Software Threat Modeling: Types and Techniques

Pooja Rani, Dalwinder Singh Salaria

1Dept. of CSE, Lovely Professional University, Phagwara, Punjab, India

Abstract

Security plays a major role in the development of secure software systems. Security should be integrated in all stages of Software Development Life Cycle (SDLC). Attacks on the vulnerable software are continuously increasing day by day. Most of the attacks are result of insecure configuration of software. Therefore, software developers should design the software having security in mind and should reduce the security flaws in the early stages of software development life cycle so that secure software is developed. In this paper, we present the review of some approaches used to introduce and fix the threats along advantages and disadvantages. Statistical techniques, Neural network, Fuzzy logic, Genetic algorithm and Neuro-Fuzzy are some techniques used for software threat modeling.

Keywords


I. Introduction

Software threat modeling allows the software developers to identify and mitigate the security issues during the early stages of software development life cycle where they are cost-effective and easy to resolve. Security software is threatened at various stages of software development life cycle, both by “insiders” or “Outsiders”. Insiders are the legitimate users and having privileges to access the resources and information of the organizations. Outsiders are not legitimate users and having no privileges to access the resources and information of organizations. Previous research shows that to integrate security into software applications at later stages of software development life cycle (SDLC) has been found more costly than when it is integrated during the early stages [1]. To develop the software that is reliable, secure, of higher quality, of affordable cost, easier to maintain and free from defects, it is preferred to find and fix security flaws during the early stages of software development life cycle, because after development and implementation of software to find and fix the security flaws is 4-8 times higher than when they are discovered and fixed early in SDLC [1].

II. Review of literature

In the past, many of the statistical techniques were used to model, mitigate the threats, but with the passage of time more new techniques are introduced to over the limitations of past techniques and provide the better accuracy. We introduced three broad areas where software is used, software threats are identified and different methods or approaches are proposed to cope up with these software threats that lead to the development of secure software system.

A. Cyber Threat

The top most priority is to combating the cyber threats. Research work for evaluating threat assessment proposes simulation work and compares the uses of different statistical measures for such evaluation. The result of simulation shows that false positives and false negatives are the metrics may not be sufficient for evaluating cyber threat assessments [14]. To forecast the threat trend, Hidden Markov Model (HMM) is proposed and has compared this model with time series trend analysis model. The Supplemental environment information is required to discover trend pattern from hidden data. This model is feasible and adaptive to dynamic environments [15]. Insider threats are the harmful acts carried out by the legitimate and trusted individuals having authorization to access the data, information or resources of an organization. Training programs are conducted to help the staff and management regarding threat awareness and mitigation. MERIT workshop is an initial step for effective training about the insider threat risk and mitigation [2]. Threat modeling is a technique that is used to identify the threats, vulnerabilities and countermeasures that can influence the software. Threat Analysis and Modeling (TAM) tool is used to introduce the threat modeling over business applications [3]. Cyber Threat Tree is used to represent and to identify the critical threats of large systems, because the large systems may have many threats that may be interdependent. Cyber Threat Tree is implemented as directed graph known as Multiple Value Decision Diagram (MDD). It provides the compact representation of threat catalogue. Cyber Threat Markup Language (CyTML) is used to convert the result of risk assessment into cyber threat tree [16].

B. Software Security

Software security deals with the development of secure software. In today’s world, our functioning of the work depends upon the use of computer systems. Insider Threat Prediction Tool (ITPT) is used to predict the misuse of computer systems by legitimate users either intentional or accidental way. Insider Threat Prediction Model (ITPM) is a three level hierarchy of mathematical function that performs the actual process of predicting the threats [4]. A single framework is provided for dependability and secure computing that is extremely useful and it also provides the way for the problem that what exactly the user expects from the system. It proposes a fault–error–failure model to identify and understand the various threats that may affect the system [5]. Regular Expression Based Attack pattern approach is proposed to identify the vulnerabilities through matching a sequence of components that trigger an event in an attack. If match exist that means vulnerability exists in software application. It increases the security awareness during early stages of development life cycle [6]. Threat Mitigation, Monitoring and Management Plan is an approach that deals with the management of risks. This approach is used at design stage of software development life cycle that makes the software system more secure. It uses Defense in Depth (DID) strategy i.e. a multi-layered approach that protects the items or data by passing the hurdles in the path of attacker and makes his work difficult [17]. Extended Model Driven Architecture (MDA) approach is used with the addition of quantitative security assessment model that provides the feedback at every phase of software development life cycle that will help to identify security flaws as early as possible [18]. Threat modeling is an approach that helps to mitigate the risks, to prioritize the type of attacks that has to address. This process involves the identification of security objectives, to create and decomposes an application, identification of threats and vulnerabilities [7]. Risk Ranking Tool (RRT) is used to prioritize the identified threats using Common Vulnerability Scoring System.
(CVSS). This tool does not require any numerical input values like probability, it translates the yes/no values into numeric values and generates a risk score by using common vulnerability scoring system (CVSS) [8]. Two approaches are introduced to identify the effects of threats and to developing countermeasures and these techniques are Software Requirement Patterns (SRPs) and Software Design Patterns (SDPs). Software Requirement Patterns (SRPs) used to identify the threats in requirement phase and Software Design Patterns (SDPs) used to identify alternative countermeasures against identified threats and can accurate comparison of the countermeasures [19]. Complexity, Code churn and Developer activity (CCD) metrics approach is used to build the vulnerability prediction model. With the guidance of complexity, code churn and developer activity (CCD) metrics, Developers can predict the work of security inspection and testing efforts helps to reduce the code to test or inspect [9]. Many software that are embedded with “agents” i.e. a block of code can be the security threats if the developer has intention to do so. Sometimes the features of software go beyond the requirements of the user may cause breach of security [20]. Apollonian Model is used to manage the knowledge acquired by the software development projects and to reduce the uncertainty of selection and prioritization of threats. It also helps to minimize the risks. This model is based on the artificial intelligence technique “Rough Set” [21]. There is also need to develop the secure products at the level of Advanced Persistent Threats (APTs). These are the high profile security attacks and incidents. Secure software should also be able to log and report the attacks that have been prevented [10].

C. Threats to Software used by Networked Organizations

Integration of threat modeling with threat analysis helps to identify, documenting the threats and countermeasures in personal networks [22]. A new approach is introduced through which an analyst provides reliability statistics for the identification of top node in the network. Controlled experiment is a method that uses the probability tables to identify the top threats in a network [23].

III. Modern Techniques

There are some other modern techniques to model the software threats.

A. Soft Computing Based Techniques

1. Fuzzy Logic

Fuzzy logic is an approach that presents a natural way of modeling the vagueness. It deals with the approximation instead fixed and exact. Risk analysis defines to study of exposures and their potential harm. Fuzzy logic risk analysis modeling techniques is also introduced that enables the users to model the real world risk scenarios [11]. A web based Fuzzy Decision Support System (FDSS) is developed to identify, analysis and prioritize the risks in electronic commerce [12]. A computer immunology model is introduced for the detection of software anomalies (masqueraders) in which fuzzy logic technique is used for the evaluation of threat. The results show the improvement over several other intrusion detection methods [24]. Secure Software System (SSS) approach is introduced to develop the secure software system. This approach has tried to avert the failed state of system by the induction of Fuzzy logic [25].

2. Genetic Algorithm

Genetic algorithms are adaptive heuristic search algorithms. Heuristic is used to generate the solutions for optimization and search problems. Genetic algorithm based approach is also introduced to network intrusion detection. The genetic algorithm is used to derive a set of rules from network audit data [28].

3. Neural Network

A Neural Network is massively parallel distributed processor made up of simple processing elements called neurons to perform various computations in faster manner. It is having ability for learning. The usage of neural network offers the various properties like Nonlinearity, Fault Tolerance, Adaptivity, Input-Output Mapping, and Neurobiological Analogy. Intrusion detection systems are designed to identify unauthorized use, misuse of information or resource and attacks on information systems. User behavior modeling approach is introduced with the use of neural network to intrusion detection system [26]. In different Bayesian Network based model is introduced for software failure prediction. Bayesian network is a tool that has adaptation ability in problems having complex variant factors [13]. Approach, neural network and support vector machine is introduced it intrusion detection system [27].

4. Neuro-Fuzzy

Neuro-Fuzzy approach is a combination of Fuzzy systems and neural network that is designed to create an architecture that uses the fuzzy system to represent the knowledge in interpretable manner and learning ability of neural network to optimize its parameters. The hybridization of these results in hybrid intelligent system. Hierarchical Neural Fuzzy Online Risk assessment (HINFRA) model is proposed for the decision making process of Distributed Intrusion Prediction and prevention Systems (DIPPS). Preliminary results show that neural network techniques could improve the performance of fuzzy controller and make the risk assessment model more robust [29].

Table 1: Summary of software threat modeling approaches

The following table summarizes all the above explained techniques with their basic idea, pros and cons:
Table 1. Summary of Software Threat Modeling Approaches with Their Advantages and Disadvantages

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Techniques</th>
<th>Key Idea</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>Fuzzy logic</td>
<td>Fuzzy logic is used in threat modeling because it uses the linguistic variables such as (cold, warm or hot etc.)</td>
<td>1. It uses the linguistic variables. 2. It is designed to use in situations where information is not exact.</td>
<td>1. It does not always provide definitive results. 2. It requires finer tuning and simulation before become operational.</td>
</tr>
<tr>
<td>B.</td>
<td>Genetic Algorithm</td>
<td>Genetic Algorithms are adaptive heuristic search algorithms that are used to generate the solutions to optimization and search problems that can be represented by vector of binary values.</td>
<td>1. It can solve the optimization problem. 2. Genetic algorithm can easily transfer to existing simulations and model. Thus it provides the flexibility.</td>
<td>1. Certain optimization problems like variant problems cannot be solved by Genetic algorithms. 2. In real time systems, it is unreasonable to use genetic algorithms for online controls without testing them firstly on simulation model.</td>
</tr>
<tr>
<td>C.</td>
<td>Neural Network</td>
<td>Neural Network is massively parallel distributed processor that is made up of simple processing elements called neurons.</td>
<td>1. It has an ability to generalize and learn. 2. It is having the capability of fault tolerance. 3. Non-linearity is feature that is distributed through the network.</td>
<td>1. It requires a large training data set to be trained properly. 2. This is black box approach means the internal working of system is unknown. 3. It provides the approximations of desired solutions.</td>
</tr>
<tr>
<td>D.</td>
<td>Neuro Fuzzy</td>
<td>It is hybrid approach of fuzzy systems and neural network. It results in hybrid intelligent system.</td>
<td>1. It represents the knowledge in interpretable manner and optimizes learning parameters. 2. Hybridization results in hybrid intelligent system.</td>
<td>1. They are based on human decision policy means we have to decide the fuzzy set.</td>
</tr>
</tbody>
</table>

### IV. Conclusion
From the above discussion, we conclude that there are many techniques which are used for modeling the software threats. Each technique has its own advantages and disadvantages. We cannot say, anyone of the approach overcomes the limitations of other approaches, but the hybrid approaches like Neural network with support vector machine [27], Neural network with Genetic algorithm [28], Neural-Fuzzy [29] results in hybrid intelligent system that can provide better level of accuracy.

### References


Pooja Rani is doing M.Tech (CSE) from Lovely Professional University, Phagwara, Punjab, India. Her research interests include software engineering.

Dalwinder Singh Salaria received his B.E. degree in CSE from SSJCOE, Jalgaon(MH), INDIA, in 2003 and the M.tech degree in CSE from Guru Nanak Dev Engineering College, Ludhiana (PB), INDIA, in 2008. He is working as an Assistant Professor with Department of CSE at Lovely Professional University (PB), India. His research interests include databases and Software engineering.