An AS-level IP Traceback System

André O. Castelucio, Ronaldo M. Salles
Military Institute of Engineering
Praça General Tibúrcio, 80 – 22290-270
Rio de Janeiro - RJ - Brazil
{castelucio, salles}@ime.eb.br

Artur Ziviani
National Laboratory for Scientific Computing
Av. Getúlio Vargas, 333 – 25651-075
Petrópolis - RJ - Brazil
ziviani@lncc.br

ABSTRACT

Distributed Denial of Service (DDoS) attacks represent a serious threat to the appropriate operation of Internet services. To deal with this threat, we propose an IP traceback system (IPTS) intended to be deployed at the level of Autonomous Systems (ASes). Our IPTS requires a priori no knowledge of the network topology while allowing single-packet traceback and incremental deployment.

1. INTRODUCTION

Current Internet services are vulnerable to large-scale distributed denial of service (DDoS) attacks. IP traceback systems (IPTS) intend to provide mechanisms to identify the route(s) taken by attack packets.

Several IPTS have been proposed in recent years [2, 5, 4]. Analyzing the IPTS proposed so far, we observe that neither of them can effectively be adopted in a large-scale network such as the Internet. We stake out that except for the system proposed by Korkmaz et al. [4], all the others require the deployment on *all* routers of the monitored network domain, thus intending to rebuild the *complete* path taken by attack packets.

In contrast, our proposed AS-level IPTS is intended to be partially deployed in large-scale networks such as the Internet—in our case, only at the border routers of some Autonomous Systems (ASes)—and requires no previous knowledge of the network topology. We argue that identifying some key points in the path where attack packets are being forwarded is enough to take countermeasures to block the ongoing attack (e.g. at the closest traceback-collaborative ASes with respect to the sources of a DDoS attack). Through a preliminary simulation study, we show that our IPTS may be partially deployed, allowing ASes to incrementally join other participating ASes, thus leading to an increased efficiency in the IP traceback. Our findings indicate that a relatively low number of ASes with the system deployed—provided these are strategically chosen—is enough for an efficient IP traceback at the AS-level.

*CoNEXT'*07, December 10-13, 2007, New York, NY, U.S.A.

2. PROPOSED AS-LEVEL IPTS

In our proposed IPTS, packet marking is similar to the one done by Laufer et al. [5]. The Generalized Bloom Filter (GBF) present in each IP packet carries the marks of routers where packets traverse. The main difference from our proposal to the original one is in the process of verifying the previous hop of a packet. We propose to use the routing protocol BGP as the vehicle for communication among collaborative ASes in order to discover which ASes have the proposed IPTS deployed. The BGP protocol uses an `Update Message` to exchange routing information among peers or neighbor BGP routers. The `Community Attribute` is used to group destinations sharing common characteristics. We propose the creation of a new `IP Traceback Community` comprising information about the presence of our traceback system on collaborative ASes. `Proxy Community Community` [1] allows the dissemination of information about a particular community to remote ASes piggybacked at the route propagation performed periodically by BGP. We use the `Proxy Community Community` to establish the new `IP Traceback Community`. This structure enables the partial and incremental deployment of our IPTS in the ASes willing to collaborate no matter how they are located in relation to each other. Moreover, it eliminates the need of deploying the system along consecutive routers in a network.

The basic operation of the proposed IPTS is illustrated in Figure 1. The attack packets traverse the path through ASes `AS1`, `AS2`, `AS4`, `AS5`, and `AS7` until they reach the victim with their GBFs containing marks for ASes `AS1`, `AS5`, and `AS7`. To initiate the traceback, the victim verifies that the mark of `AS7` is in the GBF of the incoming attack packets and sends a discovery-path packet to `AS7` (step 1), which verifies the mark of its neighbor ASes trying to identify from where the packet came, finding `AS5` in the GBF (step 2). `AS5` verifies

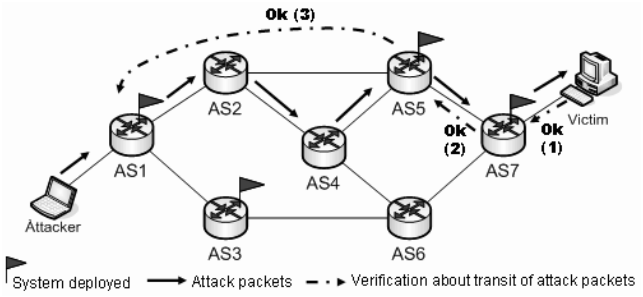

Figure 1: Operation of the proposed system.

that its neighbor ASes `AS2` and `AS4` do not have their marks in the GBF. Note that because of the procedure of exchanging the `Community Attribute`, `AS5` already knows that `AS1` should be also verified as a possible candidate for being in the attack path. As the verification of `AS1` is indeed positive, `AS5` sends a discovery-path packet directly to `AS1` (step 3). `AS1` also verifies the GBF and observes the absence of other marks in the GBF, finishing the traceback process. At this point, `AS1` can identify itself as the closest collaborative AS with respect to the source of the attack packets on this particular branch of the attack tree. This allows `AS1` to take countermeasures to block the next incoming attack packets intended to be forwarded to the victim's AS.

3. PARTIAL DEPLOYMENT EVALUATION

We evaluate two ways of placing our IPTS networks: (i) strategic placement, where highly connected ASes have the traceback system deployed first; (ii) random placement, where ASes are selected randomly to have the traceback installed.

In our simulations we use Nem [6] as topology generator with the Barabási-Albert model and NS-2 patched by BGP++ simulation module as a network simulator. We report results for AS-level network topologies containing 900 ASes (similar results were found for topologies with 300 and 600 ASes). To get each sample, we simulate 7 different network topologies with 5 randomly-chosen sets of attackers (10% of the ASes) sending traffic towards one victim. The purpose of the simulations is to analyze the performance of the partial and incremental deployment of our IPTS. We consider simulation results within a 99% confidence interval.

Results show that using strategic placement we discover almost 100% of each AS-level attack reverse path with the system deployed on 70% of the ASes in the network. On the other hand, to achieve the same results using random placement, a traceback system should be deployed in almost 100% of the network ASes. Moreover, using strategic placement, to discover almost 100% of ASes within 1 hop of distance from attacker's AS it is necessary to deploy the proposed IPTS on about 65% of network ASes. To get this result using random placement, around 95% of ASes should have the proposed IPTS installed. Using the strategic placement results suggest that deploying the proposed IPTS on about 40% of the network ASes, countermeasures against DDoS attacks may be efficiently taken, since with this deployment ratio around 90% of the AS-level attack path is discovered. Furthermore, even if just a small deployment ratio is used—around 20%—the traceback process can still point out more than 80% of the AS-level reverse path, thus allowing efficient distributed countermeasures to be taken. Further detailed results may be found in [3].

4. CONCLUSIONS

We propose a new AS-level IPTS taking advantage of BGP features to allow partial deployment. Our proposed IPTS has some advantages over previous works. It may be partially deployed in some ASes, contrasting with conventional IPTS. Due to this, deployment costs of the proposed system are smaller than others. Our IPTS can also be deployed incrementally in the Internet, thus allowing ASes to gradually start collaborating with the traceback at any moment, thereby contributing to increase the system's efficiency. As future work, we intend to verify the possibility of only using the IP Traceback Community, leaving out the Proxy Community Community, thus simplifying the operation of our system. We also consider verifying the possibility of storing hashes of Autonomous System Numbers instead of IP addresses of routers in the GBF, thus reducing the required storage space.

5. REFERENCES

[1] S. Agarwal and T. G. Griffin. *BGP Proxy Community Community*. IETF Internet Draft, January 2004.

[2] A. Belenky and N. Ansari. On IP traceback. *IEEE Communications Magazine*, 41(7), jul 2003.

[3] A. O. Castelucio, R. M. Salles, and A. Ziviani. Evaluating the partial deployment of an AS-level IP traceback system. In *23rd Annual ACM Symposium on Applied Computing- ACM/SAC 2008*, Ceará, Brazil, March 2008.

[4] T. Korkmaz, C. Gong, K. Sarac, and S. Dykes. Single packet IP traceback in AS-level partial deployment scenario. *International Journal of Security and Networks*, 2(1/2):95–108, 2007.

[5] R. P. Laufer, P. B. Velloso, D. de O. Cunha, I. M. Moraes, M. D. D. Bicudo, and O. C. M. B. Duarte. A new IP traceback system against denial-of-service attacks. In *12th International Conference on Telecommunications - ICT'2005*, Capetown, South Africa, May 2005.

[6] D. Magoni. Network manipulator. *https://dpt-info.u-strasbg.fr/ magoni/nem*, 2002.