International Journal of Pure and Applied Mathematics
Volume 115 No. 8 2017, 121-126
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue
ijpam.eu

PROFILING THREAT MODELING APPROACHES AND METHODOLOGIES FOR IT AND CLOUD COMPUTING

Unnikrishnan B[1], Kamalanathan Kandasamy[2]
Center for Cybersecurity Systems and Networks
Amrita School of Engineering, Amritapuri
Amrita Vishwa Vidyapeetham
Amrita University, India
[1]unnikrishnan.balenduhouse@gmail.com, [2]kamalanathan@am.amrita.edu

Abstract: One of the major issues in cloud services is that intruders can bypass authentication by exploiting vulnerabilities, particularly in the design phase of a software system. Hence, there is a need for a standardized approach to identify vulnerabilities to ensure user data protection. Threat models are designed to identify security bugs in advance. This paper presents a comprehensive survey on the numerous threat modeling approaches and methodologies in IT and cloud computing areas.

Keywords: Threats, Threat modeling, IT purpose, cloud computing.

1. Introduction

Security threats are a major concern for business enterprises. The ultimate aim of a security expert is to protect sensitive information from unauthorized access. In the modern IT world, rules and administration impelled organizations to follow certain standards to avoid breaches that causes economic losses, which will be discussed later on in this paper. Initially, we are addressing various information security threats. A threat is defined as A possible danger that might exploit a vulnerability to breach security and cause harm [2]. In cloud security, the main challenge is to protect data from confidentiality, integrity, and availability breaches. Threat modeling is a designed as an aligned and systematic approach to detect all possible threats in the early phase of software systems and it is used to protect systems from vulnerabilities. Threat modeling collects the background information which is in the form of external dependencies, usage scenario, external and internal security implementation. It also helps to provide standard mitigation techniques for identified threats. This paper presents a brief survey of different threat modeling approaches in IT purpose and cloud computing. These days, the IT industry has become more scalable and cost effective for developing secure applications, though there is a rising need for security in the design phase.

2. Threat Modeling Approaches

The intention for composing a threat model is to identify malicious threats and prioritize them in an organization. It is a structured way of assessing security risks for a particular application. Modern threat modeling approaches are based on an intruder point of view. The following section will present a short survey of various threat modeling methodologies and approaches.

3. Threat Modeling Approaches In General

Based on different contexts, threat modeling approaches can be broadly classified into three categories [1]. First one is software centric threat modeling. In this approach, data flow diagrams or use case diagrams are used for drawing software architecture diagrams mainly utilized for the design of the threat model of networks and systems. Microsoft secure development life-cycle(SDL) is an example for software centric threat modeling. Using this approach, we can identify threats to each component and can mitigate that threat in the design phase itself. Next is asset centric approach, which identifies assets of an organization entrusted to a software. The classification of the assets are based on data sensitivity and their essential value to an intruder. Various multi-step attacks and paths can be identified by using the asset- centric approach. A security expert can generate attack trees, attack graphs that help to identify which asset can be attacked by using an asset centric approach. Trike, Amenazas, and Securitree are examples for the asset centric approach which is used for creating attack graphs and attack trees. There is one more approach called the Attacker-Centric approach, which focuses on specific goals of an attacker. By using this approach, one identifies how the attack could happen and how to prevent that attack. An analyst can list out attack patterns to help decision making in an organization.

4. Threat Modeling Approaches For It Purposes

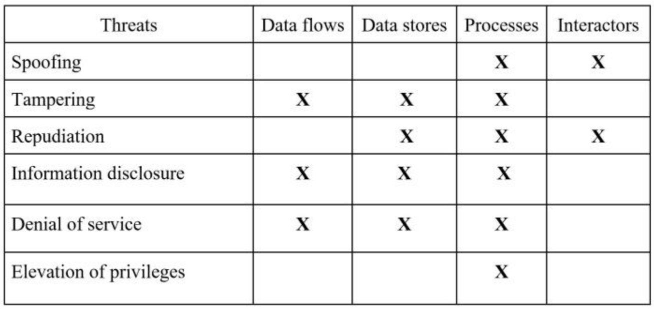
Various threat modeling methodologies are available for IT purpose.Here we presents a brief survey of existing threat modeling methodologies for IT purpose.

A. Stride

STRIDE is a well-known and most commonly used threat modeling approach. This approach was invented by Loren Kohnfelder and Praerit Garg in 1999. STRIDE

Model is an abbreviation that consists of six different categories of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privileges [1][2]. DFD is the input of this approach and each node of the DFD is applied to the system. Subsequently, the possible number of security threats will be identified, as well as feasible mitigation.

Microsoft SDL threat modeling tool applies the STRIDE approach and it is called STRIDE-per interaction[3][4].



Threats	Data flows	Data stores	Processes	Interactors
Spoofing			X	X
Tampering	X	X	X	
Repudiation		X	X	X
Information disclosure	X	X	X	
Denial of service	X	X	X	
Elevation of privileges			X	

Figure 1. STRIDE-PER-INTERACTION

B. Dread

Microsofts DREAD model is a widely used approach to manage the exponential risks associated with security threats. In this approach, each relative risk is categorized into two different metrics, one is Low, Medium, High and Ordinary Ranking[5]. DREAD model classifies security threats into five different categories.

- ***Damage Potential :*** If the attack is successful, then it is used to rank the extent of the damage.
- ***Reproducibility :*** It ranks how often an effort to reproduce an attack works.
- ***Exploitability :*** It ranks how easily to reproduce the threat exploit.
- ***Affected users :*** If an exploit is widely available, it is used to estimate fraction of installations affected.
- ***Discoverability :*** Used to discover the vulnerability by an attacker.

In DREAD model, the risk can be calculated by taking average of 5 categories[2].

RISK _ DREAD = [Damage Potential + Reproducibility + Exploitability + Affected users + Discoverability] /5.

C. Trike

Trike is a popular risk based approach with distinct implementation, threats, and risk models. A defined conceptual framework used for security auditing from a risk management perspective that enables communication among security Team members and stakeholders[5],[6]. The main features of TRIKE compared to other threat methodologies are the degree of formality and the high level of automation that is possible within the system. There are two tools available for this methodology; One is a standalone tool which is already outdated, and the other one is spreadsheet v2, which is the current version of this methodology[7]. TRIKE methodology is presently in the construction phase; it is not fully tested with real systems.

D. CVSS

Common vulnerability scoring system (CVSS) is a framework used to provide a clear representation of a vulnerability. The main features of CVSS are that it provides a standard open framework which is used to standardize vulnerability scores, and it is also used for prioritizing risks. CVSS consist of three metric groups: Base, Temporal, and Environmental [8]. These groups will produce a numeric score ranging from 0 to 10, and a Vector, used for a compressed textual representation that reflects the values used to derive the score.

E. P.A.S.T.A

Process for Attack Simulation and Threat Analysis is a new application threat methodology invented by Marco Morana and Tony UV. It is a seven step methodology used for providing dynamic threat identification, enumeration and scoring process. It is similar to the SDL process, in that an application decomposed into DFD components is used to illustrate the threat model, from which threat and vulnerability analysis can be performed[9]. This methodology gives an attack centric view by using attack trees combines with risk and impact analysis. It will definitely helps various organizations to establish an asset centric approach to improve mitigation strategy.

F. Attack Trees

Attack trees are used to provide formal way of describing the security of systems, based on potential attack type[10]. The tree structure consists of a goal which is at the root node, as well as leaf nodes(subgoal), which represent different ways of achieving that goal. It also has AND and OR options which represent alternatives and different steps towards achieving that goals[11]. A java application called SecurITree, which is an Attack tree modeling tool, is used to draw very complex diagrams using capability- based modeling.

G. T-MAP

T-MAP is an approach which is used in Commercial Off The Shelf (COTS) systems to calculate the weights of attack paths. This model is developed by using UML class diagrams, access class diagrams, vulnerability class diagrams, target asset class diagrams and affected Value class diagrams. There is a tool called Tiramisu[12], which is automated, used to calculate a list of all attack paths and produce overall threats in terms of total weight of attack paths.

H. Fuzzy logic

Fuzzy set theory is the basic principle for fuzzy logic threat modeling methodology. An automated tool support called MATLAB Fuzzy tool is used to identify the security threats. By using the STRIDE model, the input variables are passed to the fuzzy inference engine. Then engine generates a list of threats as a result[13].

A. CORAS

It is a seven step, UML based methodology of

Cloud privacy threat modeling

CPTM methodology was the first instinctive threat eling methodology for privacy preservation in the cloud puting paradigm. The main purpose of CPTM is to sensitive data EUs DPD. This methodology consists of requirements, important privacy threats, and countermeasures for identified privacy threats[13]. The overview of privacy threat modeling is given below.

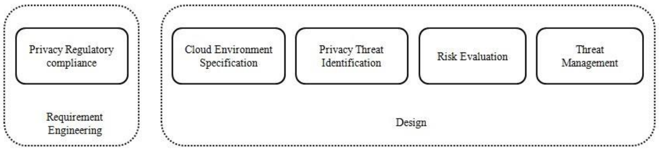

Privacy Regulatory compliance
Requirement Engineering
Cloud Environment Specification
Privacy Threat Identification
Risk Evaluation
Threat Management
Design

Figure 2. Overview of cloud privacy threat modeling

conducting risk analysis. There is a tool called diagram editor which supports this graphical threat modeling.The profile consists of use case diagrams which are used for threat modeling and unwanted behaviors[14].It is working based on Australian Risk Management Standard AS/NZS 4360:2004. CORAS threat modeling consists of four steps: establish the context, identify and analyze the risks, risk evaluation and manage risks.

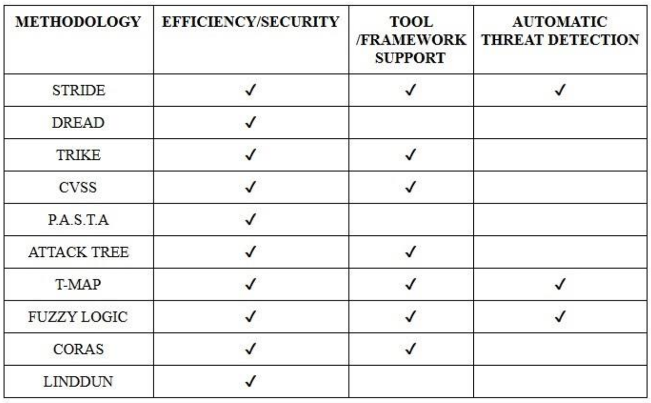
LINDDUN

LINDDUN is a privacy threat model based approach used to evoke privacy threat modeling of software based systems (Deng et al., 2011; LINDDUN portal, 2014).LINDDUN privacy threat modeling resembles STRIDE. LINDDUN consists of a three step process: model the system as DFD based on use case scenario, map the DFD elements to seven privacy threat categories, and document those identified threats. The seven privacy threat categories are:

1) ***Linkability :*** occurs if two item of interest are related(IOI, eg: request of a user)
2) ***Identifiability :*** occurs if it is possible to locate a subject (eg: user).
3) ***Non - repudiation :*** occurs only if it is possible to collect the proper evidence.
4) ***Detectability :*** occurs if an attacker can sufficiently differentiate whether the IOI exist or not.
5) ***Information Disclosure :*** is the unauthorized access to the personal information .
6) ***Unawareness :*** occurs when user is unaware about the information which he sharing to the system.
7) ***Non - compliance :*** occurs if system is not compliance with its policies and legislation.

. Threat Modeling Approaches For Cloud Computing

Table 1: Summarized Threat Modelling Methods



METHODOLOGY	EFFICIENCY/SECURITY	TOOL /FRAMEWORK SUPPORT	AUTOMATIC THREAT DETECTION
STRIDE	✓	✓	✓
DREAD	✓		
TRIKE	✓	✓	
CVSS	✓	✓	
P.A.S.T.A	✓		
ATTACK TREE	✓	✓	
T-MAP	✓	✓	✓
FUZZY LOGIC	✓	✓	✓
CORAS	✓	✓	
LINDDUN	✓		

The importance of threat modeling in cloud security is to protect assets from confidentiality, integrity and availability violations. Other than Microsoft threat modeling and Microsoft's threat analysis and Modeling (Malik et al., 2008), there are various numbers of threat modeling techniques that have been developed for threat analysis[3]. *A.*

The main drawback of CPTM methodology is that its only privacy legislation is EU. In 2016, (Ali Gholami and Erwin Laure,2016) a new extended version of cloud privacy threat modeling with two steps was developed (ie a requirement engineering phase and a design phase). This methodology identifies privacy requirements in the requirement engineering step[15].

B. Threat model framework and methodology for Personal Networks (PNs)

This threat model framework is used for building secure networks that use tools like UML sequence diagrams and attack trees to model threats. Threat model framework consists of a good detailed overview of a system by describing functionalities and deployment of a network. Personal Networks are networking devices that are used for personal purposes like telecommunications, financial transactions, information, and entertainment (Prasad, 2007) [6]. This threat model has seven step process including threat report, consist of threats and vulnerabilities rank on the basis of risk and its size[14].

C. Practical Threat Analysis

The purpose doing for practical threat analysis is to identify system vulnerabilities, and based on that, a risk mitigation plan for a specific system architecture and its functions[16].Practical threat analysis tools are used to identify system asset values and the damage level caused by the attackers. This methodology has four major steps. First step is to identify assets and their financial values. Second step is to identify system vulnerabilities and plan countermeasures against them. In last step, based on identified threats and dam- age level, threat scenarios are built, and mitigation plans are developed [17].

6.Discussions

The following table provides a summary of threat modeling approaches and methodologies that are currently being used in IT. Other than STRIDE and DREAD modeling, there are only few approaches that are currently being used with automated tool support. In this table we display the summary threat modeling methodologies with three classifiers.

Many threats are dependent on other threats so threat analysis is a vital process in IT today. Software security analysts are researching the application of formal methods in software security as none exists today.

7. Conclusion

Threat modeling methodologies are deployed in various enterprises including IT purpose and cloud computing. This paper proposes a systematic survey on existing threat modeling methodologies and approaches in IT purpose and cloud computing. Each threat modeling approach supports tools which store and create architectural representations of the model. In IT purpose, the software centric approach dominates over attack centric and asset centric approaches. Exponential growth in cloud computing has created a rising need for threat modeling. Model validation is one of the main drawbacks in threat modeling. Hence, todays tools are not sufficient for validating the threat models. Our main research focus should be on providing compatible solutions for model validation in threat modeling tools. In both IT purpose and cloud computing, existing threat model approaches have limitations for analysis of threats and vulnerabilities.

References

[1] S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal, “Threat modelling methodologies: A survey,” *Sci. Int.(Lahore)*, vol. 26, no. 4, pp. 1607–1609, 2014.

[2] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[3] A. Amini, N. Jamil, A. Ahmad, and M. Z’aba, “Threat modeling approaches for securing cloud computing,” *Journal of Applied Sciences*, vol. 15, no. 7, p. 953, 2015.

[4] The stride threat model. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[5] A. Singhal, H. Banati *et al.*, “Fuzzy logic approach for threat prioritization in agile security framework using dread model,” *arXiv preprint arXiv:1312.6836*, 2013.

[6] N. R. Prasad, “Threat model framework and methodology for personal networks (pns),” in *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*. IEEE, 2007, pp. 1–6.

[7] Threat risk modelling. [Online]. Available: https://www.owasp.org/index.php/Threat Risk Modeling

[8] N. A. Malik, M. Y. Javed, and U. Mahmud, “Threat modeling in pervasive computing paradigm,” in *New Technologies, Mobility and Security, 2008. NTMS’08.* IEEE, 2008, pp. 1–5.

[9] M. Schiffman, A. Wright, D. Ahmad, and G. Eschelbeck, “The common vulnerability scoring system,” *National Infrastructure Advisory Council, Vulnerability Disclosure Working Group, Vulnerability Scoring Subgroup*, 2004.

[10] M. M. Morana and T. UcedaVelez, *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. John Wiley & Sons, 2015.

[11] V. Saini, Q. Duan, and V. Paruchuri, “Threat modeling using attack trees,” *Journal of Computing Sciences in Colleges*, vol. 23, no. 4, pp. 124–131, 2008.

[12] Y. Chen, B. Boehm, and L. Sheppard, “Value driven security threat modeling based on attack path analysis,” in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, 2007, pp. 280a–280a.

[13] F. Vraalsen, M. S. Lund, T. Mahler, X. Parent, and K. Stølen, “Specifying legal risk scenarios using the coras threat modelling language,” in *International Conference on Trust Management*. Springer, 2005, pp. 45–60.

[14] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, “A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy

requirements," *Requirements Engineering,* vol. 16, no. 1, pp. 3–32, 2011.

[15] A. Gholami and E. L. J. Z. et al, "Advanced cloud privacy threat modeling," *Informing Science: International Journal of an Emerging Transdiscipline,* no. 1, p. 229239, 2016.

[16] R. McRee, "Pta: Practical threat analysis," *Information Systems Security Association,* pp. 37–40, 2008.

[17] Information securitymangement. [Online]. Available:http://ismsguide.blogspot.in/2007/08/practical-threat-analysis-of-complex.html.

[18] P. Saitta, B. Larcom, and M. Eddington, "Trike v. 1 methodology document [draft]," *URL: http://dymaxion. org/trike/Trike v1 Methodology Documentdraft. pdf,* 2005.

[19] A. S. Sodiya, S. A. Onashoga, and B. Oladunjoye, "Threat modeling using fuzzy logic paradigm," *Informing Science: International Journal of an Emerging Transdiscipline*, vol. 4, no. 1, pp. 53–61, 2007.

[20] Computer security. [Online]. Available: https://en.wikipedia.org/wiki/Computer /security

[21] Threat modeler. [Online].Available: http://threatmodeler.com/approaches-to-threat-modeling/

[22] S. Anbazhagan and K. Somasundaram, "Security threats and benefits of cloud computing transitioning to a new way of doing business."

[23] M. Dhanalakshmi, R .Dhivyalakshmi, R.G. Gajalakshmi, Mrs.K.DeepaThilak."Scalability and the bandwidth efficiency of VoD Systems," International Innovative Research Journal of Engineering and Technology, 2016, vol.2, pp.52-58.