E ABSTRACT

Title: SENSS Security Service for the Internet

Offeror: Jelena Mirkovic (USC/ISI), Minlan Yu (USC)

This proposal addresses TTA-2: Tools for Communication and Collaboration. We propose to build, evaluate and release client and server software for SENSS: Security Service for the Internet, and to perform strong outreach to ISPs for technology transition. SENSS servers are ran by ISPs (SENSS ISPs). SENSS APIs can be used by any interested network, usually a victim of DDoS or BGP prefix hijacking, to observe and control its traffic (carrying its IPs as source or destination) and routes at SENSS ISPs. The victims pay to SENSS ISPs for this service.

SENSS can detect and mitigate a large variety of distributed denial-of-service attacks, even in early adoption stage, and its effectiveness grows as it is more widely deployed. SENSS can also be used to diagnose and mitigate many prefix hijacking attacks, where the attacker attracts and drops or modifies victim's inbound traffic, creating denial of service in a non-traditional way. SENSS has the following desirable properties:

Simple yet powerful interfaces. Simplicity of SENSS interfaces allows the functionalities to be easily supported in today's switches, and allows for versatile use. Not only can SENSS aid networks in mitigation of DDoS and routing attacks, but also the victims can build *fully customized* solutions for these threats that best suit their needs. Further, SENSS interfaces can be used to build solutions against other security threats.

Good alignment with interests and capabilities of various participants. All intelligence and decision-making power about the detection and mitigation reside at the victim network—this aligns ownership of traffic/routes and interests that come with it, with power to observe and control these same traffic and routes in remote ISPs. Actions performed by SENSS ISPs are simple and easy to implement with today's router and switch capabilities. Attack victims pay to SENSS ISPs for services rendered; this provides economic incentive for adoption at ISPs.

Strong security. Networks can only observe and control their own traffic and routes; this is ensured via RPKI authentication and communication between ISPs and end-networks (usually attack victims) is secured using TLS. SENSS further allows delegation of victim functionality, and thus can operate in cases when channels between a victim and SENSS ISPs are clogged by attacks, or when a victim is non-reachable due to prefix hijacking. SENSS operates effectively in presence of lying ISPs, and enables a victim to detect lying and avoid the specific ISP in the future. SENSS further does not require ISPs to divulge, and does not unintentionally leak any private information about ISPs' internal operation and network architecture.

Existing solutions for DDoS floods and prefix hijacking have one or several of the following drawbacks: (1) they are not effective in sparse deployment, (2) they require new switch/router functionalities that are not readily supported by vendors, (3) they do not have economic incentives for deployment, (4) they handle only some attack variants and cannot evolve with attacks. SENSS addresses all these issues, which makes it a unique solution in today's research and operational landscape. Based on our simulation results, we anticipate that SENSS deployment at only 20 large ISPs would eliminate 80-96% traffic in DDoS attacks (while only dropping 5% of legitimate traffic), and correct 90% of ASes polluted by prefix hijacking. SENSS will successfully handle 1,000-locations-1-Tbps attacks. This project will be managed in close collaboration between the PIs, both at the USC. PI Mirkovic is a recognized expert on DDoS defense, and PI Yu is a recognized expert on SDN, which we will use to implement the SENSS ISP functionalities. PIs have worked successfully for a year on SENSS design and simulation-based evaluation. We propose to implement a SENSS server and client prototype, test them thoroughly and at scale, and transition them to deployment at ISPs, cloud providers and end networks.