Paper

IP-KRYPTO cipher machine for military use

Mariusz Borowski and Grzegorz Łabuzek

Abstract—Polish military IP networks can be effectively and cheaply secured by IP-KRYPTO cipher machines which are developed in the Military Communication Institute. The co-operation with Polish manufacturers – Optimus and ABA Kraków and the usage of COTS elements and ideas speed up the research and development works. The IP-KRYPTO cipher machine will be used for securing the "SECRET" data so it must be certified to fulfill E3 ITSEC evaluation criteria. This requirement generates additional challenges in the development process when the COTS elements are to be implemented.

Keywords— IPsec standards, ITSEC evaluation criteria.

1. Introduction

Military computer networks, among other things, need the security cryptographic services which can be implemented at several layers in a network infrastructure. Military institutions have used link-level encryption for years. In the method every communications link is protected with a pair of encrypting devices – one on each end of the link. While this method provides excellent data confidentiality between two crypto devices, other cryptographic services are inaccessible. Of course, this method does not work at all in the public networks, where few of the intermediate links are accessible or trusted to the user.

2. Usage of IPsec standards as a COTS development idea

The Internet Protocol security (IPsec) is a framework of open standards for ensuring secure private communications over IP networks. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across the public IP network.

The concept of a "Security Association" (SA) is fundamental to IPsec [2]. SA is a simple "connection" that affords security services to the traffic carried by it. Two types of SA are defined: transport mode and tunnel mode.

The transport mode SA is a security association between two hosts. In IPv4, a transport mode security protocol header appears immediately after the IP header and any options, and before any higher layer protocols (e.g., TCP or UDP).

The tunnel mode SA is essentially an SA applied to an IP tunnel. Whenever either end of a security association is a security gateway, the SA must be the tunnel mode. For the tunnel mode SA, there is an "outer" IP header that specifies the IPsec processing destination, plus an "inner" IP header that specifies (apparently) the ultimate destination for the packet.

The Internet Protocol security is based on the following two protocols:

- Authentication Header protocol (AH) [3],
- Encapsulation Security Payload protocol (ESP) [4].

The AH protocol provides integrity and authentication services, while the ESP protocol delivers mainly confidentiality. These protocols may be applied alone or in combination with each other to provide desirable set of security services. Each protocol can be used in the transport mode and the tunnel mode.

The encrypted packets look like ordinary IP packets (Fig. 1), they can easily be routed through any IP network, such as the Internet, without any changes to the intermediate networking equipment.

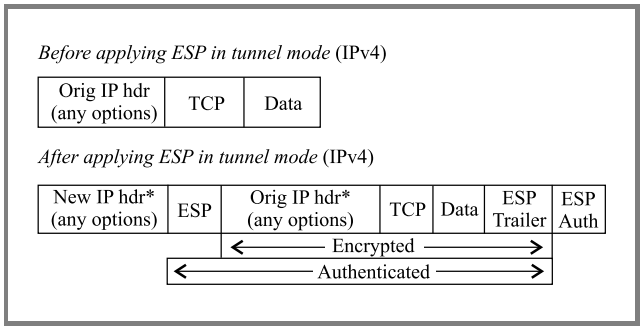

Fig. 1. Appling ESP to a packet in tunnel mode.

The only devices that know about the encryption are the end points. This feature greatly reduces both the implementation and management costs.

3. The TCE 621 IP Crypto Device – the prototype

According to the COTS strategy the IPsec standards were implemented in military IP crypto devices by many manu-

facturers. One of such approach is the TCE 621 IP Crypto Device (Fig. 2) developed by THALES Communications company which was approved for securing NATO IP networks.

Fig. 2. The TCE 621 IP Crypto Device.

The TCE 621 is inserted between a host (end system) or a company network and the IP network. This is used to establish virtual private networks (VPN) solutions, or to provide end-to-end protection of the communications between single hosts. The TCE 621 protects the communications between hosts by adding end-to-end security services to the IP protocol. All security services are provided by the IPsec ESP protocol [4] as specified by IETF.

The TCE 621 provides:

- NATO approved cryptographic algorithms;
- a 10 megabits per second Ethernet interface;
- security for between 500 and 900 IP datagrams per second, depending on pocket size;
- up to 1000 security associations;
- work in a net consisted of up to 1000 such devices;
- audit support and centralized management;
- protection against electromagnetic emanation according to AMSG 720B;
- ruggerized, temper resistant shelter.

The Polish army is not equipped with the IP crypto cipher machines of such functionality but it needs them. The Military Communication Institute, which has long tradition in building the cryptographic devices, starts research and the development process. For efficiency and the time and money saving we decided to use some of the COTS components and ideas.

4. The Optimus ABA IPSec Gate – the first Polish approximation

Polish computer companies, Optimus and ABA Kraków, developed and introduced the Optimus ABA IPSec Gate crypto devices which are based on IPsec standards.
The Optimus ABA IPSec Gate (Fig. 3) uses exclusively well-tried standard PC hardware which is cost-effective and deliverable in the long term. Moreover, the cipher machine can be integrated into every underlying IP-based IT infrastructure.
The Optimus ABA IPSec Gate is based on a specially minimized and hardened Linux operating system with implementation of IPsec standards named FreeS/Wan. All software is stored on flash RAM with manipulation protection. Moreover the software integrity is checked during the system start up, and in small regular time periods.

Fig. 3. The Optimus ABA IPSec Gate.

The Optimus ABA IPSec Gate provides the strongest encryption technology available on the commercial market, using concurrent 3DES (168-bit key) and Rijndael – AES (256-bit) algorithms as standard offerings. The unit employs the Secure Hash Algorithm (SHA-1 and SHA-2), as well as Diffie-Hellman and Internet Key Exchange (IKE) protocols [6] to perform authentication and automatic exchange of a key material.

Supported standards:

- [2], [3], [4] – main IPsec standards;
- [5], [6], [7] – IPsec standards supported session keys establishing methods;
- RFC 2403, The Use of HMAC-MD5-96 within ESP and AH;
- RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH;
- RFC 2104, HMAC: Keyed-Hashing for Message Authentication Code;
- RFC 2451, The ESP CBC Mode Cipher Algorithms;

- RFC 2408, Internet Security Association and Key Management Protocol;
- RFC 3173, IP Payload Compression Protocol (IPComp);
- RFC 2394, IP Payload Compression Using DEFLATE.

The throughput of data depends on the selected cryptographic algorithm. The data throughput of the Optimus ABA IPSec Gate is scaled with the clock rate of the underlying processor hardware and achieves up to 90 Mbit/s with AES on a Intel Celeron 1.7 GHz processor. It supports dial-up functions (PPP) via ISDN terminal adapters, analogue modems, DSL and GSM/GPRS mobile phones.
The Optimus ABA IPSec Gate was certified for securing the "RESTRICTED" data by the national security authority according to the "Protection of Classified Information Act".

5. The IP-KRYPTO cipher machine research process

The Military Communication Institute in cooperation with Optimus and ABA Kraków companies is developing an IP-KRYPTO cipher machine for use by the Polish army. The cipher machine is designated for securing the "SECRET" data in the military and government IP networks; therefore it must be worked out and produced to fulfill the ITSEC evaluation criteria.
The IP-KRYPTO cipher machine has to fulfill the E3 ITSEC evaluation criteria, but the cryptographic algorithms have to fulfill E6 criteria. For rapid development we decided to use COTS technologies and equipments. The target of the evaluation (TOE) [8] which satisfies E3 criteria must be prepared in the development process with:

- security target for the TOE;
- informal description of the architecture of the TOE;
- informal description of the detailed design;
- test documentation;
- library of test programs and tools used for testing the TOE;
- source code or hardware drawings for all security enforcing and security relevant components;
- informal description of correspondence between source code or hardware drawings and the detailed design.

While the use of IPsec standards as an example of COTS ideas is consistent with the shown criteria in regard to the deliberated specification, the implementation of software modules without the source code is unacceptable.
The main tasks in the research process:

a) designing fast and secure national cryptographic algorithms with a suitable documentation;
b) implementation of algorithms in the COTS implementation of IPsec standards named FreeS/WAN;
c) designing a secure and effective key establishing method;
d) designing a secure and temper resistant keying module;
e) designing an IP-KRYPTO motherboard with an appropriate powerful processor and solved thermal problems;
f) designing a temper resistant and satisfying lack of electromagnetic emanation (AMSG 720B) shelter;
g) designing a shelter and a motherboard which satisfy environmental and mechanical demands;
h) preparing a network planning and key generation station.

Some of the aforementioned challenges will be discussed more precisely here.
The IP-KRYPTO cipher machine demands fast and secure national cryptographic algorithms. The IPsec standards are open and suitable for the implementation of any national algorithms instead of those shown for the commercial use. The new national algorithms were designed in the Military Communication Institute. In addition to the security features also their speed of work was important because the IP-KRYPTO must support at least a 10 Mbit/s Ethernet interface.
The IP-KRYPTO cipher machine needs a motherboard with an appropriate powerful processor and the solved thermal problems. The Optimus ABA IPSec Gate manufactured by our partners uses exclusively the well-tried standard PC hardware which is cost-effective but this commercial equipment cannot be implemented in the military products. We decided to use a hardened industrial standard PC motherboard. The motherboard provides 10/100 Mbit/s Fast Ethernet Ports, a socket 478 processor and DiskOn-Module like flash memory on the board. It also supports optional IPsec encryption accelerator which uses commercial algorithms according IPsec standards. We did not decide to design national VLSI IPsec module because of small scale of production, costs and absence of trusted manufactures (national algorithms will have to be implemented in it). All IPsec operations are software implemented and executed by a fast processor. Computational power of the processor is very important but it causes problems with freezing all modules on the motherboard. Freezing

demands are additionally complicated by the needed lack of electromagnetic emanation of the cipher machine. Mechanical and environmental exposures also must be taken into consideration.

The source code or hardware drawings for all security enforcing and the security relevant components have to be shown in the certification process so the IP-KRYPTO cipher machine operates under control of the Linux operating system. The Linux OS is the open source operating system and everyone wise has an access to its code. The Linux OS used in the IP-KRYPTO crypto machine is integrated with software implementation of IPsec standards named FreeS/WAN. All security services are provided by the IPsec ESP protocol in the tunnel mode. New functions have been added to the standard FreeS/WAN software. The functions concern the ability of connecting with the device located behind a Network Address Translator (NAT-Traversal) and Dead Peer Detection (DPD). Additionally the IP-KRYPTO software is integrated with a software firewall based on iptables with an automatic configuration option. This configuration is created upon configuration parameters for maximizing security and does not reduce functionality. By default the firewall blocks all packets except packets moving in the IPsec tunnel. All applications have been compiled with the use of Gnu Compiler Collection (GCC) with stack-smashing protector. It is an extension for protecting applications from stack-smashing attacks. The protection is realized by buffer overflow detection and the variable reordering feature to avoid the corruption of pointers.

Key establishing methods for IPsec are shown in [6]. Phase 1 is where two ISAKMP peers establish a secure, authenticated channel with which to communicate. In the phase the Diffie-Hellman protocol is used for establishing a common secret. The common secret is used in Phase 2 for establishing cryptographic keys. The IP-KRYPTO cipher machine will secure the "SECRET" data, so the data must stay secret by the next fifty years. In that case we have a well known cryptographic theorem: "If the Diffie-Hellman protocol is secure than the scheme is secure". A well known method of securing the Diffie-Hellman protocol is using more numerous $GF^*(p)$ or transforming the protocol to the group of points on elliptic curves. These examples are shown in [7] and they are suitable for the commercial use where such a long time for securing the data is not required. The security of the Diffie-Hellman protocol is based on the difficulty of solving a discrete logarithms problem, other well known public key algorithms (for example RSA) are based on the difficulty of number factoring. The security of the transformations is based on mathematical problems and computational complexity. But an adversary is able to record all exchanges between two IP-KRYPTO devices and wait (it has fifty years) until new mathematical or computational methods are achieved. Thus a simple copy of the standard [6] in the developing the IP-KRYPTO cipher machine is not available.

The IP-KRYPTO cipher machine needs a secure and temper resistant keying module. The Optimus ABA IPSec Gate used a Flash RAM for hiding the keys and configuration. All data on the Flash RAM are ciphered. This is an excellent example of using the COTS technology which is fast, cost effective and suitable for securing the "RESTRICTED" data. The requirements for securing the "SECRET" data demand that the key module must have a temper resistant shelter and support an emergency clearing function executing without outer power supply.

The last step in the developing the IP-KRYPTO cipher machine will be creating a network planning and key generation station. The main goal of the station is preparation of the configuration data and cryptographic keys for all IP-KRYPTO machines and filling their keying modules.

6. Summary

In the paper we showed the IP-KRYPTO research process. If a crypto device must be used for securing the "SECRET" data, then special requirements must be fulfilled. Usage of COTS technologies and equipments is suitable in developing crypto devices for securing the "RESTRICTED" data. Such techniques implemented in the devices dedicated for securing higher clause data need an extremely cautious, well prepared and experienced developing team. The simplest way is with the use of COTS ideas and standards but military equipments must fulfill additional mechanical, environmental and electromagnetic emanation criteria.

IP-KRYPTO cipher machines demand also a network planning and key generation station. At the end of the research process the prototype of the cipher machine with the station must be certified by the national security authority according to the "Protection of Classified Information Act".

References

[1] "Cryptel®-IP. The TCE 621 IP Crypto Device", htpp://www.thalesgroup.no

[2] RFC 2401, "Security Architecture for the Internet Protocol".

[3] RFC 2402, "IP Authentication Header".

[4] RFC 2406, "Encapsulating Security Payload (ESP)".

[5] RFC 2407, "Internet IP Security Domain of Interpretation for ISAKMP".

[6] RFC 2409, "Internet Key Exchange (IKE)".

[7] RFC 2412, "OAKLEY Key Determination Protocol".

[8] "ITSEC evaluation criteria", htpp://www.cesg.gov.uk

Mariusz Borowski was born in Lublin, Poland, in 1968. He studied at the computer science faculty of the Military University of Technology, Warsaw. Graduated in 1992 and in 1995 he received a Ph.D. in the cryptographic data security at the Military University of Technology. Since his graduating he has been working at the Military Communication Institute. His main objects of interests: cryptology, computer and network security, computer aided computation.
e-mail: borow@wil.waw.pl
Military Communication Institute
05-130 Zegrze, Poland

Grzegorz Łabuzek was born in Opole, Poland, in 1978. He graduated from the Technical University of Opole in 2002. From March 2002 to March 2004 he worked in the ABA Kraków company. Since March 2004 he has been working at the Military Communication Institute. His main objects of interests: computer and network security, open source operating system, cryptology.
e-mail: labuzek@wil.waw.pl
Military Communication Institute
05-130 Zegrze, Poland