PROACTIVE THREAT MANAGEMENT FOR
SECURING SOFTWARE SYSTEMS

ABSTRACT OF THE THESIS
SUBMITTED TO THE UNIVERSITY OF DELHI
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY

By
Vandana Gandotra

Under the Supervision of
Dr. Archana Singhal

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF DELHI
DELHI – 110 007
INDIA
2012
Abstract

Software systems these days are at the centre of all areas of technology throughout the world. No one had ever predicted that software will become an indispensable part in all spheres of life whether it is financial systems, communication networks, defense technology or other exploratory missions. This has resulted in exponential growth of software industry in last few years revolutionizing the world in an unimaginable way.

In earlier times software systems and networks posed no or very little security problems as the computers were usually islands of functionality, with more or less no connectivity. Due to complexity of software systems, incredible level of interconnectivity and infusion of new technologies, there has been a steep rise in vulnerabilities and security breach incidents over the last few years as reported by CERT Coordination Centre, Software Engineering Institute, Carnegie Mellon University. Moreover, attackers these days are no longer random hackers but their attacks are targeted, purposeful and organized for financial gains giving new dimensions to security problems. Keeping in view the security requirements of present day threat environment and escalated risks for software users, a transition to a more stringent software development process is needed that focuses on security aspect of software systems. A number of security experts have therefore enhanced existing software development life cycle by incorporating various security techniques in all its phases for preserving fundamental security attributes. Secure software engineering has thus been evolved as a new approach wherein security features are ‘in-built’ rather than ‘on-bolt’. These security measures are effective to a point to avert threats but cannot meet new challenges of this information age as recent survey reports (Microsoft, Symantec and so on) indicate substantial growth in security breach incidents due to new threat perceptions. We have therefore been motivated to extend this area of research and evolve threat-oriented security model by integrating various proactive and innovative security techniques as a part of proactive risk management. Moreover, these new security measures have been designed to avert threats optimally to fulfill the needs of CEO’s who are looking for minimizing security risks with limited resources in this changing economic scenario.
This work presents a proactive approach in threat management to help system designers to implement well-structured security processes from early phases of software development life cycle to save the system from being compromised to the extent possible. Hybrid technique has been evolved in this security process for elicitation of flawless and meaningful security requirements which forms the very basis of any secure software design. Hybrid process diagram in this innovative technique also helps in determination of security features to be incorporated as countermeasures in the light of evolved security requirements. Multi-layered defense strategy has been adopted in this work as an enhancement to overcome the shallowness of single ring security. Present security measures are based on binary principle making the system to be in either of two states i.e. safe state or failed state. Proactive defense mechanism using fuzzy logic has been evolved and adopted in this security process to avert the failed state of software systems as it may be catastrophic from the user’s point of view. ‘Adaptivity and Intelligence’ is the most important attribute of security mechanisms desired these days to thwart multipronged threats from sophisticated hackers. Multi-agent system planning for threat avoidance (MASPTA) has therefore been adopted as a proactive strategy in threat management where autonomous agents coordinate and communicate with each other to achieve the goal of software security. This work also presents different methods i.e. Multi-Agent System Planning for Threat Avoidance Optimally (MASPTA-O) and Optimal Countermeasures Identification Method (OCIM) to arrive at optimal solutions for threat/vulnerability management. In the present day economic scenario it has become the principle factor for any security initiative.

As malicious users are finding new ways to intrude into the systems these days, security mechanisms should be more flexible and intelligent enough to withstand both known and unforeseen attacks. It may not be possible to achieve this objective using single security paradigm. An integrated security mechanism has therefore been proposed which comprises various proactive steps described above to address present day security issues in threat management. Threat-oriented security model having layered architecture presented in this work provide an answer to avert both known and unforeseen threats optimally to the extent possible. Every layer of this model contributes towards enhancement of security measures deployed at present
and provides two-fold protection strategy. First layer of this threat-oriented security model captures both known and unforeseen threats using threat modeling process and research honeytokens whereas in the existing security mechanisms only known threats are taken care of. Two-level optimization of threats to be mitigated in the second layer of proposed model validates its economic justification over traditional security solutions. Mitigation of identified optimum threats using multi-agent system planning is the function of third layer. Monitoring and management of these threats using meta-agents in conjunction with fuzzy logic at the fourth layer of this model overcomes the limitations of present day security mechanisms based on binary principle. Moreover, in-built guidelines described at zero layer supplement defense mechanisms of this security model by providing dual protection in case the attacker intrudes into the system boundary. Embedding of this threat-oriented security model in risk analysis segment of spiral framework having iterative nature provides progressive and rapid development of increasingly more complete versions of the engineered systems with decreasing risk.

With explosive growth of advance communication technologies, provision of electronic services in the banking organizations for fund transfers and account management etc. has become a universally accepted common practice. At the same time various survey reports indicate increase in number of malicious attacks/fraud incidents targeting online banking for financial gains in recent years. It indicates that conventional security measures are no longer sufficient to provide safe online banking environment due to changing threat perceptions. Different proactive security measures adopted in threat-oriented security model have therefore been applied and demonstrated for securing online banking applications optimally as a subject of case study to support and validate their potential in threat management. These security measures have been simulated using a web based application on Apache Tomcat Server, JADE (Java Agent Development Environment), with MySQL Server at the backend. Experimental results and analysis of security measures taken in this respect have also been presented and discussed to support the proposed work with the help of test cases.
Research Publications


