Paper

The tactical Intranet IPSec security concept

Mariusz Bednarczyk, Jacek Jarmakiewicz, and Jarosław Krygier

Abstract — The IPSec protocols architecture that can be applied in tactical Intranet based on the IPv6 protocol stack for wireless environment is the subject of the paper. The potential usefulness of the new version of IP protocol is very important for tactical communication systems. Additionally, Internet Engineering Task Force (IETF) security working group proposes recommendations covering the RFC 2401, 2402, 2406, that describe the security architecture for Internet Protocol. These standards, published by IETF are discussed here in military requirements context. The NATO C3 Technical Architecture model also recommends these issues. The concept of the IPSec architecture in military systems is described in the paper. The position of the security applications designed for subscriber devices with reference to layered model is also presented. The concept presented here is defined for the tactical level.

Keywords — IPSec, tactical Intranet, IP security.

1. Introduction

The modern Armed Forces need modern solutions, especially in the area of communication systems. For example, local area networks (LAN) have became just essential part of contemporary military units (command posts). Along with commercial of the shelf products (COTS) application, their security have became very important factor that have to be taken into account. The new standard covering the IPv6 protocol, that is still tested, includes mechanisms suitable for military systems. It is associated with security mechanisms (authentication, privacy and payload encryption) and mobile subscribers access to services and network resources as well as with the high quality of services requirements [6, 7].

The IPv6 have been designing as an evolution from IPv4 rather than as a major change. Useful features of IPv4 were carried over in IPv6 and less useful features were dropped. According to the IPv6 specification, the changes from IPv4 to IPv6 can be split primarily into the following categories [4]:

- **Inherent security support**. The IPv6 enables and enforces the IPSec authentication and encryption features through the extension headers. If authentication header (AH) is carried with the IP datagram, the receiving host must check the packet validity.
- **Mobility support**. The IPv6 protocol supports mobility management as an inherent function of IPv6 compared to the IPv4 that supports mobility through an additional protocol added on a top of IPv4 [5].
- **Built-in route optimization**. In IPv6 the correspondent node (CN) can learn so-called care-of-address (COA) of the mobile node (MN). The route optimization helps to prevent a problem of triangle routing. In triangle routing an incoming to MN traffic always passes through the home agent (HA), what can cause undesirable increasing the traffic load in the home network. Inherent route optimization is a major improvement compared to the IPv4 mobility protocol, which specifies route optimization as a separate extension to the mobility protocol. More importantly, all IPv6 nodes support route optimization while only mobile nodes in IPv4 can support the mobility extension.

The very large address space of IPv6 is the best-known feature of this protocol, but it is less interesting for military environment that has a relatively small dedicated Internet. The rich address formats are architecturally interesting: multicast supporting conferencing and broadcast applications; anycast supporting such activities as "use the nearest server". The attractiveness of such facilities is principally used to reduce the management of the network and bandwidth requirements as well. The auto-configuration facility could also reduce the running costs of the network as the address assignment can occur without participation of network administrator. However, this raise a security concern in loss of administrative control over the allocation of addresses in the network.

Tactical military networks are predominantly radio based and "on the move" with minimal fixed infrastructure. Also, security and mobility efficiency play essential role from military point of view.

The detailed background of the tactical Intranet structure that uses IPv6 protocol stack discussed here is clarified in [3] and [8]. The authors have limited the discussion only to the security problem that is applied to the tactical environment, treated the tactical network as a non-secure medium (denoted in the figures as a cloud).

2. The IPSec features

Security features of IPv6 have been obtained mainly by means of two dedicated extension header [1, 2]: *authentication header* (AH) and *encrypted security payload* (ESP) with complementary capabilities.

The AH header was designed to ensure authenticity and integrity of the IP packet. Its presence guards against two threats: the fixed fields illegal modification and packet

spoofing. On the other hand, the ESP header provides data encapsulation with encryption in order to ensure that only the destination node can read the payload conveyed by the IP packet. The two headers can be used together to provide all the security features simultaneously (Fig. 1).

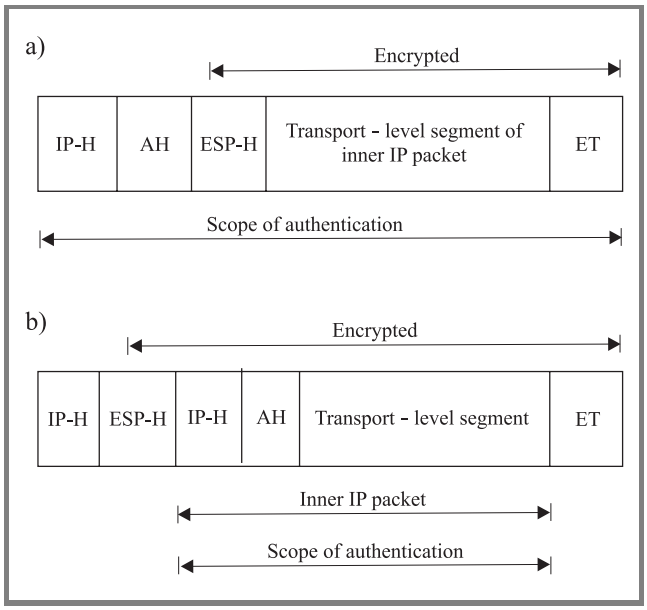

Fig. 1. Combining privacy and authentication: (a) encryption before authentication; (b) authentication before encryption. Explanations: IP-H – IP based header plus extensions headers, AH – authentication header, ESP-H – encapsulating security payload header, ET – encapsulating security payload trailing fields.

Both the AH and the ESP headers use a concept of the security association (SA) to agree on the security algorithms and parameters between the sender and the receiver. In general, each IPv6 node manages a set of SAs, one for each currently active secure communication. The *security parameters i*ndex (SPI) is a parameter contained in both the AH and ESP headers to specify which SA will be used in decryption and/or authentication the packet.

In unicast transmissions, the SPI is normally chosen by the destination node and sent back to the sender when the communication is set up. In multicast transmissions, the SPI must be common to all the members of the multicast group. Each node must be able to identify the right SA correctly by combining the SPI with the multicast address.

The negotiation of the SA (and the related SPI) is an integral part of the protocol for the exchange of security keys.

Correct application of the AH and ESP headers requires that all the communicating parties agree on a common key to be used in forming and checking the security headers. The IPv6 allows key management to occur either out-of-band or with specifically crafted protocols. However, no general agreement has been reached yet on this subject within the Internet community, with different groups stressing different needs: fast key exchange, strong authentication, lightweight protocols, and others. Key management is the area that is still mostly unsettled within the whole IPSec architecture.

The IPv6 requires each implementation to allow for manual setting of the security keys, in case of no in-line key management technique is adopted or human-based security is desired. Obviously, manual keying is possible only if the security administrators have separately agreed out-of-band on the keys to be used – for example, at a reserved meeting. This solution exhibits high personnel costs and does not scale well because it requires personal action of an operator on each network device taking part in the secure channel. Additionally, it can generate a false sense of security. The human intervention does not automatically ensure a higher level of security, due to untrusted administrators and residual problems related to hardware and software integrity of the device where the key is set. However, in spite of these disadvantages, manual key management finds application in restricted environments, with a small number of devices physically secured, that according to the security policy, can operate only when explicitly enabled by human intervention.

Within the IPSec, key management is surely the area that is less settled and the area in which much work has yet to be done before arriving at a set of protocols that completely meet the security needs at the IP level. The only decision that has already been made is that, for the sake of generality, the Internet key management protocol (IKMP) will be placed at the application layer, and it will be independent of the protocols at the lower layers.

The first proposal is to base IKMP on the coupling of the Internet security association and key management protocol (ISAKMP) and Oakley protocols, as described in the IEFT Draft, the resolution of ISAKMP with Oakley.

The ISAKMP defines a generic architecture for authenticated SA setup and key exchange, without specifying the actual algorithms to be used. In this way, it can be used with different key exchange techniques.

Oakley is a key-exchange protocol, based on a modified version of the Diffie-Hellman algorithm. Therefore, it is one of the natural partners for ISAKMP.

However, in addition to the ISAKMP-Oakley couple, different solutions are being proposed. Currently, the major competitor is simple key-management for Internet Protocols (SKIP), which bases its operations on the Diffie-Hellman algorithm. The SKIP is simple and addresses several problems of key management in high-speed networks, such as zero-message key setup and updates that permit fast dynamic rekeying (that is, frequent in-line change of the security keys to avoid analytic attacks based on accumulation of cyphertext encrypted with the same key). Moreover, although SKIP is not standardized yet, it already features many commercial-level implementations, both for UNIX workstations and for personal computers.

So the war of the key-management protocols is raging, and the likely outcome is that more than one protocol will attain

RFC status, because these protocols exhibit different merits that are valuable in different application environments.

3. Tactical Intranet security

The AH and ESP headers can be used in different ways to protect IP transmission.

In IPv6, achieving good level of security is easier and more standard than in IPv4, thanks to the AH and ESP headers. As an example, with reference to Fig. 2, let us suppose that a TCP session (channel) between host denoted H1 in network named N1 and host H2 in network N2 has to be protected only against data manipulation and origin falsification, while data privacy is not required. In this case, the AH header can be used in the following way. The firewall FW1 gets the IP packet and modifies it by adding an AH header before sending it to its partner firewall FW2. When this packet is received by the FW2, it checks the packet for integrity and origin authentication using the SPI data in the AH header. If the test is successful, then the IP header and the AH header are removed, and the remaining data (that is, the original packet) are sent to the final destination.

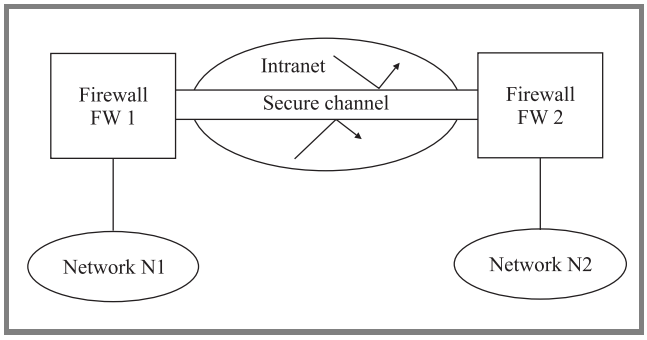

Fig. 2. An example of the tunnel between two firewalls.

If the network is implemented using only the AH header, then attackers can neither alter the transmitted packets nor insert forged packets in the channel. However, they can still read the content of the packets. To prevent disclosure of the payload, the ESP header has to be used too. Even the usage of AH in conjunction with ESP does not completely protect the traffic. Packets can be deleted by intermediate nodes or recorded and later replayed. These attacks cannot be easily contrasted at the IP level. Appropriate defenses (such as the use of unique packet identifiers and the generation of heartbeat packets) are usually placed at some upper level in the network stack. A partial solution at the IP level is likely to be offered by the new format and algorithms that are going to replace the current ones in the AH header.

In contrast to the IPv4, there is no problem with fragmentation in IPv6, because the overhead is fixed in size (the dimension of AH, or that of AH plus ESP) and fragmentation process is realized in source host.

This technique can be adopted even between the firewall and the single external host (Fig. 3). Obviously, this case is very important for guaranteed security when a mobile host is used outside the protected network, and it is a perfect complement to the mobility support features of IPv6. The firewall will act as a home agent in the neighbor discovery procedure. Mobile host will be assigned two different IP addresses: one when it is connected inside the security perimeter of the network and the other one when it is outside this perimeter. In second case, the firewall will also act as a relay, by routing packets coming from inside the corporate network to the external address, after adding the required headers (AH only, or AH plus ESP).

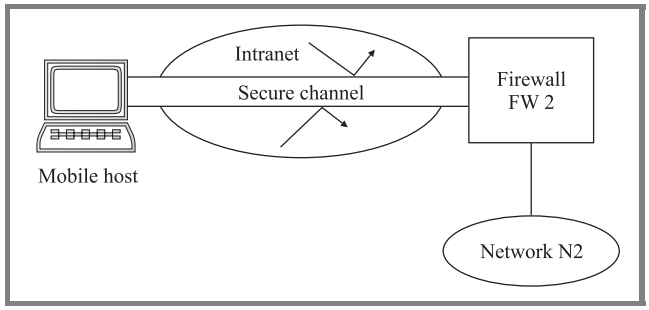

Fig. 3. Tunnel between a firewall and a single host.

This solution is not complete for application-level security because only partial protection is obtained. AH provides only host-based authentication, whereas applications usually require user-based authentication. Moreover, AH and ESP protect the data only during their transmission along the channel. After the data have been received, they are no longer protected in any way. This fact may not be relevant if the receiving host is a secure one, but there is the additional implication that origin authentication and data integrity properties are lost as well. So formal non-repudiation cannot occur after the data have been extracted from the secure channel.

The conclusion is that the security features of IPv6 do not eliminate the need for other security mechanisms, which will probably be better placed at the application level. Networked applications executing on the top of the IPv6 stack may be required in order to use the communication channel with specific features. To avoid duplication of functionality (and hence performance degradation) being able to specified at the transport layer, the security attributes of the created channel are useful.

Since IP addresses in the IPv6 are quite often dynamically assigned, it is the most importance that this process be done in a secure fashion.

Moreover, as different security properties are available through a proper combination of AH and ESP headers, it is highly desirable that they should be applied to the messages exchanged by the routers, to prevent attacks aiming to subvert the logical architecture of the network.

Following types of communications should be protected:

- The routing advertisement messages, to ensure that they are sent by an authorized router.
- The neighbor advertisement messages, to ensure that they come from authorized hosts and to avoid a risk that somebody attaches a new host to the network without proper authorization.
- The ICMP messages related to an unreachable host or network (*destination unreachable*) or to a better route (*redirect*), to ensure that these messages come from hosts or routers that were on the original path of the packets.

Securing these types of messages is surely not trivial. For example, the routing advertisements are sent to a multicast group; therefore, all the routers in the group have to know the (common) secret key to be used to verify and/or decrypt the messages. This fact implies that they can forge messages and impersonate any router in the group.
Protection of the neighbor advertisements is a serious problem. These messages can be protected only after the SA has been created between the host and the address distribution center. On the other hand, this SA can be created only after the address has been assigned to the host, so we can conclude that this is no correct solution. The break of the loop is possible. For example, priority can be given to the address assignment phase, and SA setup can be permitted only subsequently, but in this way the address assignment phase is not protected. Alternatively, public key authentication can be used. Each host is assigned a key pair (private and public key) and has to be reconfigured with the public key of the authority that signs the certificates of the routers and the address distribution centers. The last alternative is to configure the routers so that they do not advertise local prefixes. In this way, each host is forced to contact a router first.
Protection against malicious ICMP messages requires that they should be protected by the AH header, but this approach has the drawback of requiring the establishment of the SA with each router and host on the path between the source and the destination of the packets.
With respect to the messages security used by the various routing protocols, they should always be exchanged just within the frame of the SA and should be protected by the AH. For the sake of generality, this solution is highly preferable to using authentication mechanisms specific for each routing protocol.
Based on the previous analyses, we can conclude that routing security is apparently still a big problem in IPv6, but chances of solving this problem are higher than in IPv4.

4. Conclusions

The tactical military architecture is a hierarchical arrangement of mobile components. The degree of users mobility varies with the echelon and the distance from the front. The nature of military operations is such a changing that significant advantage will be achieved by the creative, timely and decisive usage of the information. Consequently, the demand for access to the information is also changing and evolving towards the new network-centric model based on more comprehensive, ubiquitous and shared information services.
From military point of view, there is no problem with address space exhaustion in the internal networks, as they are largely closed networks. Additionally, since such networks are relatively small, the problem with big routing tables does not exist.
The security features of IPv6 offer only commercial grade of security. Specific hardware encryption have to be added in military domain.
The IETF security architecture is open to apply additional encryption applications. Several solutions exist clarifying how the IPSec may be implemented to hosts in conjunction with the router or firewall. Some solutions are integrated into the native IP implementations and other ones are build-in according to bump-in-the-stack (BITS) or bump-in-the-wire (BITW) scheme [1, 9]. The second scheme enables to use an outboard crypto processor that is common designed feature of the security in military network.
Currently, the AH and ESP headers should be modified along the following guidelines:

- The AH format must be substantially changed to accommodate new and stronger authentication algorithms (HMAC – *keyed-hashing for message authentication* [10]) that support prevention of packet replay and its cancellation ([11] describes this format when used with the MD5 digest algorithm).
- The ESP specification must achieve a better orthogonality with algorithms, to simplify application of different encryption algorithms.

The benefit of these changes is that higher security will be available at the network level. Hence, applications will be able to concentrate on different security aspects, such as authorizations.

Acknowledgement

The paper is a result of the research project 0T00A047 financed by State Commitee for Scientific Research in the 2001/2002.

References

[1] R. Ramjee, T. La Porta, L. Salgarelli, S. Thuel, and K. Varadhan, "IP-based access network infrastructure for next-generation wireless data networks", *IEEE Pers. Commun.*, Aug. 2000.

[2] S. Gai, "Internetworking with IPv6 Cisco Routers", http://www.ip6.com/us/book/index.html

[3] M. Bednarczyk, J. Jarmakiewicz, and K. Maślanka, "Problems with using COTS technology in tactical communication systems based on stack of IPv6 protocol", Zegrze, 2001.

[4] D. B. Johnson and C. Perkins, "Mobility support in IPv6". Internet Draft, Apr. 2000, <draft-ietf-mobileip-ipv6-12.txt>

[5] C. Perkins, "IP mobility support", RFC 2002, Oct. 1996.

[6] W. Stallings, "IPv6: the new Internet Protocol", http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stallings/

[7] W. Stallings, *Data and Computer Communications*. 5th ed. Prentice-Hall, 1997.

[8] M. Amanowicz, J. Jarmakiewicz, J. Krygier, and K. Maślanka, "Mobility management in tactical IPv6 network", in *Proc. MILCOM'2002*, Anaheim, USA, Oct. 2002.

[9] S. Kent and R. Atkinson, "Security architecture for the Internet Protocol", IETF Standard Track RFC 2401, Nov. 1998.

[10] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: keyed-hashing for message authentication", IETF RFC 2104, Feb. 1997.

[11] M. Oehler and R. Glenn, "HMAC-MD5 IP authentication with replay prevention", IETF Standards Track RFC 2085, Feb. 1997.

Mariusz Bednarczyk was born in Poland, in 1973. He received the M.Sc. degree in telecommunications domain in 1998 from Military University of Technology, Warsaw, Poland. He engages in problems of communications and information systems (CIS) modelling and simulation and advanced wireless communication technologies as well.
e-mail: mbednarczyk@wel.wat.edu.pl
Telecommunications Institute
Military University of Technology
Kaliskiego st 2
00-908 Warsaw, Poland

Jacek Jarmakiewicz received M.Sc. degree in 1989 from Military University of Technology, Warsaw, Poland. He finished postgraduate studies in the National Institute of Telecommunications in Warsaw, in the communications network management domain. He specializes in mobility management, mobile computing, communications systems modelling and simulation, computer networks and, performance evaluation.
e-mail: jjarmakiewicz@wel.wat.edu.pl
Telecommunications Institute
Military University of Technology
Kaliskiego st 2
00-908 Warsaw, Poland

Jarosław Krygier was born in Poland, in 1971. He received the M.Sc. degree in 1996 and the Ph.D. degree in 2002 from Military University of Technology, Warsaw, Poland, both in telecommunication engineering. He engages in problems of communications and information systems (CIS) modelling and simulation, wideband CDMA technology, IPng problems, CIS interoperability and telecommunication systems engineering. He is an author and co-author of over 30 scientific papers and research reports.
e-mail: jkrygier@wel.wat.edu.pl
Telecommunications Institute
Military University of Technology
Kaliskiego st 2
00-908 Warsaw, Poland