Host-Oblivious Security for Content-Based Networks

Jongmin Jeong
Seoul National University
jmjeong@mmlab.snu.ac.kr

Ted "Taekyoung" Kwon
Seoul National University
tk@mmlab.snu.ac.kr

Yanghee Choi
Seoul National University
yhchoi@mmlab.snu.ac.kr

ABSTRACT

Network-level security systems rely significantly on network operations. This reliance has led to conventional network-level security systems based on a host-centric architecture because the network operations themselves are based on hosts. However, host-dependent network security schemes are no longer applicable in content-based networks.

In this paper, a host-oblivious network security paradigm for content-based networks is introduced, and then a comprehensive security procedure focusing on generating and sharing diverse secret keys is proposed. Then the proposed scheme, which provides not only essential security functions but also diverse security levels, is discussed. Finally, how this multiple security-level approach helps reducing inevitable performance overhead caused by implementing security functions is demonstrated.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*distributed networks, network communications*

General Terms

Security

Keywords

Content-centric networks, security, security-level

1. INTRODUCTION

Communication networks have matured in either an evolutionary or a revolutionary manner. For example, due to network interoperation, networks can accommodate heterogeneous applications such as an instant messaging, game and entertainment, healthcare, and vehicular services using a single device. Emergent identity-free content-centric networks are representative of the latter. Because the initial IP-based Internet accounted for data sharing only among a limited number of hosts, it imposed various restrictions on supporting diverse applications. In a clean-slate approach to overcome these architectural limitations, content-based networks are considered an alternative. Based on the common features of both examples, we envision that content will become an essential keyword in future networks.

Network-level security relies considerably on every aspect of network operations - the physical capacity of the infrastructure and entities, topology and its dynamics, protocol and its various operations, and different types of application data. Such reliance has led conventional network security mechanisms to follow a host-centric paradigm. In effect, a security association including a security key and cryptographic algorithm is generated based on the host information. Once a security association is established, regardless of the diverse security sensitivity of various application data, networks maintain a single security association for hosts until a session is disconnected. As a result, a host-based architecture has not provided diverse security strength for diverse contents. Moreover, because of the comprehensive revolution in network architecture, such a conventional host-dependent security scheme cannot be structurally deployed in host-oblivious content-based networks. Accordingly, we take into account the new network-level security paradigm, which is host-oblivious and capable of diverse security associations, for future content-based networks.

There are several challenges to consider before the new network security architecture is realized: 1) quantitatively defining multiple security levels; 2) indicating a required security level for specific contents to networks; 3) generating diverse security associations. The foremost crucial work will be in generating and sharing multiple security associations among entities because they present a major problem to solve in order to achieve the new approach.

In this paper, host-oblivious security procedures that provide multiple security levels for diverse contents are proposed. Since the most important element in a security association is a secure key, this paper, simply equates a security association to a security key. Since defining and indicating security levels for networks are inevitable requirements, the basics of these issues are discussed. Then brief evaluations of the proposed scheme from both security and network performance points of view are provided.

CFI '10 June 16–18, 2010, Seoul, Korea

The concept of a host-oblivious network security (HONS) is clarified, and some challenges for HONS are described in Section 2. Then in Section 3, the practical HONS scheme is proposed. In Section 4, the proposed scheme is evaluated. The conclusion is stated in in Section 5.

2. HOST-OBLIVIOUS NETWORK SECURITY

2.1 Definition

We distinguish a host-oblivious network security paradigm from a conventional host-dependent network security from two perspectives, a host-oblivious security association and multiple security levels.

Host-dependent network security (HDNS) results from conventional networks themselves, which are operated using a host-based architecture. A source initiates communication on the assumption that the source is able to identify a destination. Due to awareness of the destination, for cryptographic functions, the source simply uses a shared symmetric secret key or a public key of the destination. Because the destination also can identify the source, a security association for the both node is easily established. That is, regardless of the diversity of the application data, only a single security level based on the identity of hosts is provided during the entire communication.

There are two basic principles of the host-oblivious network security (HONS). The first is that a security association is independent from the host identification, which is caused by blindness of hosts in content-based network architecture. The second is provision of multiple security associations for diverse security-sensitivity of the various contents.

2.2 Advantages of the HONS

The HONS not only overcomes weaknesses of the HDNS for security of content-based networks but provides several advantages:

2.2.1 Immunity from Key Exposure

The fatal weakness of the host-based key and single security-level occurs in a case of key exposure in communication. Because the HONS dynamically changes security association, which is independent from not only a host but also previously used keys, it tolerates key exposure. Only the contents in a single broken session are revealed.

2.2.2 Improved Security Functions

The HONS guarantees security functions that the HDNS provides such as message confidentiality, message integrity, and node authentication. In addition, because of the host-oblivious key association, the HONS supports source and destination anonymity.

2.2.3 Overhead Diminution

Minimizing the overhead is a difficult challenge in network-security. Since security functions require additional operations in both process and networks, the overhead from the network performance point of view cannot be avoided. The stronger security function is implemented and the more contents are encrypted, the more overhead occurs. However, this does not mean that massive data always need stronger security. In content-based networks, the massive multimedia data might be used for publicity, for example. In this case, a lower security level can be applied. As a result, compared with HDNS, HONS can reduce overhead without loss of security functions.

Table 1: An Example of the Security-levels. DES (Data Encryption Standard), TDES (Triple DES), AES (Advanced Encryption Standard), ECB (Electronic Code BOOK mode) and CBC (Cipher Block Chaining mode)

	Cryptographic Parameters(quantitative)		
	Key length	Algorithm	Refreshment
Level 1	128	DES-ECB	1 month
Level 2	128	DES-CBC	1 week
Level 3	256	TDES-ECB	1 week
Level 4	128	AES-CBC	1 day
Level 5	256	AES-CBC	3 hour
Level 6	512	AES-CBC	1 hour

2.3 Security-levels

A security level decides security parameters in a security association. The higher the security-level required, the stronger the cryptographic primitives used. Discretely mapping a security-level for the content might be a relatively easy process. The reason is that this is a classifying and allocating process based on available information such as user preference and common sense in the security sensitivity of data. However, quantitatively defining a security level itself in network security is a very complex problem because various environments such as cryptographic parameters and abilities of adversary and network architectures affect security strength. This is not a simple matter of just comparing key length as several network security experts have recognized. Without the exact key, an adversary may acquire the plaintext or other meaningful information from the encrypted data. For future networks accommodating heterogeneous contents and networks, quantitatively defining security levels is especially invaluable for not only designing but also formally analyzing network-level security schemes.

Since the focus of this paper is on host-oblivious security association and security procedures rather than quantitatively defining security levels, trivial example of defining security-levels by combining security functions and cryptographic parameters is demonstrated in Table 1. The longer the key and the more complex the cryptographic algorithms are used, the more the security level is guaranteed.

2.4 Host-oblivious Key Association

Negotiating multiple secret-keys is the key point in security for content-based networks. Furthermore, such multiple keys should be independent from each other and a host-dependent key.

Generally, a method to generate a session key between two hosts is classified in two groups. One group uses an asymmetric crypto-algorithm like the Diffie-Hellman scheme [1]. The other group uses common security materials with the

assumption that nodes are able to share security materials in advance. In order to use an ID-based asymmetric cryptography such as a public key infrastructure (PKI) certificate, a host should know the destination in advance, which is in contradiction to host-oblivious content-based networks. Therefore, this paper focuses on the method of using common security materials.

We take a note of the random pool-based (RPB)[2] scheme for the host-oblivious and mutually independent multiple secure associations. The RPB scheme is one of the predeployed based key distribution schemes proposed for sensor networks. In RPB, a key distribution center (KDC) manages a key pool of keys. Before node deployment, the KDC randomly selects several keys out of the key pool for each sensor node. Then the KDC distributes them to the sensor node. When two sensor nodes want to generate a link key, they exchange the index of keys. In case two nodes share at least one key, they use one of the commonly shared keys as a link key. Chan et al. extended the basic RPB to q-composite random pool (q-RPB) scheme[3]. Compared with the basic RPB scheme, q-RPB scheme requires both nodes to share at least q numbers of keys. The final link key is generated by combining q numbers of common keys. Although q-RPB scheme makes a sacrifice in success rate in sharing a link key, it improves resilience against the node compromise attack. Such RPB schemes are probabilistic. Therefore, they are often estimated to be less efficient than deterministic schemes such as symmetric matrix-based and symmetric polynomial-based and location-based schemes. However, since most deterministic schemes are based on a host-identity, they are not applicable to host-oblivious content-based networks. Ironically, such a probabilistic and host-oblivious key generation is a very useful and efficient approach for the new network paradigm. We adopt the q-RPB scheme as a basic key association scheme. A KDC is in control of a set S of random keys out of the total key space. Each node acquires m keys from S in registration phase. Denoted are S keys of the KDC and m keys of the node by a key pool (KP) and a key ring (KR), respectively.

3. HONS ARCHITECTURE

3.1 Network Model

A KDC that distributes a key ring to a host is adopted. As a trust entity, the KDC shares a symmetric key with each node. For simplicity, a single management domain is considered. That is, every node receives the KR from the single KDC. Of course, when real deployment is taken into consideration, several issues associated with the KDC arise - how to share the key pool and generate a trust-relationship between inter-domain KDCs, for example.

A broadcast-based architecture[4][5] for forwarding a content request is recommended. A requestor broadcasts the INTEREST packet to neighbors. A neighbor having the content sends data to the source through the reverse path. The INTEREST packet is re-broadcasted to next-hop neighbors until either it reaches a node that has contents or the Time-To-Live (TTL) indicator is expired. Based on a value of the security-level (SL), we assume nodes can be aware of which cryptographic parameters should be used.

3.2 Procedures

We propose three phases for secure transmission of the contents: Registration, Request and Reply:

3.2.1 Registration

A node acquires a KR from a KDC. A host can maintain secure channel with the KDC using a symmetric key during the registration.

Step 1. A host requests for m-number of keys, $KR = \{K_i\}^m$, for $K_i \in KP$ to the KDC.

Step 2. Using a symmetric key-based authentication algorithm like challenge handshake authentication [6], the KDC and a host mutually authenticate each other. Then, the KDC sends the KR, $AUTH_X = \{KDC\_ID||nonce_X\}_{K_p}$ and nonce_X to the host X. $AUTH_X$ is a signature of the KDC, which indicates a node X is authenticated by the KDC. $nonce_X$ is to specify a node X, which plays a role of the pseudo-ID of X. KDC_ID is the identity of the KDC and K_p is the private key of the KDC.

3.2.2 Request

Step 1. A requestor randomly selects q-number of the key in his or her KR and generate a $key = \text{hash}(\{k_i\}^q)$ for $k_i \in KR$. The value of q is decided by the security-sensitivity of the content.

Step 2. A requestor broadcasts the INTEREST packet to neighbors. The INTEREST packet is broadcasted until it reaches a responder having not only contents but also q-number of the keys. $KeyIndex$ is the set of index of q-number of keys. It does not need to be successive.

INTEREST : {INTST, $\text{AUTH}_X, T\}_{key}$, HMAC_{key}, $nonce_X$, SL, KeyIndex, TTL, IID

Encryption of the $INTST$ is optional. Since the INTEREST packet does not include a requestor ID, privacy for the requestor is already provided. However, a strong adversary may infer a requester and content by combining $INTST$ with other information. For example, if the purpose of $INTST$ is to find a home-delivery service for the specific package to the address, a strong adversary can infer the identity of the requestor through both a non-encrypted destination address and a package description. $AUTH_X$ and T should be encrypted for preventing the replay attack. Table 2 concretizes each field constituting the INTEREST packet.

3.2.3 Reply

Whenever a host receives the INTEREST packet, if TTL is not expired, she or he runs following processes:

Step 1. If the host has every key in $KeyIndex$, she or he produces the $key = \text{hash}(\{k_i\}^q)$.

Step 2. The host verifies $AUTH_X$ with a public key of the KDC to check whether she can see the correct KDC_ID and the identical $nonce_X$ with non-encrypted $nonce_X$ in INTEREST.

Step 3. The host checks whether he or she has contents.

Table 2: Description of the INTEREST

INTST:=	Description of content interests
KeyIndex:=	Index of randomly selected q number of keys
key:=	Symmetric key, which is output of a one-way hash function on input q-number of the keys
$HMAC_{key}$:=	A hashed MAC(message authentication code) of the INTEREST combining with the key
IID:=	ID of the INTEREST packet
SL:=	Indicator of the security level
TTL:=	Time-to-Live to avoid loop or the exhaustive search
T:=	Packet generation time for anti-reply attack
$\{M\}_K$:=	Encrypted message M with the key K

Step 4. If so, the host, Y sends the content to the requester by encrypting it using a cryptographic algorithm based on the SL value. If either step 1 or 3 fails, the host reduces TTL by one and broadcasts it to his or her neighbors.

RESPONSE: {DATA, $\text{AUTH}_Y\}_{key}$, HMAC_{key}, IID

A RESPONSE packet is relatively simple compared with the INTEREST packet. $DATA$ and $AUTH_Y$ are encrypted with the shared key. $AUTH_Y$ is a signature indicating that the responder Y has been authenticated by the KDC. IID is the INTEREST packet indicator. The HMAC_{key} is for integrity of the RESPONSE. After receiving the RESPONSE, the requestor decrypts it with the shared key. The requester can infer the shared key from the IID.

4. EVALUATION

4.1 Security Analysis

Regardless of networks and system, the essential security functions are confidentiality, integrity and authentication. The proposed scheme provides such necessary security requirements; it also supplies host privacy.

4.1.1 Customized Confidentiality

A request packet in the most conventional broadcast communication - for example, a route request packet in ad-hoc networks - is not encrypted. The main reason is that since a source cannot identify the specific destination, the source does not know which key he or she uses for encryption. The other reason is that a request packet tends to include a much less security-sensitive message than a response packet. However, Even though, the source and destination are unknown in advance, they can share a symmetric key if they have enough shared key material. Therefore, the $INTST$ can be encrypted to avoid the node inference attack. Furthermore, the strength of confidentiality is customized by the q and SL value specified by a user.

4.1.2 Customized Integrity

$HMAC$ contributes to verification of whether the received packet is illegitimately changed in the process. As with confidentiality, $HMAC$ uses the key on input, which means that the security strength of the integrity is customized based on the content.

4.1.3 Authentication

Only a legitimate node that is authenticated by the KDC has a signature of the KDC. Therefore, both responder and requester can implicitly authenticate each other by verifying the $AUTH$ with the public key of the KDC. For the purposes of this paper, authentication requires only verification of whether a host is authenticated by a trust authority. Unlike conventional authentication schemes, the identity of the host does not play an important role.

4.1.4 Privacy

In content-based networks, node IDs can be rationally blurred. Indeed, neither INTEREST nor RESPONSE includes a node ID in our proposal. Even when node IDs are required for a specific purpose such as routing, our scheme can provide node privacy by hiding the ID through the encryption with the key.

4.2 Network Performance

As a preliminary work, this paper simply shows that the diverse security-level approach is effective from network performance point of view. We use the OPENSSL package[6] for measurement on an Intel(R) Xeon 3.00GHz machine. Figure 1 justifies that security strength and the size of content that affects network performance. The bigger a file is encrypted, the more time is required. The remarkable thing is that even though AES provides stronger security than DES, it takes less time for encryption and decryption. We also compare decryption times in similar circumstances. Although the decryption process takes slightly more time than encryption, the shape of the result is identical with those shown in Figure 1. We omit it because of limited space. Table 3 summaries the encryption time of five files of different sizes.

Figure 2 shows a five-security-level scheme that reduces the encryption time compared with a single security-level scheme. For Figure 2, we use a single file, File a in Figure 1. We define level-1, -2, -3, -4, and -5 with AES-ECB-128, AES-ECB-192, AES-CBC-128, AES-CBC-192, and AES-CBC-256, respectively. We also consider five cases that have different content numbers such as 200, 400, 600, 800, and 1000. We assume that the security level of each content follows a normal distribution with mean=3 and standard deviation=0.7. Even though the result varies according to parameters such as the distribution of the security level, the number of level, and the size of content, the common result is that diverse security level schemes are always more efficient than a single-level security scheme.

The hit rate for contents depends on the value of the KP, KR and q. In addition, each value affects the resilience of the key management scheme. Therefore, a rule to select the optimized value must be established. The fortunate thing is that each value for optimized network performance and

Table 3: Various Encryption Time According to the Size of the Content and Cryptographic Algorithms

		Encryption Time (ms)			
	Size (Kb)	DES-ECB	DES-CBC	AES-128	AES-256
File a	95,512	2.108	2.628	0.838	1.01
File b	222,536	5.112	5.101	2.02	2.514
File c	317,739	7.185	7.277	2.647	3.213
File d	1,205,449	31.74	32.022	10.836	13.036
File e	30,817,792	515.101	505.784	335.185	384.234

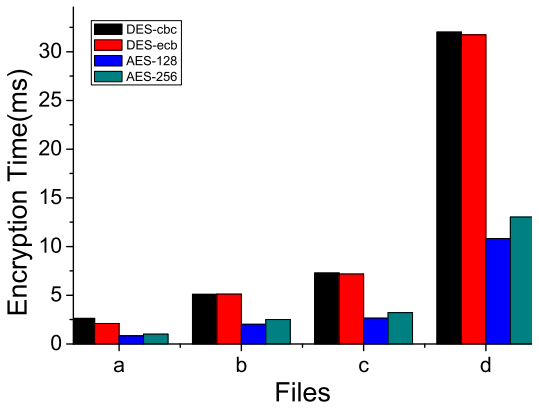

Figure 1: Various encryption time according to the size and cryptography.

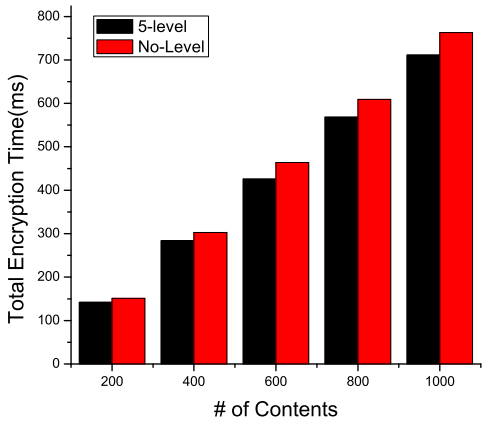

Figure 2: Overhead comparison between the multi-level and single-level security.

security can be adjusted. Given the KP, KR and the value q, Chan et al.[3] analyzed the success rate of the key negotiation between two nodes. They also showed a node-compromised fraction, which is the rate of how much the KR in the compromised node acts to identify a key between non-compromised nodes.

4.3 Further Discussion

4.3.1 Refreshment of the KR

Key is an essential requirement in cryptography regardless of either symmetric or asymmetric cryptography. Since the proposed scheme uses different keys at every request, it can provide very strict key refreshment. However, the refreshment of the KR should be taken into account because the degree of refreshment is decided by refreshment of the KR. Even though q-RPB is stronger than basic RPB against node compromise, a key exposure is still possible. Therefore, a way to regularly update the KR must be found.

4.3.2 Enhancement of the Key Generation Technique

Our proposal is based on the q-RPB schemes. Therefore, we can inherit its advantages such as a host-oblivious and multi-key generation in random. In contrast, some of weaknesses of the q-RPB scheme such as a probabilistic success rate of key generation and secure management of the KR cannot be avoided. An ongoing project is either to improve such weaknesses or design a new key generation technique satisfying various requirements for security in content-based networks.

5. CONCLUSION

Most conventional network-level security schemes use the host-centric approach, especially in generating a key association. Once a security association is established based on the host knowledge, hosts use it for security functions during the entire communication. Therefore, they only support a single security-level regardless of diverse security-sensitivity of contents. Such host-dependent network security mechanisms are not applicable to content-centric networks accommodating diverse data. Accordingly, a host-oblivious network security paradigm and propose secure procedures focusing on the diverse key generation is proposed. In addition, the basic but essential performance gains from both network and security points of view are analyzed. Considering the importance of security for the future Internet, few studies have been conducted in the literature. We assert that our insight and pilot research can stimulate studies in security for future networks.

6. ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government [NRF-2009-353-D00052]. This publication is based on work performed in the framework of the Project COAST-ICT-248036, which is partially funded by the European Community. The ICT at Seoul National University provides research facilities for this study.

7. REFERENCES

[1] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theoryc*, vol. IT-22, Nov. 1976, pp. 644-654

[2] L. Eschenauer and V. D. Gligor. A key-managment scheme for distributed sensor networks. *Proceedings of the 9th ACM Conference on Computer and Communication Security*, Nov 2002, pp.41-47

[3] H. Chan, A. Perrig and D. Song. Random key predistribution schemes for sensor networks. *Proceedings of the 2003 IEEE Symposium on Security and Privacy*. 2003, pp.197

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard. Networking named content. *CoNEXT 2009*, Dec 2009

[5] A. Carzaniga and A. L. Wolf. Forwarding in content-based Network. *Proceedings of ACM SIGCOMM 2003*. Karlsruhe, Germany. August 2003, pp. 163-174

[6] W. Simpson. PPP challenge handshake authentication protocol (CHAP). IETF RFC1994, 1996

[7] OPENSSL, http://www.openssl.org