Int. J. Communications, Network and System Sciences, **2009, 7, 641-644**
doi:10.4236/ijcns.2009.27072 Published Online October 2009 (http://www.SciRP.org/journal/ijcns/).

An Identifier-Based Network Access Control Mechanism Based on Locator/Identifier Split

Rui TU[1], Jinshu SU[1], Ruoshan KONG[2]
[1]*School of Computer Science, National University of Defense Technology, Changsha, China.*
[2]*International School of Software, Wuhan University, Wuhan, China*
Email: *ruitu@nudt.edu.cn, krs*1024@126.*com*
Received January 5, 2009; *revised May* 15, 2009; *accepted July* 12, 2009

ABSTRACT

Legacy IP address-based access control has met many challenges, because the network nodes cannot be identified accurately based on their variable IP addresses. "Locator/Identifier Split" has made it possible to build a network access control mechanism based on the permanent identifier. With the support of "Locator/Identifier Split" routing and addressing concept, the Identifier-based Access Control (IBAC) makes network access control more accurate and efficient, and fits for mobile nodes' access control quite well. Moreover, Self-verifying Identifier makes it possible for the receiver to verify the packet sender's identity without the third part authentication, which greatly reduces the probability of "Identifier Spoofing".

Keywords: Access Control, Locator/Identifier Split, IBAC, Self-Verifying Identifier, Identifier Spoofing

1. Introduction

In the current TCP/IP architecture, IP address has dual semantic functions, which indicates both the network node's routing locator and its endpoint identifier [1]. It means that the IP address is a variable label related to the location. Because of the "IP Overload" [1], IP address-based access control has met many challenges.

Firstly, IP address-based access control limits the resource access when a node changes its location. Network services often distinguish users by their IP addresses, so many services are bound with the clients' locations. As a result, when a user of an authorized organization moves to another location (and so the IP address is changed.), he will lose the access ability of the service.

Secondly, "IP Overload" makes IP address-based access control even more complex, and greatly affects its defense efficiency:

1) Because IP address is a variable label, it can't be used as an accurate identifier of the nodes. Moreover, "IP Spoofing" has made it even more critical. So it is difficult to identify the access source in the network layer, and the attackers can anonymously attack the network devices and services.

2) IP address can't match users precisely [2]. One IP address can represent different nodes at different time. On the other hand, one IP address can also represent multiple nodes simultaneously (e.g. NAT). As a result, the attacker can hide his true identity easily.

For the above reasons, the efficiency of IP address-based access control is greatly declined, and some misuses will harm the valid users.

Finally, the changes of the network topology and the ISP policies will lead to the reconfiguration of the IP addresses. Thus, many access control rules and configurations based on IP addresses have to be modified. Undoubtedly, this will make the access control management more complex.

The reason of the above drawbacks lies in that there is no accurate, unique and permanent identifier to describe a network node. So the key problem is to resolve the "IP Overload" problem. IAB announced that in order to resolve the "IP Overload", two name spaces should be introduced to denote a network node's locator and identifier separately, which is called "Locator/Identifier Split" [3]. The communication session is based on the permanent Identifier, and the routing is based on the variable Locator.

In this paper, we propose LISA Network Access Control (LISA-NAC) which is a new network access control mechanism based on the Locator Identifier Separation Architecture (LISA) [4]. The main contributions of LISA-NAC are the Identifier Based Access Control (IBAC) model and the Self-Verifying Identifier, which will make network access control more efficient.

The rest of this paper is organized as follows. Section 2 presents an Overview of LISA Architecture. Section 3

describes some new characters of LISA-NAC, including IBAC model and Self-Verifying Identifier. Section 4 gives an outline of our future work. Finally, we conclude with a summary of the main research result in Section 5.

2. LISA Overview

LISA is a network-based "Locator/Identifier Split" naming and addressing architecture, which borrowed come ideas of LISP [5]. As Figure 1 shows, the network is divided into two parts: kernel network and edge network. The kernel network uses Locator name space, while the edge network uses permanent Identifier name space. The communication session is built on permanent Identifier, but the mapped Locator is variable.

LISA adopts "Mapping + Encapsulation" method to process packets. LISA Router (Edge router) maps the Identifier space into Locator space by querying distributed mapping service system based on one-hop hash (LISA-Mapping). Moreover, LISA Router can update the mapping record in the LISA-Mapping. The Identifier space is a new name space (see Subsection 3.2). The Locator space can reuse the legacy IP address space (IPv4/v6), which will avoid updating network devices in the kernel network.

When a LISA Route receives the packet from host, it queries the LISA-Mapping for the matched Locator according to the packet's Identifier. After receiving the mapped Locator, the LISA Router adds a new packet header (including the Locator) to the original packet. So in the encapsulated packet, the inner address is an Identifier, and the outer address is a Locator. LISA uses Identifier to denote the node identity, and uses Locator to forward packet in the kernel network. When the encapsulated packet arrives at the destination (the LISA Router), the LISA Router decapsulates the packet, and forwards the original packet to the destination host according to the Identifier.

3. LISA-NAC

In order to improve the efficiency of network access control, network accountability should be mentioned. Network accountability is the capability to identify network entity (user, host and device) and distinguish maltraffic. However, limited by the "dumb" network infrastructure, it is difficult to achieve accountability in the Internet. There is no accurate, unique and permanent identifier to identify network entity. IP header is too simple, more state information (e.g. identifier) should be added to satisfy the needs of security, QoS and network management.

In the LISA, LISA-NAC runs on the permanent Identifier name space, and provides an accurate and efficient fine-grained access control mechanism for the edge network. The main features of LISA-NAC are the IBAC model and the Self-Verifying Identifier.

3.1. IBAC Model

Different from the traditional network access control, IBAC makes access control policies based on the network node's true permanent Identifier, not IP address or device port.

IBAC includes three entities: Identifier (I), Object (O) and Permission (P). There are two types of Identifiers: Individual Identifier (I^2) and Identifier Affiliation (IA).

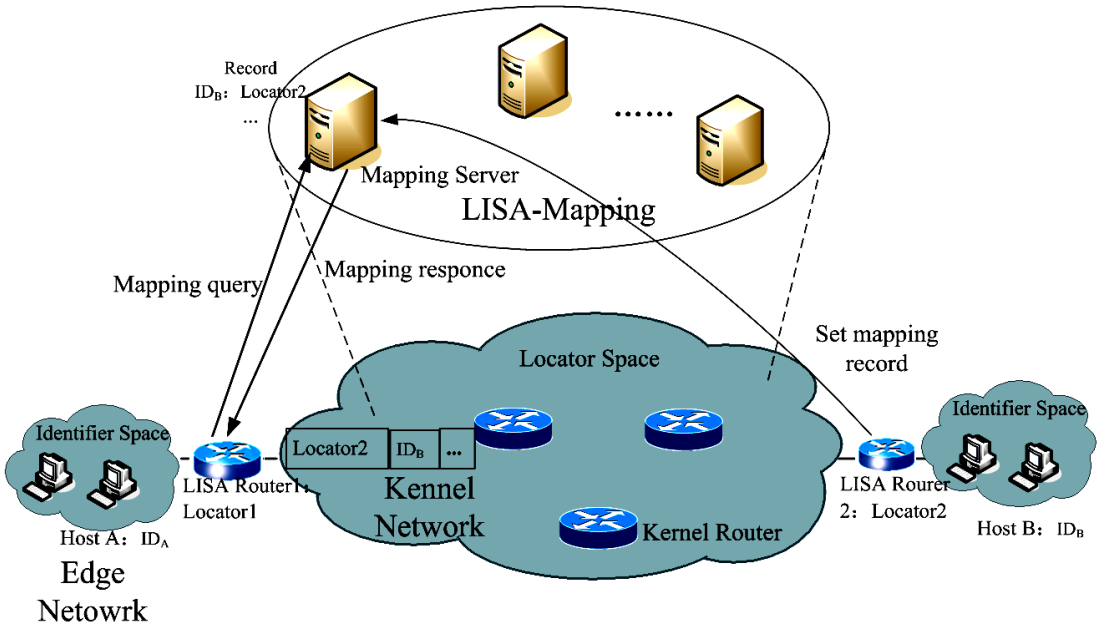

Figure 1. LISA architecture.

I^2 denotes the single network node, and IA denotes a group of network nodes.

IBAC uses three-tuple (I, O, P) to describe an authority. If there exists a (I, O, P), it indicates that I can perform P on the O. Particularly, (I^2, O, P) indicates that single I can perform P on the O, and (IA, O, P) indicates that a group of I can perform P on the O.

IBAC provides end to end security mechanism and fine-grained access control. For example, if several users share a locator (e.g. IP address), IBAC can make independent security policy for everyone. In order to simplify the format of the access control policy and reduce the ACL's size, IBAC uses the IA to classify Identifiers, and adopts unified operation on the Identifiers which have the same IA. IA is not directly in the packet header, and is stored in the LISA-Mapping system. The destination should query the LISA-Mapping system for the matched IA.

IBAC guarantees the access control policy's long term stability. Although the network entities' Locators are variable, the access control policies based on the permanent Identifier are unchanged, so the valid users can always use their services. So IBAC can fit for the mobile node's access control. IBAC avoids the policy updates due to the Locators' changes, and greatly reduces the workload of maintaining the access control policy.

In current network, in order to achieve end to end authority control, network access control should collaborate with the access control mechanisms of the system or application software. Since IBAC guarantees the end to end access control and provides network accountability, it is possible to simplify the upper layer's access control. If the Identifier can be combined with the user's biology properties in the future, the network will be aware of the user's identity and behaviors, and thus no more needs of user's accounts and passwords.

3.2. Self-Verifying Identifier

True Identifier is the basis of IBAC. Similarly, IBAC also meets the potential threat of "Identifier Spoofing". So we introduce "Self-verifying Identifier" in the LISA-NAC. With Self-verifying Identifier, the receiver can verify the sender's identity based on the packet's Identifier without the participation of third part authentication.

In the LISA, every network node gets a pair of asymmetry keys from the CA. The node holds the private key, and makes the public key as the node's globe unique identifier. In other words, the identifier name space is a public key space. LISA-NAC ensures the consistency between the Identifier and the node's identity through the digital signature mechanism.

Self-verifying Identifier simplifies packet's source Identifier verification, and strengthen the scalability because there is no need for the third part authentication. At present, we adopt 160-bit Self-verifying Identifier.

Since the Identifier is actually a public key, we should choose an appropriate asymmetry keys generation algorithm. Traditional asymmetry keys algorithms such as RSA, DSA and Diffie-Hellman often choose long keys to guarantee the key's safety. For example, a normal RSA key is 1024-bit. However, such long key is unfit for the Identifier. Firstly, long identifier increases the packet's size, which may lead to packet fragment and consumes additional bandwidth. On the other hand, since 128-bit Identifier space is enough for current IPv6 network size, it is useless to make a huge Identifier name space.

In the LISA-NAC, we use ECC (Elliptic curve cryptography) algorithm to create a pair of 160-bit asymmetry keys for every network node. ECC's advantages lie in:

1) ECC offers security equivalent to RSA using much smaller key size. For example, ECC 160-bit key offers security equivalent to RSA 1024-bit key [6]. This property will reduce the engineering challenges brought by long key.

2) ECC generates asymmetry keys pair faster than RSA does for the comparable length [7]. Considering the signature generation and verification, ECC's processing speed is much faster than that of RSA [8]. This makes it possible to implement packet digital signature verification with limited packet delay.

At present, 109-bit ECC key has knocked over with brute force. However, the secure 160-bit ECC key is approximately one hundred million times harder to crack than 109-bit ECC key [9]. So we think that 160-bit ECC key can fit the Identifier length, as well as satisfy the basic security requirements.

Figure 2 shows the verification process of Self-verifying Identifier. ID_s and ID_d denote the packet's source and destination Identifier separately. In fact, ID_s and ID_d are the sender and receiver's public key. Dig is the packet's digest. Sig is the digital signature. The receiver identifies the true sender though verifying packet's signature.

If an attacker disguises as the sender and sends a packet, he must have the sender's private key to generate

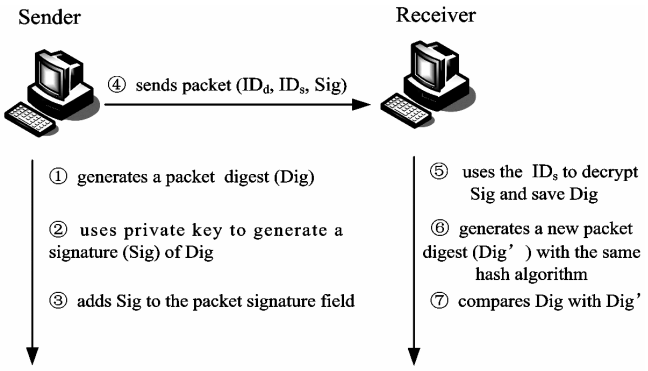

Figure 2. Self-verifying identifier verification.

the correct encrypted signature. Since the attacker doesn't have the sender's private key, when the receiver generates a new packet digest (Dig'), it must be different from the decrypted original packet digest (Dig). So the "Identifier Spoofing" can be detected.

The packet carries the public key, and there is no key exchange during the node identity verification. Obviously, it will simplify the identity verification process. Since network access control is deployed to protect the important services, it is unnecessary to include signature verification in the general packet processing. Most of the network nodes can choose the packet signature verification as an option, but the packet signature is imperative. Moreover, a node can publish its Identifier to the DNS so that all the other nodes can get its public key to encrypt data.

4. Future Work

In the LISA-NAC, verifying signature on every packet will undoubtedly add packet delay. The transmission performance degradation is what we are concerning about. A prototype is under development, and we will measure the main transmission performance (delay, loss and throughput) changes to test the feasibility of LISA-NAC.

At present, Identifier only indicates the network node's property not including the user's property. Next step, we will try to combine the Identifier with the user's biology properties. Then the network will be aware of users' identity and behaviors.

5. Conclusions

LISA separates the network node's identity from location, which makes it possible to build a network access control mechanism based on the identifier. IBAC makes network access control more accurate and efficient. Moreover, IBAC fits for the mobile node's access control. Since true Identifier is the basis of IBAC, "Identifier Spoofing" must be avoided. Self-verifying Identifier makes it possible for the receiver to verify packet sender's identity without the third part authentication, which simplifies the packet source verification. We think that LISA-NAC is a concrete step to strengthen network security through the "Locator/Identifier Split".

6. Acknowledgements

This work was supported by China "863" Project (No. 2008AA01A325) and China National Grand Fundamental Research "973" Project (No. 2009CB320503).

7. References

[1] J. Scudder, "Routing/addressing problem solution space," 2007, http://www.arin.net/meetings/minutes/ARIN_XX/PDF/wednesday/SolutionSpace_Scudder.pdf

[2] R. Tu, J. S. Su, Z. W. Meng, and F. Zhao, "UCEN: User centric enterprise network," in Proceedings IEEE ICACT'08, Phoenix Park, Korea, pp. 66–71, Feb 2008.

[3] D. Meyer and K. Fall, "Report from the IAB workshop on routing and addressing," Internet Draft, 2006.

[4] R. Tu and J. S. Su, "A hash-based locator/ID mapping mechanism," The Computer Engineering and Science, No. 1, pp. 9–12, 2009.

[5] D. Meyer, "The locator identity separation protocol (LISP)," The Internet Protocol Journal, Vol. 11, No. 1, pp. 23, 2008

[6] A. J. Menezes, "Elliptic curve public key crytosystems," Kluwer International Series in Engineering and Computer Science, 1993.

[7] N. Jansma and B. Arrendondo, "Performance comparison of elliptic curve and RSA digital signature," Technical Report, 2004. http://www.nicj.net/files/498termpaper.pdf.

[8] Certicom Corp, "The elliptic curve crypto system for smart cards," Certicom White Paper, 1998, http://www.comms.scitech.susx.ac.uk/fft/crypto/ECC_SC.pdf.

[9] W. Chou and Laerence, "Elliptic curve cryptography and its applications to mobile device," Project Report, University of Maryland, 2003, http://www.cs.umd.edu/Honors/reports/ECCpaper.pdf.

