C. PROJECT SUMMARY

IP spoofing accompanies and exacerbates many Internet security threats. In distributed denial-of-service (DDoS) attacks spoofing prevents the attack target from recognizing legitimate clients and forces inaccurate filtering response. In reflector DDoS attacks, spoofing invokes unsolicited responses from Internet servers to the target. Spoofing is also used for distributed vulnerability scanning and is basis for many intrusion scenarios. If IP spoofing were eliminated or sufficiently reduced, defenses against DDoS, distributed scanning and intrusions would be much simplified and more effective. Of particular interest are spoofing defenses that will be both *practical* and *effective*. This means that a proposed defense should significantly reduce both the danger from spoofed traffic and from reflector attacks, for the deploying network, even if it no other networks adopt the same mechanism. The proposed defense should handle spoofing in face of frequent routing changes, asymmetric paths and multipath routing all of which are common in today's Internet.

We have recently performed an extensive simulation study of spoofing defenses proposed to date: route-based filtering (RBF), interdomain packet filtering (IDPF), hop-count filtering (HCF), spoofing prevention method (SPM), Stack-Pi, packet passports and ingress filtering. Our findings indicate that only RBF and HCF are very effective in isolated deployment — they protect the deploying network from 97% of spoofed traffic and require no cooperation with other networks. Further, if HCF or RBF are deployed at the top 50 Internet autonomous systems, all Internet destinations can be shielded from 95-97% of spoofed traffic. Other spoofing defenses require more significant deployment in the Internet to achieve similar effectiveness.

RBF and HCF detect spoofing by associating the packet source with some route descriptor (previous hop in RBF, hop count in HCF). They are currently not practically deployable because there is no proposed mechanism to build these associations initially and keep them up to date in case when filters reside on asymmetric routes, the route changes or packets are forwarded on multiple paths. RBF and HCF also cannot offer effective protection against reflector attacks without core deployment.

Intellectual Merit: We propose to develop two novel mechanisms that improve and augment RBF and HCF, facilitating effective protection against spoofed and reflected traffic both in isolated deployment and with support of the Internet core. These two mechanisms are: (1) the Clouseau system, which enables routers on asymmetric paths to accurately infer associations between the route descriptor and the source address. It will support multiple associations (in case of multipath routing) and will promptly update associations when routes change, and (2) the RAD system which helps Internet networks protect their addresses from being used for spoofing and facilitates detection of reflected replies to spoofed packets.

The Clouseau system infers route descriptor information by applying randomized drops to TCP data traffic which arrives from suspicious or previously unknown sources, and observing subsequent retransmissions. If the communication with the source is validated as non-spoofed through this probing process, the previous hop or the hop count information is inferred from the traffic and used to update the associations. No communication is required with packet sources or other filters, which makes Clouseau suitable for partial deployment. Deployment of Clouseau at as few as 50 chosen Internet autonomous systems, together with RBF or HCF, will reduce amount of spoofed traffic on the Internet to less than 3%. In isolated deployment, Clouseau with RBF or HCF will reduce spoofed traffic received by the deploying network to less than 3%.

RAD adds several cryptographic marks to each packet that enable RAD routers to detect traffic spoofing addresses of RAD sources, and it facilitates detection of replies to spoofed traffic by hosts whose addresses were misused. RAD system will offer a significant protection from reflector attacks in isolated deployment and an almost perfect protection when RAD is deployed in the Internet core.

We will demonstrate the scalability and fidelity of our proposed solutions through analysis, distributed simulation and through implementation of the proposed defenses in a Linux router and in an Intel IXP programmable router. This work builds on PI Mirkovic's and PI Reiher's expertise in design of effective IP spoofing defenses and their evaluation.

Broader Impact: This work will provide means for interested networks to significantly reduce the spoofed and reflected traffic they receive in isolated deployment. Additionally, if deployed at a few strategic points in the Internet core, proposed systems will reduce the amount of spoofed traffic in the Internet to negligible levels and will greatly simplify defenses against DDoS attacks, distributed scanning and intrusions. This research will demonstrate that the proposed systems are cheap, effective and practical, both in isolated and in core deployment. We will release the Linux router and the IXP router implementation code, the simulation code and results to the public.