

## MERIT AWARD

# Traffic Redirection Attack Protection System (TRAPS)

Vrizlynn Thing Ling Ling  
Imperial College London

### Objective

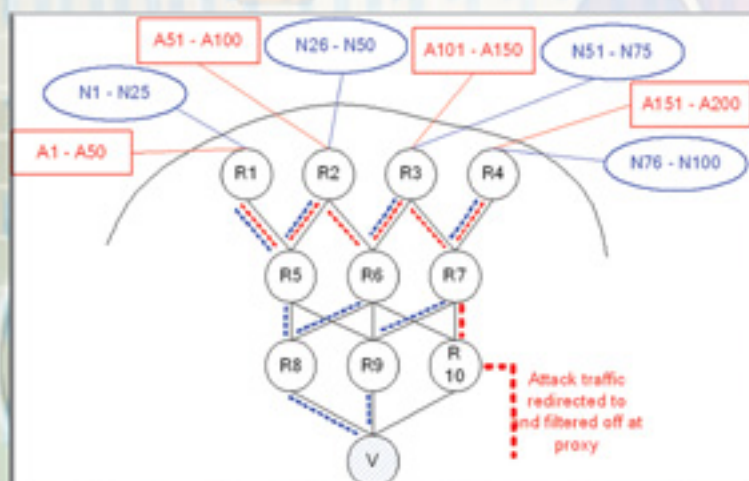
TRAPS is a network attack mitigation system to detect attacks on servers by monitoring resource usage patterns. It allows a speedy verification of the network addresses of the users during an attack to differentiate attackers from legitimate users and performs adaptive responses to mitigate the effect of the attack. These are carried out without the need to make any changes to the Internet infrastructure.

### Why the need?

High profile web servers belonging to organisations such as banks, e-commerce, and military, are often attacked. It is necessary to filter out attackers while permitting access to legitimate users. This can be difficult as attackers often use false network addresses. TRAPS provides a fast method to differentiate the attackers from the legitimate users and can also limit suspicious traffic to prevent overloading of the servers.

### How does it work?

1. Attack detection is based on resource usage pattern monitoring with threshold levels to indicate attack severity.
2. Suspicious traffic is rate limited based on current attack severity level
3. The attack victim performs a 'virtual' relocation (i.e. virtually moves to a new address) and informs suspicious users, who are generating a lot of traffic, about the new address. Attackers will not have given their correct source addresses and so will not be informed, but legitimate users will switch to the new address. Attackers will continue to use the victim's old address and so this traffic can be easily discarded.
4. Relocation is part of the Mobile IP standard implemented on most workstations. This allows TRAPS to be deployed without the need to make any changes to the potentially huge numbers of clients accessing the servers over the Internet.



A1 to A200 are 200 attackers spoofing 10,000 different addresses flooding the victim, V. N1 to N100 are legitimate users. R1 to R10 are the routers in the network, with R10 acting as the proxy for the victim.

