유비쿼터스 환경하에서의 암호화 모듈이 내장된 네트워크 게이트웨이의 분석

김정태
목원대학교

Analyses of Embedded Network Gateway under Ubiquitous Surroundings

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

As the commercial use of the Internet becomes com- mon and the demand for mobile computing through the Internet is emerging, it is necessary to construct a secure mobile environment. This paper proposes an approach with IP layer security and mobility support to meet this challenge. To evaluate our approach, we are developing a security and mobility supported system

I . Introduction

Sensor networks offer economically viable solutions fo a variety of applications. Networked microsensors technology is a key technology for the future. Cheap, smart devices with multiple onboard sensors, networked through wireless links and Internet and deployed in large numbers, provide unprecedented opportunities for instrumenting and controlling homes and the environment. Demands for mobile computing are increasing, as smaller PCs and PDAs are more and more commonly used. Users of such equipments want to communicate with their home environment, such as servers and resources, from remote IP connecting points through various communication media. For example, even when an officer worker is away, he wants to access proprietary information inside his company. In order to realize such mobile communications using the Internet for commercial use, security considerations are mandatory.

II. Security Vulnerabilities and Threats

The nature of wireless networks makes them become potential targets for attackers. Many attackers are attempting, through the convenient Internet access, to access an enterprise network for malicious purpose. A thread that spans most definitions of network security is the intent to consider the security of the network as a whole, rather than as an endpoint issue. A comprehensive network security plan must encompass all the elements that make up the network and provide five important services:

- Access. Provides users with the means to transmit and receive data to and from any network resources with which they are authorized to communicate.
- Confidentiality. Ensures that the information in the network remains private. This is typically accomplished through encryption.4
- Authentication. Ensures that the sender of a message is who he claims to be.
- Integrity. Ensures that a message has not been modified in transit.
- Nonrepudiation. Ensures that the originator of the message cannot deny that he sent the message. This is useful for both commercial and legal reasons.

III. Security Gateway

3.1 Security issues on Mobile IP

1) Packets going into the corporate network
2) Packets going out from the visiting network
3) Confidentiality of communication
Issue on combining IPsec and Mobile IP

As shown in Figure 1, this security gateway consists of six management units: traffic collection unit, traffic processing unit, authentication unit, behavior analysis unit, policy management unit, and response unit.

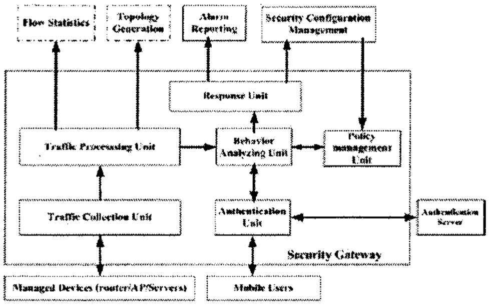

Fig 1. Architecture in secure gateway

The gateway also cooperates with an authentication server to guarantee a secure link layer access control. All six management units are integrated together to provide precaution security application services. Alarm reporting system and security configuration management are two primary applications which are taken into consideration in this paper. Specifically, by cooperating with an authentication server, access control in the link layer is provided; by monitoring and analyzing IPv6 packages, the security threats prevention can be achieved in IP layer.

IV. Requirement for security

It is a popular misconception that "security" is synonymous with "encryption:, In many cases, confidentiality via encryption is that least important element of a security solution. Network security involves a number of different elements.

1. data origin authentication
2. command authorization
3. message integrity protection
4. message replay prevention

5. data confidentiality
6. key distribution
7. trust versus trustworthiness

V. Security Processing Architectures

Security processing refers to computation that need to be performed specially for the purpose of security. For example, in a secure wireless data transaction, security processing includes the execution of any security protocols transactions, security processing includes the execution of any security protocols that are utilized at all layers of the protocol stack.

A. Embedded processor enhancement for securing processing

There have been several attempts to improvement the security processing capabilities of general purpose processors. Since most microprocessors today are word oriented, researchers have targeted accelerating bit level arithmetic operations such as the permutations performed in DES/3DES. Multimedia in struction set architecture

B. Cryptographic hardware accelerators

Highest levels of efficiency in processing are often obtained through custom hardware implementations. Since cryptographic algorithm form a significant portion of security processing workloads, various companies offer custom hardware implementations of these cryptographic algorithms suitable for mobile appliances including smart cards and wireless handsets.

C. Programmable security protocol engines

While cryptographic accelerators alleviate the performance and energy bottlenecks of security processing to some extent, achieving very high data rates or extreme energy efficiency requires a view of the entire security processings workload. In additional to cryptographic algorithms, security protocols often contains a significant protocol processing components, including packet header/trailer allocation parsing

D. Algorithms for Encryption

Our choice of algorithms represents popular symmetric encryption and hashing function schemes that form an integer part of many security protocols. RC4 is used in IEEE802.11 WEP, IDEA and MD5 are part of PGP, SHA-1 and MD5 are included in the security architecture for Internat protocol. These algorithms offer variety in the mode in which they operate and encompass different mathmatical and data manipulation operations. They work on different word sizes ranging from 8 bits to 32 bits, and hence, help assess the effectiveness of the different architecture.
Table 1 presents the parameter in analyses.

Table 1: Encryption Schemes and Parameters

Algorithm	Type	key/hash (bits)	Block (bits)
RC4	stream	128	8
IDEA	block	128	64
RC5	block	64	64
MD5	1-way hash	128	512
SHA-1	1-way hash	128	512

1) RC4 : stream cipher symmetic key algorithm. This algorithm is quite simple and operations involve the addition of 8 bit elements or swapping variables in a 256 byte state table. RC4 supports variable length keys. We consider a 128 bit key here.

2) IDEA : symmetric key block cipher that operates on 64 bit plaintext blocks. The key is 128 bits cipher that operates on 64 bit plaintext blocks. The key is 128 bits long with the same algorithm used for both encryption and decryption. The algorithm primarily includes operations from threealgebraic group: XOR, addition modular 216, multiplication modulo 216+1

3) RC5 : a fast symmetric block cipher with a variety of parameters block sixe, key size and number of rounds. We currently focus o a RC5 implementation with a 64 bit data block and 64 bit key. It uses the XOR, addition and rotation operations.

4) MD5 : one-way hash function that processes the input textin 512 bit blocks to generate a 128 bit hash. The mathmatical operations that are involved in this algorithm are: XOR, AND, OR, NOT and rotations. The algorithms also pads plaintext to 512 blocks with the last 64 bits of the last block indicating the length of the message

5) SHA-1 : also one way hash function that produces a 160 bit output when any message of any length less than 264 bits is input. The operations are similar to MD5 and constitute XOR, AND, OR, NOT and rotations

VI. Conclusion

The security gateway has been valid in successfully capturing and reporting the threat attempts. In this paper, we presented a survey investigating the computational requirements for a number of cryptographic algorithms and embedded architecture.

References

[1] The IPSEC Working Group," Ip security protocol (ipsec) charter", http://www.ietf.org/html.charters/ipsec-charter.html.

[2] SnifferPro,http://www.snifferpro.co.uk.

[3] H. Soliman, "Mobile IPv6: Mobility in a Wireless Internet", Addison-Wesley, April 2004.

[4] R. Thayer, N. Doraswamy, R. Glenn, "IP Security Document Roadmap", IEFT RFC 2411, November 1998.

[5] W. Fumy and P. Landrock,"Principles of key management," IEEE J. of Selected Areas in Communication, vol.11, pp.785-793, June 1993

[6] W. Stallings, Network and Internetwork Security, IEEE Press, 2 edition, 1995