IXP++: Towards Securing IXPs

AUTHOR ONE, AUTHOR TWO, AUTHOR THREE

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.

1. 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 [1]. 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 multilateral peerings (i.e., one-to-many) as compared to bi-lateral peerings (i.e., one-to-one) [1]. A members first establishes physical connectivity with the IXP network and then it announces the set of IP prefix destinations for which it is willing to receive traffic and starts receiving route announcements from the other members of the IXP [2].

Border Gateway Protocol (BGP) is used to spread and select the routes used to reach prefixes among pair of members or between members and a RS. The RS establishes a BGP session with each of the IXP members, collects and distributes their BGP announcements according to each member's export policy, i.e., the set of other IXP members that are allowed to receive the route announcement originated by a member [2].

Our main aim is to answer the question of verifiability and privacy of crucial information (both business and intra-domain routing related) 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. We talk about our concerns in detail:

Verifiability: 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 networks peering agreements. However, this

is difficult to do without knowing a networks routing policy and full routing state, which are not normally disclosed.

Privacy: Even though an RS eases the flow of traffic in an IXP, there's a major entry barrier for many IXPs due to which they prevent subscribing. Each member's export policy must be revealed to the IXP in order to correctly forward the BGP announcements. This information is considered confidential, primarily due to commercial reasons [2]. Apart from that, 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. In this paper, we are trying to propose solution to how the Centralized Controller in SDXs (acting as a Route Server) can allow the ASs connected to it to verify a number of nontrivial properties about inter-domain routing decisions without leaking confidential information. If all the properties hold, the peers learn nothing beyond what the inter-domain routing protocol already reveals; if a property does not hold, at least one peer can detect this and prove the violation. Furthermore, since we are ensuring privacy the two ASs who have peering agreements can provide information about their intra-domain routing which will result in better traffic engineering.

2. 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

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.

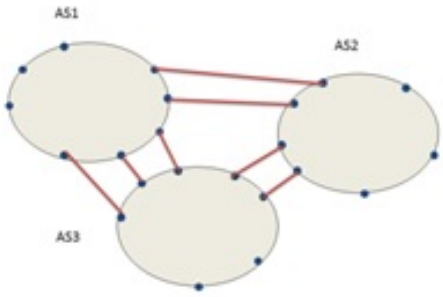

Fig. 2. Routing Problem

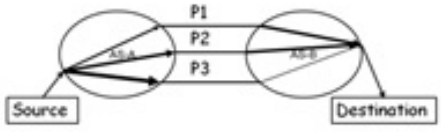

Fig. 3. High Level Problem Statement

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. DESIGN

Our proposed model provides following guarantees:

- SDX does not know about policies information made by different ASs because all policies will be encrypted. (Addressing 'information leakage problem')
- 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')
- 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, given by the equation 1:

$$G = (\delta_i, j, [a_l, b_l, \ldots], f()) \quad \textbf{(1)}$$

5. IMPLEMENTATION

We implanted our scheme using two approaches:

A. Proposed Model Using Homomorphic Encryption

As shown in figure 5, 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

$$s_l = a_l - \sum \delta_{i,j} \mu_{i,j,l} \geq 0 \forall l \quad \textbf{(2)}$$

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 doesn't know the load demand, ABWs and RBWs.

B. Proposed Model Using Private Set Intersection (PSI)

In this model, SDX will use the PSI based on Oblivious Transfer (OT) protocol [11] and selects the AS1 link which is suitable for AS2 load demand request. The protocol [11] is as follows:

- AS1 and AS2 jointly choose an RSA modulus n = pq, such that neither knows its factorization. Let $\phi()$ be Euler's 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 $\vec{\acute{x}} = x_1^{d1}, \ldots, x_v^{d1}(modn)$. AS2 submits $\vec{\acute{y}} = y_1^{d1}, \ldots, y_v^{d1}(modn)$.
- SDX computed the cross-product. $\acute{z} = \vec{\acute{x}} \times \vec{\acute{y}} = (\acute{x_1}\acute{y_1})^e, \ldots, (\acute{x_v}\acute{y_w})^e$.
- AS1 computes $\ddot{x} = x_1^f, \ldots, x_v^f(modn)$. 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 $\vec{x} \cap \vec{z}$, AS1 adds the respective element from $\vec{x}$ to the result set. AS2 performs the corresponding operations using his set $\vec{y}$.

6. EVALUATION

PSI execution times are shown in figure 6. Proposed model using homomorphic encryption takes O(1) and proposed model using PSI takes O(n) time.

7. DISCUSSION

TO be done

8. FUTURE WORK

TO be done

9. REFERENCES

Following are the 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.