SAJET

South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 68–72

ISSN No: 2454-9614

ACL Based Dynamic Network Reachability in Cross Domain

P. Nandhini [a], K. Sankar [a*]

[a)] Department Of Computer Science and Engineering (With Specialization in Networks),
Vivekanandha Institute of Engineering and Technology for Women,
Tiruchengode, Tamilnadu, India.
[b)] Department Of Computer Science and Engineering,
Vivekanandha Institute of Engineering and Technology for Women,
Tiruchengode, Tamilnadu, India.

*Corresponding Author: P. Nandhini
E-mail: nandhu3091992@gmail.com,

Received: 14/11/2015, Revised: 20/12/2015 and Accepted: 25/02/2016

Abstract

Network reach ability is designed for accepting end-to-end network behavior. Quantify network reach ability within one administrative domain is a complicated problem. The problem of quantifying network reach ability across multiple administrative domains is more complicated. It helps in identify violation of security policies across the network because the privacy of security policies of individual administrative domains is a serious concern and needs to be protected through this process. Here proposed the first cross-domain privacy-preserving protocol for quantifying network reach ability. The protocol constructs the representations of the Access Control List (ACL) rules and determines network reach ability while preserving the privacy of the individual ACLs. This protocol can determine the network reach ability along a network path through different administrative domains. Our protocol have implemented and evaluated on both real and synthetic ACLs. Two ACLs each containing thousands of rules the comparison time is less than 6s and total communication cost is less than 2100 KB. The online processing time of an ACL containing thousands of rules is less than 25s.

Keywords: Cross domain, Network reaches ability quantification, Privacy preserving.

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Network reach ability for a given network path from the source subnet to the destination subnet is defined as the set of packets that are allowed by all network devices on the path. Several critical concerns like router misconfiguration, policy violations, and service availability can be verified through an accurate quantification. Quantifying network reach ability is a difficult and challenging problem for two reasons.

Control Lists (ACLs), dynamic routing, and network address translation (NAT), have been deployed on network devices for restricting network reach ability. To perform an accurate analysis, administrators need to collect all the reach ability restriction information from these network devices. Collecting such information is very difficult due to the privacy and security concerns. Second, the explosion of the Internet has caused an increase in the complexity and sophistication of these devices, thus making reach ability analysis computation all expensive. Keeping the reach ability restriction information private is important for two reasons.

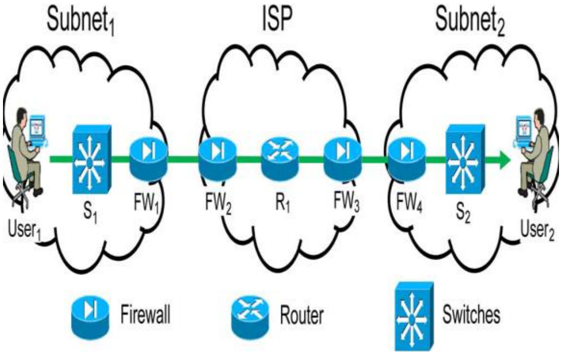


Fig. 1. Example of end-to-end network reachability

First, such information is often misconfigured and has security holes that can be exploited by attackers if it is disclosed. In reality, most firewall policies have security holes [10]. Disclosing ACLs allows attackers to analyze and utilize the vulnerabilities of subnets along a given path. For example, if ACLs along a path from Subnet1 to subnet 2do not block some worm traffic, attackers can break into subnet2 from subnet1 In practice, neither ISPs nor private networks disclose their ACLs. Second, the reachability restriction information of a network device contains private information, e.g., the ACLs of a network device contain the IP addresses of servers, which can be used by an attacker to launch more targeted attacks.

2. **Cross Domain Network Reachability**

Cross-domain approach of network reachability can be very useful for many applications. We illustrate this using two example scenarios. First, a global view of the network reachability can help ISPs to define better QoS policies to improve traffic management. For example, the data of the different paths through which a particular type of traffic is allowed by the ACLs can help the ISPs to maintain a rated list of the best-quality paths in case of path failures. Second, since network reachability is important for many companies that provide their services over the Internet, performing a privacy-preserving estimation of the network reachability could become a new business for the ISPs and other parties involved in this computation. The ISPs can answer the reachability queries of these companies using this global knowledge and even provide some information the quality of various paths. To our best knowledge, no prior work has addressed the problem of privacy-preserving network reach ability quantification. Keeping the reachability restriction information private is important for two reasons. First, such information is often misconfigured and has security holes that can be exploited by attackers if it is disclosed. In reality, most firewall policies have security holes. Disclosing ACLs allows attackers to analyze and consume the vulnerabilities of subnets along a given path.

Privacy- preserving cross- domain network reachability quantification have implemented and evaluated our protocol on both real and synthetic ACLs. The experimental results show that the online processing time of an ACL with thousands of rules is less than 25 seconds; the comparison time of two ACLs is less than 6 seconds and the communication cost between two ACLs with thousands of rules is less than 2100 KB. The Advantages are Streamlines the supply chain from point of origin to point of sale. Reduces labour costs through less inventory handling. The Limitations are Potential partners may not have the necessary storage capacities. An adequate transport fleet is needed to operate.

The key challenges in network reachability include misconfiguration of ACLs, changes of routing policies, and link failures, which could prevent accessibility to essential network services. To estimate reachability, existing approaches analyze ACLs while considering other critical parameters like dynamic routing policies, packet transforms, and variations in protocol operations.

2.1 Technical Challenges

There are four key challenges in the privacy-preserving quantification of network reachability.

1. Protecting the privacy of the ACL rules is crucial. Since a rule has to be sent to other parties to enable comparison, it is necessary to propose a protocol that will not reveal the rule but still allows the different ACLs to calculate the intersection.

2. Computing the reachability information when ACLs are updated is an important performance-related issue. It is necessary to explore optimization approaches in such scenarios without sacrificing the privacy of individual ACLs.

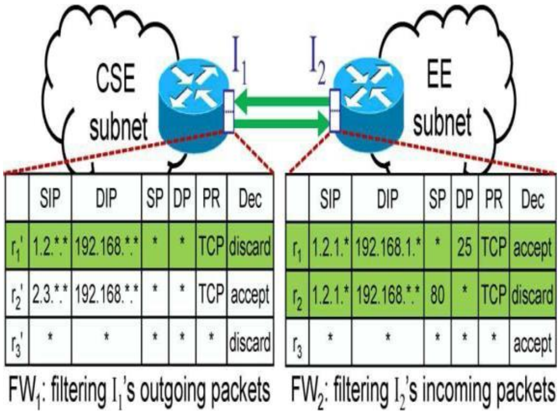
3. Communication cost is high as even calculating the intersection of a small number of ACLs is a tedious process and requires a number of messages to be exchanged among different parties.

4. It is computationally expensive. An ACL may consist of many rules, and each rule consists of multiple fields. Therefore, comparing multiple ACLs with a large number of rules can be quite expensive, even if only a few ACLs are involved in the process.

3. Cross Domain Inter Firewall Optimization

Cross domain privacy-preserving inter-firewall optimization focus on removing inter-firewall policy redundancies in a privacy-preserving manner. Consider two adjacent firewalls 1 and 2 belonging to different administrative domains Net1 and Net2. Let FW1 denote the policy on firewall 1's outgoing interface to firewall 2 and FW2 denote the policy on firewall 2's incoming interface from firewall 1. For a rule r in FW2, if all the packets that match r but do not match any rule above r in FW2 are discarded by FW1, ruler can be removed because such packets never come to FW2.

Fig. 2 illustrates inter-firewall redundancy, where two adjacent routers belong to different administrative domains CSE and EE. The physical interfaces connecting two routers are denoted as I1 and I2, respectively. The rules of the two firewall policies FW1 and FW2 that are used to filter the traffic flowing from CSE to EE are listed in two tables following the format used in Cisco Access Control Lists. Note that SIP, DIP, SP, DP, PR, and Dec denote source IP, destination IP, source port, destination port, protocol type, and decision, respectively. Clearly, all the packets that match r1 and r2 in FW2 are discarded by r′1 in FW1. Thus, r1 and r2 of FW2 are interring firewall redundant with respect to r'1 in FW1.



	SIP	DIP	SP	DP	PR	Dec
r_1'	1.2.*.*	192.168.*.*	*	*	TCP	discard
r_2'	2.3.*.*	192.168.*.*	*	*	TCP	accept
r_3'	*	*	*	*	*	discard

FW_1: filtering I_1's outgoing packets

	SIP	DIP	SP	DP	PR	Dec
r_1	1.2.1.*	192.168.1.*	*	25	TCP	accept
r_2	1.2.1.*	192.168.*.*	80	*	TCP	discard
r_3	*	*	*	*	*	accept

FW_2: filtering I_2's incoming packets

Fig. 2. Example inter-firewall redundant rules

4. Privacy-Preserving Protocols

Similarity join consists of grouping pairs of records whose similarity is greater than a threshold, *T*. Privacy preserving protocols for similarity join are used to protect the data of two sources from being totally disclosed during the similarity join process. Protocol to perform similarity join using phonetic encodings, which proposed a privacy preserving record matching protocol on both data and schema levels, which concentrated on the e health applications and its intrinsic.

To our knowledge, the existing privacy preserving protocols for similarity join, concentrated only on the syntax representation of the values, and did not consider the semantic relationships among them. Besides, in our previous work, we showed that the similarity join performance would be improved considerably when using long attributes as join attributes, instead of short attributes.

5. Approach

We propose the first cross-domain privacy-preserving protocol for quantifying network reachability. We note that the domains could be connected through multiple ISPs, or they could be independently administered domains within the same ISP.

The following are our key contributions.

1) We propose the first cross-domain privacy-preserving protocol to quantify network reachability across multiple domains. Our protocol can accurately compute the intersection of the rules among the ACLs along a given network path without the need to share these rules across those domains. This is the first step toward privacy-preserving quantification of network reachability, and it can be extended to other network metric measurements that are sensitive in nature. Furthermore, we propose an optimization technique to reduce computation and communication cost of our protocol. It reduces the number of ACL encryptions and the number of messages from to $O(n^2)$to O(n).

2) We describe an approach to handle ACL updates in an effective manner.

3) We conducted extensive experiments on both real and synthetic ACLs, and the results show that our protocol is efficient and suitable for real applications.

5.1 ACL Technique

5.1.1. ACL pre-processing

In the first phase, we transform all the ACLs into an equivalent representation, firewall decision diagram (FDD), and then extract the non overlapping rules with accept decisions.

5.1.2. ACL encoding and encryption

In the second phase, to perform privacy-preserving comparison, we reduce the problem to that of computing privacy-preserving intersection of two numerical ranges.

5.1.3. ACL comparison

In the third phase, the destination ACL computes the intersection of its non overlapping rules with the rules from its adjacent ACL, and then the adjacent ACL further repeats this computation with its neighbouring ACL until the source ACL is reached.

5.1.4. Optimization

Finally, all the ACLs collaboratively decrypt the encrypted intersection of the non overlapping rules, but only the first party (with the source ACL) obtains the result. To reduce the computation and communication cost, we use the divide-and-conquer strategy to divide the problem of computing reach ability of ACLs to the problem of computing reach ability of three ACLs. This optimization technique reduces the number of ACL encryptions and the number of messages in our protocol from $O(n^2)$to $O(n)$.

6. Conclusion

In this paper, we addressed the problem of confidentiality-preserving quantification of network reachability across different domains. Protecting the confidentiality of access control configuration is important as the information can be easily abused. We propose an efficient and secure protocol to quantify the network reachability accurately while protecting the privacy of ACLs. We use the divide- and-conquer strategy to decompose the reachability computation, which results in a amount reduction of the computation and communication costs. To validate our protocol, we conducted the experiments on both real and synthetic ACLs. Network reachability quantification is an important requirement for effective network management. It has a number of applications like organization verification and discovery of security vulnerabilities in network.

References

[1] F. Chen, B. Bruhadeshwar, and A. X. Liu, “Privacy-preserving cross-domain network reachability quantification,” in *Proc. IEEE ICNP*, 2011, pp. 155–164.

[2] A. X. Liu and F. Chen, “Privacy preserving collaborative enforcement of firewall policies in virtual private networks,” *IEEE Trans.Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 887–895, May 2011.

[3] F. Chen, B. Bruhadeshwar, and A. X. Liu, “Cross-domain privacy-preserving cooperative firewall optimization,” *IEEE/ACM Trans. Netw.*, vol. 21, no. 3, pp. 857–868, Jun. 2013.

[4] A. X. Liu and F. Chen, “Collaborative enforcement of firewall policies in virtual private networks,” in *Proc. PODC*, 2008, pp. 95–104

[5] J. Cheng, H. Yang, S. H. Wong, and S. Lu, “Design and implementation of cross-domain cooperative firewall,” in *Proc. IEEE ICNP*, 2007, pp.284–293.

[6] Al-Shaer.E, Marrero.W, El-Atawy.A., and ElBadawi.E, “Network Configuration in a box: Towards end-to-end Verification of Network Reachability and security,” in *Proc. IEEE ICNP*, (2009), pp. 123–13.