A goal-based modeling approach to develop security requirements of fault tolerant security-critical systems

ABSTRACT

Large amount of (security) faults existing in software systems could be complex and hard to identify during the fault analysis. So, it is not always possible to fully mitigate the internal or external security faults (vulnerabilities or threats) within the system. On the other hand, existence of faults in the system may eventually lead to a security failure. To avoid security failure of the target system we need to make it flexible and tolerant in the presence of security faults. This paper introduces a goal-based modeling approach to develop security requirements of security-critical systems (SCSs) by explicitly factoring the faults into the requirement engineering process. Our approach establishes a model for security requirements (SRM) with respect to the formally described model of security faults (SFM). We care for fault tolerance in SRM by taking into consideration partial satisfaction of security goals. The proposed approach factors this partiality into the goals by applying proper mitigation techniques during the refinement process. This eventually contributes to a fault tolerant model for security requirements of the target system.

Keyword: Intrusion tolerance; Security fault; Threat; Vulnerability