A Survey of Information Intelligent System Security Risk Assessment Models, Standards and Methods

Zijian Ying[1,2,4], Qianmu Li[1,2,3,4(✉)], Shunmei Meng[1], Zhen Ni[3], and Zhe Sun[2]

[1] School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
qianmu@njust.edu.cn
[2] Jiangsu Zhongtian Technology Co., Ltd., Nantong 226009, China
[3] School of Information Engineering, Nanjing Xiaozhuang University, Nanjing 211171, China
[4] Intelligent Manufacturing Department, Wuyi University, Jiangmen 529020, China

Abstract. This paper describes the theoretical hierarchy of information security risk assessment, which includes the models, standards and methods. Firstly, this paper generalizes and analyzes the security risk assessment models on the macro scale and proposes a common security risk assessment model by reviewing the development history of the models. Secondly, this paper compares different security risk assessment standards and classifies them into information security risk assessment standards, information security risk assessment management standards and information security risk assessment management implementation guidelines on the mesoscale. Then, on the micro scale, this paper generalizes security risk assessment methods and analyzes the security risk assessment implementation standards, which is the specific implementation method of security assessment work. Finally, this paper proposes a cloud security event description and risk assessment analysis framework based on the cloud environment and the common security risk assessment model we proposed.

Keywords: Assessment models · Security risk · Security standard

1 Introduction

As an important part of network security research, security risk assessment area has undergone several decades of development. Risk assessment is the foundation of all other security technology. According to the definition of information system security risk assessment criterion, security risk assessment is the process of evaluating information security attributes with related technology and management standards. Security risk assessment can be divided into macroscale, mesoscale and microscale in structure. On the macroscale, assessment model is the structural foundation of the security risk assessment. On the mesoscale, assessment standard provides reference for security risk assessment. On the microscale, assessment method provides specific ideas for security risk assessment. The structure of the three-scale model is shown in the Fig. 1. Using

X. Zhang et al. (Eds.): CloudComp 2019/SmartGift 2019, LNICST 322, pp. 603–611, 2020.
https://doi.org/10.1007/978-3-030-48513-9_48

model, standard and assessment method to deal with security threats and protect property is the idea of risk assessment in network security area.

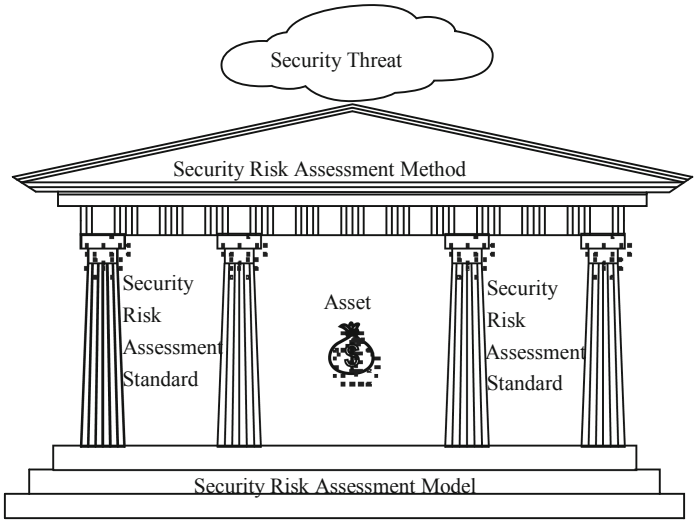

Fig. 1. Cloud computing security risk assessment theory structure.

Some mature technical architectures have been built to address security risk assessment problems in different scales. However, as the rapid development of the information technology, more and more security threats come out, which means security risk assessment technology need to develop either. Meanwhile, the ubiquitous network brings new characters and threats unlike before. This means better methods should be taken to do security risk assessment and protect properties.

This paper sums the models, standards and methods in the theoretical hierarchy of information security risk assessment, proposes a common security risk assessment model, and classifies the different standards and methods.

2 Security Risk Assessment Models

Protection Detection Response (PDR) Model. PDR model, as shown in Fig. 2, is originally proposed by Winn Schwartau. This model considers that protection is the first step, detection is the real-time monitoring of network and reaction is the in-time feedback to the invasion.

Protection Policy Detection Response (P2DR) Model. P^2DR model, as shown in Fig. 3, is a dynamic network security system model which is improved from PDR by ISS Company. This model centers on the policy and surrounds with response, protection and detection. Policy contents general policy and specific security policy.

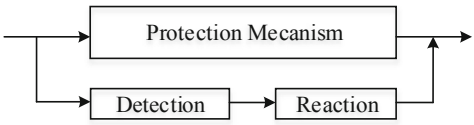

Fig. 2. PDR model.

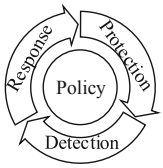

Fig. 3. P^2DR model.

Protection Detection Reaction Restoration (PDR2) Model. PDR^2 model, as shown in Fig. 4, is improved from PDR model. This model is very similar to the P^2DR model, and the only different is upgrade the recover segment to the same level with protection, detection and reaction. This model extends the concept of the security from information security to information assurance, and highlight the automatic failure recovery capability.

Policy Assessment Design Implementation Management ER Education (PADIMEE) Model. PADIMEE model, as shown in Fig. 5, is improved from P2DR model by ISS Company and become a more systematic model. Based on analyzing the object, requirements and safety period, this model build a cyclic security model.

Assessment Policy Protection Detection Reaction Restoration (APPDRR) Model. APPDRR model, as shown in Fig. 6, is a passive dynamic defense model for local system

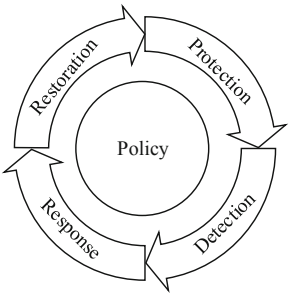

Fig. 4. PDR^2 model.

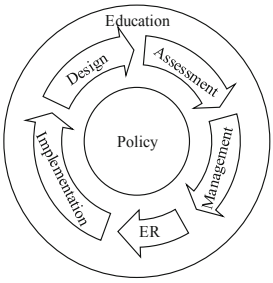

Fig. 5. PADIMEE model.

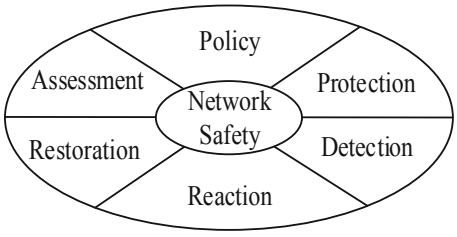

Fig. 6. APPDRR model.

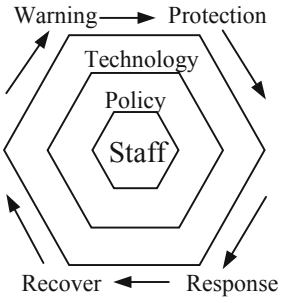

Fig. 7. WPDRRC model.

proposed by Venus which is based on PDR^2 model. This model considers that security is relative and represents a spiral improvement process. Security will be gradually improved in it.

Warning Protection Detection Response Recover Counterattack (WPDRRC) Model. WPDRRC model, as shown in Fig. 7, is an information system security assurance system. It improves by adding Warning and Counterattack before and after PDR^2 model. It centers on staff and uses policy as the basis of the communication technology.

A Security Risk Analysis Model. Figure 8 shows the internal links among the information security models above:

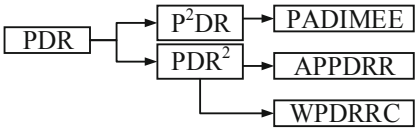

Fig. 8. Information security model evolution.

It has been observed that information security is a cyclic process and the key is protection, detection and the mutual excitation of feedback.

3 Security Risk Assessment Methods

The main components of the security risk assessment method are two aspects, one is risk analysis and the other is risk resolution. The accuracy of risk analysis will have a huge impact on many of following works. Overall, the security risk assessment method consists of the following eight elements: asset description, threat identification, consequence analysis, vulnerability analysis, threat assessment, risk assessment, risk priority and risk management.

With the development of technology, security risk assessment methods have evolved from traditional assessment methods to comprehensive risk assessment management methods.

3.1 Traditional Security Risk Assessment Methods

Attack Trees Analysis (ATA). ATA is an analytical method for exploiting system weaknesses from the perspective of an attacker. It uses the tree structure to describe the possible attacks on the system. Because most risk assessment methods need to make assumptions based on existing information, the accuracy of the assessment will be limited by the accuracy of the hypothesis. To ensure the best results, the conclusions drawn from the attack tree analysis need to be compared to other analysis results or assessed by experts. However building a 100% accurate attack tree model is almost impossible. And this step will greatly increase the complexity of the method. The evaluator needs to grasp the

degree of assessment and make the attack tree model good enough. In order to prevent this step from consuming too many resources, the following three conditions need to be considered:

1) Defender's system has vulnerabilities.
2) Attackers need to have enough ability to exploit these vulnerabilities.
3) The expected benefit is the motivation for the attack, and the attacker can gain benefits by attacking.

The main advantage of ATA is that it can be easily rewritten according to the needs and characteristics of the organization. This method also provides the conclusion that which attacks are most likely to occur in terms of the overall system. From a certain perspective, security is not a result, security is a process, and attack tree analysis can form a basic understanding of this process. From a certain perspective, security is not a result but a process, and ATA can form a basic understanding of this process.

Failure Tree Analysis (FTA). FTA is a top-down assessment method. It uses a tree diagram to organically link system security failures to internal failures. In the fault tree, the root node indicates a fault, and the leaf node indicates an event that may cause a fault, which in turn extends. Different layers are linked by logic gate symbols and the upper layer probability is calculated according to the underlying probability. However, the fault tree cannot analyze the hazards and risks caused by the fault time, so it can only be used as a method of some steps in the risk analysis.

Failure Mode Effect and Criticality Analysis (FMECA). FMECA is a single component failure mode analysis and hazard analysis tool. Its purpose is to reduce the possibility of failure and improve the reliability of system operation. FMECA is a bottom-up approach that identifies faults in the form of a discussion and records the results in a table. The disadvantage of this approach is that there are too many limitations in a single unit, ignoring the connections and commonalities between the units.

Hazard and Operability Study (HAZOP). HAZOP is a structured inspection method for potential hazards of the system. It uses structured checks to determine the abnormal operation of the system from normal design. And the purpose of this method is to identify threats. The HAZOP analysis is conducted in the form of a discussion, and the analyst uses a variety of analysis techniques to collect system information into the document as an input to the analysis. In the analysis process, use some system-related questions to form special guidance words to help improve the comprehensiveness of the analysis. This way not only ensures that the analysis results are consistent with the characteristics of the system, but also adds extra information. The results of the analysis are saved in the form of a table.

Petri-net. Petri-net is a graphical modeling tool based on mathematical theory. Petri-net can automatically control the state of the system with the change of the state of the token in the system to describe a dynamic complex system. It is often used in the field of security analysis to analyze security threats that are passed through the system.

Analytic Hierarchy Process (AHP). AHP uses a hierarchical approach to quantify empirical judgments and form quantitative decision values. However, this method is subject to human factors, and there are fluctuations between various indicators and lack of consistency.

The traditional method lacks comprehensive considerations for security risk technology and management, and a single assessment method cannot objectively and accurately reflect the security status of complex information security system engineering.

3.2 Comprehensive Security Risk Assessment Methods

Comprehensive risk assessment methods have a set of implementation steps and theoretical systems, and their solutions for risk assessment are more comprehensive than traditional risk assessment methods. They may contain some traditional analytical methods. However, in addition to these, they generally follow certain security standards and also provide solutions to systemic risks.

CCTA Risk Analysis and Management Method (CRAMM). CRAMM is a security service framework system proposed by the British government. Its purpose is to provide a structured and consistent approach to information security management, as shown in Fig. 9. It is an automated qualitative assessment method, but in order to achieve good results, experts need to participate in the assessment. The purpose of this method is to assess the security of related information systems and networks. To achieve the goal, the method focuses on three aspects:

1) Identify assessment assets
2) Identify threats and vulnerabilities and calculate risks
3) Identify and give countermeasures according to priority

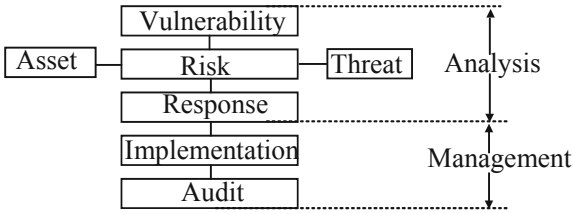

Fig. 9. CRAMM method.

Operationally Critical Treat, Asset, and Vulnerability Evaluation (OCTAVE). OCTAVE is a method developed by Carnegie Mellon University to define the security risks of assessing information within a system organization. This approach provides a new approach to information security for large organizations. OCTAVE enables organizations to view security issues from a risk-based perspective and describe the technology

in a commercial perspective. OCTAVE Allegro is a new version that was published in 2007. This version is based on the previous two previous versions of OCTAVE Original (1999) and OCTAVE-S.

OCTAVE Allegro focuses on information assets. One of the advantages of using OCTAVE Allegro is that it can be conducted in the form of a seminar. It provides the required collaborative environment, the necessary guides, work forms and questionnaires, and all of the above mentioned content is free. OCTAVE Allegro consists of four stages and eight steps. The results of each step are recorded by the worksheet and used as input for the next step.

Consultative Objective and Bi-functional Risk Analysis (COBRA). COBRA is a risk analysis method created by C&A. COBRA is designed to provide organizations with the means to self-assess their own information technology without the need for additional consultants. COBRA follows the guidance of ISO 17799 and its risk assessment process includes two aspects: One is COBRA Risk Consultant; the other is ISO Compliance.

COBRA Risk Consultant is a questionnaire-based computer program that contains a number of standardized questions to gather information about asset types, vulnerabilities, threats, etc. This approach generates appropriate recommendations and solutions by evaluating relevant threats. COBRA Risk Consultant is designed based on self-assessment, which can be used without relevant knowledge and without expert involvement. The reports generated by COBRA Risk Consultant are professional business reports that can be read by security professionals or non-professionals. ISO Compliance contains standard questions related to the broad categories specified in the ISO 17799 standard.

Control Objectives for Information and related Technology (COBIT). COBIT is the most internationally recognized and most authoritative standard for security and information technology management and control proposed by ISAKA and has been developed to COBIT 5.

A Platform for Risk Analysis of Security Critical Systems (CORAS). CORAS was formally proposed by Greece, Germany, Norway and the United Kingdom in 2003. It is a qualitative risk assessment method and provides a complete set of graphical language to model threats and risks.

3.3 Security Risk Assessment Methods Comparison

There is no unified evaluation system for security risk assessment methods. This paper presents a simple assessment framework for comparing the various methods described above. The framework evaluates the above methods from the eight aspects: data requirement(DR), tool support(TS), operability(O), application cost(AC), application range(AR), method type(MT), policy assurance(PA) and support organization(SO). This helps relevant organizations to select appropriate security risk assessment methods based on their needs. Table 1 shows the comparison results.

Table 1. Assessment to the security risk assessment method.

Name	TS	O	AC	AR	MT	PA	SO
ATA	–	Easy	Low	Small	Qualitative	Low	–
FTA	–	Easy	Low	Small	Qualitative	Low	–
FMECA	–	Medium	Medium	Small	Qualitative	Low	–
HAZOP	–	Easy	Medium	Medium	Qualitative	Low	–
Petri-net	–	Difficult	Medium	Medium	Quantitative	Low	–
AHP	–	Easy	Low	Medium	Comprehensive	High	–
CRAMM	–	Difficult	High	Wide	Quantitative	Low	UK
OCTAVE	Y	Difficult	Low	Wide	Comprehensive	High	CMU
COBRA	Y	Medium	Medium	Wide	Qualitative	High	C&A
COBIT	Y	Difficult	Medium	Wide	Qualitative	High	ISAKA
CORAS	Y	Medium	Medium	Wide	Comprehensive	High	EU

4 Cloud Security Event and Risk Analysis Framework

Modeling analysis is one of the important assessment methods and decision-making mechanisms for network security. It can help system designers to clearly understand and identify potential security threats, attacks and vulnerabilities in the system. The basic idea of the model-based attack assessment method is to put the network into operation, and use some threat analysis models of information systems and network security, such as STRIDE, UML, etc., to describe and assess potential threats in the system in advance to prevent problems before they occur. For example, Kkoti et al. combined the STRIDE threat detection model and attack tree technology to implement a threat detection model that can effectively analyze Open Flow security.

Combined with the general security risk assessment models summarized in this paper, a cloud security event description and risk analysis implementation framework is proposed, as shown in Fig. 10. The security event description and risk analysis tools are at the application layer. The network nodes are at the access layer. And the controllers at the control layer are used as bridges to communicate the upper and lower layers. The network node passes the obtained security information to the controller, which aggregates it and passes it to the analysis tool in the application layer. The network node passes the obtained security information to the controller and the controller then aggregates it and passes it to the analysis tool in the application layer. The analysis tool analyzes based on existing model libraries, experience pools, and acquired safety information, and generates analysis reports. The security expert assigns a security policy to the controller based on the analysis report. The controller translates the policy to form a rule command for the network node and passes it to the network node for configuration, thereby forming a closed loop of analysis, protection, and feedback. This model combines the advantages of a ubiquitous network structure with the advantages of a security risk assessment model. It separates and reconstructs the secure data plane from the control plane for modularity,

service, and reusability, and decoupling physical and virtual network security devices from their access modes, deployment methods, and implementation functions. At the same time, the model abstracts the underlying layer into resources in the security pool, and intelligently and automatically organizes and manages the business through the top-level unified software programming method, and completes the corresponding security protection functions in a flexible and efficient manner to achieve the purpose of reducing security risks.

5 Conclusion

This paper described the models, standards, and methods involved in the theoretical hierarchy of security risk assessment. Firstly, this paper generalized and analyzed common security risk assessment models on the macroscale. Then, this paper compared and classified different security risk assessment standards on the mesoscale, and divided them into information security risk assessment standards, information security risk management standards, and information security risk management implementation guidelines. What's more, this paper generalized security risk assessment methods and analyzed security risk assessment guidelines on the microscale. This is the implementation method for specific security assessment work. In the end, this paper proposed a cloud security event description and risk analysis implementation framework based on the cloud environment and the security risk assessment model proposed before.

Acknowledgement. This work was supported in part by Military Common Information System Equipment Pre-research Special Technology Project (315075701), the Fundamental Research Funds for the Central Universities (30918012204), 2018 Jiangsu Province Major Technical Research Project "Information Security Simulation System" (electric power and energy), Shanghai Aerospace Science and Technology Innovation Fund (SAST2018-103).

References

1. Xiaolong, X., Liu, Q., Zhang, X., Zhang, J., Qi, L., Dou, W.: A blockchain-powered crowdsourcing method with privacy preservation in mobile environment. IEEE Trans. Comput. Soc. Syst. (2019). https://doi.org/10.1109/TCSS.2019.2909137
2. Qi, L., Chen, Y., Yuan, Y., Shucun, F., Zhang, X., Xu, X.: A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. World Wide Web J. (2019). https://doi.org/10.1007/s11280-019-00684-y
3. Qi, L., et al.: Finding all you need: web APIs recommendation in web of things through keywords search. IEEE Trans. Comput. Soc. Syst. (2019). https://doi.org/10.1109/tcss.2019.2906925
4. Li, Q., Meng, S., Wang, S., Zhang, J., Hou, J.: CAD: command-level anomaly detection for vehicle-road collaborative charging network. IEEE Access **7**, 34910–34924 (2019)
5. Li, Q., Meng, S., Zhang, S., Hou, J., Qi, L.: Complex attack linkage decision-making in edge computing networks. IEEE Access **7**, 12058–12072 (2019)
6. Li, Q., et al.: Safety risk monitoring of cyber-physical power systems based on ensemble learning algorithm. IEEE Access **7**, 24788–24805 (2019)
7. Li, Q., Wang, Y., Pu, Z., Wang, S., Zhang, W.: A time series association state analysis method in smart internet of electric vehicle charging network attack. Transp. Res. Rec. **2673**, 217–228 (2019)