Poster: Securing Software Defined Internet Exchange Points (SDXs)

Muhammad Muqsit Nawaz
LUMS
17100259@lums.edu.pk

Faizan Safdar Ali
LUMS
17100152@lums.edu.pk

Muhammad Fareed Zaffar
LUMS
fareed.zaffar@lums.edu.pk

Usman Nazir
LUMS
usman.nazir@gmail.com

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 SDX++, a domain privacy-preserving security mechanism that employs homomorphic encryption and private set intersection in complex networks to prevent leaking of crucial business information.

CCS CONCEPTS

•**Networks** → *Security protocols; Network privacy and anonymity;*
•**Security and privacy** → **Privacy-preserving protocols;**

1 INTRODUCTION

With newer Internet Exchange Points (IXPs) being established every day for mutual benefits of Autonomous Systems (ASes), 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 [1]. Due to being densely connected physical components in todayfis Internet, many internet exchange points have started to use route servers (RSes) as a free valued-added service to their members. An RS greatly simplifies routing for its members because they can establish multilateral peerings (i.e. one-to-many) with RS as compared to bi-lateral peerings (i.e. one-to-one) with every other member[7]. Even though many internet exchange points have started to employ Software Defined Networking (SDN), the basic architecture of having a RS at the heart of the exchange point remains the same.

A members first establishes physical connectivity with the IXP network and it announces the set of IP prefix destinations for which it is willing to receive traffic and it starts receiving route announcements from the chosen members of the IXP[6]. Border Gateway Protocol (BGP) is used to advertise as well as select the routes used to reach prefixes among pair of exchange points members or between a member and a RS. The RS establishes a BGP session with each of the IXP members, collects and distributes their BGP announcements according to each memberfis export policy, i.e., the set of other IXP members that are allowed to receive the route announcement originated by a member[6].

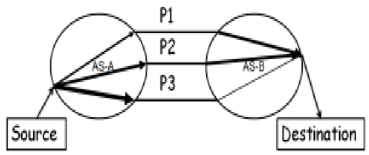

Figure 1: A sends traffic to B via P3 resulting in overloading B's link

2 PROBLEM STATEMENT

Existing inter-domain routing protocols can verify validity properties about individual routes, such as whether they correspond to a real network path[3]. But, it is often useful to verify more complex properties relating to the route decision procedure for example, whether the chosen route was the best one available, or whether it was consistent with the network peering agreements. However, it is difficult to do so without knowing a networkfis intra-domain routing state which is not normally disclosed due to security concerns, resulting in an fiUnoptimized Traffic Engineeringfi. Moreover, a RS which eases the flow of traffic in an exchange point also proves to be a major entry barrier for many ASes. Each memberfis export policy must be revealed to the exchange point in order to correctly forward the BGP announcements. This information is considered confidential, primarily due to commercial reasons[6]. These aforementioned scenarios give rise to fiInformation Leakage Problemfi which deters somes ASes from subscribing to the RS.

2.1 Unoptimized Traffic Engineering

As shown in figure 1, there are three paths available from AS A to AS B. Without knowing the intra-domain routing state of B, A might send its traffic over a path over which B has lesser available bandwidth. Even though the path associated with peering point P3 has most available bandwidth for A, choosing this path will have the direct impact of overloading on the link in B. Therefore, we need to design a technique using which ASes can perform optimized traffic engineering in a cooperative fashion without compromising intra-domain routing information.

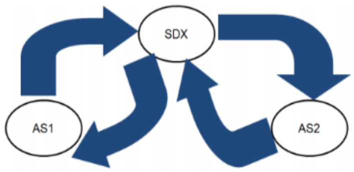

Figure 2: Proposed solution

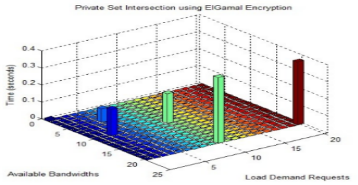

Figure 3: Simulation

2.2 Information Leakage Problem

On higher level, ASes implement their business policies on an SDX controller as forwarding rules. These rules represent business relationships of ASes which is why they must be protected from holistic ASes who can exploit them to their business advantage. An SDX controller which is a centralized entity in many cases is known to be susceptible to many attacks including fiMan in the middlefi and fiMalware Insertionfi attacks. These attacks can greatly compromise the crucial information stored at the controller.

3 DESIGN

In this paper, we show how the ASes connected to a SDX can verify a number of nontrivial properties about inter-domain routing decisions without leaking confidential information. Two ASes who have peering agreements can now provide information such as available bandwidth about their intra-domain routing which will result in better traffic engineering. Moreover, the confidential business information stored at the RS will now be preserved which greatly mitigates the security concerns of ASes. Our proposed model provides the following guarantees:

(1) SDX does not know about business policies of different ASes because all policies will be encrypted (Addressing fiInformation Leakage Problemfi)
(2) ASes will conduct traffic engineering in a scalable fashion without having to reveal confidential intra-domain information. (Addressing fiUnoptimized Traffic Engineeringfi)

We have implemented proof of concept protocols using homomorphic encryption and Private Set Intersection (PSI) which verify global invariants ensuring optimized traffic engineering and business policy preservation. For this purpose, our global invariant is a triplet, which consist of encrypted load demands requests, available bandwidths from all ASs and a function ensuring above guarantees using our proposed model. This is given by the equation 1:

$$s_l = a_l - \sum \delta_{i,j}\mu_{i,j,l} \geq 0 \forall l \tag{1}$$

4 IMPLEMENTATION

We implemented our scheme using two approaches:

4.1 Proposed Model Using Homomorphic Encryption

As shown in figure 2, we consider the case of two Ass with SDX. AS1 uses homomorphic public-key encryption and provides its public key to SDX and AS2 using its out-of-band relationship. The basic idea behind this protocol is that SDX can verify the membership of the remaining bandwidth (RBW) sl as shown in equation 2 in the randomly permuted set (RPS) provided by AS1. The notations are explained in the table II

$$s_l = a_l - \sum \delta_{i,j}\mu_{i,j,l} \geq 0 \forall l \tag{2}$$

AS1 send encrypted bandwidth E(BW) and RPS to SDX to verify ABW. AS2 sends the encrypted load demand δ to SDX to establish link with AS1. The protocol is as follows:

- AS1 sends available bandwidths (ABWs) EA(al) to SDX.
- AS2 sends load demand EA(-δ) to SDX.
- SDX compute the products (RBWs) EA(sl) for various values of EA(al) by the homomorphic property.
- SDX then checks the value that belong to the RPS and selects that link for B to send traffic.
- The RBWs can also be used to serve other load demands requests. In this whole process SDX doesnfit know the load demand, ABWs and RBWs.

4.2 Proposed Model Using Private Set Intersection (PSI)

In this model, SDX will use the PSI based on Oblivious Transfer (OT) protocol [5] and selects the AS1 link which is suitable for AS2 load demand request. The protocol [5] is as follows:

- AS1 and AS2 jointly choose an RSA modulus n = pq, such that neither knows its factorization. Let $\phi()$ be Eulerfis totient function. They can do so using any generic secure computation.
- Furthermore using this secure protocol they generate the following exponents: d1; d2; e; and f. The exponents are generated, such that (d1 + d2)e = f(modϕ(n)). These exponents are distributed as follows: SDX obtains e; AS1 obtains d1 and f; AS2 obtains d2 and f.
- AS1 submits $\acute{\vec{x}} = x_1^{d1}, \dots, x_v^{d1}(modn)$. AS2 submits $\acute{\vec{y}} = y_1^{d1}, \dots, y_v^{d1}(modn)$.
- SDX computed the cross-product. $\acute{z} = \acute{\vec{x}} \times \acute{\vec{y}} = (\acute{x}_1\acute{y}_1)^e, \dots, (\acute{x}_v\acute{y}_w)^e$.
- AS1 computes $\ddot{x} = x_1^f, \dots, x_v^f(modn)$. AS1 and SDX engage in a regular, private set intersection protocol with the sets $\ddot{x}$ and $\vec{z}$, respectively. For each element in the intersection $\ddot{x} \cap \vec{z}$, AS1 adds the respective element from $\vec{x}$ to the result set. AS2 performs the corresponding operations using his set $\vec{y}$.

Table 1: NOTATIONS USED FOR TEST SCRIPT

Variable	Description	Private to
d_i, $1 \leq i \leq D$	Unique Destination Prefixes	None
p_j, $1 \leq j \leq P$	Peering points between AS1 and AS2	None
$a_l; \vec{A} = (a_1, \ldots, a_n)$	Links in AS1	AS1
$u_{i,j,l}; \vec{U}_{i,j} = (u_{i,j,l})_l$	1 if route to dest. d_i from p_j uses link a_l, 0 otherwise	AS1
s_l, $1 \leq l \leq N$	Remaining bandwidth on link a_l of AS1	AS1
$\delta_{i,j}; \vec{\Delta} = (\delta_{i,j})_{i,j}$	Load demand from destination d_i at p_j	AS1, AS2

5 EVALUATION

PSI execution times are shown in figure 3. Proposed model using homomorphic encryption takes O(1) and proposed model using PSI takes O(n) time.

6 RELATED WORK

Privacy preservation problem in an IXP has been Discussed by Chiesa et al., however, their work is limited to securing business policies using the Secure Multiparty Computation (SMPC)[6]. On the other hand, we are taking the network view at SDXs into account due to which our scheme also prevents unoptimized traffic routing. Gupta et al. has talked about SDX[1] in detail and a detailed discussion on secure internet routing has been presented by S. Goldberg[3]. A. J. Gurney has proposed a routing security with privacy protections[2]. J. Winnick has talked about traffic engineering between neighboring domains[4].

7 CONCLUSION

REFERENCES

[1] M. Shahbaz S. P. Donovan B. Schlinker N. Feamster J. Rexford S. Shenker R. Clark A. Gupta, L. Vanbever and E. Katz-Bassett. 2014. Sdx: A software defined internet exchange. *ACM conference on SIGCOMM.* (2014), 551–562.

[2] W. Zhou M. Sherr A. J. Gurney, A. Haeberlen and B. T. Loo. 2014. *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 p. 15.

[3] S. Goldberg. 2014. Why is it taking so long to secure internet routing?. In *Communications of the ACM Vol 57.* 56–63.

[4] S. Jamin J. Winick and J. Rexford. 2012. *Traffic engineering between neighboring domains.*

[5] F. Kerschbaum. 2012. Collusion-resistant outsourcing of private set intersection. *in Proceedings of the 27th Annual ACM Symposium on Applied Computing. ACM* (2012), 1451–1456.

[6] Marco Canini Michael Schapira Thomas Schneider Marco Chiesa, Daniel Demmler. 2016. Towards Securing Internet eXchange Points Against Curious onlooKers. *ANRW* (July 2016).

[7] Anja Feldmann Nikolaos Chatzis Jan Boettger Walter Willinger Philipp Richter, Georgios Smaragdakis. 2014. Peering at Peerings: On the Role of IXP Route Servers. *IMC Vancouver, BC, Canada* (November 2014). DOI: http://dx.doi.org/10.1145/2663716.2663757