CT-ISG: Improving Measurable Performance with an Integrated Enterprise Cyber-Defense System

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, including email virus, worms, and DDoS, are getting more sophisticated, spreading quicker, and causing more damage. Not only are big web sites such Amazon, Yahoo, and Microsoft being attacked, individuals and smaller organizations have been invaded. Attacks originally exploited the weakness of the individual protocols and operating systems but now have started to attack the basic infrastructure of the Internet. There is an urgent need to enhance the effectiveness of the cyber defense and critical to improve the *measurable* performance of network systems when under attacks.

Current network systems lack coordination in sharing intrusion detection and firewall log information, have few mechanisms for sharing resources to form collective cyber defense against cyber attacks and uncertain threats, and lack support for establishing alternate system configurations and network routes. A key contributing factor leading to cyber attacks today is the lack of an integrated, cohesive platform that extends beyond the network level, to protect the applications and security devices at system level as well. This project aims to design and develop an integrated enterprise cyber-defense system to improve measurable performance and to enhance performance predictability and controllability of network systems. In particular, this project will (1) develop efficient information fusion techniques to enhance distributed intrusion detection correlation and to improve the coordination among IDSs and firewall devices through timely exchange of critical decisions and related log data. Efficient layer coding of cyber defense data and secure information sharing will be investigated. We will utilize and enhance the IDIP protocol framework for cooperative intrusion detection, traceback, push-back, and network restructuring; (2) develop effective Quality-of-Service (QoS) based intrusion mitigation techniques to provide predictable and controllable network systems performance. We will utilize QoS differentiation techniques as means against uncertain cyber threats and use them as part of a more gradual, but earlier, defensive push-back of potential attacks; (3) develop effective intrusion tolerance techniques for service availability. We will develop multi-path routing mechanisms and use them to increase the security, reliability, and aggregate bandwidth of network connections.

This project will integrate the developed techniques into a practical enterprise cyber-defense system. The autonomous cyber-defense systems will be evaluated with special consideration of their impact on the predictability of network system performance. A major limitation of existing work on evaluation of cyber-defense and IDS systems in particular, is that the experimental designs have been inadequate to allow computation of (statistical) confidence intervals which are prerequisite for using them as predictive measures. This interdisciplinary aspect of the project will use ideas from biometric system evaluation and stratified sampling design to produce evaluation methodologies that include confidence intervals. It will also produce a tool-set to help automate evaluations and produce datasets for offline evaluations of intrusion and anomaly detection. The success of the project will enhance the network system security and help ensuring predictable performance when the system is under cyber attacks.

Intellectual merits: The intellectual merit of this proposal lies in the development of novel information fusion techniques for efficient distributed intrusion detection and handling, development of effective QoS differentiation techniques for intrusion mitigation, multi-path routing mechanisms for intrusion tolerance, and the integration of the techniques into a practical enterprise cyber-defense system for improving measurable performance under cyber attacks. The movement of 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.

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.