Advances in Artificial Intelligence, Big Data and Algorithms
G. Grigoras and P. Lorenz (Eds.)

doi:10.3233/FAIA230796

Automated Security Policy Feasibility Assessment

Yunfan WANG[a,1], Wenhao YE[b], Ning LI[b] and Liurong PAN[c]
[a]*State Grid Key Laboratory of Information & Network, State Grid Smart Grid Research Institute co., Ltd., China*
[b]*State Grid Hunan Electric Power co., Ltd., China*
[c]*Hunan SGIT Technology co., Ltd., China*

Abstract. Security policy feasibility assessment is to evaluate the ability of the implemented policy to resist threats, fix system vulnerabilities, etc., whether it is in the user's acceptable range, and also a measure of security and cost balance. There has been outstanding progress in the current research on automated security policies, and the implementation and application of various security policies are progressing well, but we should pay more attention to security policy effectiveness, which better reflects the risks and the scope and degree of risks accepted by the existing system. However, in many security policy evaluations, there is basically no comprehensive evaluation of existing security policies, and more often the existing vulnerabilities and the degree of risk after being threatened are presented, without quantitative and qualitative feasibility assessment. Based on the existing security policy evaluation methods, a method for assessing the feasibility of automated security protection policies is introduced.

Keywords. Security policy feasibility assessment, System vulnerabilities

1. Introduction

How to evaluate the feasibility of security policies has become a hot research topic in the field of network security, and security policies should maintain completeness, correctness, and consistency [1]. Policy completeness research mainly focuses on the description of user completeness, process and its execution completeness, duty isolation completeness and log completeness in business information systems [2]. For the study of network security policy, many completeness security principles have been proposed, such as good architecture transformation, authorization execution, etc. [3], which are the basis of security policy establishment. The correctness of the security policy reflects the conformity of the policy to the security requirements of the system is an information security risk assessment process to identify and estimate the impact of assets on users through an abstract information security model to analyze their vulnerability, threat level and risk factor. It is mainly measured by economic loss indicators and does not provide feedback on existing security measures and their effectiveness reports lacking comprehensive consideration of the impact of policy features and the effect of policy implementation with the consequence that the management of security policy is passive

[1] Corresponding Author: Yunfan WANG, State Grid Smart Grid Research Institute co., Ltd., China, Nanrui Road 8, 210003 Nanjing, China; Phone: +86 13914491366; Email: wangyunfan95@qq.com

and its security assurance capability cannot Adapt to the dynamic change requirements of the network environment [4]. The consistency of the security policy requires the avoidance and elimination of conflicts in the definition and implementation of policy rules reflects its enforceability and non-contradictory nature.

In this paper, the feasibility assessment of automated security policy is proposed mainly for measuring the security policy effectiveness through assessing its ability to resist threats, capability of repairing system vulnerabilities, whether the degree of this ability in the user acceptance range, and the security cost. Besides, it is also measuring the balance between security performance and cost. Since the assessment of security policy effectiveness is influenced by many factors, such as the user's need for security, the vulnerability of the system, and which threats to the system, these factors have uncertainty and lack of information, and cannot be described in precise language, but only an approximate, vague, subjective judgment, and can only be described in more vague or more exact language, which is consistent with subjectivity and expresses subjective precision. Therefore, a quantitative qualitative method is also needed for effective assessment. This paper then proposes a qualitative and quantitative assessment of the feasibility of automated security policies by first establishing a set of security policy assessment processes and then a mathematical model for security policy effectiveness assessment. The hypothesis that the confidence measure of the degree of security policy effectiveness which is close to 100% is determined to be correct through example analysis, accumulation of evidence, and step-by-step synthesis of evidence. The reasonableness of this assessment model was verified by eliminating the hypothesis that the confidence measure is less than 50%.

2. Related Work

Various security issues related to security policies have received great attention in today's society. There has been a lot of research on security policies, but not much action has been taken on the feasibility assessment of security policies, which is mostly vague.

Tang C et al. [5] verify the effectiveness of the network security policy, by a network security policy evaluation model based on the security capability is proposed. Based on the establishment of security domain and security policy, the relationship between the application target of defense means and the characteristics of information security attributes is analyzed, protection factor and sensitivity factor are established, and then the value of security policy security coefficient is obtained to evaluate the level of security policy capability. The results show that the model can effectively reflect the protection capability of the security policy and provide a new solution for evaluating the security policy. The evaluation process for how to evaluate security policies and give the evaluation process is a key point for security metric results. Based on the formal description of policies and policy association, Xia B et al. [6] proposed an evaluation method including subject, object, authority, and impact and illustrated its effectiveness.

Stavrou E et al. [7] proposed a feasibility assessment methodology to help evaluate and compare intrusion recovery protocols in WSNs. The methodology defines aspects of intrusion recovery protocols that should be evaluated using a number of evaluation criteria and guides researchers in determining the direction of evaluation they should follow. Heinzle B et al. [8] proposed a self-assessment framework that allows users to determine feasible security metrics for ISMS specifically for the user.

Z Qin et al. [9] introduced evidence theory to address uncertainty or unknowable information in the assessment. In the research and analysis process, the security policy is divided into 3 major indicators: security management, threat resistance, and vulnerability remediation, and the indicators and their sub-indicators are constructed into a security policy evaluation indicator tree by gradually synthesizing the accumulated evidence in a hierarchical evaluation upwards The credibility of incorrect assumptions is gradually approached to 0% while the credibility of correct assumptions is gradually approached to 100%. Finally, the reasonableness of the evaluation is verified by example analysis.

3. Process for Assessing the Feasibility of Automated Security Policies

This paper discloses a method for evaluating the feasibility of an automated security protection policy, comprising the following six steps: defining security defense objectives, collecting real state information, defining desired state information, comparing, and analyzing, scoring, and displaying evaluation results. The most important of these steps is scoring, where an evidence-based security policy evaluation method is used to score whether the implemented policy meets expectations and to perform a quantitative and qualitative analysis of the automated protection policy. Thus, the problem can be identified and the parameters of the implemented policy can be adjusted accordingly to meet the target expectations. The flow chart of the assessment steps is as follows.

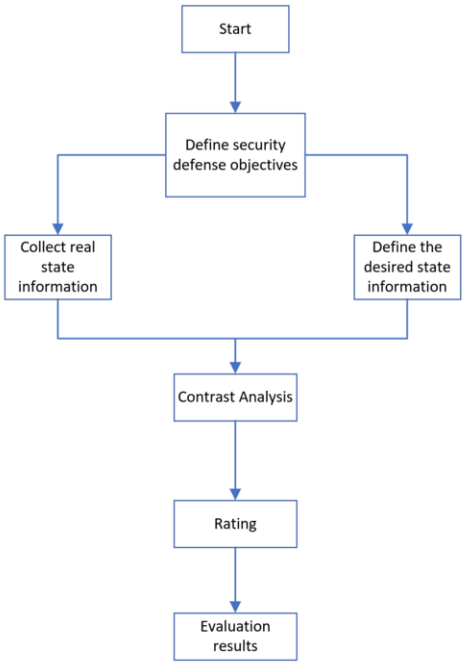

Figure 1. Automated Security Policy Assessment Flowchart.

3.1. Define Security Defense Objectives

According to the IETF/DMTF definition, a policy is a description of the system behavior rules, and its common description form is "if condition then action". Therefore, the formal description of a policy is as follows: Policy (Subject, Target, Action, Condition, Flag) indicates that the policy is a five-tuple consisting of Subject, Target, Action, Condition and Flag. Target denotes the object of this policy rule; Action denotes the behavior managed by this policy rule. For the convenience of description, the subject, object and action are collectively referred to as entities, and a behavior execution of the subject on the object is called a session. condition denotes the execution constraints of the behavior managed by this policy rule, which consists of subject constraints, object constraints and session environment constraints. The description of each constraint further indicates the entity to which the constraint belongs and the condition variable. flag indicates the policy type, which takes the value of True or False, where True is a positive policy and False is a negative policy. According to the implemented automated security policy, the achievable policy and the attack method to verify whether the policy is feasible are obtained from the originally set policy library, so as to obtain the security capability and target of the automated security protection policy.

3.2. Collect Real State Information

The device status information collection system consists of a collector, storage unit, coordination center, analysis engine, report generator and visualization interface. The coordination center is used to coordinate the collectors to collect time and event-driven data; the analysis engine is used to find defects and identify the required event-driven data to assist in prioritization and response through risk scoring methods. The core element of finding defects is the specification identification of the target state, which is a machine-readable defined value defined by an organization to reduce system security risk through a numerical value, list or rule, etc. It is used to compare with the actual state value, and a mismatch between the two values indicates a defect in the effectiveness of one or more security controls. The real state data is collected by information collectors, which can be sensors, scanners, digital input devices, etc. Afterwards, the impact of the designed security protection policy on the system and the actual situation of each device in the event of an attack is collected and the details are recorded for subsequent use in the form of a graphical display.

3.3. Define the Desired State Information

When designing an automated security protection policy, you can find the policy library related to the design based on the relevant security policy implemented, and then record the new state of each device when the corresponding security policy is under attack, and record the desired state information of each device and system.

3.4. Contrast Analysis

The contrast analysis process is designed to detect defects by calculating the difference between the real state and the target state information. Defect detection is usually performed in terms of security sub-capabilities and is based on a judgment statement that compares the evaluated objects. The defect detection process requires documentation,

including defect detection information and countermeasures, listing the defect detection name, evaluation criteria, sub-capability name and target, evaluation criteria notes, selection of the defect or not, and defect response. After the defect detection is completed, the information recorded based on the real state and the target state should be compared and then integrated and recorded to form a comparison document.

3.5. Rating

Design an evidence-based theory of security policy evaluation method for quantitative analysis of comparison documents to conduct a more accurate scoring result.

Related Modeling:

The evaluation tree model is shown in Figure 2:

(1) Suppose the effectiveness of the security policy is measured by m indicators T_s, where s = 1, 2, 3, ..., m. If T_s can also be subdivided, it is subdivided into a second layer of indicators T_{sp} according to the actual situation, and T_{sp} denotes the pth sub-indicator of the sth indicator, and so on if it can also be subdivided, forming a tree structure.

(2) L experts $\{x_1, x_2, x_3,..., x_L\}$ are used to form an evaluation group according to the comparison documents, and each expert gives a judgment for each indicator of the lowest level of the tree structure in (1), and the affiliation degree of fuzzy theory is used to construct a mass function of the experts, forming L experts who provide L evidences for the indicator, and sequentially upward, the evaluation results of the same parent node of the same layer of children nodes are used as the evidence of the upper parent node, and the evidence is gradually synthesized upward, and finally the comprehensive evaluation results of the security policy (root node) are obtained.

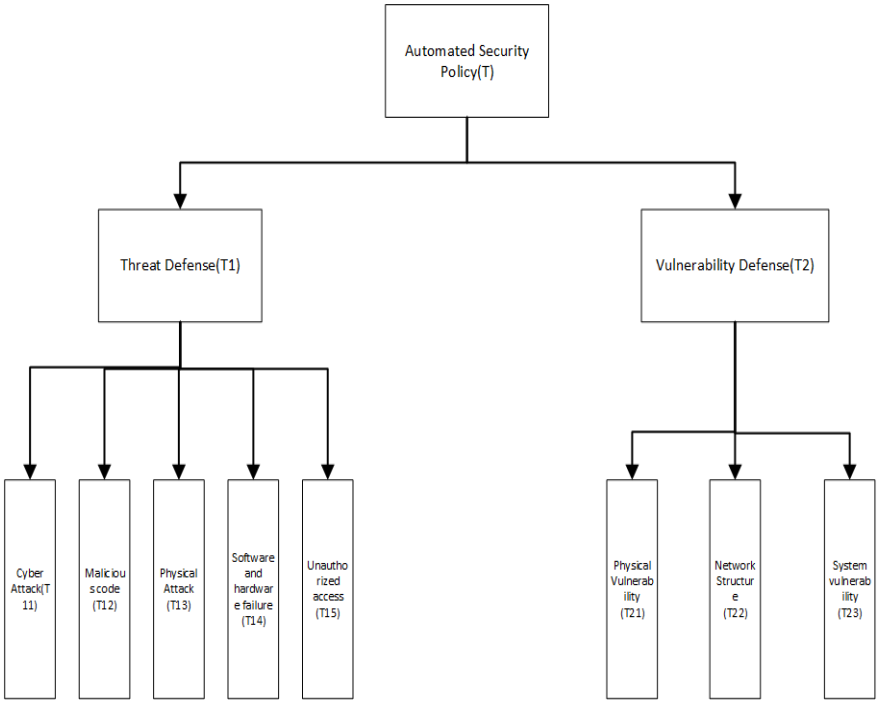

Figure 2. Scoring Model Assessment Tree

The specific steps are as follows:

(1) The same identification framework Θ can be used for all the rubrics, which is the set of rubrics Θ = {high (h_1), medium-high (h_2), medium (h_3), low (h_4)}.

(2) $T = \{T_1, T_2\}$: the effectiveness of the security policy is evaluated into 2 indicators and the relative weight of T_r a_r $(r = 1,2)$ is derived based on the weight analysis method.

(3) $T_1 = \{T_{11}, T_{12}, T_{13}, T_{14}, T_{15}\}$, T_1 will again be divided into 5 sub-indicators, and again according to the weight analysis method, the relative weights of T_{1u} a_{1u} $(r = 1,2,3,4,5)$ are obtained. Similarly, the relative weight values of the elements of the indicator subset T_2 can be obtained for the application; the relative weights of the L-bit experts are obtained.

(4) Define the fuzzy rubric of expert 1 for leaf node T_{ru} to each rank affiliation function in Θ as $\mu_1^{T_{ru}}(h_k)$.

(5) $m_1^{T_{ru}}(h_k)$: denotes the basic credibility assignment of expert 1 to T_{ru} with respect to h_k, constructed from the affiliation function and expressed as follows:

1) $\mu^{T_{ru}}(h_1)$, $A = \{h_1\}$; $\mu^{T_{ru}}(h_2)$, $A = \{h_2\}$; $\mu^{T_{ru}}(h_3)$, $A = \{h_3\}$; $\mu^{T_{ru}}(h_4)$, $A = \{h_4\}$; $1 - \sum_{k=1}^{4} \mu^{T_{ru}}(h_k)$, $A = \Theta$; Denote this as the loss vector:

$$m_1^{T_{ru}} = \left(m_1^{T_{ru}}(h_1),\ m_1^{T_{ru}}(h_2),\ m_1^{T_{ru}}(h_3),\ m_1^{T_{ru}}(h_4),\ m_1^{T_{ru}}(\Theta)\right) \tag{1}$$

2) $m_1^{*T_{ru}}(h_k)$: denotes the basic confidence assignment of expert 1 after discounting the basic confidence assignment of T_{ru} with respect to h_k.

3) $m^{T_{ru}}(h_k)$: The mass function denoting L $m_1^{*T_{ru}}(h_k)$'s obtains the basic credibility assignment of T_{ru} with respect to h_k according to the following equation (2). m is called the basic credibility assignment function on the identification frame Θ, and for any $A \subseteq \theta$, m(A) is called the basic credibility of A:

$$m(A) = (m_1 \oplus m_2 \oplus, \ldots, \oplus m_n)(A) = \frac{1}{n} \sum_{\cap_{i=1}^{n} E_i = A} m_1(E_1) m_2(E_2), \ldots, m_n(E_n) \tag{2}$$

4) $m^{*T_{ru}}(h_k)$: denotes the basic confidence assignment after $m^{T_{ru}}(h_k)$ is discounted.

5) $m^{T_r}(h_k)$:denotes the basic credibility assignment of the rth indicator T_r with respect to h_k. The basic credibility assignment function $m^{*T_{ru}}(h_k)$of all indicators in the next layer of T_r is synthesized by equation (2).

6) $m^{*T_r}(h_k)$:denotes the basic confidence assignment after $m^{T_r}(h_k)$ is discounted.

7) $m^{T}(h_k)$:denotes the basic credibility assignment to T with respect to h_k, which is synthesized by the basic credibility assignment function of T_r at the next level of T according to equation (2).

8) Finally, the vector of comprehensive evaluation results of T on the set of rubrics θ is obtained:

$$m^T = \left(m^T(h_1), m^T(h_2), m^T(h_3), m^T(h_4). m^T(\Theta)\right) \tag{3}$$

According to Definition 1, we can obtain the integrated evaluation result of security policy T on θ trust measure: Bel(h_k). The values greater than 50% are treated as trust and those less than 50% are treated as untrust. A trust degree is obtained, and if Bel(h_3) > 50% and the rest is less than 50% then the security policy effectiveness trust degree is considered as medium.

$$Bel(A) = \sum_{D \subseteq A} m(D), \ (D \subseteq \Theta) \tag{4}$$

Θ is the identification framework, the mass function m: $2^{\Theta} \to [0,1]$ is the basic confidence assignment function on Θ, then the function Bel is the trust test on Θ.

3.6. The Evaluation Results

The scores are evaluated in conjunction with the established rubrics to qualitatively assess the feasibility of the implemented security protection strategy.

4. Example Application Analysis

In the information security risk assessment of a city land and resource bureau, the system security policy effectiveness is assessed as an example. Suppose there are five experts forming the evaluation team, and the security policy effectiveness is evaluated according to Figure 1 and the previous mathematical model.

(1) Evaluation of the security policy indicator set T_1 The opinions of five experts on the evaluation of the indicators of T_{11}-T_{15} are shown in Table 1.

Table 1. Evaluation opinion of T11-T15

Experts	T_{11}	T_{12}	T_{13}	T_{14}	T_{15}
X_1	medium	medium	low	medium	low
X_2	medium	medium	medium	medium	low
X_3	low	medium	low	medium	low
X_4	medium	medium-high	low	medium	low
X_5	medium	medium	medium	medium	low

The relative reliability of the experts is taken as a_{1u}=(0.9,0.19,0.51,0.31,0.9). The mass function of 5 experts is established and synthesized to obtain the evaluation results of 5 sub-indicators:

$m^{T_{11}} = (0,0.0684,0.8463,0.0422,0.0431)$;

$m^{T_{12}} = (0.0013,0.0989,0.8289,0.0415,0.0294)$;

$m^{T_{13}} = (0,0.0173,0.4375,0.5111,0.0341)$;

$m^{T_{14}} = (0,0.0939,0.8710,0.0044,0.0307)$;

$m^{T_{15}} = (0,0,0.0650,0.9078,0.0272)$;

According to the weight calculation method, the relative weights (degree of reliability) of subindicators T11-T15 a2=(0.9,0.9,0.21,0.55,0.14) can be obtained. Discounting and synthesizing the mass function of these five subindicators yields the comprehensive assessment result of T1 indicator:

$m^{T_1} = (0.0003,0.0393,0.89,0.0327,0.0377)$.

(2) Evaluation of security policy indicator set T_2 The opinions of five experts on the evaluation of each indicator of T_{21}-T_{23} are shown in Table 2.

Table 2. Evaluation opinion of T21-T23

Expert	T_{21}	T_{22}	T_{23}
X_1	medium	medium	low
X_2	medium	low	medium
X_3	low	low	medium
X_4	low	medium	low
X_5	medium	medium	low

Again, the relative reliability degree of the experts' comments is taken as a_1u=(0.9,0.19,0.51,0.31,0.9). The mass function of 5 experts is established and synthesized to obtain the assessment results of 3 sub-indicators.

$m^{T_{21}} = (0,0.0476,0.8063,0.0885,0.0576)$;

$m^{T_{22}} = (0,0.0588,0.8497,0.0412,0.0503)$;

$m^{T_{23}} = (0,0.0034,0.2375,0.7305,0.0286)$;

Similarly, according to the weight calculation method, the relative weights (degree of reliability) of the sub-indicators T_{21}-T_{23} a2 = (0.42,0.76,0.9) can be obtained. Discounting and synthesizing the mass function of these three subindicators yields the comprehensive assessment result of T_2 indicator:m^{T_2} =(0,0.0111,0.6314,0.3089,0.0486).

(3) Calculation of the basic credibility assignment of the security policy T (assessment target) with respect to the rubric. First, according to the weight analysis method, the relative weights (degree of reliability) of indicators T_1, T_2 can be found a=(0.9,0.9). The mass function of T_1, T_2 is discounted and synthesized to obtain the final comprehensive evaluation result of security policy T:

$m^{\mathrm{T}} = (0.00004,0.00695,0.93314,0.04347,0.01641)$.

According to Definition 1, the combined evaluation results of the security policy T can be obtained as the level of trust on Θ; Bel(h_1)=0.00004≈0%,Bel(h_2)=0.00695≈7%, Bel(h_3)=0.93314≈93.3%,Bel(h_4)=0.04347≈4.3%. Therefore, values greater than 50% are treated as trusted and those less than 50% are treated as untrusted. That is, we can get the security policy validity for the assumption that h_3 is "medium" is trusted.

5. Summary

This thesis proposes a method for evaluating the feasibility of automated security protection policies, which contains six main steps: defining security defense objectives, collecting real state information, defining desired state information, comparative analysis, scoring, and evaluating results. The specific workflow includes: first defining the relevant protection policies involved in the change of the automated protection policy, and then obtaining the relevant attack methods. Then the corresponding attack is performed to obtain the true state information. Then it compares with the defined desired information, scores it using an evidence-based theory, and finally obtains the corresponding evaluation results, and finally understands the feasibility of the implemented automated security protection policy. The present invention provides a method for assessing the feasibility of an automated security protection policy, which provides a qualitative and quantitative scientific and effective assessment method for the implemented security protection policy. It is possible to prove more effectively whether the implemented method is practicable or not.

Acknowledgements

This work is supported by the Science and Technology Project of State Grid Corporation of China (Research on key technologies of automatic security protection for new business applications, No.5108-202218280A-2-154-XG).

References

[1] Tang C , Yao S , Cui Z , et al. A Network Security Policy Model and Its Realization Mechanism[C]// Springer Berlin Heidelberg. Springer Berlin Heidelberg, 2006.
[2] Wen HZ, Zhou YB, Qing SH. A framework-based model for formal business security policies[J]. Journal of Electronics,2005(02):222-226.
[3] Clark D D , Wilson D R . A Comparison of Commercial and Military Computer Security Policies[C]// 1987 IEEE Symposium on Security and Privacy. IEEE, 2014.
[4] Longley, Dennis, et al. "Feasibility of automated information security compliance auditing." Proceedings of The Ifip Tc 11 23 rd International Information Security Conference: IFIP 20 th World Computer Congress, IFIP SEC'08, September 7-10, 2008, Milano, Italy 23. Springer US, 2008.
[5] Tang C , Yu S . Assessment of Network Security Policy Based on Security Capability[C]// IEEE Singapore International Conference on Communication Systems. IEEE, 2009.
[6] Xia B , Zheng Q S . The Method of Quantitative and Qualitative of Security Policy Assessment[J]. Journal of Zhongyuan University of Technology, 2011.
[7] Stavrou E , Pitsillides A .Security Evaluation Methodology for Intrusion Recovery Protocols in Wireless Sensor Networks[C]//Acm International Conference on Modeling. ACM, 2012.DOI:10.1145/2387238.2387267.
[8] Heinzle B , Furnell S .Assessing the Feasibility of Security Metrics[C]//Springer Berlin Heidelberg.Springer Berlin Heidelberg, 2013.DOI:10.1007/978-3-642-40343-9_13.
[9] Qin Z , Zhang S B . Evaluation Model of Validity of Security Strategy Based on Evidence Theory[J]. Journal of Kunming University of Science and Technology(Science and Technology), 2010.