# Application of STRIDE-based Business Process Risk Assessment Method

**Jing Yuan [a], Weihong Ren [b]**

The Third Research Institute of the Ministry of Public Security, Beijing, 100142, China

[a]email: yuanj1101@163.com, [b]email: Renweih@cspec.org.cn

**Keywords:** Business process; Risk assessment; Threat modeling; Network security; data flow

**Abstract:** In order to accurately and comprehensively measure network security risks, the paper proposes a risk assessment method based on business processes. The method is based on STRIDE threat modeling method, and adopts a cocoon-peeling layer-by-layer analysis method from a business perspective. By decomposing business scenes, a data flow diagram is drawn, potential threats of all objects in the data flow diagram are analyzed, and a corresponding threat list is formed. On this basis, corresponding threat mitigation measures are found for each type of threat, and the existing security problems are analyzed. According to the importance of the business process, the possibility of threats and the severity of security problems, the network security risks of the business are measured. This method has been applied in the core business system of a large enterprise, which can truly reflect the network security risks of business processes and verify its feasibility and effectiveness.

## 1. Introduction

In the development of information security theory and technology, information security risk assessment has become a generally accepted and mature method to find information security problems [1]. The conventional approach to information security risk assessment is to evaluate the security attributes such as confidentiality, integrity and availability of information systems and information processed, transmitted and stored by them according to relevant information security technologies and management standards, such as international standards BS7799, ISO17799, national standards GB/T 22239, etc. [2]. Therefore, the general information security risk assessment is based on preset standards. These standards are the security baselines that the information system is expected to achieve. Different testing methods are used to obtain corresponding evaluation evidence around the security baselines. This method is also referred to as "baseline risk assessment method".

The so-called safety baseline on which the "baseline risk assessment method" is based is a set of safety control measures or practices specified in many standards and specifications. These measures and practices are applicable to all systems in a specific environment, can meet basic safety requirements, and can enable the system to reach a certain level of safety protection.

At present, both the government and enterprises are no longer satisfied with the more extensive "baseline risk assessment method". Compared with their own basic network security, they pay more attention to the personalized security protection needs closely combined with business. Then, how to obtain the personalized security protection needs of the business and carry out the corresponding security risk assessment based on this is the focus of the evaluation service organization.

Taking the business process risk assessment of a large enterprise's core business system as an example, this paper focuses on how to combine STRIDE-based threat modeling method to carry out business process risk assessment.

## 2. STRIDE-based business process risk assessment method

### 2.1 STRIDE Introduction

STRIDE is a tool developed by Microsoft for threat modeling, or a set of methodologies, which

DOI: 10.25236/iwass.2020.062

divides threats into the following six dimensions to examine:

STRIDE [3] is an acronym for the following six threat types:

Spoofing: impersonating an interactive party or a business operation;

Tampering: maliciously modifying data, including information flow content, data storage content, operation instruction content, etc.;

Repudiation: Malicious denial of operations done by the user, such as denying that the user has made a transfer operation;

Information disclosure: Information is exposed to people who are not allowed to access it;

Denial of Service: to prevent a business function from functioning normally;

Elevation of Privilege: unauthorized operation in business, such as illegally viewing other people's account transaction records.

### 2.2 Business Process Risk Assessment Method

In order to follow STRIDE, in the process of business process risk assessment of the core business system of a large enterprise, the project team divides each business into different business processes. For each business process, considering how the S, T, R, I, D and E threat attacks in the model affect the key assets involved in the business process and the relationships among the assets, identify and record these threats, and calculate the risk value of the threats faced by the business process through the possibility of the threats occurring and the severity of the hazards to the business process, so as to evaluate the overall risk of the business process of the system.

As shown in the following figure, the business process risk assessment process based on STRIDE threat modeling can be summarized into five phases: architecture analysis, business process analysis, threat identification, threat and problem analysis, and risk assessment [4].

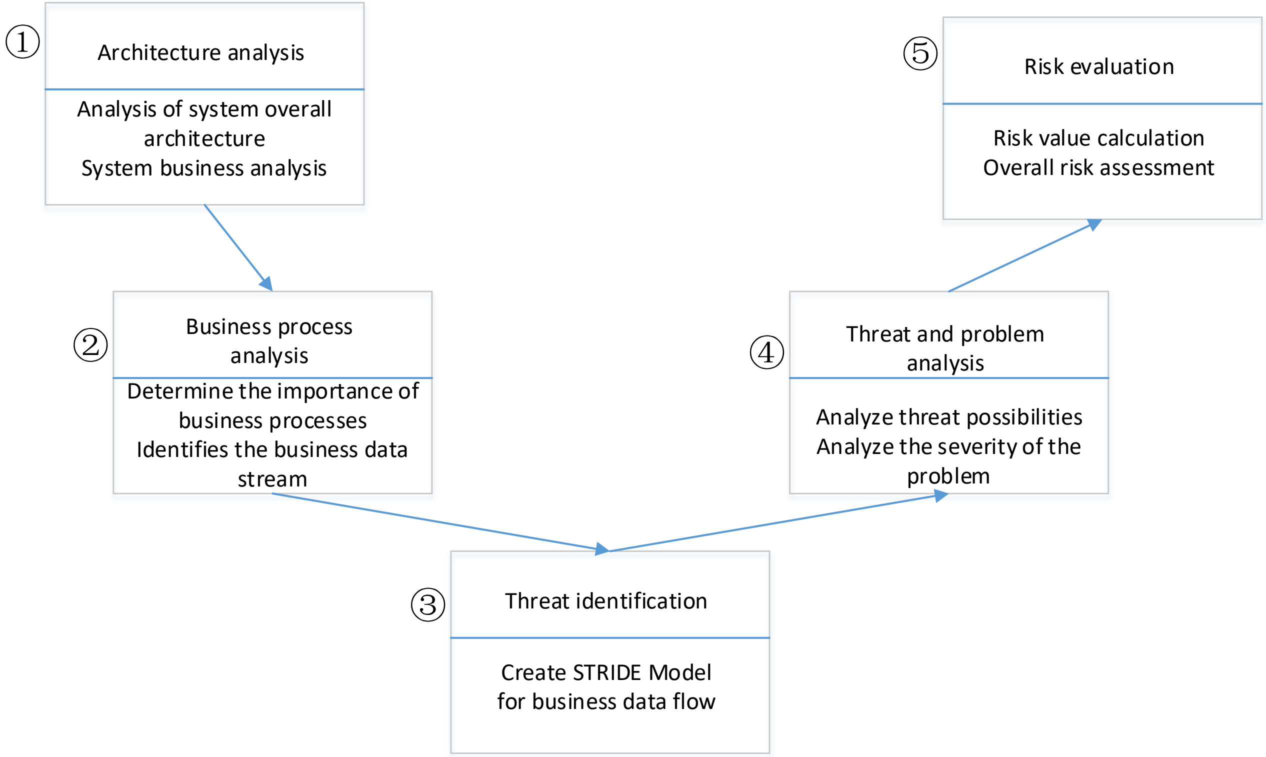

①
Architecture analysis
Analysis of system overall architecture
System business analysis
②
Business process analysis
Determine the importance of business processes
Identifies the business data stream
③
Threat identification
Create STRIDE Model for business data flow
④
Threat and problem analysis
Analyze threat possibilities
Analyze the severity of the problem
⑤
Risk evaluation
Risk value calculation
Overall risk assessment

Fig.1 Risk Assessment Process Based on Threat Modeling

Among them, the system structure and business process analysis phase clearly and accurately demarcates the system business process and identifies the business data flow through the overall structure and business analysis of the information system. In the threat identification, threat and problem analysis phase, the STRIDE model is built on the business data stream to identify the key links and threats faced by the business process, understand the security measures taken by the business process, find the existing security problems, and analyze the threats and the severity of the problems. The risk calculation and evaluation stage is based on the previously established model to analyze the impact of the destruction of the security of key business data streams on business processes, calculate the security risk value of threats to business processes and evaluate the overall security risk of business processes.

## 3. Application of Business Process Risk Assessment Method

In the process of business process risk assessment of a large enterprise's core business system, the project team applied and implemented each stage of the method based on STRIDE threat modeling and the specific characteristics of the business system. The details are as follows.

### 3.1 Architecture and Business Process Analysis

Architecture analysis is the evaluator's understanding process of the overall architecture and business of the business process. The purpose is to accurately understand the platform structure, security boundary, business process and related internal and external environment of the evaluated system, and to establish a model so as to deeply understand the business of the evaluated system. This is the basis for correct data flow analysis.

The related business of the system can be divided into two situations: one is deployed in the private network and not directly connected with external systems; the other is deployed in the intranet and connected to external systems through boundary isolation equipment.

Because the function of the target system is relatively complex and the system is relatively large, in view of the actual project, it is not possible to conduct an all-round evaluation of each business process. Therefore, through the investigation of all business units and data in the core business system, the business processes and their context relationships are sorted and classified, the context relationships between business subsystems are analyzed, the importance of each business function and data is clarified, and the key links in the key business processes are selected to carry out relevant analysis.

Through the detailed investigation of the specific process of each business flow in each subsystem and the data flow of relevant parties (as shown in the example in Fig. 2), the system structure and data flow model of each subsystem are summarized, analyzed and refined. As shown in Fig. 3, each business flow includes 3 data flows: DF1 business processing, DF2 user authentication, DF3 information storage and extraction.

### 3.2 Threat Identification and Analysis

Threat identification is to build STRIDE threat modeling for each data stream of the information system, analyze the threat sources for each data stream, analyze whether each data stream and its associated assets are vulnerable to various threats, identify and record these threats.

Since the system is deployed in an intranet or a private network, there are four types of threat sources: external personnel with malicious intent (hackers on the internet, third-party technical or business cooperation personnel, etc.), internal personnel with malicious intent, internal personnel who inadvertently cause misoperation, and software and hardware system failures. For the business data flow model in Fig. 3, the corresponding STRIDE threat model is shown in Fig. 4.

Based on the six threat types proposed by STRIDE, the risk assessment adopts nine types of threat, including spoofing, tampering, repudiation, disclosure, denial of service (DoS), elevation of privilege, misoperation, insertion of malicious code, software failure, etc., as shown in Table 1.

These threats can be direct or indirect attacks on business processes by threat sources, causing damages to confidentiality, integrity and availability. It may also be accidental or deliberate. At the same time, the possibility of threats to the business flow in different networks is respectively assigned the value, and the value range is an integer of 1~3.

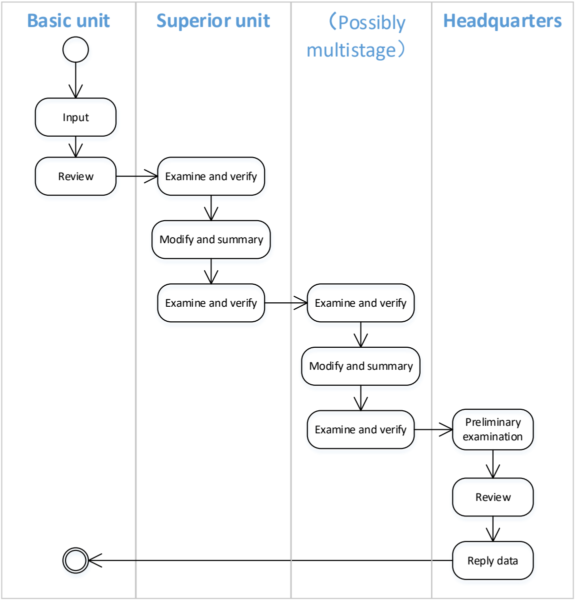


Fig. 2 An example of traffic data flow

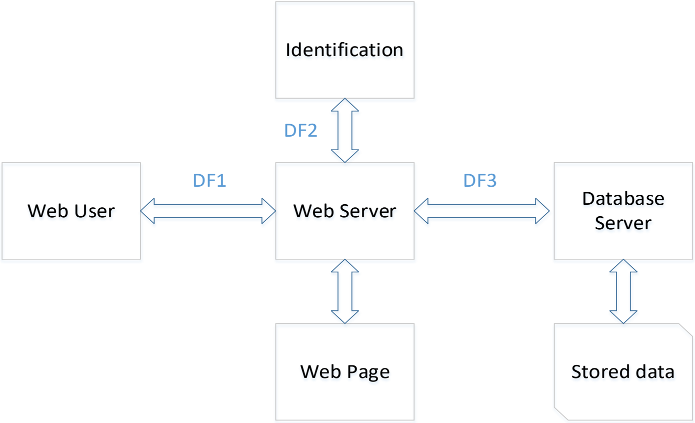
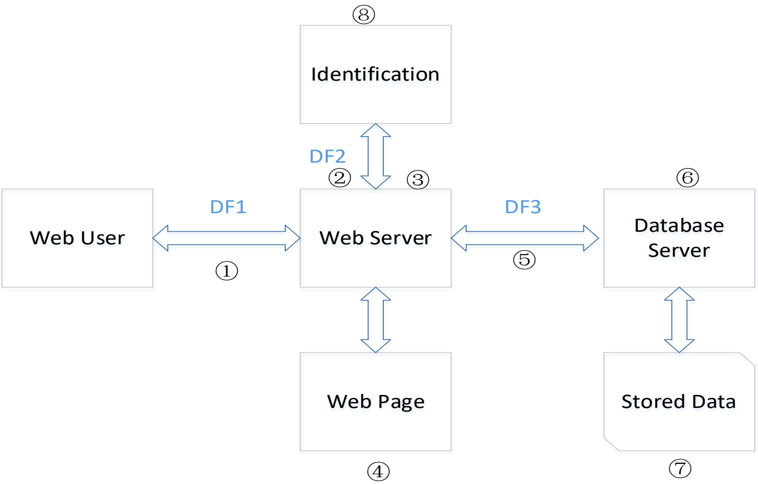


Fig.3 Business data flow model



Threat①: Tamper, Disclosure, Misoperation
Threat②: Denial of Service (DoS)
Threat③: Disclosure, overstepping authority or abuse
Threat④: Tampering, Software Failure, Insertion of malicious code
Threat⑤: Tampering and Disclosure
Threat⑥: Denial of Service (DoS)
Threat⑦: Tampering, Disclosure
Threat⑧: Spoofing, Repudiation, Elevation of privilege

Fig.4. STRIDE Threat Model for Business Data Flow

Table 1 Threat List

| No. | Threats | Explanation |
|---|---|---|
| 1 | spoofing | Input by spoofing an authorized operator；Confirm by spoofing an authorized reviewer；Authorized transfer by spoofing an person in charge |
| 2 | tampering | Tampering with the data in transmitted and stored, operation instruction, etc., destroying the integrity of information reduces the security of the system or makes the information unavailable. |
| 3 | repudiation | Repudiating the operation he has done, for example, the user repudiates that he has done the transfer operation. |
| 4 | disclosure | Disclosure of user name, password, bank card number, payment instructions and other sensitive information during information flow, data storage, or operations. |
| 5 | denial of service （DoS） | Make a certain business function not work normally |
| 6 | elevation of privilege | Unauthorized access to resources in the business, or abuse of their own authority to destroy the business system, such as illegal access to other person's account transaction records. |
| 7 | misoperation | Should be performed without performing the corresponding operation, or accidentally perform the wrong operation. |
| 8 | insertion of malicious code | Malicious codes are inserted into the business system through information input boxes, uploading files, etc. |
| 9 | software failure | The application software fails due to design defects, etc. |

### 3.3 Identification and Analysis of Safety Problems

On the basis of the threat identification results, combined with the existing network security related standards and protection technologies, the project team analyzes the security protection measures used by the system against various threats for each threat category, and forms the evaluation indexes for this risk assessment. These evaluation indexes include five major aspects:

(1) Business logic security, such as multiple approvals of key nodes, etc.;

(2) Business architecture security refers to the security risks in the organization, process, IT system and other aspects that support the business, although there are not problems of the business logic.

(3) Security of business authority refers to how to realize effective sorting of business authority and separation of responsibilities in system configuration due to numerous roles and positions of enterprise personnel.

(4) Business data security refers to the security risk control of relevant personnel, processes and systems during the whole life cycle of business data from generation to destruction.

(5) Application security.

For example, in terms of business architecture security, the security protection measures that can be used to counter spoofing threats include two-way authentication, data validity check, user identity authentication, etc., thus forming corresponding evaluation indexes as follows:

Table.2 Examples of evaluation indexes

| Threats | Evaluation indexes |
|---|---|
| spoofing | What authentication mechanism does the user client adopt and how does the server verify the real client (e.g. IP/MAC binding, soft certificate, etc.)? |
| | Is the input subject to security check (format, length, content, etc., input using special keyboard, etc.)? |
| | Does the user have to be authenticated to access the system (e.g. does the user pass authentication directly by entering the link)? |
| | Does the identity authentication to users adopt two factors (e.g. password+token, password+certificate, etc.)? |
| | Are passwords checked for length and complexity? Does The password be at least 8 digits in length, and at least 2 combinations of letters, numbers and special characters? Does the password be modified regularly for 6 months? |
| | Is there a limit on the number of login failures? |
| | Is there a local security check when the client starts the business process? |
| | Do you perform secondary authenticationin important business operations (e.g. payment instructions)? Is the authentication strong enough (password, dynamic password, verification code, key, etc.)? |

The identification and analysis process of safety problems is to analyze the adopted and missing safety protection measures according to the corresponding evaluation indexes for each business process, form the safety problems existing in each business process and assign the severity of the safety problems, with the value range being an integer of 1~3. In this project, the assignment is mainly considered the following three aspects:

1) Exposure of security problems to business processes

The degree of exposure is understood in terms of technology and management. If there are major vulnerability in business processes at the technical level or similar problems of "structural vulnerability" exist in management, the degree of exposure will be very high.

2) The difficulty of security problems can be exploited

The difficulty of being exploited refers to the successful exploitation of the security problem, the technical strength required by the attacker and the cost of the resources needed. The stronger the technical strength required or the higher the cost of resources required, the more difficult the security problem is be exploited.

3) The prevalence of safety problems

According to the information of vulnerability database (such as CVE), some vulnerabilities are currently recognized as "high-risk vulnerabilities". Once such vulnerabilities are exploited, they will bring serious impacts to business systems.

According to the above principles, the project team comprehensively adopts test methods such as business process sorting, document consulting and analysis, security configuration examination, tool testing and manual verification and comprehensive analysis to obtain evidence, which is used to evaluate the security measures taken by the business processes of the core business system, find the existing security problems, and assign the severity of the security problems by each business process respectively.

### 3.4 Risk Assessment

Business process security risk refers to the occurrence of security incidents and their impact on the organization caused by human or environmental threats using the security problems existing in the business system and its management system [5].

The risk analysis principle of this report is as follows:

$$\text{Risk} = R(A, T, V) = A + T + V \times 2. \tag{1}$$

Where R represents a security risk calculation function; A represents the importance of the business process; T represents the possibility of a threat; V represents the severity of the security problem. According to the calculation results and expert analysis, the risk results are grouped as follows: high risk is 10~12, medium risk is 7~9, and low risk is 4~6.

## 4. Conclusion

STRIDE-based business process risk assessment method advocates analyzing threats from a business perspective and adopts a cocoon-peeling layer-by-layer analysis method. By decomposing business scenarios, drawing data flow diagrams, analyzing potential threats of all objects in the data flow diagrams, and forming corresponding threat lists. On this basis, corresponding threat mitigation measures are found for each type of threat, and the existing security problems are analyzed. According to the importance of the business process, the possibility of threats and the severity of security problems, the network security risks of the business are measured. This method of risk assessment is different from the method of roughly estimating the impact of threats on business based on the perspective of network security technology. It is a new solution. Its results are more accurate and comprehensive, and more in line with the requirements of business risk management.

## References

[1] Yuanjing, Bimaning, Jianglei, etc. The further application of risk assessment methods in testing and evaluation for classified cybersecurity protection [J]. Police Technology, 2014, June Supplement: 76-79.

[2] GB/T 20984, Information Security Technology—Information Security Risk Assessment Specification [S].

[3] expsky@360 A-Team.STRIDE Informal Discussion on Threat Modeling [OL]. https://www.secrss.com/articles/3298, 2018-06-13.

[4] Hewei, Tanshuguang, Chenping. A risk assessment method based on STRIDE threat model [J]. Information Security and Communication Secrecy, 2009, 10: 47-49.

[5] Liangzhiqiang, Lindansheng. Research on Information Security Risk Assessment Mechanism Based on Power System [J]. Information Network Security, 2017, 17 (4): 86-90.