

Ph.D. Dissertation Defense

Adaptive Trust and Reputation System as a Security Service in Group Communications

Ph.D. Candidate: Pitipatana Sakarindr

Date: October 21, 2009

Time: 3:00 – 5:00 P.M.

Room: ECEC 202

Abstract

Group communications has been facilitating many emerging applications which require packet delivery from one or more sender(s) to multiple receivers. Owing to the multicasting and broadcasting nature, group communications are susceptible to various kinds of attacks. Though a number of proposals have been reported to secure group communications, provisioning security in group communications remains a critical and challenging issue.

This work first presents a survey on recent advances in security requirements and services in group communications in wireless and wired networks, and discusses challenges in designing secure group communications in these networks. We then propose effective security services to secure group communications. This dissertation introduces the taxonomy of security services, which can be applied to secure group communications, and the evaluation of existing secure group communications schemes.

This work next discusses the proposed trust and reputation system for an anonymous network, referred to as the Adaptive Trust-based Anonymous Network (ATAN). The distributed and decentralized network management in ATAN does not require a central authority so that ATAN alleviates the problem of a single point of failure. In some existing anonymous networks, packets are routed onto intermediate nodes anonymously without knowing whether these nodes are trustworthy. On the other hand, an intermediate node should ensure that packets which it forwards are not malicious, and it will not be allegedly accused of involving in the attack. To meet these objectives, the intermediate node only forwards packets received from the ‘trusted’ predecessor, which can be either the source or another intermediate node. In ATAN, our trust and reputation system aims to enhance anonymity by establishing a trust and reputation relationship between the source and the forwarding members. The trust and reputation relationship of any two nodes is adaptive to new information learned by these two nodes or recommended from other trust nodes. Therefore, packets are anonymously routed from the ‘trusted’ source to the destination through ‘trusted’ intermediate nodes, thereby improving anonymity of communications.

This work analyzes a number of vulnerabilities against trust and reputation systems, and proposes a threat model to predict attack behaviors. In the threat model, the behaviors are classified into two categories: selfish (but not malicious) and malicious. This work also considers that multiple attacking agents actively and collaboratively attack the whole network as well as a specific individual node. The behaviors may be related to both performance issues (i.e., disrupting the network activities, and undermining the availability of the system) and security issues (i.e., revealing integrity or fabricating confidentiality of information). Then, this work extensively examines and substantiates the security of the proposed trust and reputation system.

Committee Members:

Dr. Nirwan Ansari, Professor, ECE Dept., NJIT (Advisor)

Dr. Roberto Rojas-Cessa, Associate Professor, ECE Dept., NJIT

Dr. Edwin Hou, Associate Professor, ECE Dept., NJIT

Dr. Yanchao Zhang, Assistant Professor, ECE Dept., NJIT

Dr. Rajarathnam Chandramouli, Thomas E. Hattrick Chair Professor of Information Systems, ECE Dept., Stevens Institute of Technology