International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:2, 2008

Domain-based Key Management Scheme for Active Network

Jong-Whoi Shin, Soon-Tai Park, and Chong-Sun Hwang

***Abstract*—**Active network was developed to solve the problem of the current sharing-based network–difficulty in applying new technology, service or standard, and duplicated operation at several protocol layers. Active network can transport the packet loaded with the executable codes, which enables to change the state of the network node. However, if the network node is placed in the sharing-based network, security and safety issues should be resolved. To satisfy this requirement, various security aspects are required such as authentication, authorization, confidentiality and integrity. Among these security components, the core factor is the encryption key. As a result, this study is designed to propose the scheme that manages the encryption key, which is used to provide security of the comprehensive active directory, based on the domain.

***Keywords*—**Active Network, Domain-based Key Management, Security Components.

I. Introduction

THE concept of "active network" was introduced to solve the problem of the current sharing-based network – difficulty in applying new technology, service or standard, and duplicated operation at several protocol layers [1]. The conventional data network performs the function that transports the bit from one end system to another. The operation function on this network is performed at the extremely limited area only such as header processing in the packet switching network, and signal processing in the connection-oriented network.

Active network changes the traditional concept like this, by performing the customized operation. For example, users on the active network are able to transfer the customized compression program to the network node, and request the node to execute the program when processing the packet at the receiving end [2]. Conversely, the active network provides the software framework that enables customization of the communication process to fit into the network application.

The active network loads the executable code that called "capsule" onto the packet when transporting the packet. Depending on execution of this code, the state of the network node can be changed. However, this benefit entails the problem that security and safety should be guaranteed without fail, since the network node is placed in the sharing-based network. To secure security and safety of the active directory, the security requirement should be satisfied such as authentication, authorization, confidentiality and integrity. With regards to these requirements, it involves the encryption key that is the core factor of the security.

Accordingly, this study proposes the scheme that manages the encryption key, which is expected to be used in order to secure security of the extensive active network, based on the domain.

Manuscript received June 30, 2006.

Jong-Whoi Shin (phone:+82 2 405 5256; fax: +82 2 405 5219; e-mail: jshin@kisa.or.kr) and Chong-Sun Hwang (e-mail: hwang@disys.korea.ac.kr) are with Department of Computer Science and Engineering, Korea University, 1, 5ka, Anam-Dong, Sungbuk-Ku, Seoul, Korea. Soon-Tai Park (e-mail: cptpark@kisa.or.kr) is with the Korea Information Security Agency (KISA), 78, Garak-Dong, Songpa-Gu, Seoul, Korea.

II. Security Threats on the Active Network

Compared with the current networks, the active network can be easily exposed to the threat and attack. Since the execution code that changes the network node state is enclosed with the capsule, the receiving node should verify that the packet is received from the authorized sender, and perform the accurate operation for the execution code.

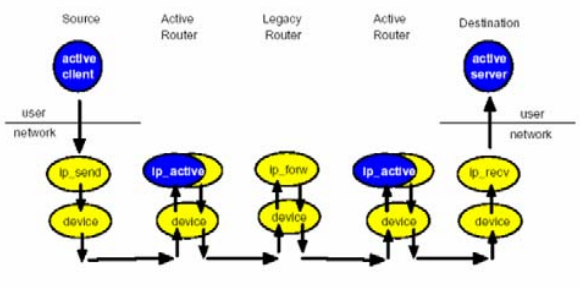

Fig. 1 Application Processing on the Active Directory

As shown in Fig. 1, the possible security threat that may occur during application processing on the active directory include information modification, information disclosure, service stealing, denial of service, and composed attack [3][5].

- Information modification: Modifies the data maliciously without proper privilege.
- Information disclosure: Discloses the information to

the person having on service privilege.

- Service stealing: Unauthorized users access to the service as if they are allowed.
- Denial of service: Intentionally hinders network resource or service, or completely blocks them.
- Composed attack: The most serious threat to the active node, which shuts down the system by consuming all available bandwidths through transmission of the large amount of active packets to the central router.

Especially, the denial of service is hard to handle, and has the following types.

- Consumption of the limited resources: Attack that eats up network connection (TCP-SYN flooding), saturated bandwidth (UDP floods, spoofed ICMP Echo message attack, spam, etc.) and other resources.
- Modification or destruction of the information components
- Physical destruction or modification of the components

III. Security Methods of the Active Network

The traditional concept of "security" includes authentication, access control, and encryption. Active network application and router secure the basis of reliability through mutual authentication, and encryption and digital signature protects integrity and privacy of the active network capsule that contains the code and the data [4]. Security techniques available in the active network environment can be broadly divided into active node protection technique and active packet protection technique [5].

A. Active Node Protection Technique

Techniques for active node protection include active packet authentication, monitoring and control, limitation, and proof carrying code technique.

- Packet authentication technique guarantees the identity using the certificate that is generated by the algorithm like the public key signature algorithm
- Monitoring and control technique uses the reference monitor to limit information, system resource and service that allows the use and access of the active packet.
- Limitation technique prevents the active packet from monopolizing the node resources by putting various limitations such as execution duration of the active packet, scope of the packet-forwarding node, and number of duplicated packets.
- Proof carrying code (PCC) technique transports the certificate of accuracy together with each active packet as a pair.

B. Active Packet Protection Technique

Techniques for active packet protection include encryption and fault tolerance.

- Due to the characteristics of the active packet, packet encryption or decryption at each relaying node should be supported, and the packet path should be modified dynamically. Therefore, the concept of moving encryption is needed since the program transported by the active packet should be decrypted to run in the node, even though it is encrypted [6].
- Fault tolerance technique involves duplication, archiving and redirection. Duplication is to copy the packet to each node, whereas archiving is to save the packet temporarily to cope with node fault. Redirection is to find out the alternative path when the default configured path is disconnected. Duplication and archiving are not the proper method for the network packet since they consumes many memory and bandwidth. Redirection and encryption techniques can have wider application for packet protection, since they basically consumes the CPU cycle only.

IV. Security Methods of the Active Network

A. Concept of "Domain-Based"

The encryption technique of the current network performs encryption for the source and the destination only, even though the entire network path should be protected. However, the active directory requires encryption for the nodes in the middle that needs to access to the content, due to the characteristics of the active packet, since the active packet normally transports the program code and the data at the same time [7].

Considering this characteristics, this study proposes the key management mechanism that configures the target node group, which should run the specific program, among actives nodes (e.g., router or switch) that compose the active directory, and guarantees authentication, access control, integrity, denial blocking, and confidentiality among domain members. The domain-based key management mechanism supports the minimum key update and dynamic management of the members in configuring the domain. Additionally, the overload of the key manager is reduced by separating the domain structure into the control unit and

packet transmission unit, and various threats can be prevented that may occur during active packet transmission. As a general rule, the domain-based key management scheme applies the public key infrastructure for member authentication and packet encryption by default. Applying the public key infrastructure together with the domain-based structure is expected to support more efficient key management, since it has the feature of enhancing efficiency and portability of key management on the active network.

B. Proposing the Key Management Scheme

B.1 Components and System Coefficient

The followings are the system coefficients and components that are used by the scheme.

- DKM_i: Domain key manager i
- DKA_i: Domain key assistant manager i
- DME_{list}: Domain member list
- SDB_i: Sub-domain border i
- N, DMB_i: Node (Router) and domain border i
- ADB_i: Active domain border i
- PKM: Public key manager of each manager and border
- DME_i, DI: Domain member i and initial domain configurator
- AKey: Active key generated by PKM
- K_{P_DKMi}, K_{P_DKAi}: Public key of DKM_i and DKA_i
- K_{P_Bi}: Public key of each Bi
- K_{DKMi_DKAi}: Shared key between DKM_i and DKA_i
- K_{DMEi}: Secret key of domain member DME_i
- K_{DKAi_DMEs}: Shared key with the member that is managed by each DKA_i
- Hdr: Domain identification information
- ID*, Sig*, IP*: Identifier of *, signature and IP address
- M: Packet

B.2 System Protocol

1) Domain initialization stage

1. DKM_i, DKA_i and each border receives its public key certificate from PKM_i through secure unicast channel.
2. Each domain divides the member with DKM_i, and manages the responsible DKA_i hierarchically. When public key certificate is received, managers on the domain start mutual authentication.

2) Domain configuration stage

1. The initial domain configurator (DI) composes the domain member list (DME_{list}), and performs signature in association with its identifier ID_{DI} and then, sends it to PKM_i. $Sig_{DI}(ID_{DI}||DME_{list}) \rightarrow PKM_i$, $DME_{list} = (ID_{DME1}||\ldots||ID_{DMEn})$
2. PKM_i verifies DI and DME_{list} through signature check, and generates AKey for active packet service. However, reliability of AKey is enhanced by providing it to the related border only, when the domain is configured.
3. PKM sends DME_{list} to that domain safely, using the public key.

3) Domain member subscription stage

1. DKM_i generates K_{DKMi_DKAi}, which will be used for secret communication with DKAi within the domain, and sends it to DKA_i safely via unicast channel.
2. Each node that will be subscribed to the domain will be verified by DKA_i, using its signature. Then, it encrypts its secret key K_{DMEi} using K_{P_DKAi}, and sends it safely.
3. DKA_i decrypts the message received from the subscription applicants for encryption and domain member list generation. Then, DKA_i sends the list to DKM_i.
4. DKM_i decrypts and verifies the domain member list received from each DKA_i, and compares it with DME_{list}.
5. DKA_i sends K_{DKAi_DMEs} to each member, using the received secret key $KDME_i$. At the same time, it is also sent to DKM_i and SDB_i safely.

4) Active packet transmission stage

1. Each member encrypts the active packet "M," using K_{DKAi_DMEs} and sends it to the border SDB_i. $K_{DKAi\_DMEs}(M) \rightarrow SDBi$

2. SDB_i decrypts the encrypted receiving information to check Hdr. If it is not present, it encrypts the active packet "M" with AKey and sends it to each SDB_i'.

3. Each $SDB_{i'}$ decrypts the received information, and encrypts it using the shared key of the domain to which it belongs and then, sends it to the domain member.

4. Member of each sub-domain $DME_{i'}$ decrypts the information received by $K_{DKAi\_DMEs'}$ to check the message. Transmission of other messages is performed, based on the above-described protocol.

5) New member subscription and withdrawal stage

1. For new member subscription, take the same steps as described in 3) Domain member subscription stage.

2. When the current member withdraws, DKA_i updates the key by generating a new $K_{DKAi\_DMEs'}$ and transferring it to the remained members ($DME_{i'}$, DKM_i, and SDB_i).

V. Conclusion

This study proposed the scheme that enables to manage the encryption key based on the domain, which is the core element of various functions that are provided for security and safety of the active network such as authentication, confidentiality, and integrity. The proposed key management scheme is expected to allow more efficient key management than the current one, by managing the key in the vast active network, based on the domain. Various further studies are needed including development of the mechanism that resets a setting key after a certain period of time when the key management setting is configured, development of the efficient key sharing mechanism, and performance test on the domain-based key management using the test best.

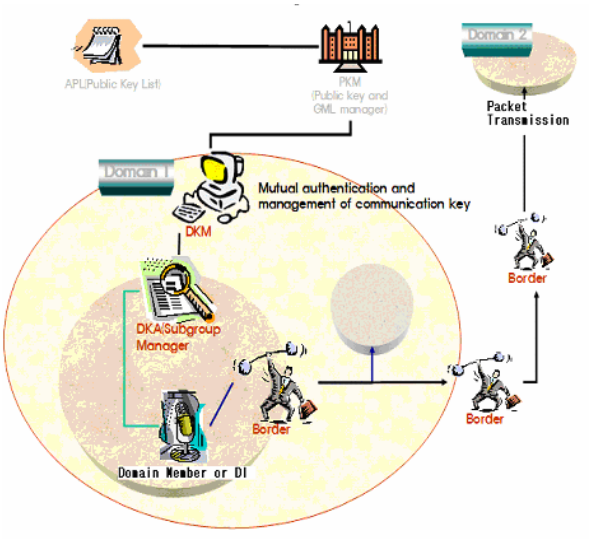

Fig. 2 Structural Diagram of the Proposed Key Management Scheme

References

[1] David L.Tennehouse, et al., *"A Survey of Active Network Research"*, IEEE Com. 1997.
[2] David L. Tennenhouse and David J. Wetherall, *"Towards an Active Network Architecture"*, Comp. Commun. Rev. vol 26, no 2, Apr. 1996.
[3] AN Security Working Group, *"Security Architecture for Active Nets"*, Jul. 1998, Modified by Seraphim Group, May 2000.
[4] Roy H. Campbell, et al., "Seraphim: Dynamic Interoperable Security Architecture for Active Networks", IEEE OPENARCH 2000.
[5] K. Psounis, "Active Networks: Applications, Security, Safety, and Architectures", IEEE Communication Surveys, 1999.
[6] J.M. Park, K.J. Chae, *"Active Network Security Technology Trend"*, Sigcomm Review, Dec. 2000.
[7] Y.S. Kim, J.C. Na, S.W. Sohn, *"A Secure Method for Transferring Active Packets"*, Proc. of WSEAS'01, Cairns, Australia, Dec.17 ~ 21. 2001.