange. IPsec uses two wire-level protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). The first protocol provides for authentication and data integrity. The second protocol provides for authentication, data integrity, and confidentiality [13]. In IPv6 networks both the AH header and the ESP header are defined as extension headers. Additionally, IPsec provides for a third suite of protocols for protocol negotiation and key exchange management known as the Internet Key Exchange (IKE). This protocol suite provides the initial functionality needed to establish and negotiating security parameters between endpoints. Additionally, it keeps track of this information to guarantee that communication continues to be secure up to the end.

5.1.1 Authentication Header
The authentication header prevents IP packets from being tampered or altered. In a typical IPv4 packet, the AH is part of the payload [14-15]. There was a question about the integration of AH protocol in to the IPv6 protocol format during its implementation time. The problem was that IPv6 extension headers can change in transit as information they contain is updated through the network. To solve this problem, IPv6 AH was designed with flexibility in mind - the protocol authenticates and do integrity check only on those fields in the IPv6 packet header that do not change in transit. Also, in IPv6 packets, the AH is intelligently located at the end of the header chain - but ahead of any ESP extension header or any higher level protocol such as TCP/UDP [9].

The AH header protocol also provides optional protection against replay attacks. The protocol uses its sequence number field as part of a sliding window mechanism that prevents arbitrary packet delays and malicious replay [9, 15].

5.1.2 Encapsulating Security Payload
In addition to providing the same functionality the AH protocol provides - authentication, data integrity, and replay protection - ESP also provides confidentiality. In the ESP extension header, the security parameter index (SPI) field identifies what group of security parameters the sender is using to secure communication. ESP supports any number of encryption mechanisms. However, the protocol specifies DES-CBC as its default. Also, ESP does not provide the same level of authentication available with AH. While AH authenticates the whole IP header (in fact, only those fields that do not change in transit), ESP authenticates only the information that follows it [9].

ESP provides data integrity by implementing an integrity check value (ICV) that is part of the ESP header trailer - the authentication field. The ICV is computed once any encryption is complete and it includes the whole ESP header/trailer - except for the authentication field. The ICV uses hash message authentication code (HMAC) with SHA-1 and MD5 as the recommended cryptographic hash functions [15].

5.1.3 Transport and tunnel modes
In IPv4 networks, IPsec provides two modes of securing traffic. The first one is called transport mode and it is intended to provide secure communication between endpoints by securing only the packet’s payload. The second one is called tunnel mode and it is intended to protect the entire IPv4 packet. However, in IPv6 networks, there is no need for a tunnel mode because, as mentioned above, both the AH and ESP protocols provide enough functionality to secure IPv6 traffic [10].

5.1.4 Protocol negotiation and key exchange management
In addition to AH and ESP, IPsec also specifies additional functionality for protocol negotiation and key exchange management [9]. IPsec encryption capabilities depend on the ability to negotiate and exchange encryption keys between parties. To accomplish this task, IPsec specifies an Internet key exchange (IKE) protocol. IKE provides the following functionality:
- Negotiating with other people the protocols, encryption algorithms, and keys, to use.
- Exchanging keys easily with changing them often.
- Keeping track of all these agreements.
To keep track of all protocol and encryption algorithm agreements, IPsec uses the SPI field in both the AH and ESP headers. This field is an arbitrary 32-bit number that represents a security association (SA). When communication is negotiated, the receiver node assigns an available SPI which is not in use, and preferably one that has not been used in a while. It then communicates this SPI to its communication partner establishing a security association. From then until that SA expires, whenever a node wishes to communicate with the other using the same SA, it must use the same SPI to specify it. The other node, on receipt, would look at the SPI to determine which SA it needs to use. Then it authenticates and/or decrypts the packet according to the rules of that SA, using the agreed-upon keys and algorithms the SA specifies. The node then uses the same same information to verify that the data has not been modified as well as that no one between the two nodes has read the exchanged data.

Both nodes must negotiate a set of keys, before all this happens. The keys will be used to guarantee that the SA parameters are securely exchanged. IPsec allows for using both automatic and manual key exchange. However, because manual exchange does not scale well, IPsec recommends using IKE. IPsec IKE offers a robust mechanism to authenticate communication parties based on a public key infrastructure (PKI). Encryption keys are generated with a Diffie-Hellman algorithm based on each node’s public and private key pairs. This mechanism offers perfect forward secrecy (generating keys that are not reliant on previously generated key values) as well as reasonable scalability.


From a security point of view, the new IPv6 protocol stack shows a significant advance in relation to the old IPv4 stack. However, despite its innumerable virtues, IPv6 still continues to be by far vulnerable. In this section, we review some of the areas of IPv6 where security continues to be an important issue.

6.1 Dual-stack Related Issues

Presently, the Internet continues to be mostly IPv4-based. However, it is reasonable to expect that this scenario will change soon as more and more networks are migrated to the new protocol stack. Unfortunately, migrating millions of networks is going to take quite some time. In the meantime, some form of 6to4 dual-stack will supply the desired functionality [9]. Without a doubt, IPv6-IPv4 dual stacks increase the potential for security vulnerabilities - as a consequence of having two infrastructures with specific security problems. However, most of the issues are not a direct result of specific IPv6 design flaws but mostly a result of inappropriate or careless configuration [16].

6.2 Header Manipulation Issues

The use of extension headers and IPsec can deter some common sources of attack based on header manipulation. However, the fact that EH must be processed by all stacks can be a source of trouble - a long chain of EH or some considerably large-size could be used to overwhelm certain nodes (e.g., firewalls) or masquerade an attack. Best practice recommend is to filter out traffic with unsupported services [10]. Spoofing continues to be a possibility in IPv6 networks [11]. However, because of ND, spoofing is only possible by nodes on the same network segment. The same does not apply to 6to4 transition networks. Although one approach to 6to4 transition is using some form of dual-stack functionality, another approach is using some type of tunneling. Because tunneling requires that a protocol is encapsulated in another, its use could be
a source of security problems such as address spoofing - in this case if the spoofed address is used to masquerade an external packet as one that was originated from the inside network [11].

6.3 Mobility

Mobility is a totally new feature of IPv6 that was not available in its predecessor. Mobility is a very complex function that raises a considerable amount of concern when considering security. Mobility uses two types of addresses, the real address and the mobile address. The first is a typical IPv6 address contained in an extension header. The second is a temporary address contained in the IP header. Because of the characteristics of this networks (something more complicated if we consider wireless mobility), the temporary component of a mobile node address could be exposed to spoofing attacks on the home agent. Mobility requires special security measures and network administrators must be fully aware of them [10-11, 18].

6.4 Flooding Issues

Scanning for valid host addresses and services is considerably more difficult in IPv6 networks than it is in IPv4 networks. As mentioned earlier, to effectively scan a whole IPv6 segment may take up to 580 billion years - because the address space uses 64 bits. However, the larger address space does not mean that IPv6 is totally invulnerable to this type of attack. New features such as multicast addresses continue to be source of problems [17]. Smurf-type attacks are still possible on multicast traffic. Again, filtering out unnecessary traffic is the recommended best practice [10].

7. Conclusion

The Internet security has become a critical issue because; nowadays small, medium and big enterprises all are using the Internet and the Internet-like infrastructure for their day-to-day businesses. Security loop-holes in the IPv4 were improved by incorporating IPsec. But its implementation responsibility remains fully with the end nodes. The IPv6 protocol has the embedded IPsec. It provides a considerable improvement of security compared to that of IPv4. The IPv6 provides innumerable features improving both the overall functionality as well as specific-security functions. Although IPv6 offers better security (larger address space and the use of encrypted communication), the protocol also raises new security challenges. Thus we see that new protocol creates as many new security problems as it solves old ones. And the transition from the old to the new protocol stack may present even more challenges. Especially, the Internet attackers have a better expertise in the new protocol stack domain. Thus, it will be a continuous war between the Internet-based system managers and the rivals as well as the malicious attackers.

References