# Quad Chart for: SENSS: Security Service for the Internet

Challenge:

- Distributed attacks (e.g. DDoS) need distributed solutions

- Today's internet has no framework for automated inter-ISP collaboration

Solution:

- SENSS offers **easy to deploy, effective, automated collaboration mechanism** for DDoS defense

- **ISPs** deploy SENSS servers, receive messages from clients, provide monitoring or filtering

- **Edge networks** deploy SENSS clients, detect attacks, devise signatures and decide which actions are needed by which SENSS servers

- All communication is secured from eavesdropping or impersonation

- Clients can only influence their own incoming traffic
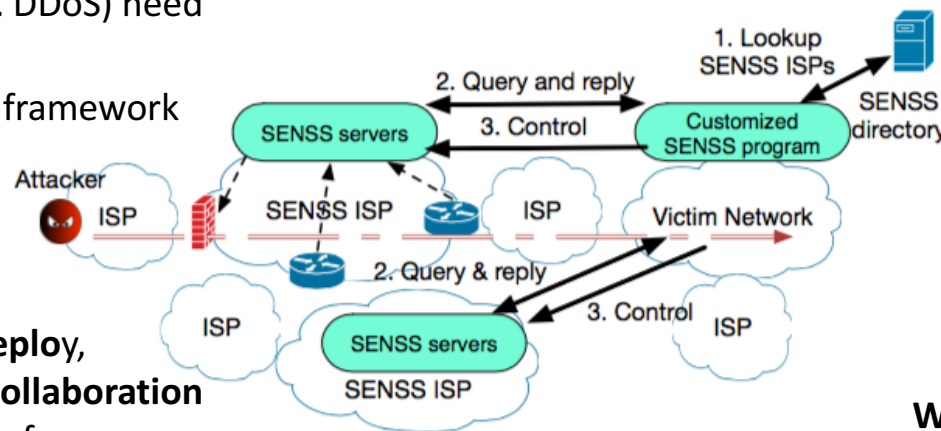
Value proposition:

- Increase ISP offering in DDoS defense at zero equipment/software cost

- Solution where attack victim has full control over mitigation and can measure its impact

- Foundation for inter-ISP collaboration

What we need to TTP

- Opportunities to pilot the research

- Feedback on features to support

- Feedback and discussion on ISP concerns

DHS DDoSD #D15PC00184
USC/Yale
PI: Jelena Mirkovic, USC and Minlan Yu, Yale
Team: Sivaram Ramanathan, Ameya Hanamsagar,
Davut Yavuz, Goran Scuric, Ying Zhang

Contact us

- mirkovic@isi.edu

- minlanyu@yale.edu