# SENSS: Software Defined Security Service

Minlan Yu* Ying Zhang† Jelena Mirkovic* Abdulla Alwabel*
University of Southern California* Ericsson Research†

## 1 Motivation

Network attacks have long been an important problem, and have attracted a lot of research in academic and commercial sector. 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. The implications of network attacks on the victim can be huge. For example a distributed denial-of-service (DDoS) can overwhelm the victim and make it unable to handle its regular business. A large-volume DDoS attack can further cause collateral damage to traffic that shares links with the victim's traffic, leading to large traffic drops, BGP session interruptions and routing interruptions [4]. Besides the data plane attacks, control plane misconfigurations and attacks on the interdomain routing protocol BGP [3] can have dire implications for victim networks. For example, the prefix-hijacking attack injects and propagates false routes to the Internet, causing victim's traffic to be redirected to the attacker networks for sniffing, modification or dropping [1]. Traffic sniffing and modification are very difficult to detect and mitigate, and create huge security and privacy issues for the victim, while blackholing severely affects online businesses and critical infrastructures.

Many solutions have been proposed to detect and mitigate *individual* attacks. For example, in DDoS realm many victim-deployed or ISP-deployed DDoS defenses, overlay-based DDoS defenses [2] and content replication to sustain high-volume attacks have been proposed and deployed. In routing realm, detection approaches that monitor live BGP data feeds and conduct data plane probing have been proposed to diagnose prefix-hijacking attacks.

But ultimately, traffic flows, attacks, and their routes are the results of actions of multiple networks, each following its individual interests and priorities. Thus, while many attack instances can be handled by the victim and its local ISP, there will always exist attacks that cannot be diagnosed or mitigated without help from remote networks, which are involved in sourcing or carrying traffic to the victim. Today's Internet lacks such wide-scale, general service for automated inter-ISP collaboration on security problem diagnosis and mitigation.

There have been numerous research works on inter-ISP collaboration for attack diagnosis and mitigation, such as collaborative DDoS defenses, collaborative worm defenses, and collaborative routing defenses. However, most proposals are still not deployed today because: (1) Most of the proposals only focus on detection or mitigation of one attack type or variant; (2) Some solutions require complex changes of the data plane or new router functionality, which are difficult to achieve; (3) Some solutions do not create 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), a generic interface for Internet attack diagnosis and mitigation. SENSS has three key features:

***(1) Victim-oriented:*** The victim of a security attack has the most incentive to detect and mitigate the attacks. The victim also has the most knowledge about the problems it is experiencing, the traffic it sees, and the help it needs to diagnose and remedy problems. Our proposed service enables this victim to directly request security services from multiple remote ISPs. For security and privacy reasons we design mechanisms for victims to only have visibility and control of their own traffic, i.e., the traffic that carries either source or destination IPs from the victim's address space.

***(2) Simple detection/mitigation interface from an ISP:*** We define a simple interface for victims to request services from ISPs, such as statistics gathering, traffic filtering, rerouting, or quality of service guarantees. The interface is both expressive to support the detection/mitigation of a variety of attacks (e.g., prefix hijacking, DDoS), and easy to implement in today's ISPs.

***(3) Programmable attack detection and mitigation across ISPs:*** With the simple interface provided by ISPs, victims can easily *program* their own attack detection and mitigation solutions across ASes. A victim can first query multiple ISPs to trace back the attack, identify the best locations for remediation, and then issue commands for ISPs to take mitigation actions (e.g., filtering the traffic, guaranteeing bandwidth or rerouting).

**SENSS Architecture** The SENSS service exposes an interface at each deploying ISP that enables remote victim networks to query this ISP about their *mission traffic* – traffic that carries either source or destination IPs from the victim's prefixes – and to request filtering services, bandwidth guarantees or route modifications. The ISP authenticates these requests, processes them and implements them by setting up rules in its OpenFlow switches. In case of queries, the ISP returns the requested information to the remote customer network. This reply is also protected through cryptographic means to ensure authenticity and freshness. We use the same definition of *flow* as does OpenFlow and we define a *tag* to be a unique identifier of an AS that neighbors an ISP that deploys SENSS. A traffic *aggregate* is a combination of flow, tag and direction (IN or OUT) fields.

Table 1 defines SENSS messages from the customer (victim network) to the provider (SENSS ISP) and replies or actions taken by the provider. A **traffic query** asks about the distribution of traffic across ASes that neighbor with a SENSS ISP. It specifies the traffic aggregate of interest and the duration of observation. The ISP returns the list of packets or bytes sent by or sent to each neighbor. This helps SENSS customer trace back its traffic and identify best points to deploy mitigation. A **route query** asks a SENSS ISP about the best route it has to the customer's prefix. The provider replies with a full AS path. This enables the customer to diagnose route detour attacks and blackholing and to mitigate them. The victim networks can also ask the SENSS ISP to **filter, guarantee bandwidth, demote routes, or modify routes** for its traffic (see Table 1 for details). For security all messages between the victims and SENSS ISPs are encrypted, signed and timestamped. Further, a SENSS ISP verifies, using RPKI, that the customer is authorized to control traffic and routes for a given IP prefix. This ensures that networks can only influence traffic that flows to or from them.

| **Message** | **Fields** | **Reply/Action** |
|---|---|---|
| Traffic query | aggregate, duration | a list of <tag, #bytes or #packets, direction> for the aggregate |
| Route query | prefix | AS paths from the provider to the prefix |
| Traffic filter | aggregate | filter all traffic matching the aggregate |
| Bandwidth guarantee | aggregate, bw | guarantee bandwidth *bw* for traffic matching the aggregate |
| Route demotion | prefix, <path> | demote route to prefix that has specified AS path segment |
| Route modification | prefix, $<path_1>$, $<path_2>$ | modify the false AS path segment to the correct one |

Table 1: SENSS messages from the customer to the provider and replies/actions by the provider

**SENSS Uses** We now briefly discuss we can detect and mitigate a variety of DDoS and routing attacks with SENSS.

***(1) DDoS:*** For those DDoS attacks where we can identify TCP/IP header level signatures, we can easily use *traffic filter* at remote ISPs to drop the traffic close to attack sources. However, sometimes, a victim may not be able to devise a useful signature, when the attack traffic are spoofed with randomized flow fields. To detect such DDoS attacks, during periods of no attack, a SENSS customer may occasionally use *traffic query* to SENSS ISPs for the amount of traffic they receive from their neighbors and route to this customer. That way the customer gains visibility into most commonly used Internet paths by its mission traffic. During a DDoS attack without signature, the SENSS customer (i.e., the victim) issues a similar *traffic query*. It then compares the traffic distributions before and during the attack, and identifies upstream ISPs that have previously routed little traffic to the victim, but now route a lot. These ISPs are likely routing mostly attack traffic, and SENSS customer issues traffic filter messages to those to mitigate the attack. We evaluated SENSS with real CDN traffic, DDoS attacks, and Internet topology, and find that with only 30 deployed ISPs, we can already eliminate 94% of the attack traffic.

***(2) Prefix hijacking:*** It's easy to use SENSS for the blackhole based prefix hijacking where an attacker announces the victim's prefixes and drops the traffic. The victim uses *route query* to detect the bogus route and uses *route demotion* to reduce the false route's propagation. The interception attack is harder to detect, because an attacker transparently intercepts the victim's traffic by creating arbitrarily shorter AS path in the BGP announcement. SENSS can detect this attack by *identifying the conflicts in control and data plane*, by using *route query* to obtain control plane routing information and using hop-by-hop *traffic query* to obtain data plane path. Once an inconsistency is detected, the victim may ask a set of SENSS ISPs to perform mitigation, i.e., use *route modification* to change the false path segment in the BGP updates to the true data plane path. From the simulation with real traffic traces and Internet topology, we show that with only 18 SENSS ISPs to help mitigate the attack, we can correct 82% of the polluted ASes.

# References


[1] The new threat: Targeted internet traffic misdirection. `http://www.renesys.com/2013/11/mitm-internet-hijacking/`.

[2] A. Keromytis, V. Misra, and D. Rubenstein. SOS: An Architecture for Mitigating DDoS Attacks. *IEEE Journal on Selected Areas in Communications*, 2004.

[3] M. Lad, R. Oliveira, B. Zhang, and L. Zhang. Understanding resiliency of internet topology against prefix hijack attacks. In *DSN*, 2007.

[4] 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`.