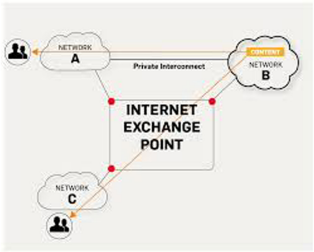
IXP++: Towards Securing IXPs

Muhammad Muqsit Nawaz, Faizan Safdar Ali, Dr. Muhammad Fareed Zaffar, Waqar Aqeel, Usman Nazir
LUMS School of Science and Engineering Pakistan



1 Problem Statement

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. There are following three main components of our promlem statement

A. Routing Problem from the characteristics of BGP

Fig-1 : Routing Problem

In BGP, Autonomous Systems (ASs) are abstracted as a node in a graph as shown due to privacy 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.

B. Inter-domain Routing Problem

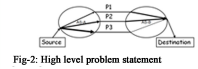


Fig-2: High level problem statement

As shown in figure 2, In Autonomous System (AS) A, the path associated with peering point P3 has most a vailable bandwidth 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 s calable 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. Detailed discussion on SDX and secure internet routing has been presented in many papers. There have been efforts in Verifying network-wide invariants in real time. Traffic engineering between neighboring domains is alsodone. A survey of interdomain routing policies is discussed. Some proposed private and verifiable interdomain routing decisions.

2 Proposed Solution

The proposed solution provides the following guarantees : (1) SDX does not know about policies information made by different ASs. (2) ASs will conduct traffic engineering in a scalable fashion without having to reveal confidential intradomain information. (3) Proof of concept protocols using homomorphic encryption and PSI

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:

$$G = (\delta_{i,j}, [a_l, b_l, ...], f()) \quad (1)$$

As shown in figure 4, we consider the case of two ASs with SDX. AS1 uses homomorphic public-key encryption and provides its pu -blic key to SDX and AS2 using its out-of-band relationship. The basic idea is SDX can varify the bandwith using the equation 2

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

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:
1) AS1 sends available bandwidths (ABWs) $E_A(a_l)$ to SDX.
2) AS2 sends sends load demand $E_A(-\delta)$ to SDX.
3) SDX compute the products (RBWs) $E_A(s_l)$ for various values of $E_A(a_l)$ by the homomorphic property.
4) SDX then checks the value that belong to the RPS and selects that link for B to send traffic.
5) 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:
1) 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.
2) Furthermore using this secure protocol they generate the following exponents: $d1, d2, e$, and f. The exponents are generated, such that $(d1 + d2)e = f(mod\phi(n))$. These exponents are distributed as follows: SDX obtains e; AS1 obtains $d1$ and f; AS2 obtains $d2$ and f.
3) AS1 submits $\overrightarrow{x}' = x_1^{d1}, ..., x_v^{d1}(modn)$. AS2 submits $\overrightarrow{y}' = y_1^{d2}, ..., y_w^{d2}(modn)$.
4) SDX computes the $v \times w$ cross-product $\overrightarrow{z} = \overrightarrow{x}' \times \overrightarrow{y}' = (x_1'y_1')^e, ..., (x_v'y_w')^e$.
5)AS1 computes $x'' = x_1^f, ..., x_v^f(modn)$. AS1 and SDX engage in a regular, private set intersection protocol with the sets x'' and $\overrightarrow{z}$, respectively. For each element in the intersection $x'' \bigcap \overrightarrow{z}$, AS1 adds the respective element from $\overrightarrow{x}$ to the result set. AS2 performs the corresponding operations using his set $\overrightarrow{y}$.

TABLE II. 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; $\overrightarrow{A} = (a_1, ...a_N)$	Links in AS1	AS1
$u_{i,j,l}$; $\overrightarrow{U}_{i,j} = (u_{i,j,l})_l$	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
$\delta_{i,j}$; $\overrightarrow{\Delta} = (\delta_{i,j})_{i,j}$	Load demand from destination d_i at p_j	AS1, AS2

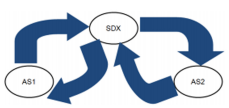


Fig. 4. Proposed Solution (b): Verifying load demand

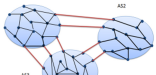


Fig. 3. Proposed solution (a): No need to hide internal links

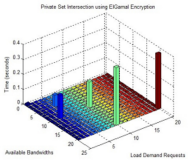


fig-5: Simulation

3 Evaluation and Future Work:

PSI execution times are shown in figure 5. Proposed model using homomorphic encryption takes O(1) and proposed model using PSI takes O(n) time. In the future we are trying to extend this concept over all the wide-area-networks and the data centers where this kind of communication and traffic engineering takes place. We are also working on making RSes more secure rather than controller of SDX.