INTERNET BANKING SECURITY ENHANCEMENE WITH A THREAT ORIENTED APPROACH

Elham Judi[1], Reza Azmi[2] & Maryam Esmaeili[3]

[1]MS student of Alzahra University, judi.elham@gmail.com

[2]Assistent professor of Alzahra University, azmi.reza@gmail.com

[3]Assistent professor of Alzahra University, esmaeili_maryam@alzahra.ac.ir

Abstract

Nowadays Internet banking which uses variety of Internet based software and hardware technologies is current and expanded. Web based bank services provide users with managing financial affairs such as the money transfer process between accounts easier and faster than before. Nevertheless, security threats have been widely recognized as one of the main obstacles to the adoption of Internet banking.

For encountering possible threats, different security services and mechanisms are proposed. We propose a security framework to enhance Internet banking security. This framework is used to identify and evaluate threats of Web based money transfer process and elicit its attack tree.

The authors also propose to add a defense tree which includes security services and mechanisms; in conjunction with attacks risk to the attack tree. It is concluded that the combination of these methods will help to make decisions about selecting appropriate security services and mechanisms.

Keywords: Internet based money transfer; Threat modeling; Attack trees; Defense trees; Risk assessment; Security services and mechanisms

I. Introduction

The increasing volume of electronic commerce demands corresponding electronic payment processes which offered by financial institutions and banks. In addition, previous activities like bills payment, money transfers between accounts, and credit card related transactions need to be processed online. In fact, the customer oriented demand on Internet banking increases [1]. Moreover, Internet banking makes transactions faster, easier and cheaper.

Nevertheless, the benefits of this new approach stand against severe security issues, which it brings along.

Integrity, confidentiality and availability are typical requirements for a secure system. Any potential occurrence, malicious or otherwise, that might damage these properties is a threat. In addition, any action targeting at violation of one of them is called an attack, the possibility for an attack is called a vulnerability [2]. The threats of Web based bank services are increasing day by day. These threats have emerged as the main barrier to the adoption of Internet banking among the costumers [3].

Security services are inevitable for encountering the threats of Web service and mitigating their risk. They typically implement portions of security policies and are implemented via security mechanisms [4].

There are different security services and plenty of mechanisms to satisfy them. Selecting appropriate security services and their mechanisms becomes one of the elaborated decisions of IT managers. In this paper, a threat oriented approach is proposed to evaluate security of Internet banking and selecting countermeasures based on the risk metric by means of threat modeling. For this intention, money transfer process via Internet is selected.

The rest of the paper is organized as follows. After the literature review and introduction of the methodology, we will examine the concept of threat modeling. It presents the STRIDE model and then proposes a security framework. Afterwards, we introduce attack and defense trees. Section VI defines concepts of security service and mechanism. Section Ⅶ discusses the risk metric and introduce a method to measure it, for making security decisions. We examine Web based money transfer process in section Ⅸ. Finally, we conclude about the work presented in this paper.

II. literature review

In recent years many researchers have started research around Internet banking security. The concerns of some researches include the issue of Internet banking risk control like in [5] and [6]. Dimitriadis, C [7] proposed an attack tree to analyze the security of Internet banking based on authentication mechanisms. The findings demonstrated addressing and assessing the security of Internet banking requires specialized knowledge on vulnerabilities, attacks and countermeasures. Aburrous et al [1] proposed an intelligent performance assessment model for evaluating e-banking security websites and showed that direct internal attack risk has a large impact on e-banking security performance. Karim, Z [3] and others in towards secure information systems in online banking, found out the threats of information security of online banking with some real successful fraudulent activities happened in the past and proposed different security measures that can be taken to protect the internet frauds. Lao, G and Wang, X [8] from Shanghai University, considered Internet banking security problems and explored various of security mechanism measures to analyze the current representative of the online banking security measures with the case of professional version of China Merchants Bank's personal Internet bank.

Identification and evaluation of Internet banking attacks by eliciting threats in an organized manner can help further analysis and extract attack and defense trees which could be useful in selecting appropriate security services and their mechanisms to mitigate risk. However, to our knowledge, there is no study that examines this. Aiming at this purpose we propose a threat

oriented framework to evaluate security of Internet banking and selecting countermeasures based on the risk metric by means of threat modeling.

III. Methodology

In this article, our proposed framework is used to identify threats and elicit attack and defense trees. A method for assessing risk is introduced. For measuring risk of attacks the experimental method based on experts' opinions is used.

IV. Threat Identification

A. STRIDE Threat Model

Threat modeling is a risk assessment process. It is used to find out security problems before investing money, time and resources [9]. One of the main outputs of threat modeling is the STRIDE model. STRIDE is an abbreviation of following words:

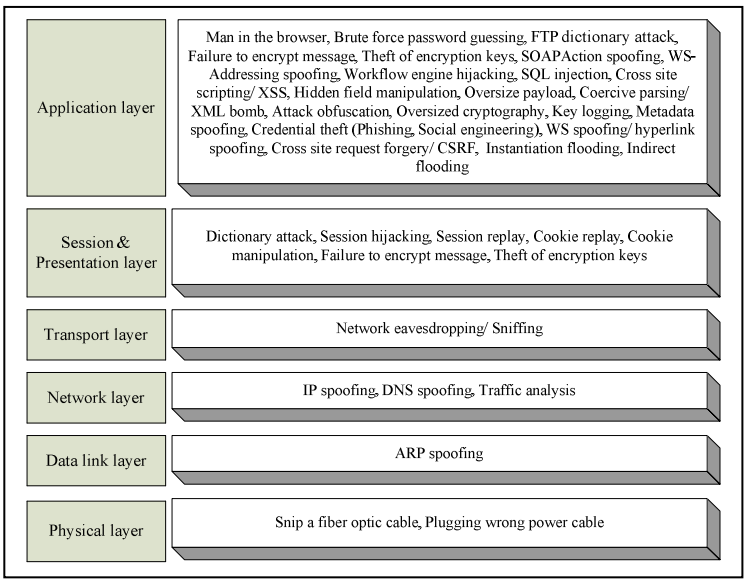
- Spoofing: Illegal access and use of a user's authentication information such as user name and password;
- Tampering: An unauthorized modification of data. For example altering data as it flows between two computers over the Internet;
- Repudiation: The ability of the users to deny that they performed specific actions or transactions and there is no way to abide the agreements.
- Information Disclosure: The unwanted exposure of information to people who are not allowed to access it;
- Denial of Service: The process of making a system or application unavailable to the legitimate users;
- Elevation of Privilege: Unprivileged users gain privileged access.

STRIDE is the commonly used method of determining threats to classify them and evaluate security of a system. Attacks are analyzed and categorized, with respect to the attacker's objective in STRIDE model [10].
On the other hand, attackers sometime do not pursue especial and just one objective. For example cross-site request forgery attack could simultaneously be a spoofing and elevation of privilege attack.

B. Layered Security Framework

In this section, we introduce a security framework for Internet banking. Our approach is based on Open Systems Interconnection (OSI) model. This model has defined a seven layer stack that consists of Physical, Data link, Network, Transport, Session, Presentation and Application layers. The framework is shown in Fig. 1, it consists of:

- Physical layer threats: The Physical layer provides the hardware means of sending and receiving data on a carrier, including cables, cards and physical aspects. Snip a fiber optic cable is one of this layer's threats.
- Data link layer threats: The Data link layer is where the logical information like IP addresses is translated into the actual electrical pulses that travel over the Physical layer. It furnishes transmission protocol knowledge and management and handles errors in the Physical layer, flow control and frame synchronization. ARP spoofing is a threat of a Data link layer.



Internet banking Security Framework

- Network layer threats: The Network layer handles the routing of the data; sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level. IP spoofing, DNS spoofing and Traffic analysis are this layer threats.
- Transport layer threats: The Transport layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. Network eavesdropping is an example of threats in this layer.
- Session & Presentation layers threats: The Session layer establishes and manages and terminates connections between applications. The Presentation layer establishes context between Application layer entities, in which the higher layer entities may use different syntax and semantics if the presentation service provides a mapping between them. These two layers are closely related, so we consider them with together. Dictionary attack, Session hijacking, Session replay and Cookie replay are these layers threats.
- Application layer threats: The Application layer provides a means for the user to access information on the network through an application. This layer is the main interface for the user to interact with the application and therefore the network. Man in the browser, Brute force password guessing, FTP dictionary attack, Failure to encrypt message, Theft of encryption keys, SOAPAction spoofing, WS-Addressing spoofing, Cross site request forgery are this layer's threats.

V. Attack and Defense Trees

In order to decompose a high level threat into intermediate objectives and finally to individual attacker actions, the concept of threat logic trees was created. Attack tree structures with child nodes having AND or OR relationships. The root node is the attacker's main goal. It is then decomposed into sub-goals and the sub-goals are further decomposed until leaf nodes representing the individual attacker actions are determined [11]. An attack tree is a way of collecting and documenting the potential attacks in a structured and

hierarchical manner. The mentioned method for determining and analyzing threats is a useful tool which could help extract attack trees.
Attack tree provides a logical way to think about security. An attack tree is an appropriate mean in making security decisions. It could be used in selecting security services and mechanisms.
While attacks are shown in attack trees, security services and mechanisms could be demonstrated in defense trees. The roots of the defense trees are security services and their loafs are security mechanisms. Indicating defense trees beside attack trees is a useful mean to analysis and find suitable countermeasures.

VI. Security Services and Mechanisms

A security service is a processing or communication service that is provided by a system to give a specific kind of protection to the resources and assets. Security services drive the enterprise policies that need to be enforced in all relevant points within the infrastructure. They address what security policies should be accomplished [12]. Security services are implemented via security mechanisms. Authentication, Authorization, Data confidentiality, Traffic flow confidentiality, Audit, Integrity, availability and Time management are examples of security services.
A security mechanism is a technical tool or technique that is used to support a security service. It might operate by itself, or in conjunction with others, to provide a particular security service [4]. For example, Digital signature, Username and password, Smart card, Token, Biometrics and Single sign on are some of the mechanisms which satisfy Authentication security service.

VII. The Risk Metric

By technology advancement, the number of ways and methods to encounter threats is increasing. In order to select appropriate security services and mechanisms the risk metric is used.
To compare the amount of risk for each threat the Microsoft's DREAD model is used. DREAD is an abbreviation of five bellow words:

- Damage potential: How great is the damage if the vulnerability is exploited?
- Reproducibility: How easy is it to reproduce the attack?
- Exploitability: How easy is it to launch an attack?
- Affected users: As a rough percentage, how many users are affected?
- Discoverability: How easy is it to find the vulnerability?

Defining amount of risk is possible by assigning to each attribute a rating between 1 (low) and 3 (high) and calculating the sum of them. The sum of ratings falls in the range of 5 to 15. Threats with overall ratings of 15 to 12 are classified as high risk, 11 to 8 as medium risk, and 7 to 5 as low risk [13].
In this paper, the DREAD model is used to calculate loafs risk. AND nodes risk is calculated by regarding:

$$R_N=\text{Max}\ \{R_i\},\ i=1:\ m; \qquad (1)$$

While R_N is the nodes risk, R_i is the leafs risk and m is the number of leafs. OR nodes risk calculation is via:

$$R_N=\Sigma\ R_i/n,\ i=1:\ n; \qquad (2)$$

R_N is the OR node's risk, R_i is the leafs risk and n is the number of leafs.

VIII. Web based Money Transfer Process

Fig. 2 demonstrates Money Transfer process via the Internet. It is a Web base service. By means of the proposed framework, we determined threats and then extracted the attack tree which is shown in Fig. 3.
The attacker's goal is Transfer money to his own desired account himself. For achieving this goal, he might experience one of the ways which is shown as the sub goal. The leafs indicate attacks. Their risk is calculated by using the DREAD model. The nodes risk and the root's total risk, are calculated based on (1) and (2).
Defense tree is added at Fig.4. As mentioned, it's leafs are security mechanisms, and the roots are security services. For simpilification we just show part of the defense tree.

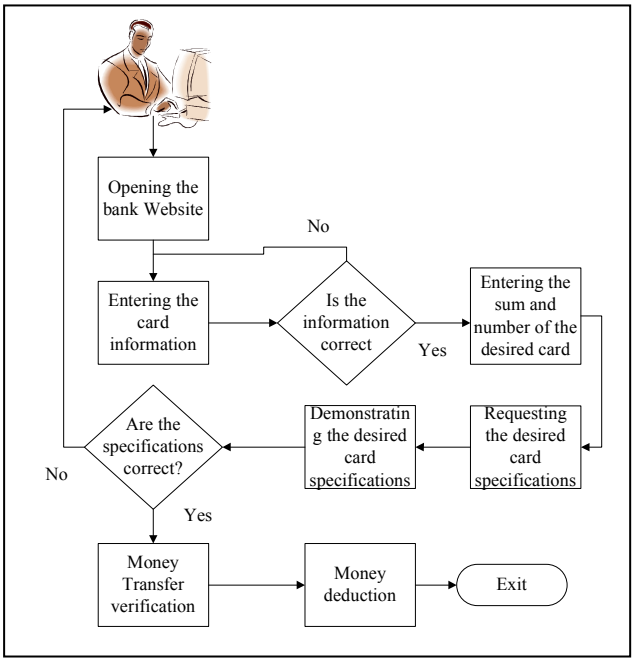


Figure 1. Web based Money Transfer process

For selecting security services and mechanisms, these steps are followed:

1. Calculate risk in the attack tree, with a bottom-up approach.
2. Select high risk nodes with an top-down approach.
3. Choose and prioritize security services and mechanisms based on loafs risk.

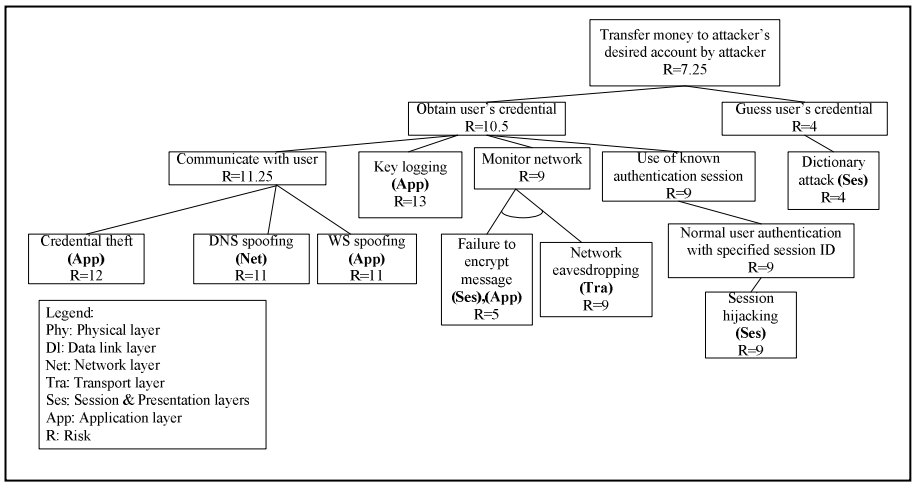


Figure 2. Web based Money Transfer process attack tree

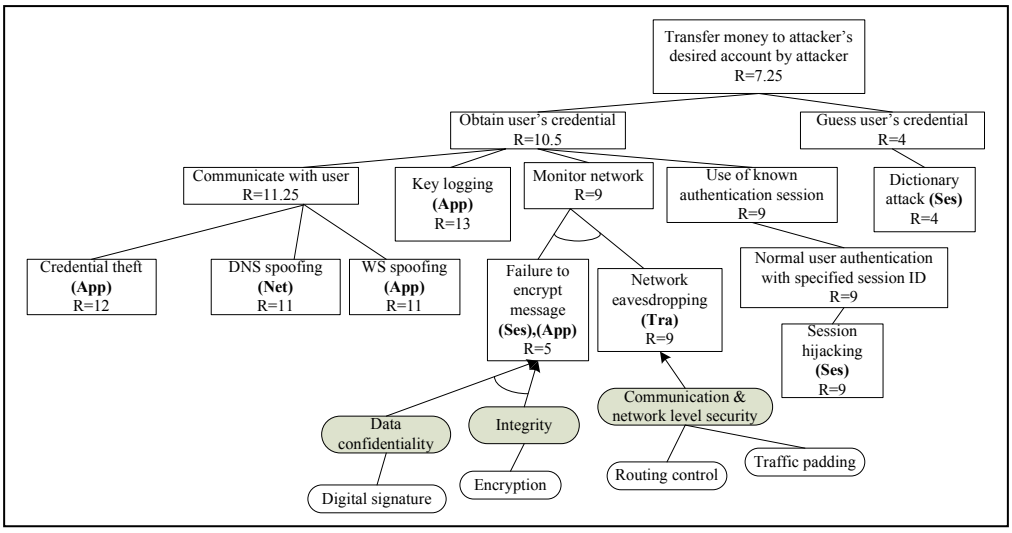


Figure 3. Web based Money Transfer process attack and defense tree

Ⅸ.Conclusion

Internet banking makes transactions faster, easier and cheaper. Nevetheless, it faces severe security threats. For encountering possible threats, different security services and mechanisms are proposed. Our security framework helps to enhancement Internet banking security by identifying and evaluating threats of Web based banking services and eliciting attack trees. The defense trees which include security services and mechanisms are added to the attack trees. Finally, selecting appropriate security services and mechanisms is possible by risk assessment.

References

[1] M. Aburrous, M. A. Hossain, F. Thabatah, K. Dahal, (2008). *Intelligent Quality Performance Assessment for E-Banking Security using Fuzzy Logic*. Fifth International Conference on Information Technology, Apr. , 420 – 425.
[2] M. Jensen, N. Gruschka, R. Herkenhoner and N. Luttenberger, (2007). *SOA and Web services: new technologies, new standards-new attacks*. Proc. IEEE Fifth European Conference on Web Services (ECOWS'07), IEEE Press, Nov., pp. 35-44.
[3] Z. Karim, K. M. Rezaul, A. Hossain, (2009). *Towards Secure Information Systems in Online Banking.* Internet Technology and Secured Transactions.
[4] T. Erl, (2009). *SOA Design Patterns.* Prentice Hall.
[5] S. Laforet, X. Li, (2005). *Consumers' attitudes towards online and mobile banking in China*," International Journal of Bank Marketing, Vol. 23, No.5, pp. 362-380.
[6] Y. Zhu, (2006). *How to strengthen Internet banking security management*. Modern Finance, No. 10, pp. 32.
[7] C. K. Dimitriadis, (2007). *Analyzing the Security of Internet Banking Authentication Mechanisms.* INFORMATION SYSTEMS CONTROL JOURNAL , Vol.3, pp.1-8.
[8] G. Lao, X. Wang, (2010). *Study of Security Mechanisms in Personal Internet Banking-Take China Merchants Bank as an Example.* Computational Intelligence and Software Engineering (CiSE).
[9] J. P. Jesan, (2008). *Threat modeling Web-applications using STRIDE average model.* Computer Security Conference.
[10] L. Jiang, H. Chen, F. Deng and Q. Zhong, (2011). *A security evaluation method based on threat classification for Web service*. JOURNAL OF SOFTWARE, vol.6, NO. 4, pp.595-603.
[11] K. Edge, G. Dalton, R. Raines, R. Mills, (2006). *Using attack and protection trees to analysis threats and defenses to homeland security*. IEE Military Communications Conference (MILCOM).
[12] A. Buecker, P. Ashely, M. Borrett, M. Lu, S. Muppidi and N. Readshaw, (2007). *Understanding SOA Security*. IBM Publication.
[13] F.Swiderski, W. Snyder, (2004). *Threat Modeling*, Microsoft.