C. PROJECT SUMMARY

Dynamics of Internet-scale events such as worm propagation, distributed denial-of-service attacks, flash crowds, routing instabilities, and DNS attacks depend on the configuration of all the networks that generate or forward legitimate and malicious traffic. To fully understand these events researchers need simulation tools that reproduce all the relevant event details and event traffic's interaction with the Internet architecture. Collaborative defenses against Internet-scale attacks have also been proposed. The effectiveness of these defenses depends on the underlying Internet topology and the deployment locations, so high-fidelity Internet simulation is necessary to properly evaluate these defenses.

Current network simulators cannot be used to study Internet-scale events. They are general-purpose, packet-level simulators that *reproduce too many details* of network communication, which limits scalability. Even distributed versions of network simulators such as GTNetS and PDNS, designed for large-scale events, have limited scalability because each packet and its handling are simulated in minute detail. For example, PDNS requires powerful, 100+ CPU clusters, to simulate worm propagation with up to 1.28 M vulnerable hosts. Many researchers do not have an access to such a large cluster. Another drawback of the current network simulators is that they *lack a built-in Internet model*. Researchers that aim to simulate Internet-scale events must themselves assemble the Internet topology, and determine end-host communication patterns, link bandwidths and routes. The effort required to set up a realistic Internet model from scratch is considerable so many researchers adopt simplfied models (e.g., assuming infinite bandwidth links, assuming highly symmetric Internet topology etc.) which leads to incorrect results.

Intellectual Merit: We propose to develop a distributed Internet simulator, called *iSim*, with the following novel features: (1) It will provide a built-in Internet model, including the topology, routing, link bandwidths and delays, (2) Instead of being a general-purpose simulator, *iSim* will provide a common simulation core for traffic generation and message passing, on top of which we will build separate modules that customize messages and level of simulation details for the event of interest. Customization modules will ensure that all and only the relevant details of the event of interest are simulated, cutting down the simulation time. We will also provide an interface for new module specification, and for existing module modification, (3) The *iSim* will be deployed in the Emulab and DETER testbeds, and will provide an easy-to-use graphical interface for experiment control. This will bring the Internet event simulation at the fingertips of all interested researchers.

The *iSim* work builds upon our recent achievements in creating an Internet-scale simulator of worm propagation events, called PAWS. PAWS is a distributed simulator, deployed on the Emulab testbed. It is more accurate than existing worm simulators, because it faithfully replicates Internet topology at the AS level, simulates the limited bandwidth of the inter-AS and customer access links, and simulates the exact worm scanning pattern observed during the real spread. PAWS achieves short simulation time by selectively replicating only those details of network communication that are relevant for worm spread events: a worm's scanning strategy, packet size and propagation method. Only source and destination IPs are carried in the worm packets, thus reducing the message size, and messages are aggregated and transmitted between simulation nodes at discrete time intervals. For comparison, performance of PAWS with 8 Emulab machines is comparable to the performance of PDNS on a dedicated 136-CPU cluster. During the proposed work we will restructure and extend PAWS to evolve it from the customized worm simulator into the *iSim*'s general-purpose simulation core with a worm module. This is a significant modification of our current code. We will further provide customization modules for simulation of popular worm defenses, distributed denial of service attacks and popular DDoS defenses, and IP spoofing and popular spoofing defenses.

Broader Impact: The proposed simulator will create opportunities for teachers, students and researchers to replicate and study Internet behavior in a variety of settings. The simulator will promote research in worm detection and defense, IP spoofing prevention and DDoS defense. We further expect that the simulator will be extended by interested researchers to add novel event models and thus will expand its customer base. The simulator will be open source, written in C++ following object oriented programming principles and with a modular architecture.

iSim will be deployed in Emulab and DETER testbeds and will thus be easily usable by a broad academic and commercial community. We will further provide a graphical interface for experiment control and statistics gathering, and an online tutorial for *iSim*. We will broadly disseminate our tools, code and simulation experiences through a Web site and through refereed publications.