SOS: secure overlay services
Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein.

Presented by Efstratios Ntallaris
The paper tries to:

- Address the problem of securing communication infrastructure
- Using a proactive approach (‘surrounding’ the location target and using aggressive filters)

However:

- Does not solve general DoS problem
● Two main principles:
  ○ elimination of the communication “pinch” (constitute DoS targets)
  ○ ability to recover
● The attackers know the IP addresses of the overlay nodes
● Attackers do not have unobstructed access to the network core
● Attackers do not have much resources to congest all the overlay nodes
ARCHITECTURE DESCRIPTION

● Goal of SoS:
  ○ communication between confirmed user and target
  ○ target has given prior permission to the target

● user packets must be authenticated and authorized by the SOS infrastructure

● Attackers launch DoS attacks from variety of points which are called compromised locations.

● The information stored in the infrastructure is difficult to be replicated (assumption)
SOS Architecture

- distributed firewall in the network
- filter construction to the routers far away from the target
  - these routers can handle high load of traffic
  - several routers with filters and independent paths
- when user changes location(IP) the filter must be notified and modified
- the filter does not protect for legitimate IP spoofing (we need something more secure)

Figure 1: Basic SOS architecture.
Reaching well filtered target

- First, Target selects a subset of nodes Ns (powerful filters), that participate in the SOS overlay to act as forwarding proxies
- Small amount of rules
- The filter allows any source address that matches the address of \( n \in Ns \) do more complex security techniques for verification.
- To hide the identity of the Ns nodes, there are secret servlets
To activate a secret servlet, the target sends a message to the overlay node that it has been chosen as a secret servlet. It will compute the key for each of a number of well-known consistent hash functions, based on the target site’s network address. (these hashes will identify a number of overlay nodes that will act as beacons). If legitimate packet reaches secret servlet, it passes it to the filter and then to the target.

New challenge:
- constructing a route mechanism that will route to a secret servlet with the minimal amount of identity information of that destination.
Connecting to the Overlay (SOAP)

- The servlets or the target will contact them, notifying the beacons of the servlets existence.
- Beacons, after verifying the validity of the request, will store required information to forward the traffic to servlets.
- A source that wants to communicate with the target contacts an overlay access point (SOAP).
- After authenticating and authorizing the request, forwards the packets through the beacons.
- SOAP route the packet to an appropriate beacon by applying appropriate hash functions to the target address.
- The beacon routes the packet to a secret servlet that then routes the packet (through the filtering router) to the target.
DoS attacks robustness:

- If an access point is attacked, the confirmed source point can simply choose an alternate access point to enter the overlay.
- If the node within the overlay is attacked, node exits.
- All nodes on the overlay are allowed to fail.
- If a secret servlet’s identity is discovered and targeted, target can choose another set of secret servlets.
Summary of SOS Architecture

- Attacks the problem with a proactive mechanism
- Aggressive packet filtering
- Overlay network can safe-heal during or after DoS