SENSS: Observe and Control Your Own Traffic in the Internet

Abdulla Alwabel
USC/ISI

Minlan Yu
USC

Ying Zhang
Ericsson Research

Jelena Mirkovic
USC/ISI

ABSTRACT

We propose a new software-defined security service – SENSS – that enables a victim network to request services from remote ISPs for traffic that carries source IPs or destination IPs from this network’s address space. These services range from statistics gathering, to filtering or quality of service guarantees, to route reports or modifications. The SENSS service has very simple, yet powerful, interfaces. This enables it to handle a variety of data plane and control plane attacks, while being easily implementable in today’s ISP. Through extensive evaluations on realistic traffic traces and Internet topology, we show how SENSS can be used to quickly, safely and effectively mitigate a variety of large-scale attacks that are largely unhandled today.

Categories and Subject Descriptors

C.0 [Computer-Communication Networks]: General—*security and protection*; C.2.3 [Network Operations]: Network Management, Network Monitoring

General Terms

Security, Design

Keywords

Security, Privacy, SDN, Design, Management

1. INTRODUCTION

With a rapidly growing number of critical as well as business applications deployed on the Internet today, network attacks have both become more lucrative for the attackers and more damaging to the victims. Data plane attacks, such as distributed denial-of-service (DDoS), can render the victim unoperational for days [5], and can impact Internet services such as routing infrastructure. Control plane misconfigurations and attacks on the interdomain routing protocol BGP [2, 4] can also have dire implications for victim networks, leading to traffic rerouting, sniffing, modification or dropping.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage, and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s). Copyright is held by the author/owner(s).

SIGCOMM’14, August 17–22, 2014, Chicago, IL, USA.

ACM 978-1-4503-2836-4/14/08.

<http://dx.doi.org/10.1145/2619239.2631459>.

Figure 1: SENSS architecture.

Many solutions have been proposed to detect and mitigate *individual* attacks in data plane and control plane at the victim or at the victim’s ISP. While many attack instances can be handled by the victim and its ISP, there will always exist attacks that cannot be diagnosed or mitigated without help from remote networks. Today’s Internet lacks such *wide-scale, general service for automated multi-ISP collaboration on security problem diagnosis and mitigation*.

There have been numerous research works security solutions that require inter-ISP collaboration. However, these proposals are still not deployed today because of three reasons: (1) Focus on detection or mitigation of one attack type or variant; (2) Requirement for complex changes of the data plane or new router functionalities, which are difficult to achieve; (3) Lack of proper incentives for ISPs to collaborate with each other.

2. SENSS

Inspired by software-defined networking, which provides a simple interface (flow-based rules) to facilitate the advancement of networking protocols, we propose SENSS – Software dEfiNeD Security Service. SENSS enables an end network to request help from remote ISPs to observe and control its traffic and routes, to diagnose and mitigate a variety of Internet attacks. SENSS has three key features:

Simple and expressive interfaces at ISPs: SENSS introduces simple interfaces for victims to request services from remote ISPs including traffic query, traffic control, route query, and route control. These interfaces are expressive to support the detection/mitigation of a variety of attacks.

Victim oriented programming for diverse attacks: The victim can make strategic decisions on which actions to take and where, based on the information it gathers from SENSS, combined with the victim’s knowledge of its network, business and priorities.

Incentives for SENSS adoptions. End networks have every incentive to use SENSS, since they receive much needed help and they pay only when they use the service. It is economically appealing for ISPs because they can charge the victims for the services they provide. Also, the information and services exposed by SENSS interfaces are similar to those that today’s ISPs already perform for their direct customers.

We give an overview of the SENSS architecture in Figure 1. A SENSS-deploying AS (called *SENSS AS*) provides SENSS service

Figure 2: Attack bandwidth eliminated.

Figure 3: #queries to drop 95% attack.

Figure 4: Accuracy in partial deployment

Attack	Query	Control
DDoS w/ signature	Traffic queries	Traffic filter based on signatures at identified ASes
DDoS w/o signature	Traffic queries to get and compare traffic distribution	Non-specific traffic filters at identified ASes
DDoS reflection	Reduces to DDoS w/ or w/o signature, depending on attack details	
Crossfire	Traffic queries to identify bottlenecks	Bandwidth guarantees at identified ASes
Blackholing	Route queries to detect the bogus route	Route demotion to reduce the false route's propagation
Interception	Route queries to obtain control plane routes; Traffic queries to obtain data plane paths	Route modification to change the false path segment at polluted ASes

Table 1: Example SENS applications

by exposing query and control interfaces. The victim first detects it is under attack through local observations, and initiates attack diagnosis. It queries multiple ASes about its traffic or about the AS's routes to victim prefixes. Then, the victim analyzes the replies to its queries locally, to identify best action to take and best locations for remediation. Finally, it issues control messages to chosen SENS ASes to mitigate the attack. The communications between the victim and ASes are authenticated and encrypted.

In reality, there will be only a few ASes deploying SENS at the beginning. We assume that Tier 1 and Tier 2 ASes are more likely to be the first to deploy SENS. We show some example applications in Table 1.

3. EVALUATION

We developed a simulator in C++ to simulate both the DDoS attacks and the prefix hijacking attacks on AS-level Internet topology. We also implemented different victim programs for different attacks. These programs interact with SENS ASes by sending queries to the ASes, making decisions based on the replies, and sending more queries or control commands. To simulate DDoS attacks, we setup up some attack and legitimate traffic flows on our AS topology. To simulate prefix hijacking, each time, we select one attacker and one victim, and let the attacker hijacks the victim's route by announcing the victim's prefix either as its origin AS (blackholing) or as an immediate next hop to the neighbor AS (interception).

3.1 Data plan attacks

For brevity, we focus on several variants of DDoS attacks and describe how to use SENS to diagnose and mitigate them. Real victims are likely to deploy their own decision process when handling real attacks, that may not resemble what we describe here.

The victim seeks to deploy filters at enough remote SENS ASes to drop most of the attack traffic. To achieve this, the victim first sends traffic queries the attack signature to identify the ASes with high attack traffic, and then installs traffic filters at these ASes.

In some DDoS attacks the victim cannot identify a useful signature. The victim install filters at points carried little traffic before attack that carry a lot in the attack. In Figure 2 we show the median percentage of attack traffic eliminated. With light attacker distribution we need 30 deployment points to eliminate more than 95% of the attack, while with heavy attacker distribution we can achieve this with 10 deployment points. Figure 3 show the number

of messages (queries and filters, together) required to achieve 95% attack filtering. For all traffic distributions less than 36 messages are needed.

3.2 Control Plane Attacks

In the control plane, attackers leverage prefix hijacking either to absorb the victim's traffic (*i.e.*, blackholing) or to divert the traffic (*i.e.*, interception), to inspect it or to modify it, before sending it to the victim. In both blackholing and interception attacks, victim communicates with the small number of chosen ASes, sending *route queries* to obtain the control plane routing information and *traffic queries* to identify the victim's traffic distribution. To identify best SENS ASes to query the victim first builds an AS-level Internet topology, *e.g.*, from sources like Routeviews [1], and annotates it with AS relationships, *e.g.*, using algorithm [3]. Blackholing is mitigated by either downgrades the malicious route or promotes the victim's route, by sending route demotion messages to a number of SENS ASes. To mitigate interception attacks, the victim modifies the control plane to match the data plane by asking a few ASes to correct their route to the victim.

For mitigation, the victim may ask all the deployed ASes to perform the *route control*, which will correct as many polluted ASes as possible. However, to minimize the number of control requests, it may also try to select a small set of SENS ASes to perform mitigation.

Figure 4 shows that with 30 ASes deployed, the detection accuracy can reach 90% for BH and 70% for IC. After that, the accuracy increases slower with more deploying ASes.

4. REFERENCES

- [1] University of Oregon Route Views Archive Project. www.routeviews.org.
- [2] V. J. Bono. 7007 Explanation and Apology. NANOG 97-04.
- [3] L. Gao. On Inferring Autonomous System Relationships in the Internet. In *Proc. IEEE Global Internet Symposium*, 2000.
- [4] M. Lad, R. Oliveira, B. Zhang, and L. Zhang. Understanding resiliency of internet topology against prefix hijack attacks. In *DSN*, 2007.
- [5] T. N. Y. Times. How the Cyberattack on Spamhaus Unfolded. <http://www.nytimes.com/interactive/2013/03/30/technology/how-the-cyberattack-on-spamhaus-unfolded.html>.