Project Summary

Collaborative Research: DefCOM — Distributed Defense Against DDoS Attacks

Many critical functions today are realized through the use of network services. Distributed denial-of-service (DDoS) attacks represent a major threat to network operation. They overwhelm a key resource at the victim network generating a flood of seemingly legitimate packets, deny services to legitimate clients and frequently create heavy Internet congestion. Attackers need not possess any particular skill to perpetrate DDoS attacks, and face virtually no risk of attribution. In spite of numerous research and commercial efforts, there are still no effective DDoS defenses.

An effective solution to the DDoS problem must accurately detect and characterize attack instances, and quickly stop large proportions of the attack traffic, while at the same time recognizing legitimate traffic that shares the attack signature and delivering it reliably to the victim. Unfortunately, there is no single deployment point on the attack tree that successfully meets all three requirements. Detection of the attack is most effective close to the victim, while the response (stopping the attack traffic) and separation of legitimate traffic from the attack traffic is most successful close to the sources. Additionally, in partial deployment cases when many potential sources do not deploy a source-end defense, adequate victim protection can be achieved only by enlisting the help of backbone routers to constrain attack traffic. These factors clearly indicate that the DDoS problem requires a distributed cooperative solution. We propose a distributed system for DDoS defense, called DefCOM. DefCOM nodes will be distributed throughout the Internet (organized into peer-to-peer overlay) and will act jointly to detect and respond to DDoS attacks. Attack response is twofold: on one hand, defense nodes constrain suspicious traffic, relieving the victim from high-volume incoming streams that consume its resources; on the other hand, nodes cooperate to detect legitimate traffic within the suspicious stream and ensure its correct delivery to the victim. Thus, DefCOM achieves the primary goal of DDoS defense — cancelling of the denial-of-service effect. In addition to this, DefCOM design has a solid economic model where networks deploying defense nodes directly benefit from their operation. DefCOM further offers a framework for existing security systems to join the overlay and cooperate in the defense. These features create excellent motivation for wide deployment, and the possibility of large impact on DDoS threat. Several challenges are addressed: precise separation of legitimate from attack traffic, distributed response to the attack, methods to guarantee safe delivery of legitimate traffic to the victim, scalable and secure cooperation between overlay nodes, and handling the malicious participants in DefCOM.

Intellectual Merit of the Proposed Activity. DefCOM offers a unique functionality in DDoS defense field — automatic separation of legitimate from the attack traffic and service guarantee to legitimate clients even if they share the attack signature and path to the victim. In addition to leading to more robust, more reliable networks, this project will create an Internet-wide infrastructure and secure communication layer that can be used for cooperative defense against other security threats. Expected merit from this research includes: (1) improved network robustness and resiliency in case of DDoS attacks, (2) service guarantee to legitimate clients of DDoS victim during the attack, and (3) development of techniques for cooperation between Internet domains. The project builds upon the expertise of Dr. Mirkovic in network security and Dr. Reiher in security and distributed systems.

Broader Impacts Resulting from the Proposed Activity. Improved network robustness and service availability guarantees will strengthen the critical infrastructure and will foster greater use of the Internet for important services. Development of overlay infrastructure and secure communication protocols will promote cooperation of Internet domains and joint response to distributed threats. DefCOM modules will be implemented using an open-source software and broadly disseminated.

DefCOM will involve two graduate students. They will receive valuable training and education as a result of their participation in this project. PIs will actively seek to involve undergraduates and students from underrepresented groups in research and educational activities within the DefCOM project.