A Threat Analysis Methodology for Security Evaluation and Enhancement Planning

Janki Patel

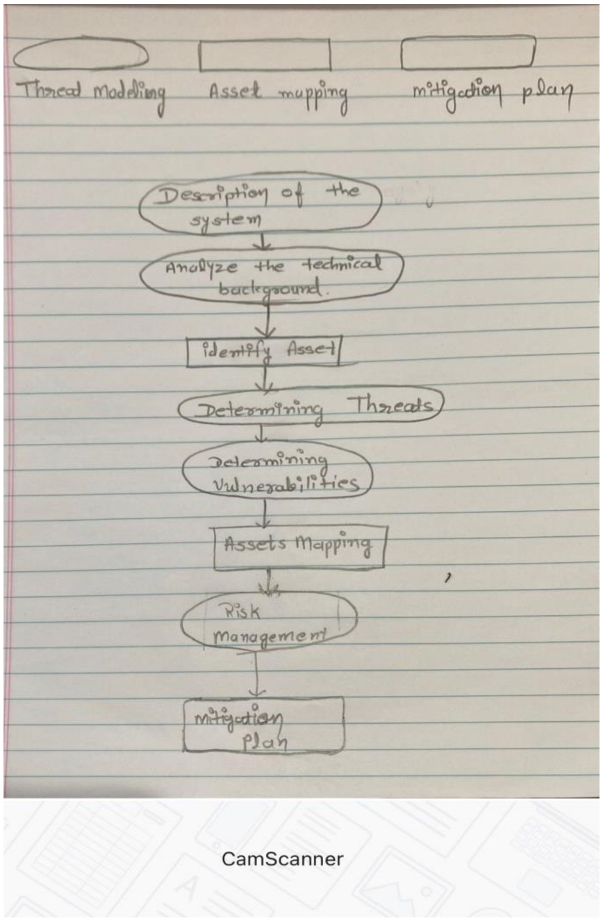
(10457365)

Paper Link

https://www.researchgate.net/publication/221215586_A_Threat_Analysis_Methodology_for_Security_Evaluation_and_Enhancement_Planning

In this research paper, how we can find out any kind of attack through plan as well as how we can protect any system from any kind of attack for that how we can plan for the system. Security is most important thing for everyone specially in network area where it has personal information of user. To planning for threat modeling for the system which help prevent the attack or identify that and also UML diagram helpful for that.

- Threat analysis methodology
  Threat analysis can be divide in three main part which is threat modeling, asset mapping and mitigation plan. Here , I define the step of threat analysis



threat demonstrating is valuable when we done this threat examination in the beginning of the stage when we are making framework. Resource planning include unmistakable and immaterial asset of the application which distinguish passage point of framework. it is utilized as base incentive for threat chance and furthermore focus on countermeasures. In the third stage building alleviation plan where examination will choose which resource of threat will remember for relief plan as per the experience for that expert ask that assessed the moderation level for every countermeasure give to the danger and another is gauge complete degree of alleviation give to threat risk. Yield of this set countermeasure which alleviate threat identifier. Presently we will clarify every single step of threat approach.

I. **Step 1:Description of the system**: - for that it need to understand each connection and the scenario and also user case diagram which help to understand batter what system is and easy to learn from every perspective.
II. **Step 2:Analyze technical background of use case:** - to analyze each everything for that UML sequence diagram is best choice through that it can understand object interaction with timing . In this it has to analyze how our system will user and who will use it.

III. **Step 3:Identify Asset: -** In this it has to determine each every which damage in network. Asset can be tangible or abstract. Asset is depend on situation as well as on the user.

IV. **Step 4: Determining Threat: - Using** data which we gathered so far though that we can start to identify the threat. According to the threat source are define by human , natural and environmental. Threat is corelated with asset as well as entity.

V. **Step 5: Determining Vulnerabilities: -** In this step to determine vulnerabilities of the system. when each and every scenario are defined then it is easy to deduct what threat are exploiting in the use case analyzed. Each and every vulnerability define as ID which has name and their threat.

VI. **Step 6: Asset Mapping: -** we as of now characterize resource in the past advance. Presently it is likewise critical to decide courage of the resource and their danger. Bases on that esteem it will focus on it. For doling out the worth by three diverse way

   a. High asset:- in that value have protect them with high level of security. It is directly linked with main control of the system with service which has higher security.
   b. Medium asset: - In that value has linked with common service and it is also important as intermediate financial value.
   c. Low Asset: - it is for minor importance.

VII. **Step 7: Risk Management: -** In this progression It is oversee between what is worthy and what is conceivable. It is feasible to separate data from threat and vulnerabilities for most elevated threat esteem.

VIII. **Step 8: Mitigation Plan : -** In the last advance of the threat investigation is that development of a relief plan that include decision of the countermeasures. Additionally, to make a relief plane it is important to recognize the countermeasures. During that progression the threat picked for relief ought to act naturally tended to by one or extra countermeasures.

The consequences of the technique could be a bunch of projected countermeasures that will alleviate the threat that were recognized. Since the execution of the relative multitude of projected countermeasures is, in the greater part of the cases, unfeasible on account of requirements in spending plan, time and assets, the objective of a useful threat investigation technique is to propose the arrangement of the most effective countermeasures against the known threat.

- Metrics and measurements to prioritize threat and vulnerabilities

Legitimate security measurements - important inside the last strides of the arranged strategy territory unit a serious troublesome interest in an extremely threat examination in order to work out the remaining of organization security execution and to any improve it by limiting openness to heavy threat and vulnerabilities. Security experts need to focus on the threat with regards to the particular framework and thusly need

- An organized outline of the assurance setting, which may epitomize all vulnerabilities of the framework, their interrelation and their communication with security components inside the framework.

- A typical mensuration communicating the seriousness and hazard of every vulnerabilities, and in this way the significance of the relating danger.

Assault Trees address assaults against a framework all through a tree structure, with the objective because of the premise hub and elective courses of accomplishing that objective as leaf hubs. all through this system, there are typically numerous potential ways that among the tree for degree wrongdoer by means of abuse differed vulnerabilities and from multiple points of view. In the subsequent advance tree and hub needs to allocate any worth to characterize which is on basic circumstance. When it allotted ideal way for aggressor are uncovered. CVSS is stander approach to allocate esteem on the assault tree hub. The CVSS evaluation partitions the vulnerabilities issues into 3 territories:

- Base, for characteristics straightforwardly describing the vulnerabilities.

- Temporal, for qualities concerning the vulnerabilities exploitability and deep rooted.

- Environmental, for qualities reliable to the specific framework and setting.

Conclusion

In this paper proposed to characterize threat system which coordinate threat demonstrating with formal threat investigation for PNs. It is rely upon three technique threat modeling, asset planning and building mitigation plan. Besides, another arranged way to deal with portray the framework and to detect the resources has been received using the UML use case charts, we can utilize UML use case explicit. The recognizable proof of the threat, passage focuses and vulnerabilities closes the threat demonstrating area. the need to evaluate threat and vulnerabilities during this part has been led by means of utilization of a joined philosophy to rank threat and vulnerabilities abuse each assault trees and CVSS rating framework, as outlined by the gave guide to a private Network extortion circumstance. At last the moderation organize are frequently give out. This arranged work is advantageous in every framework to achieve an entire threats investigation, assessing threat and vulnerabilities with ordinary measure, with weight on client driven designs like that of a PNs.

I am definitely agree with author point of you. This process is work for each and every application and also work best for that to identify threats and vulnerability. Through that we can give priority of threat as well as we can decide which threat we have to focus first. At the end of it is very helpful for any projects.