IMPACT: Improving Measurable Performance Against Cyber Threats

PROJECT SUMMARY

The past few years have seen significant increase in cyber attacks on Internet, resulting in degraded confidence and trusts in the use of 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 Internet, such as the root DNS servers. Therefore, there is an emergent need to enhance the effectiveness of the cyber defense. To gain back the trust and confidence of Internet users, it is critical to improve the *measurable* performance of networks and systems when under attacks.

Current network systems lack support for establishing alternate system configurations and network routes, lack coordination in terms of sharing intrusion detection and firewall log information, have little or no mechanisms for sharing resource to form collective cyber defense against cyber attacks. To improve the performance of network systems against cyber threats, we propose to develop new secure protocols to facilitate the reconfiguration of network connections even under DDoS attacks. These include a new secure DNS system that supports query via indirect route and enhances DNS entries with multiple indirect routing information. These new capabilities ensure reliable alternate way for query on the critical DNS information. New secure indirect routing and transport protocols with multiple paths will be developed to increase the security, reliability, and aggregate bandwidth of network connections.

There is a consensus that a key contributing factor leading to cyber threats is the lack of an integrated, cohesive strategy that extends beyond the network level, to protect the applications and security devices at system level as well. This project also aims to integrate the network-side techniques with server-side support to enhance performance predictability of network systems, and to use QoS differentiation mechanisms as part of a more gradual, but earlier, defensive push-back of potential attacks.

We also propose to enhance distributed intrusion detection and handling techniques, improving the coordination among IDS 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. Information on further cyber attacks on secure indirect routes will be used to assist the traceback of spoofed traffic. We will utilize and enhance the IDIP protocol framework for cooperative intrusion, detection, traceback, push-back, and network restructuring.

The new 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 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.

Our research will blend formal modeling/analysis, experimentation, and evaluation. The success of the project will enhance the network system security and help ensure predictable performance when the system is under cyber attacks.

Intellectual merits: The intellectual merit of this proposal lies in the development of new secure network protocols, effective distributed intrusion detection and handling systems, and efficient reliable QoS techniques for assuring network system 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 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. The knowledge derived from the study of reliable trustworthy network system will present advancements in science and engineering.