Department of Electrical Engineering,
Syed Babar Ali School of Science and Engineering,
Lahore University of Management Sciences, Lahore, Pakistan

Senior Year Design Project (Sproj) Proposal

"ADDRESSING PRIVACY CONCERNS IN WIDE AREA NETWORKS"

Submitted by

Student Name 1: Faizan Safdar Ali **Roll No: 17100152**

Student Name 2: M. Muqsit Nawaz **Roll No: 17100259**

Under the supervision of

Dr. Fareed Zaffar
Designation:
Email:

Signatures of Approval

Project Advisor:

Project Co – Advisor(s) (if any):

Contents

1 Abstract

During the last few years, thousands of medium-to-large Internet Exchange Points (IXP) have emerged around the world. They operate a route server and offer its use as a free value-added service to their members. Original architects of IXPs and SDX (next generation Software Defined Exchange Points) paid less attention to accountability and security. Hence, this poses fundamental questions regarding the privacy concerns of confidential business information that is exchanged between members and Route Server (RS) services. Due to such reasons, Autonomous Systems (ASes) deter from providing intra-domain routing information, consequently resulting in an un-optimized traffic engineering. We have designed IXP++, a domain privacy-preserving security mechanism that employs homomorphic encryption and private set intersection in complex networks with SDXs to prevent leaking of crucial business information. For the future work, we are intended to extend this idea to more Wide area networks and data centers where this kind of communication and traffic engeneering takes pleace.

2 Introduction

With newer Internet Exchange Points (IXPs) being established every day for mutual benefits of Autonomous Systems (ASes) involved, new privacy concerns arise. There are currently some 350+ Internet Exchange Points (IXPs) worldwide, and some of the largest and most successful IXPs have more than 500-600 members and carry as much traffic as some of the global Tier-1ISPs. Due to being densely connected physical components in today's Internet, many of them have started to use route servers (RSes) as a free valued-added service to their members. An RS greatly simplifies routing for its members, that is, most members use an IXP's RS to establish multi-lateral peerings as compared to bi-lateral peerings.

Our main aim is to answer the question of verifiability i.e. the questions for example, whether the chosen route was the best one available, or whether it was consistent with the networks peering agreements, and privacy of crucial information (for example the route policies of the ASes) in SDXes. Since more and more IXPs are moving towards SDXes, we believe that implementing IXP++ in a software defined environment is the most viable option. When we want to exchange intra-domain routing information for the purpose of verifiability and an optimized route selection, privacy concerns arise and some network administrators avoid it for precisely this reason. For example a couple of Internet providers in the Nairobi central business district offered to host the IXP. The challenges were (1) how to choose between the two ISPs and (2) the high levels of dissatisfaction expressed by the other ISPs about having to trust a competitor to handle the IXP without seeking for itself an undue advantage.

3 Problem Statement

A. Routing Problem from the characteristics of BGP

In BGP, Autonomous Systems (ASs) are abstracted as a node in a graph as shown in figure 2 due to confidentiality of intra-domain information, e.g., link quality, routing, flow info, policies etc. The problem with this approach is that traffic engineering by one AS can send flows over bad paths in neighboring ASs as explained in following high level problem statement.

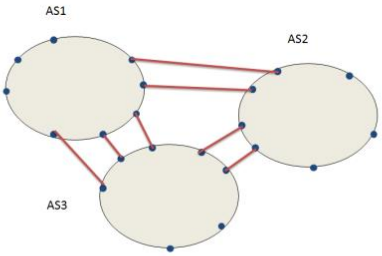

Fig. 2. Routing Problem

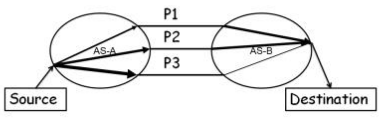

Fig. 3. High Level Problem Statement

B. Inter-domain Routing Problem

As shown in figure 3, In Autonomous System (AS) A, the path associated with peering point P3 has most available bandwidth path and choosing this path will have direct impact of overloading on the link in AS-B. We have to design a technique so that neighboring domains conduct traffic engineering cooperatively in a scalable fashion without having to reveal confidential intra-domain information? Preventing this from happening requires that, sl, the available bandwidth on any link in B after traffic engineering by A, should be non-negative.

C. Information leakage problem

The second major problem is we cannot believe on single entity SDX which has all the (export) policies information made by autonomous systems. To get rid of these problems we propose our solution below, which requires no extra hardware or software.

4 Related Work

The work most related to ours is [2], which used SMPC (Secure Multi-Party Computation) to solve the privacy preservation problem in an IXP setting. But we are talking about SDXes which expands the horizons and hence we can use intra-domain routing information for making informed decision rather than blindly implementing policy. Detailed discussion on SDX and secure internet routing has been presented in [3][4]. [5] proposed a routing security with privacy protections. [6] presented verifying global invariants in multi-provider distributed systems. Verifying network-wide invariants in real time is presented in [7]. Traffic engineering between neighboring domains is done in [8]. A survey of interdomain routing policies is discussed in [9]. [10] proposed private and verifiable interdomain routing decisions. [11] This paper basically talks about the privacy concerns that arise when a large number of ASs are participating in an IXP. At IXPs, we have two different types of peerings: bilateral and multilateral. An RS is used to minimize the number of BGP sessions (using multilateral peering)

and to ease the exchange of BGP announcements among multiple members. An RS establishes BGP sessions with each of the IXP members for collecting and distributing routes, according to some **export policy**, which must be revealed to RS first. This information is considered confidential due to commercial reasons and hence should be protected.

5 Design and Implementation

Our proposed model provides following guarantees:

1) SDX does not know about policies information made by different ASs because all policies will be encrypted. (Addressing ‘information leakage problem')

2) ASs will conduct traffic engineering in a scalable fashion without having to reveal confidential intra-domain information. (Addressing ‘lack of knowledge about congestion in neighboring ASs’ and ‘bad intra-domain traffic engineering decision problem’)

3) Proof of concept protocols using homomorphic encryption and PSI that verify global invariants ensuring safe traffic engineering and verify policy safety in inter-domain routing.

For this purpose, our global invariant is a triplet, which consist of encrypted load demands requests, available bandwidths from all ASs and function which provides above guarantees using one of our proposed model.

6 Project Goals and Objectives

Our main aim is to make the both type of exchange points more flexible, efficient and secure when it comes to sharing critical data between the two autonomous systems. Moreover, our project will concentrate on implementing this idea on all the networks which come under the scope of Wide Area Networking.

7 Proposed Timeline

Sproj-1 …….. Try implementing the basic encryption on exchange points

Sproj-2 …….. Extending this idea to other WANs.

8 References

1. Peering at Peerings: On the Role of IXP Route Servers
2. Towards Securing Internet eXchange Points Against Curious onlooKers
3. S. Goldberg, "Why is it taking so long to secure internet routing?" Communications of the ACM, vol. 57, no. 10, pp. 56–63, 2014.
4. A. Gupta, L. Vanbever, M. Shahbaz, S. P. Donovan, B. Schlinker, N. Feamster, J. Rexford, S. Shenker, R. Clark, and E. Katz-Bassett, "Sdx: A software defined internet exchange," in Proceedings of the 2014 ACM conference on SIGCOMM. ACM, 2014, pp. 551–562.
5. A. J. Gurney, A. Haeberlen, W. Zhou, M. Sherr, and B. T. Loo, "Having your cake and eating it too: Routing security with privacy protections," in Proceedings of the 10th ACM Workshop on Hot Topics in Networks. ACM, 2011, p. 15.
6. S. Machiraju and R. H. Katz, "Verifying global invariants in multiprovider distributed systems," in Proc. SIGCOMM Workshop on Hot Topics in Networking (HotNets), 2004, pp. 149–154.
7. A. Khurshid, W. Zhou, M. Caesar, and P. Godfrey, "Veriflow: verifying network-wide invariants in real time," ACM SIGCOMM Computer Communication Review, vol. 42, no. 4, pp. 467–472, 2012.
8. J. Winick, S. Jamin, and J. Rexford, "Traffic engineering between neighboring domains," 2002.
9. P. Gill, M. Schapira, and S. Goldberg, "A survey of interdomain routing policies," ACM SIGCOMM Computer Communication Review, vol. 44, no. 1, pp. 28–34, 2013.
10. M. Zhao, W. Zhou, A. J. Gurney, A. Haeberlen, M. Sherr, and B. T. Loo, "Private and verifiable interdomain routing decisions," in Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication. ACM, 2012, pp. 383–394.
11. Towards Securing Internet eXchange Points Against Curious onlooKers