Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol 2, No.1, 2012

Multilayer Security Mechanism in Computer Networks

Rajeshwari Goudar, Pournima More
Computer Department, MAE Alandi, University of Pune 411015, Maharashtra, India
rmgoudar66@gmail.com

Abstract

In multilayered security infrastructure, the layers are projected in a way that vulnerability of one layer could not compromise the other layers and thus the whole system is not vulnerable. This paper evaluates security mechanism on application, transport and network layers of ISO/OSI reference model and gives examples of today's most popular security protocols applied in each of mentioned layers. A secure computer network systems is recommended that consists of combined security mechanisms on three different ISO/OSI reference model layers : application layer security based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens, transport layer security based on establishment of a cryptographic tunnel between network nodes and strong node authentication procedure and network IP layer security providing bulk security mechanisms on network level between network nodes. Strong authentication procedures used for user based on digital certificates and PKI systems are especially emphasized.

Keywords: Multilayered Security Systems, PKI systems, Smart Cards.

1. INTRODUCTION

In computer network systems, only general and multilayered security infrastructure can manage with the possible attacks. This paper presents security mechanisms on application, transport and network layers of ISO/OSI reference model and gives examples of the today most popular security protocols applied in each of the mentioned layers (e.g. S/MIME, SSL and IPSec). We recommend a secure computer network systems that consists of combined security mechanisms on three different ISO/OSI reference model layers: application layer security (end-to-end security) based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards), transport layer security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure and network IP layer security providing bulk security mechanisms on network level between network nodes – protection from the external network attacks. These layers are projected in a way that a vulnerability of the one layer could not compromise the other layers and thus the whole system is not vulnerable. User strong authentication procedures based on digital certificates and Public Key Infrastructure (PKI) systems are especially emphasized.

2. MULTILAYERED SECURITY INFRASTRUCTURES

In modern computer networks, following important security features should be included:

- User and data authentication
- Data integrity
- Non-repudiation
- Confidentiality

This means that in secure computer network systems, the following features need to understand:

- Strong user authentication techniques based on smart cards
- Integrity of electronic data transferred either via wired or wireless IP networks
- The non-repudiation function

By using digital signature technology based on asymmetrical cryptographic algorithms, these features are implemented. Also, the confidentiality and privacy protection of transferred data must be preserved during whole transmission data paths and they are done by using symmetrical cryptographic algorithms. In this Section, we will give the overview of modern security mechanisms and cryptographic protocols. The considered security mechanisms are based on Public Key Infrastructure (PKI), digital certificates, digital signature technology, confidentiality protection, privacy protection, strong user authentication procedures and smart card technology. Some overviews of these techniques are given in [2].

The multilayered security architecture is proposed to be implemented in order to limit the potential harmful attacks to the particular network. Modern computer networks security systems consist of combined application of security mechanisms on three different ISO/OSI reference model layers:

- Application level security (end-to-end security) based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards) – internal network attacks protection.
- Transport level security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure – external network attacks protection.
- Network IP level security providing bulk security mechanisms on network level between network nodes – external network attacks protection.

These layers are projected in a way that vulnerability of one layer could not compromise the other layers and thus the whole system is not vulnerable.

2.1 Application Level Security Mechanism

Application layer is on top of the OSI (Open System Interconnectivity) server layer model. This layer handles issues like network transparency, resource allocation and problem partitioning. The application layer is concerned with the user's view of network (e.g. formatting electronic mail messages).

Application level security mechanisms are based on asymmetrical and symmetrical cryptographic systems, which realize the following functions:

- Authenticity of the relying parties (asymmetrical systems)
- Integrity protection of transmitted data (asymmetrical systems)
- Non-repudiation (asymmetrical systems)
- Confidentiality protection on application level (symmetrical systems)

Application level security domain consists of the most popular protocols like: S/MIME, PGP, Kerberos, proxy servers on application level, SET, crypto APIs for client-server applications, etc. Most of these protocols are based on PKI X.509 digital certificates, digital signature technology based on asymmetrical algorithms (e.g. RSA, DSA, ECDSA) and confidentiality protection based on symmetrical algorithms (e.g. DES, 3DES, IDEA, AES, etc.) [3]. Most of the modern application level security protocols, such as S/MIME and crypto APIs in client server applications, are based on digital signature and digital envelope technology. Nowadays, the most popular cryptographic protocol on the application level is S/MIME standardized protocol for secure e-mail protection. In modern e-commerce and e- business systems, RSA algorithm is mainly used according to PKCS1 standard which is a part of the PKCS set of de-facto standards describing a method for encrypting data using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, according to the syntax described in PKCS7 standard. There is a lot of work on optimization of RSA algorithm implementation in hardware security module based on signal processor [4], [5], [6]. [7], [8], [9].

For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5, SHA-1, RIPEMD-160, SHA-224, SHA-256, SHA-384, SHA-512), and then an

octet string containing the message digest is encrypted with the RSA private key operation of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS7 to yield a digital signature. It should be pointed that the state-of-the-art solution for all the three security functions, authenticity, data integrity and non-repudiation, could be today achieved only by use of the PKI smart cards with signature generation on the card and where the signature private key is generated on the card and never leaves the card. For digital envelopes, the content to be enveloped is first encrypted by a symmetric encryption key with a symmetric encryption algorithm (such as DES, 3DES, IDEA, AES...), and then the symmetric encryption key is encrypted with the RSA public key of the intended recipient of the content. The encrypted content and the encrypted symmetric encryption key are represented together according to the syntax in PKCS7 to yield a digital envelope. Security systems on application level consist also of the user authentication procedure which could be one, two or three-component authentication procedure.

2.2 Transport Level Security Mechanism

Transport-layer security relies on secure HTTP transport (HTTPS) using Secure Sockets Layer (SSL) since it is provided by the transport mechanisms used to transmit information over the wire between clients and providers. Transport security is a point-to-point security mechanism that can be used for authentication, message integrity, and confidentiality. When running over an SSL-protected session, the server and client can authenticate one another and negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. Security is “live” from the time it leaves the consumer until it arrives at the provider, or vice versa, even across intermediaries. The problem is that it is not protected once it gets to its destination. One solution is to encrypt the message before sending.

Transport-layer security is performed in a series of phases, which are listed here:

- The client and server agree on an appropriate algorithm
- A key is exchanged using public-key encryption and certificate-based authentication
- A symmetric cipher is used during the information exchange

TLS/SSL encryption requires the use of a digital certificate, which contains identity information about the owner as well as a public key, used for encrypting communications. These certificates are installed on a server; typically, a web server if the intention is to create a secure web environment, although they can also be installed on mail or other servers for encrypting other client-server communications.

Transport Layer Security (TLS) Protocol provides privacy and data integrity between two communicating applications.

The protocol composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (TCP) is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- Private - symmetric cryptography is used for data encryption (DES, RC4, etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.
- Reliable - message transport includes a message integrity check using a keyed MAC. Secure hash functions (SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

The TLS Record Protocol is used for encapsulation of various higher level protocols.

TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS Handshake Protocol provides connection security that has three basic properties:

- The peer's identity can be authenticated using asymmetric or public key, cryptography (RSA, DSS, etc.). This authentication can be made optional, but is generally required for at least one of the peers.
- The negotiation of a shared secret is secure: the negotiated secret is unavailable to eavesdroppers, and for any authenticated connection the secret cannot be obtained, even by an attacker who can place himself in the middle of the connection.
- The negotiation is reliable: no attacker can modify the negotiation communication without being detected by the parties to the communication.
- TLS is based on the Secure Socket Layer (SSL), a protocol originally created by Netscape. One advantage of TLS is that it is application protocol independent. The TLS protocol runs above TCP/IP and below application protocols such as HTTP or IMAP. The HTTP running on top of TLS or SSL is often called HTTPS. The TLS standard does not specify how protocols add security with TLS; the decisions on how to initiate TLS handshaking and how to interpret the authentication certificates exchanged are left up to the judgment of the designers of protocols which run on top of TLS.

2.3 Network Level Security Mechanism

The network layer is responsible for packet forwarding including routing through intermediate routers. The network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination host via one or more networks while maintaining the quality of service functions.

Network level security mechanisms include security mechanisms implemented in communication devices, firewalls, operating system security mechanisms, etc. These methods provide the base for understanding of Virtual Private Networks (VPN). The complete IP traffic (link encryption) between two network nodes is encrypted to achieve security protection. The most popular network layer security protocols are: IPSec (AH, ESP, IKE), packet filtering and network tunneling protocols, and the widest used is IPSec. IPSec consists of network node authentication based on asymmetrical cryptographic algorithms and link encryption based on symmetrical algorithms, similar to the transport level security protocols. IPSec is a combination of group of protocols consisting of AH – Authentication Header and ESP – Encapsulated Security Payload protocols in transport and tunnel mode, as well as IKE – Internet Key Exchange. AH is used for authentication of the IP packets, ESP is used for encryption and authentication of the IP packets and IKE is used for node authentication and IPSec session key establishment. For security on the network level, the most often used is the IPSec ESP protocol in tunnel mode, since attacker does not know internal addresses (source and destination) – only public addresses of IPSec gateways could be seen externally. Firewalls could be computers, routers, workstations and their main characteristics is to define which information and services of internal network could be accessed from the external world and who from internal network is allowed to use information and services from the external network. Firewalls are mostly installed at breakpoints between insecure external networks and secure internal network. Depending of the needs, firewalls consist of the one or more functional components from the following set: packet filter, application level gateway, and circuit level gateway. There are four important historical examples of elementary firewalls: Packet Filtering Firewall, Dual-Homed Firewall (with two network interface), Screened Host Firewall, and Screened Subnet Firewall (with Demilitarized Zone – DMZ between internal and external networks).

3. CONCLUSION

In this paper, different mechanism in the modern computer security systems are analyzed. It is concluded that only multilayered security architecture protect internal and external attacks in modern computer networks. Also, the most frequently used security mechanisms on the application, transport and network layers are analyzed to conclude that more than one layer should be covered by the appropriate security mechanisms in order to achieve high quality protection of the system. The analysis is done regarding

security challenges and appropriate security mechanisms with potential vulnerabilities. It is concluded that, appropriate security mechanism can be applied in a way that vulnerabilities of one layer do not affect another layer, thus the whole system is not vulnerable.

REFERENCES

[1] C. Huitema, IPV6: The New Internet Protocol. Englewood Cliffs, NJ: Prentice-Hall, Nov. 1999.
[2] W.Ford, M.S.Baum, Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Second Edition, Prentice Hall PTR, Upper Saddle River, NJ 07458, 2001.
[3] M.Markovi_, "Cryptographic Techniques and Security Protocols in Modern TCP/IP Computer Networks," Short- Tutorial, in Proc. of ICEST 2002, Oct. 1-4, 2002.
[4] B.Schneier, Applied Cryptography, Second Edition, Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc., New York, Chichester, Brisbane, Toronto, Singapore, 1996.
[5] RSA Laboratories: PKCS standards.
[6] T.Unkaševi, M.Markovi, G.Djorevi, "Optimization of RSA algorithm implementation on TI TMS320C54x signal processors," in Proc. of TELSIKS'2001, September.
[7] G.Djorevi, T.Unkaševi, M.Markovi, "Optimization of modular reduction procedure in RSA algorithm implementation on assembler of TMS320C54x signal processors," DSP 2002, July, Santorini, Greece, 2002.
[8] M.Markovi, T.Unkaševi, G.Djorevi, "RSA algorithm optimization on assembler of TI TMS320C54x signal processors," in Proc. of EUSIPCO 2002, Toulouse, France, Sept. 3-6, 2002.
[9] M.Markovi, G.orevi, T.Unkaševi, "On Optimizing RSA Algorithm Implementation on Signal Processor Regarding Asymmetric Private Key Length," in Proc. Of WISP 2003, Budapest, Sept. 2003.

ABOUT AUTHOR

Rajeshwari Goudar received Bachelor Degree from Karnataka University & Post Graduate Degree in Computer Engineering from Kolhapur University, having 15 years of teaching experience, now serving as Associate Professor in MAE Alandi Pune, Maharashtra, India. Research areas of interest are Network Security, Computer Networking, Image Processing and Biometric Cryptography.
Pournima More received Bachelor Degree of Engineering in Computer Technology from Pune University & pursuing Post Graduate degree in Computer Engineering from MAE Alandi Pune University, having 4 years of teaching experience, now serving as Professor in PGMCOE Pune. Research areas of interest are Network Security, Computer Networking.