International Journal of Grid and Distributed Computing
Vol. 5, No. 2, June, 2012

Half-Broadcast Encryption for Anonymity

Jongseok Choi and Howon Kim*
Information Security and System LSI Laboratory,
Computer Engeneering Department,
Pusan National University,
Busan, Korea
{jschoi85,howonkim}@pusan.ac.kr

Abstract

Broadcast Encryption(BE) have been widely used to pay TV, distributed systems and others. In general concept of this encryption, most BE schemes have to broadcast all packets to all network because of intermediate nodes cannot know accurate nodes needing broadcasted packets due to encryption. In this paper, we propose Half-Broadcast Encryption(HBE). Recently, a number of distributed systems have been designed as hierarchical model composed of several levels. In the model, HBE communicates as top-down with reducing $log_w gbn$ traffic than general broadcast encryption. In the proposed scheme, intermediate nodes decides whether they broadcast received packets with protecting anonymity of destinations. For the reason, HBE can reduce the packets over the network to more than half due to flexible broadcasting without any identity of destination.

Keywords: *Cloud computing, key agreement protocol, encryption*

1: Introduction

Recently, distributed systems have been the focus of a number of security experts because of the attention placed by various agencies on cloud and grid computing. As the result there are many studies[1, 2, 3] on distributed systems. Distributed systems are generally composed of a root level and other levels, together forming a hierarchical topology. In a hierarchical model, it is difficult to provide user anonymity because cloud and grid computing are currently based on a unicasting network, which should know the address of a child node before sending the message. A number of authentication schemes have been proposed so far. The well-known SSL Authentication Protocol (SAP)[4] based on the standard X.509 certificate-based PKI framework has low efficiency, because the PKI framework involves communication and computation costs for each node per level; in other words, it needs to communicate and verify the certificate as the count of levels. To overcome this disadvantage, Shamir[5] proposed Identity-Based Cryptography (IBC), which uses user IDs as public keys. However, it is hard to implement the scheme using realistic software or hardware. Boneh and Franklin first proposed Identity-Based Encryption (IBE)[6], making it possible to implement realistic software or hardware by using Weil pairing. Since then,

*Corresponding author

Lim[7] has initially applied IBE to grid computing. Mao et al.[8] proposed an identity-based, certificate-free, non-interactive authentication framework for grid computing. The Private Key Generator (PKG) used in their scheme is the bottleneck of their framework, because private key corresponding to the public key should be maintained by the PKG or trusted agency. To overcome this issue, Lim and Robshow[9] proposed a hybrid approach, combining it with IBC, which removes the non-interactivity and makes the scheme certificate free. Li et al.[10] proposed pairing based on Identity-Based Authentication for Cloud Computing (IBACC). IBACC is more efficient and lightweight than SAP. However the ID-based schemes[11, 12, 13, 14, 15, 16, 17] have abused the identity of nodes as private information. This means that the scheme cannot ensure user anonymity.
In this paper, we propose Broadcast-Based Anonymous Authentication (BBAA) for distributed systems. Our contributions are that the scheme is non-PKI and that it ensures anonymity with a hierarchical network. To achieve the first property, BBAA is based on pairing similar to the IBE of Boneh and Franklin[6]. To satisfy the second property, BBAA broadcasts messages about ownership when the root node needs to communicate with a child node. Intermediate nodes at each level can recognize whether or not the packet is going to their child node. Therefore, the proposed scheme reduces network traffic compared to an all-broadcasting network.

2: Bilinear map

There are two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q. For clarity, we denote $\mathbb{G}_1$ using additive operation and $\mathbb{G}_2$ using multiplicative operation. Somtimes $\mathbb{G}_1$ is also written multiplicatively. We assume that P and Q are two generators of $\mathbb{G}_1$, and the bilinear map used to our scheme has to fully satisfy following properties:

Bilinearity It is satisfactory as following equation.

$$\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_q^*, \qquad \hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab} \tag{1}$$

Non-Degeneracy If everything maps to the identity, that is obviously not interesting:

$$\forall P \in \mathbb{G}_1, P \neq 0 \Rightarrow \langle \hat{e}(P, P) \rangle = \mathbb{G}_2 \tag{2}$$

Computability $\hat{e}$ is efficiently computable.

3: Hierarchical Model for Cloud Computing

In this section we describe a Broadcast-Based Hierarchical Model (BBHM) that comprises multiple levels. In the model, each node has to possess its own ID and a root node should know the IDs of all nodes.
Our BBHM is composed of a root level and multiple sublevels. The root node can know the path from the top level to any node and the public keys and IDs of each node. Note that no node can recognize the IDs of any other node.
In BBHM there is a root node at the 0-level that can know the IDs of all nodes. Each node can have child nodes up to 254, except 0, and 255 in IPv4. If a network is IPv6 or other,

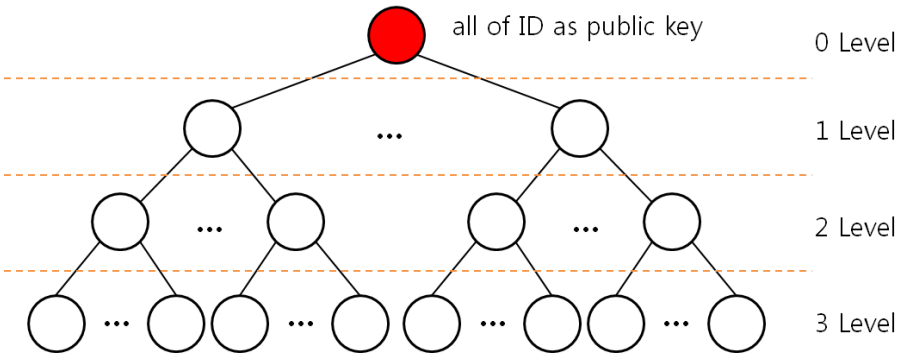

Figure 1. Hierarchical Model

each node can accommodate as many child nodes as the number of available hosts.
In the model, each node that is not a root node has its identity ID. We denote an identity of a node by ID_{order}^{path}. Let a node be the third node in the 4-level and have three parent nodes and a root node. The identity of the node should be $ID_{003}^{002015001}$ if the parent nodes are the second node in the 1-level, the fifteenth node in the 2-level, and the first node in the 3-level, respectively. Note that this does not mean that any node knows the path of a packet.

4: Novel Approach

Private security anonymity of users is currently considered as very important information. The issue also comes up in cloud computing because cloud computing systems make nodes communicate using a unicasting network in which intermediate nodes need to know the child node or destination node. To contend with this issue we propose BBAA. The proposed scheme uses a broadcasting network to protect the anonymity of nodes when a root node communicates with another node.
The proposed scheme has two advantages: 1. It protects the anonymity of users, which means that the proposed scheme does not need to reveal IDs of a node to other nodes, and 2. it is computationally efficient. The scheme is more efficient than SAP because it does not require a PKI framework, which would lead to network traffic and computational overhead. The proposed scheme differs from a general broadcasting network in reducing the amount of network traffic.
In general broadcasting, all nodes communicate with all of their child nodes. Thus, a packet can expand over the whole network when the root node sends a message to a node. Adopting a broadcast network for cloud computing is difficult because of network traffic. If cloud computing uses general broadcasting, the system could take up the entire network traffic whenever the server provides a large data service to the lowest level node. Therefore, it cannot concurrently provide numerous nodes with different services.

In the proposed broadcasting concept, intermediate nodes can know whether packet is going to their child node, although they cannot determine the destination of the packet. This property enables the scheme to cut the amount of network traffic in half.

BBAA is composed of an initialization phase and an authentication phase.

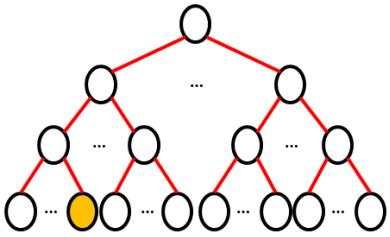

Figure 2. A general broadcast network

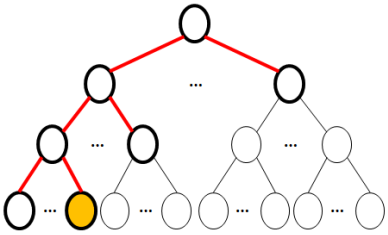

Figure 3. Half-Broadcast Network

4.1: Initialization

During initialization, the root node generates the parameters and distributes these to other nodes. Each node is assigned an ID that is used as a public key. Note that the node IDs are only known to the root node. After initialization, the generated parameters are

$$\langle \hat{e}, G_1, G_2, H_1, H_2, H_3, P, ID, P_{pub} \rangle. \tag{3}$$

Step1 Generate two groups G_1, G_2 of a prime q and a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$.

Step2 Choose a generator $P \in G$ and three functions $H_1 : \{0,1\}^* \rightarrow G_1^*$, $H_2 : G_2 \rightarrow \{0,1\}^n$, $H_3 : \{0,1\}^* \rightarrow G_2$. Let H_3 be a both-way function.

Step3 Assign ID and $level$ to all nodes.

Step4 Generate a public information $P_{pub} = xP$ and public keys of each nodes $n_i P_{pub} = y_i P$ where P_{pub} can be known to every nodes but $n_i P_{pub}$ can be known to the root node and its own node. At this each nodes can recognize their own private key y_i.

4.2: Authentication

The authentication phase is performed by partial broadcasting in which a message can reach its destination by repeatedly broadcasting and authenticating. Note that the scheme does not need to reveal the destination ID. The authentication phase is composed of two concepts: verification and forwarding. Verification decides whether a current node forwards a received message; if the message is not going to a child node of the current node, the node will not broadcast the message. The authentication phase comprises the following steps.

Step1 The root node computes

$$M_i = \langle \hat{e}(\sum_{l=1}^{d} H_1(ID_l), P_{pub}) \hat{e}(S, P_{pub}) \rangle. \tag{4}$$

Where l means a level variable and d is a level of a destination node. Note that only IDs of intermediate nodes between the root node and the destination node is used to the sum; the IDs are the pathway to destination node from the root node. S is a service the root node provide the node with. And i is zero at the root node and will increase as the level.

Step2 The root node computes and parallels following parameters:

$$\begin{gathered} H_2[\hat{e}(\sum_{l=2}^{d} H_1(ID_l), P_{pub})], \\ H_2[(\hat{e}(\sum_{l=3}^{d} H_1(ID_l), P_{pub})], \\ \cdots, \\ H_2[\hat{e}(H_1(ID_d), P_{pub})] \end{gathered} \tag{5}$$

The root node multiply the computed values and $\hat{e}(H_1(S), P_{pub})$ respectively to complete this step. Therefore this step produces the following parameters:

$$\begin{gathered} V_{1,\cdots,d} = \langle H_2[\hat{e}(\sum_{l=2}^{d} H_1(ID_l), P_{pub})] \hat{e}(H_1(S), P_{pub}), \\ \cdots, \\ H_2[\hat{e}(H_1(ID_d), P_{pub})] \hat{e}(H_1(S), P_{pub}) \rangle \end{gathered} \tag{6}$$

Step3 The root node encrypts the service provided to the node as following.

$$C = \langle \hat{e}(H_1(ID_d), P_{pub}) \cdot H_3(S) \rangle \tag{7}$$

Step4 The root node finally broadcasts or sends the following packet to node or nodes in the next level:

$$P_i = \langle M_i, V, \hat{e}(H_1(S), P_{pub}), C, rP \rangle \tag{8}$$

Step5 Nodes verifies the packet whether they have to broadcast to the lower level or not. In the first nodes compute as following.

$$M_{i+1} = \langle \frac{M_i}{\hat{e}(H_1(ID), P_{pub}} \rangle \tag{9}$$

In the next the nodes verify M_{i+1} as following.

$$M_{i+1} = ? V_1 \tag{10}$$

A node proceeds the next step only if the above equation is held; a node which can hold the equation will be only one node.

Step6 The node removes V_1 from P_i and reconstitutes as following:

$$P_{i+1} = \langle M_{i+1}, V_{i+2,\cdots,d}, C, rP \rangle \tag{11}$$

Step7 The proposed scheme repeats Step6 and Step7 up to a destination.

Step8 When the packet arrives at the destination it would compose as following:

$$P_{d-1} = \langle M_{d-1}, V_d, C, rP \rangle \tag{12}$$

The node verifies the packet as Step6 then finally can use the service by decrypting the packet. In order to decrypt it the node computes as following.

$$\frac{C}{\hat{e}(H_1(ID_d), P_{pub})} = H_3(S) \tag{13}$$

Since H_3 is a both-way function, the node can compute a service S.

5: Analysis

In this section, we analyze the effects of the proposed authentication on communication cost, anonymity, and reverse direction request.

5.1: Communication cost

First, to evaluate the scheme we compare it with a general broadcast network. As mentioned, general broadcasting makes use of full network traffic, but BBAA entails partial broadcasting. For the comparison, we assume that the network is formed as a w-balanced tree and the root node provides the lowest node with a service. In general broadcasting, we need bandwidth to send the packet to the end level from the first level where there are w-level nodes; the count of the nodes increases as a high level. Therefore, the network traffic is about

$$PacketSize \times \sum_{i=1}^{endlevel} w^i \tag{14}$$

However, the proposed scheme does not fully broadcast the packet, because intermediate nodes can recognize whether the packet is in their own line or not. This is because the packet decreases at a high level in this scheme, although it is based on the broadcasting network. Traffic is reduced by a factor of $\frac{1}{w}$ compared with that of general broadcasting as the level increases. Therefore, this scheme requires the network traffic to be

$$PacketSize \times w \times endlevel \tag{15}$$

Transforming these two equations to big-O notation, in which m denotes the packet size, we have for the general broadcasting network about

$$O(m \times w^n) \tag{16}$$

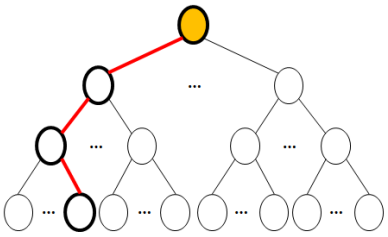

Figure 4. Request to the root node from the lower node

whereas in the proposed scheme we have

$$O(m \times n) \tag{17}$$

To specifically compare the performance between the two schemes, we computed the relationship in which the packet size is treated as a constant. As we saw with the above equation, network traffic is no longer caused by the increasing number of packets; however, the general broadcasting network has to send more packets all over the network. Expressing the general broadcasting network as gbn and the broadcast-based anonymous authentication as bbaa, respectively, we have the following relation.

$$bbaa \cong log_w gbn \tag{18}$$

5.2: Reverse direction request

We have described the general scheme for providing a service in Section 3. Imagine that the lower node wants to request a service from the root node. We would not consider this case because the pathway is only one step from the root node to the request node; we can guess the method for anonymity very easily. For example, the node sends an encrypted packet using the public key of the root node that includes a service name and the ID of the node. Then, intermediate nodes cannot recognize which node is sending the packet using User Datagram Protocol (UDP) because the nodes cannot decrypt the packet.

6: Conclusion

Recently, there has been increasing research interest in cloud computing systems in which a server provides a client with a service, thus resulting in anonymity and compliance issues. However, cloud computing cannot still protect the anonymity of users.
In this paper, we proposed Broadcast-Based Anonymous Authentication to overcome the issue of anonymity. The proposed authentication has three advantages. The first is that it protects the anonymity of a user who receives a service from a server; it is hard to protect anonymity of users in a general hierarchical cloud model, because an intermediate provider can know a pathway and a destination for unicasting. The second advantage is that it removes SAP from cloud computing; the clients and intermediate providers can store some parameters instead of certificates that need to be verified by a certificate authority. The third advantage of BBAA is that there is less network traffic than in a general broadcasting network; the traffic decreases progressively toward the bottom level, because, in the

proposed scheme, the intermediate nodes can intelligently decide whether to forward the packet to the next level.
Our paper can contribute as a starting point to study anonymous authentication in cloud computing. The scheme helps users use cloud computing services without senses on another.

ACKNOWLEDGEMENTS

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0026621).

References

[1] Gul and M. Hussain, Distributed Cloud Intrusion Detection Model, International Journal of Advanced Science and Technology Vol. 34, (2011)

[2] L. J. Yong, Z. L. Chen, Z. Yong and C. Yong, Middleware-based Distributed Systems Software Process, International Journal of Advanced Science and Technology, Vol. 13, (2009)

[3] H. Kim, H. Lee, W. Kim and Y. Kim, A Trust Evaluation Model for QoS Guarantee in Cloud Systems, International Journal of Grid and Distributed Computing, Vol.3, No.1, (2010)

[4] O. Freier, P. Karlton and P.C. Kocher. The SSL Protocol Version 3.0, INTERNET-DRAFT, (1996)

[5] Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology Proceedings of Crypto '84, (1984) August 19-22; Santa Barbara, USA

[6] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil pairing. In Advances in Proceedings of Crypto 2001, (2001) August 19-23; Santa Barbara, USA

[7] H.W. Lim and M. Robshaw. On Identity- Based Cryptography and Grid Computing. Proceedings of International Conference on Computational Science 2004. (2004) June 6-9; Krakow, Poland

[8] W. Mao. An Identity-based Non- interactive Authentication Framework for Computational Grids, HP Lab, Technical Report HPL-2004-96 (2004)

[9] H.W. Lim and M.J.B. Robshaw. A dynamic key infrastructure for GRID, Proceedings of the European Grid Conference (EGC 2005), (2005) February 14-16; Amsterdam, Netherlands

[10] H. Li, Y. Dai, L. Tian and H. Yang. Identity-Based Authentication for Cloud Computing, The 1st International Conference on Cloud Computing 2009, (2009) December 1-4; Beijing, China

[11] Y. Desmedt and J. Quisquater, Public-key systems based on the difficulty of tampering, Advances in Cryptology Proceedings of Crypto '86, (1986) August 17-21; Santa Barbara, USA

[12] D. Huhnlein, M. Jacobson and D. Weber, Towards Practical Non-interactive Public Key Cryptosystems Using Non-maximal Imaginary Quadratic Orders, Selected Areas in Cryptography, (2000) August 14-15; Waterloo, Canada

[13] U. Maurer and Y. Yacobi, Non-interactive public-key cryptography. In Advances in Cryptology Crypto '91, (1991) August 11-15; Santa Barbara, USA

[14] S. Tsuji and T. Itoh, An ID-based cryptosystem based on the discrete logarithm problem. IEEE Journal on Selected Areas in Communication, vol.7. no.4, (1989)

[15] H. Tanaka, A realization scheme for the identity-based cryptosystem. In Advances in Cryptology Crypto '87, (1987) August 16-20; Santa Barbara, USA

[16] S. E. Alaoui, P. L. Cayrel, and M. Mohammed, Improved identity-based identification and signature schemes using Quasi-Dyadic Goppa codes, International Journal of Advanced Science and Technology, Vol. 35, (2011)

[17] Zhang and Q. Xu, An ID-based Anonymous Signcryption Scheme for Multiple Receivers, International Journal of Advanced Science and Technology, Vol. 20, (2010)

Jongseok Choi

He is currently a master's candidate in the Computer Engineering Department, Pusan National University. He received B.S. in Information Security, Tongmyong University, Republic of Korea, in 2011. His researches include mobile security, privacy, public key cryptography.

Howon Kim

received the BSEE degree from Kyungpook National University, Daegu, Rep. of Korea, in 1993, and the MS and PhD degrees in electronic and electrical engineering from Pohang University of Science and Technology (POSTECH), Pohang, Rep. of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Rep. of Korea. He is currently working as an associate professor with the Department of Computer Engineering of Pusan National University, Busan, Rep. of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems and their security issues. He is a member of the IEEE, IEEE Computer Society, and IACR.