CT-ISG: Improving Measurable Performance with QoS-Adaptive Cyber-defense Techniques (IMPACT)

PROJECT SUMMARY

The past few years have seen significant increase in cyber attacks on the Internet, resulting in degraded confidence and trusts in the use of the Internet and computer systems. The cyber attacks are becoming more sophisticated, spreading quicker, and causing more damage. Attacks originally exploited the weakness of individual protocols and systems, but now start to target the basic infrastructure of the Internet. There is an urgent need to enhance the effectiveness of the cyber-defense, to provide end users with timely information and more control, and to improve the *measurable* performance of network systems when under attacks.

Current intrusion detection systems (IDSs) lack of adaptivity and dynamic reconfiguration capability under uncertain threats and new cyber attacks. They also lack coordination in sharing intrusion detection information and have few mechanisms for sharing resources to form collective cyber defense against cyber attacks. Equally important in improving trustiness of cyber infrastructures is the design of evaluation tools to allow the computation of statistical confidence intervals. This IMPACT project focuses on the research and design of a high confidence software framework that supports the dynamic configuration and deployment of adaptive intrusion detection systems, and support real-time distributed control for managing intrusion detection and responses. In particular, this project will (1) design adaptive IDSs with dynamic reconfiguration capability, taking into account quality-of-service (QoS) control technologies and novel intrusion tolerance capabilities, (2) design a distributed real-time control infrastructure for managing and correlating intrusion detection and responses, (3) enhancement of existing core networks and systems QoS support technologies for intrusion mitigation under uncertain and new threats, (4) development of novel intrusion tolerance approaches to reduce the impact of the severe cyber attacks by making new network capabilities such as multi-path indirect routing and delivering timely network/system information to end users, and (5) development of evaluation tools to allow at least statistical confidence in the experimental results. This interdisciplinary aspect will use ideas from biometric system evaluation to produce evaluation methodologies that include confidence intervals and predictive measures. This project will also develop a prototype cyber-defense system, integrating the designed novel technologies, to demonstrate the success and effectiveness of IMPACT framework on improving measurable performance of cyber infrastructures.

Intellectual merits: The intellectual merit of this proposal lies in the adaptivity design of IDSs with consideration of QoS control technologies, the design of a distributed real-time intrusion correlation infrastructure, and the interdisciplinary study of performance evaluation tool sets. Applying evaluation methodologies to provide sound statistical confidence is a necessary precursor to improving performance predictability, and will impact many other research groups in the area. The resulting innovations and practice will help protect our critical cyber infrastructures and enhance their trustiness.

Broader impacts: The broader impacts are the promotion of the education of graduate and undergraduate students in a critical area of the US national security, and the training of existing workforce on new information assurance technologies. Our novel outreach components will help bridge the gap between advanced cyber-defense research and general community awareness of these issues....to be enhanced by the existing IA curriculum and the development of PhD program in security...