Abstract

Today, enterprise networks face security threats due to improper security policies and their incorrect implementations. Typically, an enterprise network consists of a set of network zones interconnected through various access routers (layer 3 devices). The security policy of such networks define a set of rules for allowing/denying various service access paths based on certain constraints. These policy rules may contain complex access constraints (such as, temporal, spatio-temporal). The implementation of these policy rules are realized in a distributed manner in the routers through a set of access control lists (ACLs). One of the major challenges for the network administrator is to verify the correctness of security implementations with respect to the enterprise security policy. This verification problem becomes more complex due to presence of inconsistent *hidden service access paths* in the security implementation which are often ignored. In this thesis, a Boolean satisfiability (SAT) based approach has been presented to formalize the core verification problem. The thesis studies several non-trivial variants of the core problem, such as the verification of security implementations under network topology changes and verification of security implementations in Wireless LAN. The thesis also presents a network security analysis tool for systematic analysis of security implementations with various service access queries.

Key words:
Network Security, Security Policy, Access Control Lists (ACL), Formal Verification, Wireless LAN, Role based Access Control (RBAC).