

Online Banking Security Analysis based on STRIDE Threat Model

Tong Xin and Ban Xiaofang

*Department of Information Systems Evaluation China Information Technology
Security Evaluation Center, Beijing, China
tongxin2030@163.com*

Abstract

This paper refers important issues regarding how to evaluate the security threats of the online banking effectively, a system threat analysis method combining STRIDE threat model and threat tree analysis is proposed, which improves the efficiency of the threat analysis greatly and also has good practicability. By applying this method to the online banking system threat analysis, we construct STRIDE threat model on the analysis of the key business data, and then we construct threat tree on the security threat by layer-by-layer decomposition. Thus it gives a detailed threat analysis of the online banking system. This security threat analysis has important significance for the online banking system security analysis and for revealing the threats that the online banking facing.

Keywords: Threat modeling; Data flow diagrams; online banking; STRIDE threat model; data stream; threat tree

1. Introduction

On the basis of security trends and developments of the last decade, where vulnerabilities and incidents reported have increased significantly and attacks are constantly getting more sophisticated while requiring less intruder knowledge [5], innovative threat evaluation techniques for systems and software are needed. In the last few years, several innovative approaches to threat modeling have emerged.

Online banking has been adopted more regularly to support and enhance the performance of the banking industry operations and management. Online banking systems provide us with easy access to banking services. Via a more sophisticated and user-friendly interface, a browser or a dedicated standalone application, people can use the Internet to connect to the bank's computer system. This increasing trend has meant that security issues of confidentiality, integrity, and privacy have become progressively more serious in online banking systems to both the banks and customers. Study on risk evaluation and threat mining of online banking system have received widespread attention [1, 2, 6].

This paper discusses the security of today's online banking systems. We present a system threat analysis method which combines the STRIDE threat model and threat tree analysis. Through applying this threat analysis method to the online banking system threats analysis, we construct the online banking system threat model. Firstly, we analyze the key business online banking system data flow diagram, and then by constructing STRIDE threat model to identify the threats, and through the establishment of threat tree reducing gradually the complexity of threat analysis of online banking system. It is of important significance to the security analysis and risk evaluation of online banking system, and to deeply mining vulnerabilities and risks of online banking system.

This paper is organized as follows. Section 2, we decompose the data flow of the online banking system by using the data flow diagram. In Section 3 we analyze the online banking threat based on STRIDE model. And then the method of constructing a threat tree is shown in Section 4. The last section concludes the paper.







2. Data Flow Analysis of Online Banking System

According to the difference of business process operations, we divide the online banking business process into different data streams: processing, transmission, and information storage. In this section, we use the data flow diagram to describe the online banking business process in detail.

2.1. Representation of Data Flow Diagram

In threat modeling analysis, the data flow diagram (DFD) is usually used to reflect the data flow interaction relationship between online banking system and external interactors. The symbols of data flow diagram are shown in Table 1.

Table 1. Data Flow Diagram Symbols

Symbol	Elements Name	Description
	External Interactor	Input to the system
	Process	Transforms or manipulates data
	Multiple Process	Transforms or manipulates data
	Data Storage	Location that stores temporary or permanent data
	Data Flow	Depicts data flow from data stores, processes or interactors
	Boundary	Machine, physical, address space or trust boundary.

2.2. Analysis of the Online Banking System

The online banking system is a system that provides online banking services for customers, and is also a system that exposed to the Internet environment. The external interactors of online banking system mainly include:

Online banking client (1.0): can request to the online banking system, anything that can be making the request to the online banking system, such as the browser and contract *etc.*

B2B/B2C system (2.0): can request to the online banking system, including the third party electronic payment platform and agency payment platform.

The management stuff (3.0): can be initiated by management operation request to the online banking system, online banking system to provide the corresponding management interface for management personnel to carry on the management to the online banking system, such as log audit.

Core bank account system (4.0): Suppose the online banking internal network environment and itself are credible.

The main business of online banking can be divided into: Login (5.1), query type of transactions (5.2), set type of transactions (5.3), transfer type of transactions (5.4), electronic

payment (5.5), asset/cash changing transactions (5.6) and system management (5.7). The first level data flow diagram decomposition of these business process operations is shown in Figure 1.

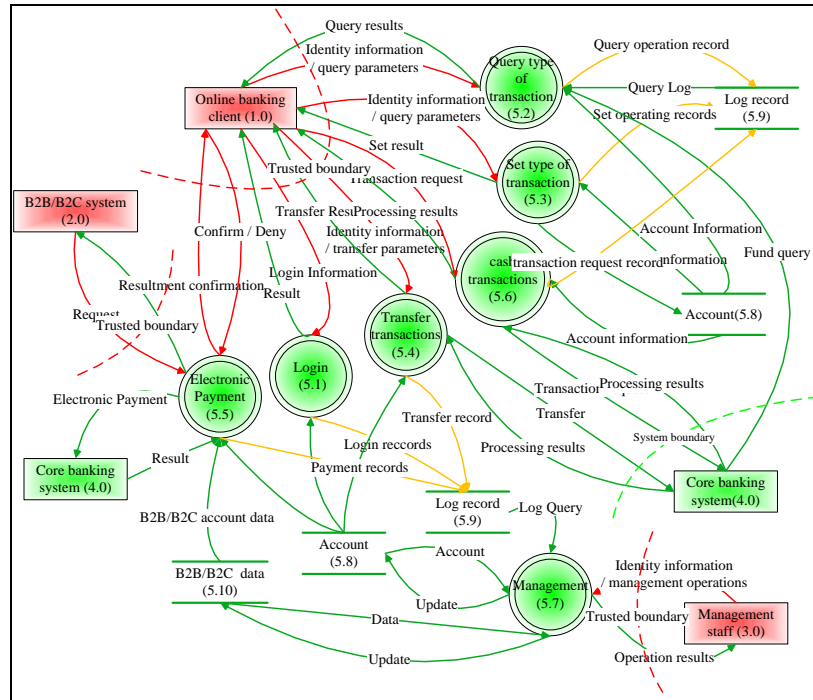


Figure 1. Critical Business Data Flow Diagram

Figure 2- Figure 8 give the 2nd level data flow diagram decomposition of the above 7 types business operation, respectively.

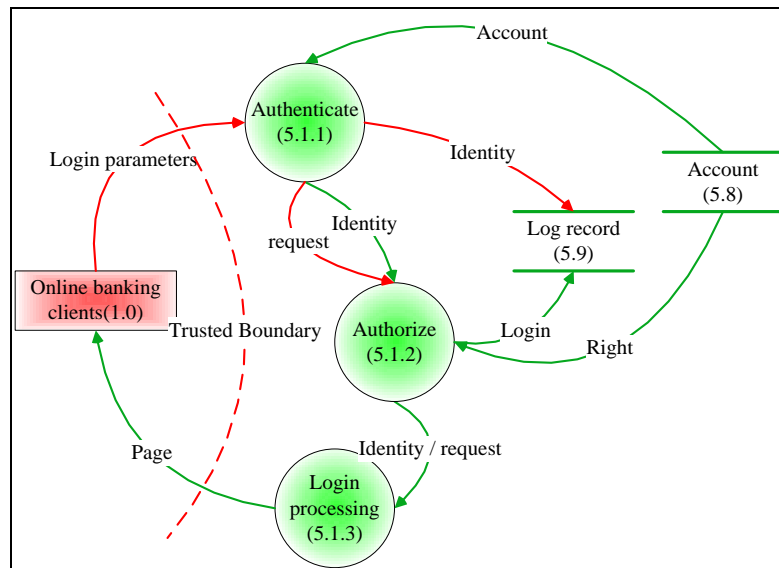


Figure 2. Login Process

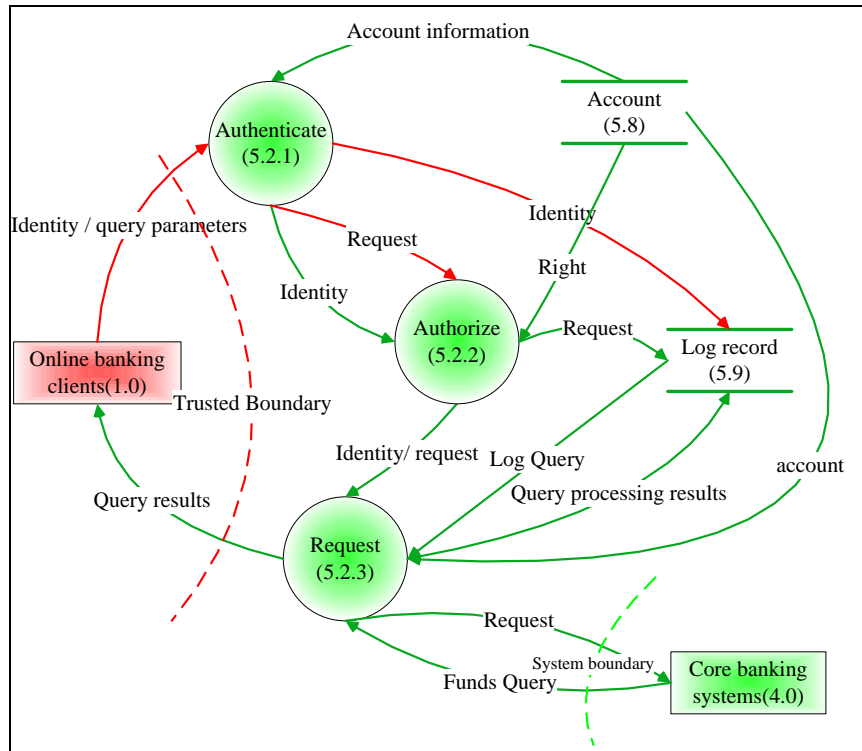


Figure 3. Query Type of Transactions Process

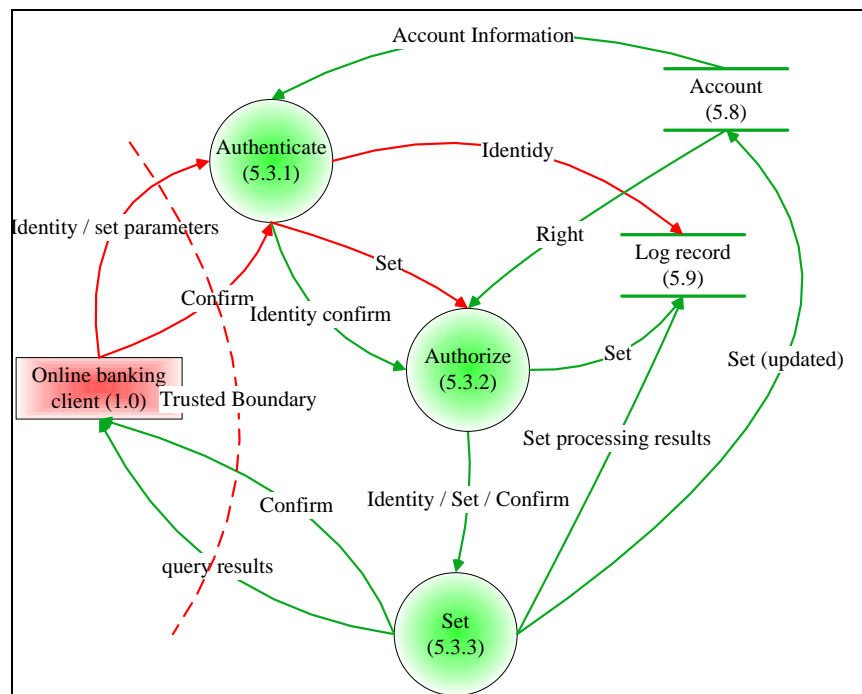


Figure 4. Set Type of Transaction Process

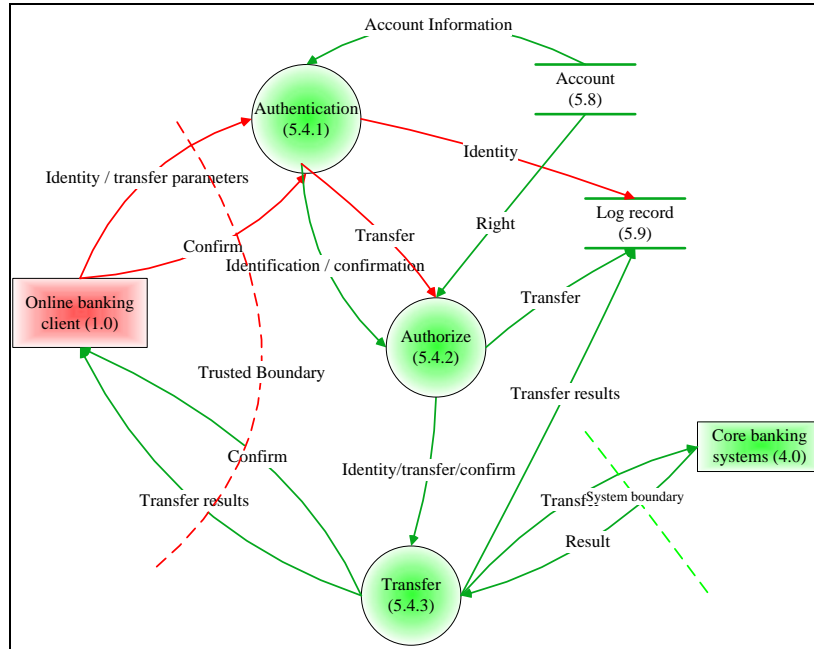


Figure 5. Transfer Type of Transaction Process

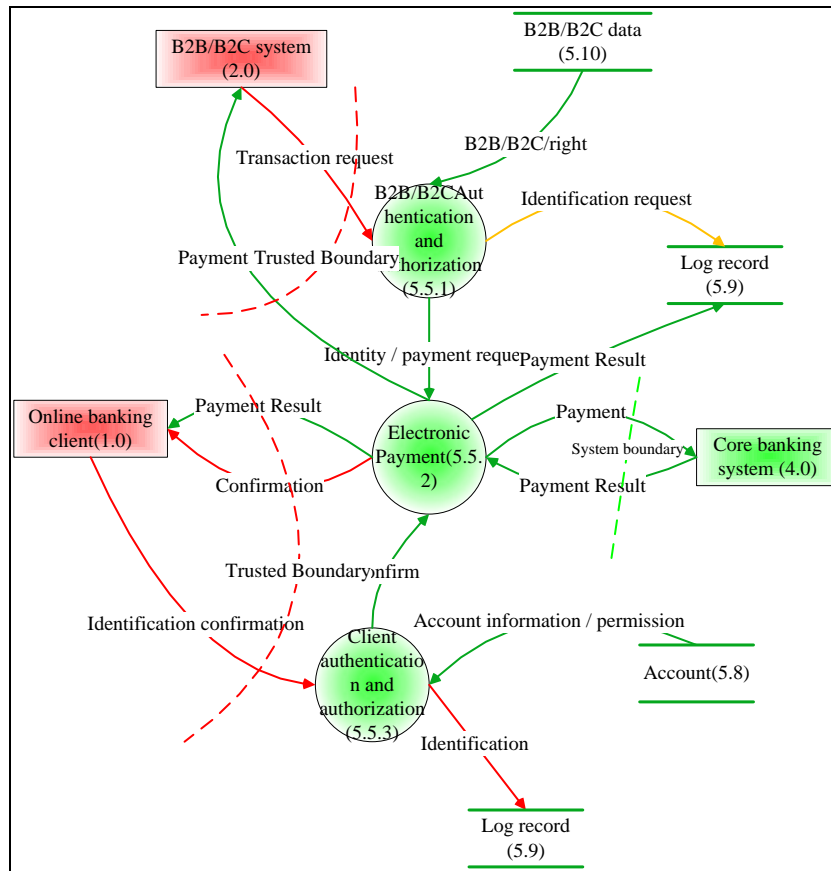


Figure 6. Electronic Payment Process

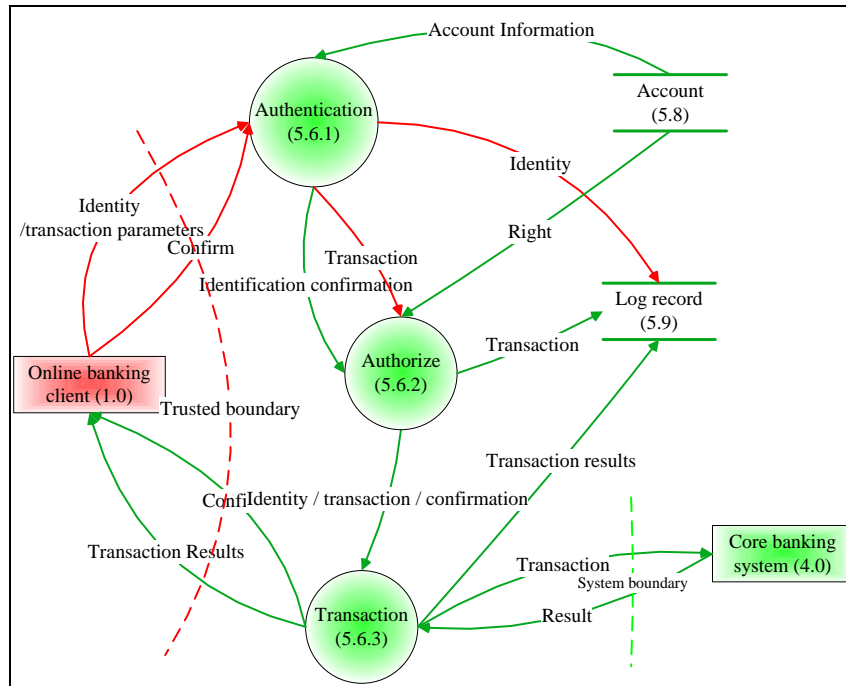


Figure 7. Assets/cash Changing Process

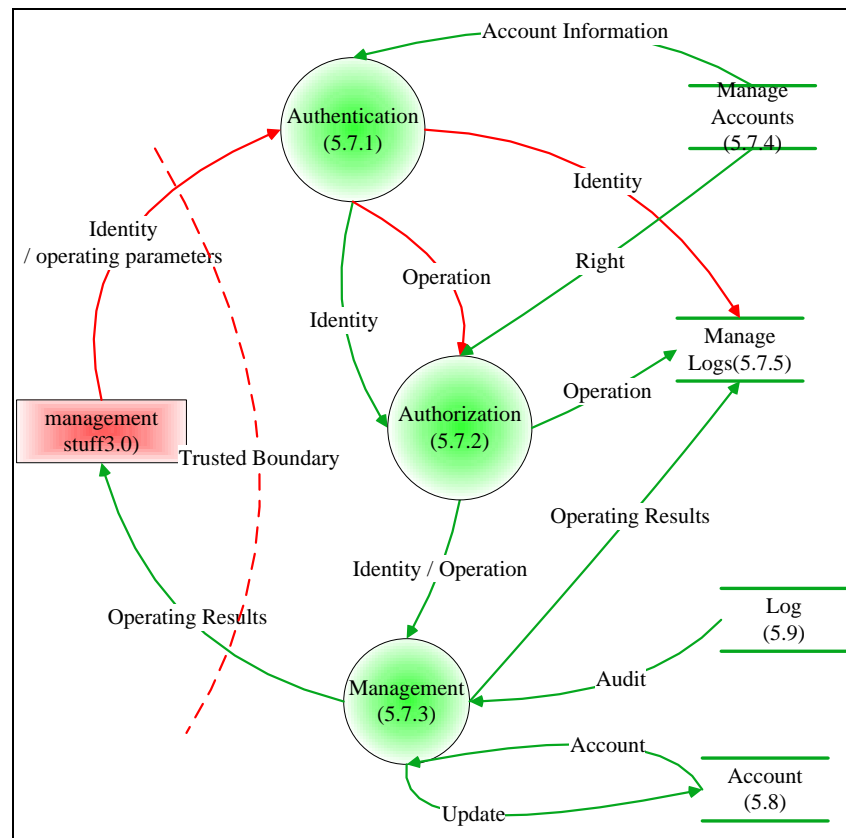


Figure 8. System Management Process

3. Analysis of the Online Banking Threat based on STRIDE Model

STRIDE [3, 4] model derive from an acronym for the following six threat categories: Spoofing Identity, the illegal use of another user authentication information. Tampering with Data, a maliciously modified data. Repudiation, users refuse to engage in activities, and there is no way to prove he was repudiation. Information Disclosure, information is exposed to the access to it is not allowed. Denial of Service, refuses to the legitimate user service. Elevation of Privilege, no privileged user access privileges, so as to have enough ability to damage or destroy the entire system. By considering threats of these various categories for each single element in the DFD, STRIDE greatly supports the identification of threats within the application.

This section will be based on online banking system data flow analysis as the foundation, analysis of whether each data flow and its associated asset information is vulnerable to any type of S, T, R, I, D and E threat, threat model to construct the entire online banking system.

3.1. Security Hypothesis

Hypothesis 1: Suppose that the bank internal network environment is a secure environment, which has a relatively perfect management system and secure mechanism.

Hypothesis 2: Suppose that the components of the online banking system can satisfy function as they claim.

3.2. Analysis of Online Banking External Interactor Threats

This paper aims at the threat analysis of the online banking system, including external interactor, the data flow and the data storage involved in 7 types of key business operations, rather than each a separate analysis of operations [8]. The external interactor threat analysis 1st and 2nd directory are shown in Table 2.

Table 2. External Interactor Threat Analysis

Threat	External interactor		
	<i>Online banking client (1.0)</i>	<i>The B2B/B2C system (2.0)</i>	<i>Manage staff (3.0)</i>
S (Spoofing Identity)	S1 Counterfeit other user identity	S1 B2B/B2C is a fraud site	S1 Forged managers identity
	S1.1 Illegally obtained certificate	S1.1 The server site to URL	S1.1 Obtain certificate illegally
	S1.1.1 Legal certificates obtained by the attacker	S1.2 Domain spoofing	S1.1.1 Administrators legal certification obtained by attackers
	S1.1.2 Forged certificate	S1.3 Content spoofing	S1.1.2 Forged certificate
	S1.2 Certification unsecure	S1.4 Framework is embedded in a web site	S1.2 Authentication is unsecure
	S1.2.1 Lack of authentication mechanisms	S1.5 ARP spoofing hijacked route back to the false site information	S1.2.1 Administrator authentication is insufficient
	S1.2.2 Certification is not sufficient	S2 B2B/B2C is a fake site	S1.2.2 No administrator authentication
	S1.2.3 Server's authentication vulnerability, which can be bypassed	S2.1 Illegally obtain certificate	S2 Management host is counterfeit operation after being invaded
	S1.2.4 Authentication algorithm unsecure leading Man-in-the-Middle attack	S2.1.1 B2B/B2C legal certificate obtained by attacker	
	S1.2.5 Certification process is re-executed	S2.1.2 B2B/B2C certificate is fake	
	S1.2.6 Passwords be cracked	S2.2 B2B/B2C authentication is not secure	
	S1.3 Password Security	S2.2.1 Not for the certification of B2B/B2C	
	S1.3.1 Password strength is insufficient, can be cracked		
	S1.3.2 Default password is insecure		

	<p>S1.3.3 Password storage is not secure</p> <p>S1.4 Brute force</p> <p>S1.4.1 Lack of mechanism to resist brute force</p> <p>S1.4.2 Mechanism of resistance to brute force can be bypassed</p> <p>S1.5 Session mechanism is not perfect</p> <p>S1.5.1 Lack of session timeout mechanism</p> <p>S1.5.2 Lack of session state examination</p> <p>S2 Counterfeit client identity communication</p> <p>S2.1 Malware simulate keyboard actions</p> <p>S2.2 Malware simulate client sending message</p> <p>S2.3 Malware fake user's operation</p>	<p>S2.2.2 B2B/B2C authentication is not sufficient</p>	
<p>T (Tampering with Data)</p>	<p>T1 Client is embedded malicious program</p> <p>T1.1 Malware tampered the user request data or the server returns data</p> <p>T1.2 The data of malware tampered with user input</p> <p>T1.3 Malware modify browser memory</p> <p>T1.4 Malware to modify the message sent or received</p> <p>T1.5 Malware display data by user actions in the interface</p> <p>T1.6 Malware modify keyboard input</p>	<p>T1 B2B/B2C site is embedded malware</p> <p>T2 B2B/B2C site is controlled by attacker</p>	
<p>R Repudiation</p>	<p>R1 Users deny carried out transactions</p> <p>R1.1 Lack of transaction signature mechanism</p> <p>R1.2 Log record is not perfect</p> <p>R1.2.1 No log records</p> <p>R1.2.2 Log records inadequate</p>	<p>R1 B2B/B2C business party deny carried out transaction</p> <p>R1.1 No valid signature</p> <p>R1.2 Log record is not perfect</p> <p>R1.2.1 No log records</p> <p>R1.2.2 Log records inadequate</p>	<p>R1 Executives deny operation</p> <p>R1.1 No valid signature</p> <p>R1.2 record is not perfect</p> <p>R1.2.1 No log records</p> <p>R1.2.2 Log records inadequate</p>
<p>I (Information Disclosure)</p>	<p>I1 Malware to steal user sensitive information, such as passwords, certificate, and input</p> <p>I1.1 Malware to steal passwords and other sensitive information via the keyboard record</p> <p>I1.2 Malware to obtain sensitive information such as user password by screenshots</p> <p>I1.3 Malware to steal the browser data in memory</p> <p>I2 Sensitive information without secure handling</p> <p>I2.1 Sensitive information stored in the local lead to information leakage</p> <p>I2.2 Encryption key is stored on the client</p> <p>I2.3 Used client temporary files does not be deleted in time</p> <p>I3 Fake site to cheat user input</p> <p>I3.1 User is fished</p>		

	I4 Security mechanism is not perfect I4.1 No message security mechanism I4.2 Weak message security mechanism I4.3 No channel security mechanism		
D (Denial of Service)	D1 Channel overload, leading log processing hang or crash D1.1 Abnormal parameters lead to a large number of consumption of server memory or CPU D1.2 Abnormal parameters cause the server to a business is to hang or crash D1.3 Multiple concurrent operations cause the server is not responding D1.4 SYN FLOOD/HTTP FLOOD attack D1.5 Large number of network packet blocking network D2 Undermine message integrity	D1 Channel overload, leading log processing hang or crash D1.1 Abnormal parameters lead to a large number of consumption of server memory or CPU D1.2 Abnormal parameters cause the server to a business is to hang or crash D1.3 multiple concurrent operations cause the server is not responding D1.4 SYN FLOOD/HTTP FLOOD attack D1.5 large number of network packet blocking network D2 failure message integrity	D1 Channel overload, leading to hang or crash log processing D1.1 Abnormal parameters lead to a large number of consumption of server memory or CPU D1.2 Abnormal parameters cause the server to a business is to hang or crash D1.3 multiple concurrent operations cause the server is not responding D1.4 SYN FLOOD/HTTP FLOOD attack D1.5 Large number of network packet blocking network D2 Server data has physical damage or destruction D3 Host unstable, which causes data errors
E (Privilege Escalation)	E1 Client security vulnerabilities E1.1 Client control of security vulnerabilities, leading to hanging horse E1.2 Client system kernel driver of security vulnerabilities E1.3 Client components of security vulnerabilities, leading to a remote attack E1.4 Not on the client control authority to define arbitrary, leading to read and write files E1.5 Cross-domain attack E2 The server security vulnerabilities E2.1 The server has cross-site scripting vulnerabilities		

4. The Construction of Threat Tree

Threat tree [4, 7, 8] provides a formal and systematic method for the analysis of system threat. Typically, modeling all threats of a system is very complex. Therefore, all threats with a single threat tree to system modeling is not realistic, since the threat tree will be very large. Based on the above reasons, this paper considers the STRIDE threat model and the threat tree analysis together. Firstly, according to the STRIDE model, we divide system threat into five aspects: S, T, R, I, D, E, so there are corresponding threats target in every aspects (see Table 2). Then using the threat tree threat analysis on each aspect of threat category, we can reduce the complexity of threat tree structure greatly.

4.1. Logic Relationship of Threat Tree

A threat tree models threats by organizing threat actions hierarchically, that is, it is a data structure contains nodes which are hierarchically connected by directional edges. When be represented by text, a threat tree can be expressed by threats and the relationship “AND (conjunction)” and “OR (disjunction)”.

4.2. Construction of Threat Tree

Analysis of potential threats in the online banking system, and decompose the attack mode which threat tree may face, the basic method is as following:

1. Classify online banking security threats by using the STRIDE threat model.
2. From the attack mode to determine the threat of these themes, decompose gradually, and then form the middle layer nodes. For example, the top-down analysis of attack pattern.
3. Check the child nodes to determine the need for further decomposition, if necessary, make the child nodes as the current target, repeat the above steps, and break them down into smaller modules.

When the node cannot be decomposed, terminate the decomposition process, i. built an inverted threat tree. At this time, all the leaf nodes are independent of each other, and also can be assessed components.

This paper only gives online banking client fake threat tree as an example (Figure 9).

```

OR 1 Counterfeit other users' identity
  OR 1.1 Illegally obtain certificate
    OR 1.1.1 Legal certificate obtained by attacker
    1.1.2 Forged certificate
  1.2 Unsecure certification
    OR 1.2.1 Lack of authentication mechanisms
    1.2.2 Certification is insufficient
    1.2.3 Server s' authentication vulnerability, which can be bypassed
    1.2.4 Authentication algorithm is unsecure, leading man-in-middle attack
    1.2.5 Certification process is re-executed
  1.3 Cracked passwords
    OR 1.3.1 Password Security
      1.3.1.1 Password strength is insufficient, which can be cracked
      1.3.1.2 Unsecure default password
      1.3.1.3 Unsecure password storage
    AND 1.3.2 Brute force
      OR 1.3.2.1 Lack of mechanism to resist brute force
      1.3.2.2 Mechanisms to resist brute force can be bypassed
  1.4 Session mechanism is not perfect
    OR 1.4.1 Lack of session timeout mechanism
    1.4.2 Lack of session state check
2 Communication with forged client identity
  OR 2.1 Malwares simulate keyboard to launched operation
  2.2 Malwares simulate client to send packets
  2.3 Malwares counterfeit user initiate operation
  
```

Figure 9. Online Banking Client Fake Threat Tree

To the online banking system, a threat tree is a set of all the threats it is facing. Thus, any threat in the threat tree may be a security risk of the online banking system. The detailed analysis of an external entity can see in the 2nd and 3rd directory of table2.

5. Conclusions

Threat modeling can help system security evaluators understand the system threats may face, and can grasp the vulnerability that the threat could exploit, and it also enable evaluators seek purposefully vulnerabilities and risks in the field testing so as to find attack paths quickly and efficiently in penetration testing.

Threat tree is a system threat modeling tool with tree representation structure, it has the advantages of structured and reusable. However, the present studies are lack of systematic and holistic in the use of threat tree system threat analysis, thus it is difficult to carry out effective use of threat tree. This paper combines STRIDE threat model with the threat tree analysis, greatly reducing the threat tree constructed complexity, making it easier to use and maintain the threat tree. Through the threat analysis of online banking system, this method can well describe the online banking system security threats, and can provide guidance for system security analysis and evaluation.

Acknowledgements

I am grateful to Mr. Zhang Li, the director of information system risk evaluation department of China Information Technology Security Evaluation Center. His knowledge and support has led to innumerable improvements of this paper. Thanks are also due to a number of my colleagues who generously read the paper entirety and to give me the benefit of their tremendous suggestions. Each of them deserves credit for the quality and style of this paper.

References

- [1] C. Joris, D. Valentin and D. Danny, "On the Security of Today's Online banking Systems", *Computers & Security*, vol. 3, no. 21, (2002).
- [2] R. Nigel, "Securing online banking", *Card Technology Today*, vol. 10, no. 17, (2005).
- [3] S. Hernan, S. Lambert, T. Ostwald and A. Shostack, "Uncover Security Design Flaws Using The STRIDE Approach", *MSDN Magazine*, (2006).
- [4] H. Michael and L. David, "Writing secure code: practical strategies and proven techniques for building secure applications in a networked world", Microsoft Press Corp, WA, (2002).
- [5] W. Stallings, "Cryptography and Network Security – Principles and Practices", Upper Saddle River, Pearson Education International, Upper Saddle River, New Jersey, (2006), pp. 9-11.
- [6] C. Möckel and A. E. Abdallah, "Threat modeling approaches and tools for securing architectural designs of an e-banking application", 2010 Sixth International Conference on Information Assurance and Security, Atlanta, USA, (2010) August 23-25.
- [7] M. Ikuya and Y. Yamaoka, "Threat tree templates to ease difficulties in threat modeling", *Proceedings 2011 International Conference on Network-Based Information Systems*, Tirana, Albania, (2011) September 7-9.
- [8] Threat Risk Modeling. Open Web Application Security Project (OWASP), http://www.owasp.org/index.php/Threat_Risk_Modeling.

Authors



Tong Xin, she received the Ph.D. degree in information security from Beijing University of Posts and Telecommunications University in 2008. She is Associate Researcher of information system risk evaluation department of China Information Technology Security Evaluation Center. Her scientific research direction: information system risk assessment and communication security.



Ban Xiaofang, she is the vice director of information system risk evaluation department of China Information Technology Security Evaluation Center. She has very rich practical experience on information system security risk assessment. Her scientific research direction: network security and information system risk assessment.