Business, Management and Economics Engineering
ISSN: 2669-2481 / eISSN: 2669-249X
2022 Volume 20 Issue 2

MODELING THREAT TREES THROUGH STRIDE MODEL CONCEPT FOR THE BANKING SECTOR

Priti Saxena
PhD Research Scholar Veer Madho Singh Bhandari Uttarakhand Technical University, Dehradun, India, Email- pritisaxena82@gmail.com

Dr. R. B. Patel
PhD Supervisor - Professor and HOD Department of Computer Science and Engineering, Chandigarh College of Engineering and Technology (Degree Wing), Sector 26, Chandigarh, India, Email- drpatelrb@gmail.com

ABSTRACT
A rapidly expanding industry in India is the banking sector. Online banking has given a lot of benefits for banking from anywhere and everywhere concept. But, this has brought threats and attacks along with it. This article works on the creation of threat trees to keep a check on the threats. The details of these can be incorporated during the requirement and design phase. The creation of threat trees proves beneficial to the programmers to keep the preventive measure ready in advance during design and implementation, and trace the vulnerabilities to reduce the cost for corrections.
KEY WORDS: Security, Vulnerabilities, e-banking, privacy, online banking portals, threat modelling.

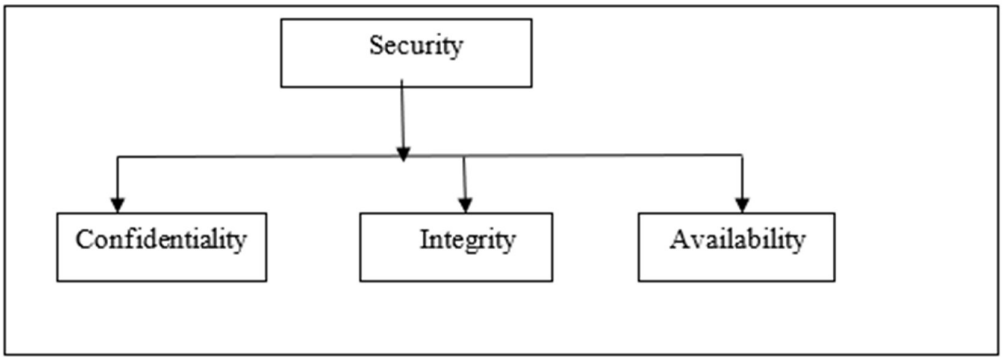
INTRODUCTION
In order for the security measures of an organization to be deemed adequate, they need to adequately handle all three aspects of the CIA Triad [1]. It is generally agreed that the CIA Triad, which organizes three properties called confidentiality, availability, and integrity, is the fundamental information security component. Every single security vulnerability as well as security control are analyzed in great depth. The three main characteristics of information security which are of main concern are:

1. Confidentiality
2. Integrity
3. Availability

Other factors which are somehow related are:

1. Trustworthiness
2. Accountability
3. Audibility
4. Non – repudiation
5. Privacy

Figure 1. Three essentials for security framework



For doing the analysis of the security, it is mandatory Confidentiality
Information is protected from unauthorized access by confidentiality. The vast majority of information systems store data that is particularly sensitive in some way. As a result of the fact that confidential information is often worth something, systems are frequently targeted by criminals on the lookout for vulnerabilities that they may exploit. Direct attacks, including recording network data and stealing passwords, are examples of threat vectors. More layered attacks, like phishing and social engineering, are few threat vectors examples that include many layers of attack. Disclosures of secret information are not always done on purpose.
There are several countermeasures to protect users' privacy. Software such as passwords, access control lists, and authentication methods may be used to restrict who can use what. However, as technology has progressed, their usefulness has diminished.

Integrity
It ensures that data is not modified without permission. These security measures ensure that information is comprehensive and correct. It is important to protect not just information at rest on computers, but also information in transit through means like email. Access control and authentication are countermeasures used to prevent unauthorized modifications by authorized users, hence maintaining the system's integrity. Transactions may be more trusted when verified using hashing and digital signatures. Control from the administration is also crucial.
Availability
Only authorized users should have access to an information system. Timely and consistent system access is guaranteed by availability safeguards. Problems with hardware and insufficient bandwidth in the network are two examples of potential hazards. Hackers regularly employ denial-of-service attacks to cause interruptions in website functionality. Protecting the availability of a system is the job of availability countermeasures like firewalls and routers.

OBJECTIVES OF THE STUDY
The objectives to be covered in this research contains the following:
1. Review CIA triad and its importance in security.
2. Study of the present status of cybersecurity along with the security concerns.
3. Study of the work done in the past in the field of online security.
4. Case studies of the various attacks faced by financial and non-financial organizations.
5. A glimpse into the three forms of cybercrimes – cyber threat, cyber-attack and cyber fraud.

6. Study of STRIDE and modeling client fake threat trees for preventive measures.

PROBLEM STATEMENT

Evaluation of the threats, frauds and attacks in the present online banking system and modeling of fake client threat trees for the systematic evaluation of threats in the banking system.

ORIGINALITY

In the current study, new threat trees that are based on more recent vulnerabilities have been developed to assess the concern level regarding privacy and security, as well as the satisfaction level regarding privacy and security, with regard to the use of a variety of online banking services.

BACKGROUND LITERATURE

Organization places policies for keep their assets secure and places various awareness programs to train the employees, but because of lack of interest, unacceptance to the new system of working, placement of wrong access right because of negligence factor organization are facing a lot of problems related to the security of the individual and resources. As per the data the year 2014 is known as the year of cyber-attacks as the attacks reached the highest peak as shown by Andrea in this study. Andrea has pointed out the name of non – profit organization like secure Domain Foundation (SDF) which provides awareness to people about cyber-attack, risk and cyber-crime [2].M .Uma and J. Padmavathi in 2013 shown in their study about the lack of proper info related to cyber-crime which becomes an obstacle in figuring out the appropriate countermeasure in the information Security [3].

As per the study, there is a correlation between Government sector and cyber espionage, hence in activism technique and cyberwar activities happens. Cyber-crime is correlated to industries and business sector. Jayanthi and Mansurali have proposed the concept of profitable learning in the banking sector. They studied the findings of last three of P & B, found the loss of many crores due to cyber-attacks and cyber-crimes [4]. Bhasin analyzed that finding new countermeasures frauds, formulating strategies to detect frauds, organizing extortion determination rules keeps the organizations away from the loss of income and resources [5].There are various way to do the fraud in the system. Some of them are listed below [4]:

1. Data and documents belonging to another person are obtained and used for personal gain.
2. A person gets money which surpasses his limit of access by giving false info. About his pay.
3. A person takes credit by using a false name and no proof exists of that name in the system.
4. False documents are used to gain access to the system resources.
5. From 2008 – 2018 banks were the biggest target of frauds.

Bhasin explained online or web banking fraud as a kind of fraud where fraudsters who are normally people working in the company performed frauds through systems or tricking people [6]. Ramana and Krishna showed a detailed survey of frauds in Indian banks. They explained a method for small banking industry for the determination and prevention of fraud.

They noted an increase in retail banking fraud [7]. Kundu and Rao have looked at numerous previous instances of fraud and used a trend strategy map for foresight and decision making [8]. Decision-making relies on a wide variety of computational intelligence approaches, which Prem and Karman reviewed in various points[9].Yergo, found that even a small attempt of fraud is considered as a crises in banks. A strategy of fraud triangle was implemented to identify the motifs behind the bank fraud, but it was not successful [10]. Pani and Swain, investigated all the facets of fraud in Indian banks. Evaluation is done using the secondary data available like KYC [11]. They give detailed information about kinds of threats, sources of internal threat and external threats, security measures, security methods [11]. As per the study of the past, India saw the second highest number of data breach in 2018. Two tools have been utilized, one is unauthorized use of payment cards and APP (Authorized Push Payment) [12]. Statista listed biggest cyber-crime breaches as of 2021 in an article, in 2018, an early breach was of security of India's national ID database Aadhar with over 1.0 million record lost [12]. In 2014, hacking of online platform of Yahoo was uncovered which has affected 500 million user accounts. In 2016, Yahoo revealed another hack dated back in 2013. As of 2020, the average cost goes near 4 million user dollars mostly affecting healthcare sector. Annual spend has rised from 75.6 billion in 2015 to 124 billion US dollar by 2019 [13].Statista reported in 2019, about 2093 cases of online banking fraud across India. Maharashtra had the highest cases of about 552 banking frauds that year [14]. In 2019, over 44.5 thousand cybercrimes incidents were registered in Karnataka and Uttar Pradesh. In a Country like India the actual figure could he under – reported due to lack of cybercrime, awareness or the mechanism to classify them [15].A paper reviewed the major types of fraud the bank is facing. List included identify Fraud, Phishing, Card Fraud [15].

The term "online banking" refers to the practice of initiating monetary transactions through the internet. With no need for on-site inspections, businesses may save money and make life more convenient for their customers. The term "online banking" may also refer to banking done entirely over the Internet.[18]. It is always said that where ever innovation happens, it brings both risks as well as benefits. Tremendous growth has been seen in the past five years in internet banking it be e –commerce or e– shopping or online banking the internet has provided a great frameworks to work at ease irrespective of the location. But on the other side this diversion has placed us more vulnerable to a different type of attacks.

Present Scenario of E-Banking in India

According to Eriksson, Sayar, and Wolfe [19], the emergence of e-banking has profoundly changed the method in which banks typically run their operations as well as the ways in which customers carry out their banking activities. This transformation has occurred as a result of e-banking. According to a poll conducted by Amato, e-banking has shown amazing development in recent years and has emerged as one of the primary channels via which banks distribute their goods and services [20].E-banking, as described by Daniel and Sathye [21], is the "automatic delivery of both new and old banking goods and services to consumers through electronic, interactive communication channels." E-banking refers to the usage of systems that enable users of financial institutions, whether they persons or companies, to access their accounts, conduct business, or gain information on different financial products and services over a public or private network, such as the internet. Customers may access e-banking services through the use of a variety of sophisticated electronic devices, including touch-tone telephones, kiosks,

ATMs, PDAs (personal digital assistants), PCs (personal computers). In their research, Chou and Chou identified five fundamental services that are associated with online banking. These services are the following: transferring funds to other accounts; paying bills; transaction histories and viewing account balances; requesting credit card advances; and ordering checks for faster services that can be provided by foreign and domestic banks [22].

Benefits of e-banking

E-banking is advantageous for both banks and the consumers of such institutions. From the viewpoint of the banks, e-banking has made it possible for them to reduce their operating expenses by reducing the amount of people needed and by requiring essentially no physical space [23]. In accordance with the feedback from patrons. Using the bank's internet, banking transactions may be completed at any time and from any location [24]. In addition, there is no longer a need to wait for one's time to arrive, and information on financial services may now be obtained in a simple and expedient manner. The following types of services are the primary components that make up the realm of online banking [24]:

1. ATMs (Automated Teller Machines)
2. Mobile Banking
3. Internet Banking
4. Non-Cash Retail Payments: RTGS, NEFT, ECS, Credit Cards, Debit Cards

Futuristic cyber-attacks

Nowadays, everything from our financial transactions to our transportation systems are interconnected in some way or another. The once-discretionary practice of protecting one's network is now an absolute need. These might be fired by anybody, anywhere. The security measures in place can only detect common threats. A trust exploitation attacker seeks to gain control of a trusted host in order to launch attacks against other hosts in the network [36]. Hosts inside a company's network that are firewall-protected yet accessible to trustworthy hosts outside the firewall are vulnerable to attack from those hosts.

METHODOLOGY

Threat modeling strategy

In computer security, a vulnerability may be exploited to carry out an activity that might have a negative effect on a computer system. This is what we mean when we talk about a threat. To minimize the attacks, evaluation of threats plays a vital role. Using threat modeling helps in the identification of cyber security threats, prioritize the threats and helps in performing actions in effective risk mitigation. With threat modeling a proactive cybersecurity threat assessment can be performed. Threat mapping, threat intelligence, risk assessment, mitigation capabilities, and asset identification, are the five components that make up the process.

I have used STRIDE methodology for threat modeling. Microsoft's engineering team developed this threat model to aid in the process of finding security flaws in a given system. It makes it most effective for evaluating individual system.

Data Flow Analysis of Online Banking System

Online banking is broken down into three distinct data flows—processing, transmission, and information storage—to account for the variety of activities involved in the business process. There are essentially three categories into which internet banking's primary features fall.

1. Login process
2. Query type of information

3. Set type of information
4. Transfer type of transaction
5. Electronic payment transaction
6. Asset/ Cash changing
7. System management

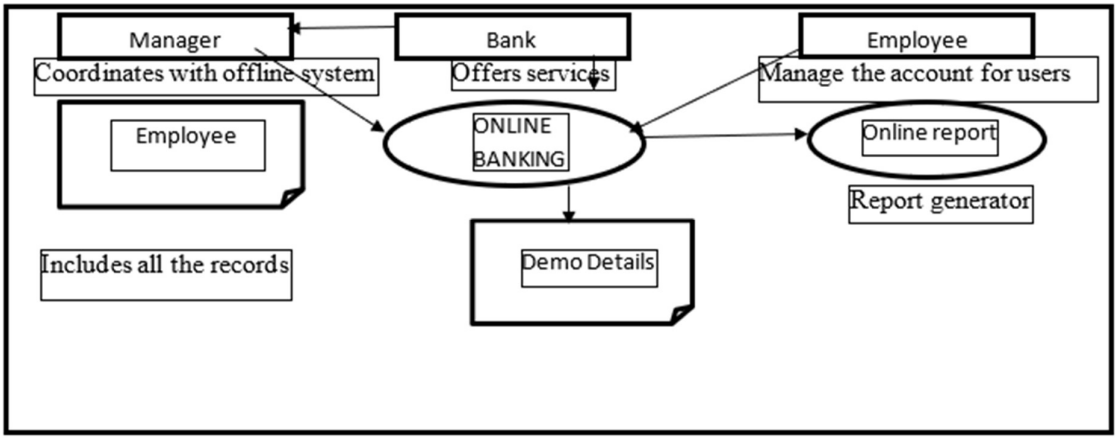


Figure 2. Flow in a banking system

Figure. 2 shows a data flow depiction of a typical online banking system, illustrating the fundamental movement of data between various nodes.

Analysis of the Online Banking System

Customers may take use of online banking services provided by the system, which is open to the environment of the Internet. The following are the most important external inter-actors in the online banking system:

Online banking customers may make requests to the system for internal banking functions, and B2B and B2C systems can make requests to the online banking system for their own functions. Management might request auditing services from the management stud. Financial institution banking network infrastructure based on the core banking system.

ANALYSIS OF THE ONLINE BANKING THREAT BASED ON STRIDE MODEL

The STRIDE model is an acronym that stands for the following six different types of threats: Spoofing Identify, the unethical use of the authentication information belonging to another user. Tampering with data, or data that has been manipulated dishonestly. Repudiation occurs when users decline to participate in activities, and there is no way to demonstrate that he was repudiation. Disclosure of information, in which sensitive data is made publicly available but unauthorized users are prevented from accessing it. The genuine user is denied service when there is a denial of service. Elevation of Privilege, as well as the absence of privileged user access rights, in order to be able to cause enough harm or destruction to the whole system. STRIDE provides a significant amount of help for the detection of dangers inside an application by taking into account threats from a wide variety of categories for each individual element in DFD.

The following discussion will use an examination of the data flows in an online banking system as the basis for determining whether or not the system as a whole is susceptible to the S, T, R, I, D, and E classes of threats.

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.

Table 1 shows various external inter actors categorized under STRIDE model after which evaluation and modeling of threat trees will be done.

Figure 3.Threat analysis for Spoofing with online banking client

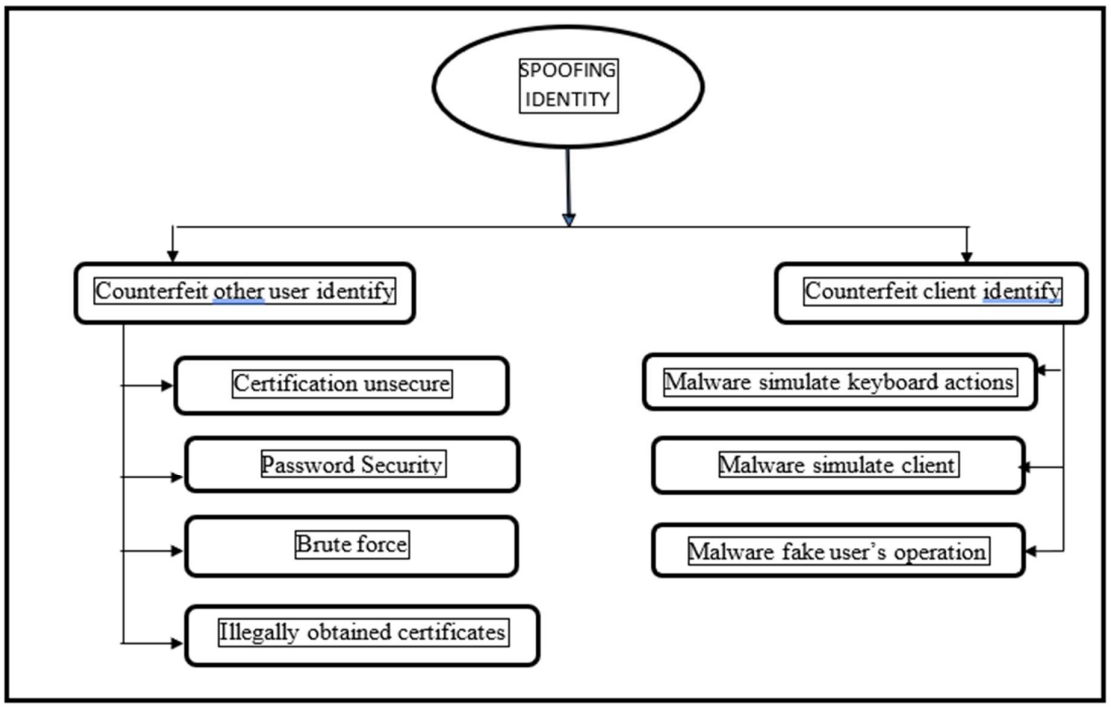


Figure 4. Threat analysis for external factors of spoofing with online banking client

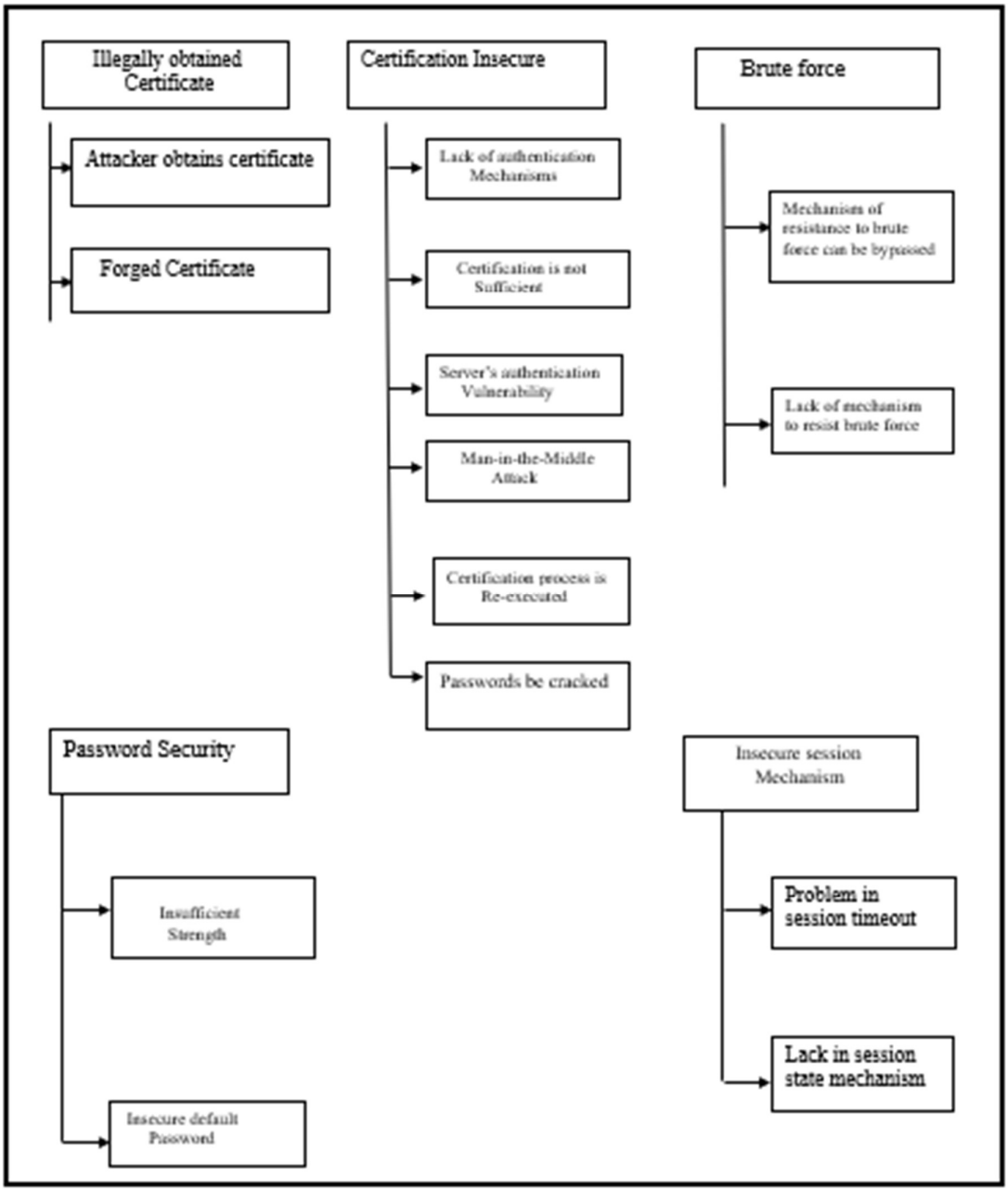


Figure5.Threat analysis for Repudiation with online banking client

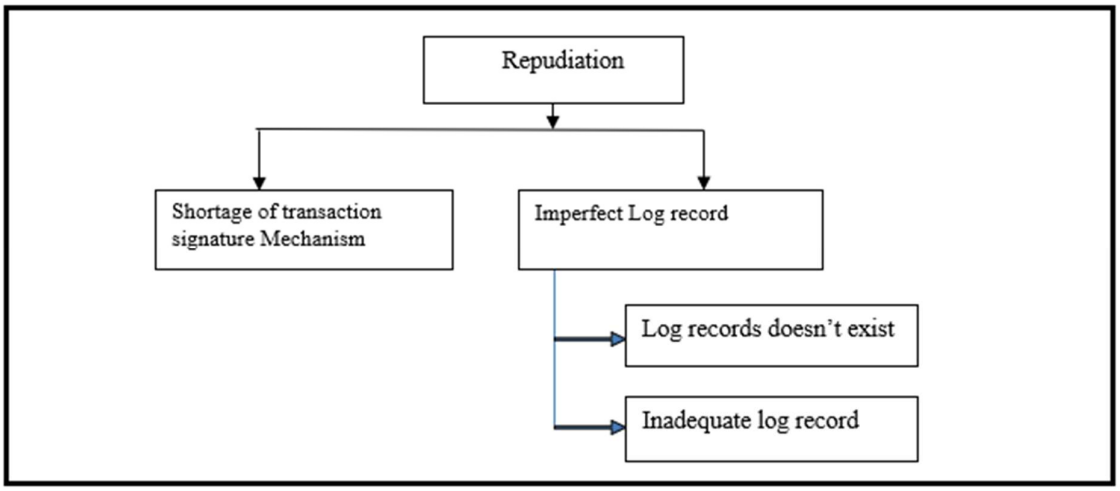


Figure 6. Threat analysis for Tampering with external factors

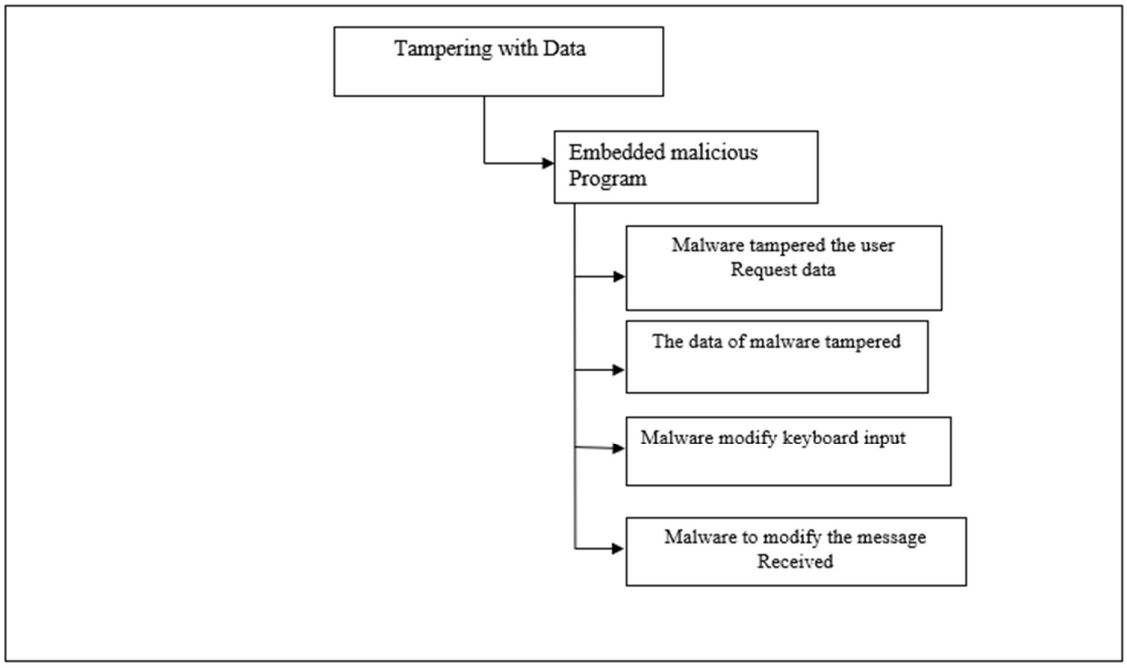


Figure7.Threat analysis for DOS with online banking client

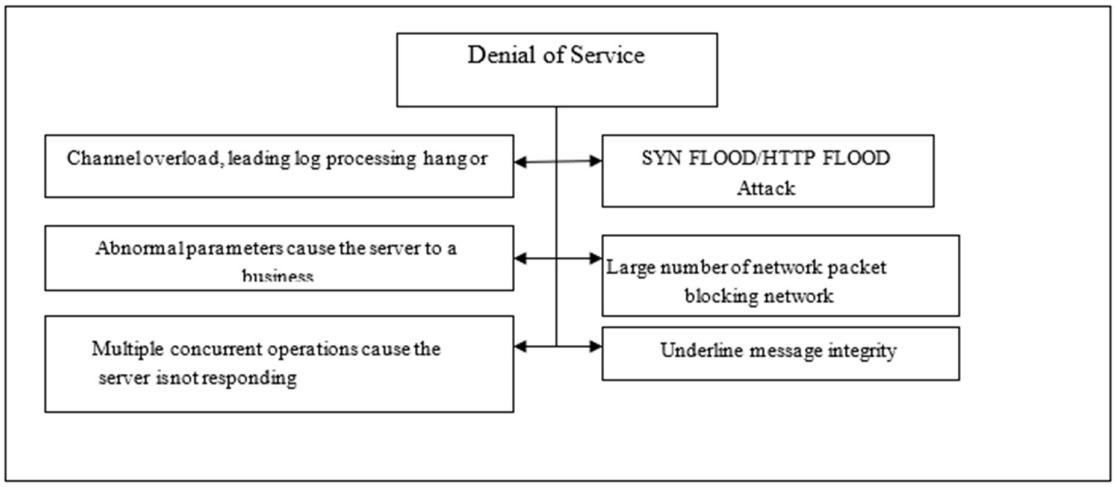


Figure 8. Threat analysis for Privilege with online banking client

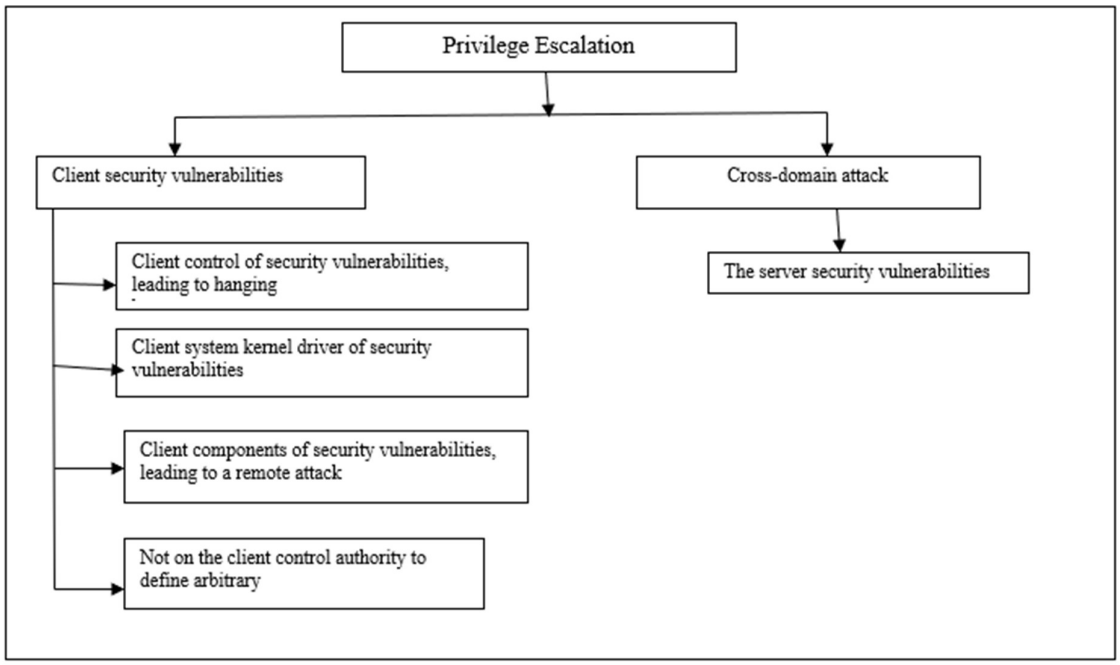
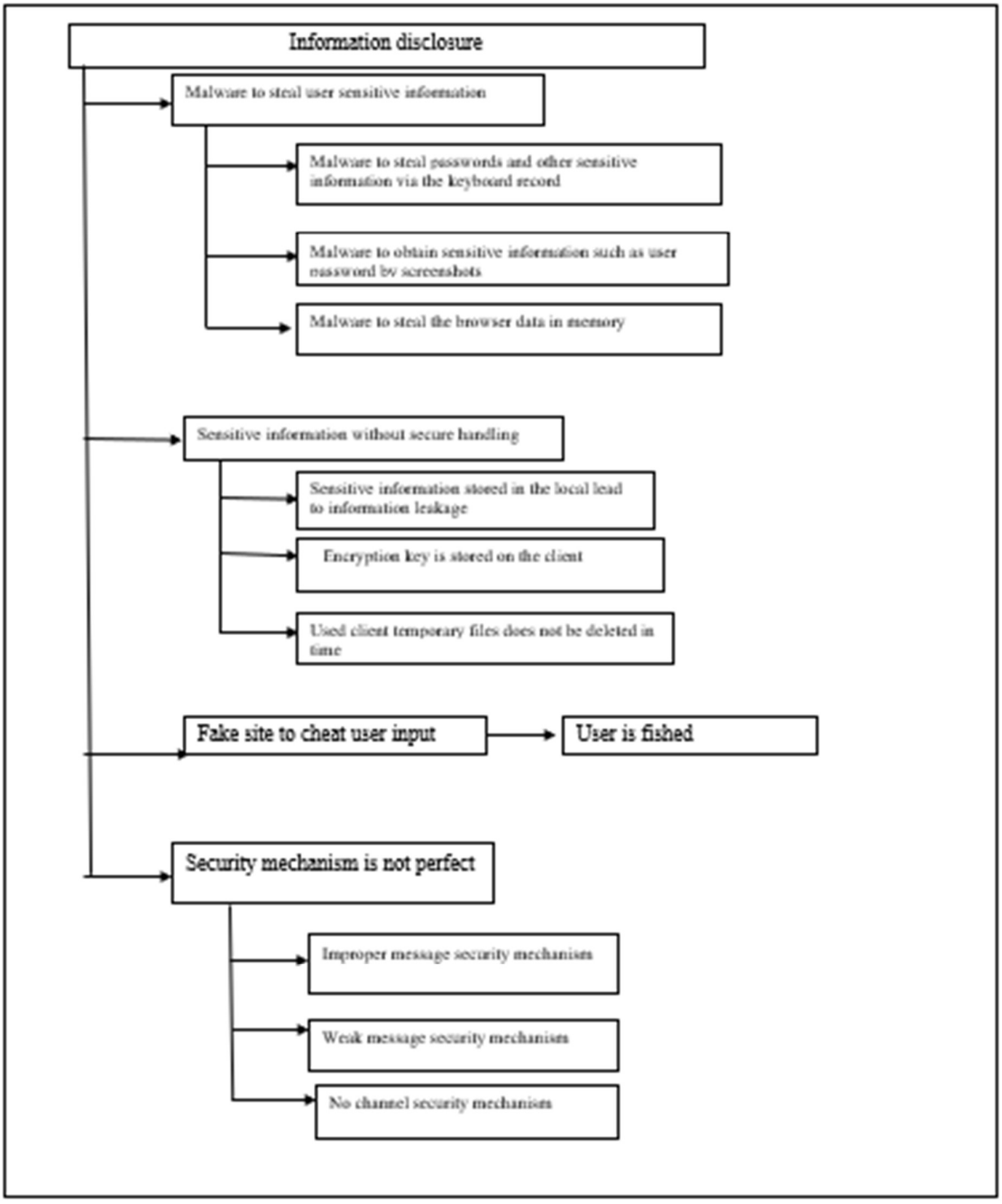


Figure9. Threat analysis for Information disclosure with external factors



THE CONSTRUCTION OF THREAT TREE

The threat analysis provided by a threat tree is formal and methodical. The process of simulating all possible risks to a system is often highly involved. Therefore, it is unrealistic to simulate all risks to a system using a single threat tree, since the resulting tree would be very huge. Because of the above, this work integrates the STRIDE threat model with the threat tree analysis. To begin, we use STRIDE paradigm by classifying risks to the system as either "S," "T," "R," "I," or "D" and "E," respectively, to ensure that every facet of the system is adequately

protected (see Table 2). The complexity of the danger triangle may be considerably reduced by doing a threat tree analysis on every component of the threat category.

Logic Relationship of Threat Tree

A threat tree is a data structure consisting of nodes linked in a hierarchical fashion by directed edges that is used to represent threats by arranging threat actions in a hierarchical fashion. A textual representation of a threat tree may be written in terms of threats and "AND (conjunction)" along with "OR (disjunction) connection.

The following is a simple approach to analyzing possible risks to an online banking system and dissecting the attack mode that it might encounter.

1. Apply the STRIDE paradigm to the problem of online banking security classification.
2. If the attack mode indicates that additional decomposition is required, the child nodes may stand in as the current target, at which point the previous stages are repeated and the node is further subdivided into smaller modules.
3. Examine the child nodes to see whether additional decomposition is required; if so, set the child nodes as the current target; if further decomposition is required, set the child nodes as the current target again; and so on.

I made a threat tree in reverse since it seemed more logical to stop the decomposition process when a node could not be broken down. All the leaf nodes may be evaluated separately at the moment.

FORMULATION OF FAKE THREAT TREES

Online banking client fake threat tree (Spoofing S)

OR 1. Forged other user's identity
OR 1.1 Illegitimately obtaining certificate.
OR 1.1.1 Attacker gained Legal certificate.
1.1.2 Fake certificate.
1.2 Insecure certification
OR 1.2.1 Lack of authentication mechanisms.
1.2.2 Insufficient Certification.
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 a re – executed.
1.3 Cracked passwords
OR 1.3.1 Password Security.
1.3.2 Password strength is insufficient.
1.3.3 Insecure password.
1.3.4 Insecure Storage.
AND
1.3.2 Brute force
OR 1.3.2.1 Lack of mechanisms.
1.3.2.2 Resisting mechanisms by passed.
1.4 Imperfect session mechanism
OR 1.4.1 Lack of session time out 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.

For Tampering with Data (T)
OR 1 Client embedded malicious program.
OR1.1 Malware tampered the user request data or the server return data.
1.2 The data of malware tampered with user input.
1.3 Malware modify browser memory.
1.4 Malware modifies the sent or received.
1.5 Malware display data by user actions in the interface.
1.6 Malware modify keyboard input.
Repudiation (R)
OR 1. Users deny carried out transactions.
OR 1.1 Lack of transaction signature mechanisms.
1.2 Log record is not perfect.
1.2.1 No log records.
1.2.2 Log records inadequate.

Information Disclosure (I)
OR 1 Malware to steal user sensitive info, such as passwords, certificate and input.
1.1 Malware to steal passwords and other sensitive information via the keyboard record.
1.2 Malware to obtain sensitive info. Such as user password by screenshots.
1.3 Malware to steal the browser data in memory.

OR 2 Sensitive information without secure handling.
2.1 Sensitive information stored in local computer leading to information leakage.
2.2 Encryption key is stored at the client end.
2.3 Used client temporary files does not be deleted in time.

OR 3 Fake site to cheat user input.
3.1 User is fished.
OR 4 Security mechanism is not perfect.
4.1 No message security mechanism.
4.2 Weak message security mechanism.
4.3 Absence of communication channel security mechanism.

Denial of Service (D)
OR 1 Channel overload, leading log processing hang or crash
1.1 Abnormal parameters Read to a large number of consumption of server memory or CPU.
1.2 A company's server freeze or reboot if it encounters any abnormal parameters.

1.3 Multiple activities running in parallel are the reason of the server not responding.
1.4 HTTP FLOOD/SYN FLOOD attack
1.5 Large number of network packet blocking network
2. Underline message integrity.
Privilege Escalation (E)
OR 1 Client security vulnerabilities
1.1 Client control of security vulnerabilities, leading to hanging horse.
1.2 Client system Kernel driver of security vulnerabilities.
1.3 Not on the client control authority to define arbitrary leading to read and write files
1.4 Client components of security vulnerabilities , leading to a remote attack
1.5 Cross domain attack
2. The server security vulnerabilities
2.1 The server has cross site scripting vulnerabilities.

RESULT

According to the findings of a study, different banks' online banking websites have varying degrees of privacy and security features. The making of threat tree will provide great assistance during the software development planning phase as more proactive measures will be implemented which will reduce the further cost due to attacks.

RESEARCH IMPLICATIONS

The results of the research have repercussions for the financial services sector in two different ways. To begin, the lenders will have a better chance of making their internet portal safer if they improve the privacy and security measures it has. The second advantage of doing this research is that it will help financial institutions better comprehend the actions taken by customers who utilize online banking. They will be familiar with the newly discovered weaknesses.

RESEARCH LIMITATIONS

One of the major problem faced during study is the unavailability of the primary data due to security reasons of the bank. Most of the work is done using the secondary data.

REFERENCES

[1] D. Popescul (2011) The Confidentiality – Integrity – Accessibility Triad into the Knowledge Security. A Reassessment from the Point of View of the Knowledge Contribution to Innovation, Proceedings of The 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage, Kuala Lumpur, Malaysia, Editor Khalid S. Soliman, ISBN: 978-0-9821489-5-2, Pp. 1338-1345.

[2] Andrea Bendovschi (2015) Cyber – attacks – Trends, patterns and security countermeasures, 7th International Conference on Financial Criminology, Wadham College, Oxford, United Kingdom. Procedia Economics and Finance, Elsevier Vol.28, Pp. 24 – 31.

[3] M.Uma, G.Padmavathi (2013) A survey on various cyber- attacks and their classification, Department of Computer Science, Avinashilingam Deemed University for Women, Coimbatore. International Journal of cyber security, Vol.15, No. 5, Pp. 390 – 396.

[4] P. Mary Jayanthi, A. Mansurali et.al (2020) Significance of Fraud analytics in Indian Banking sectors, Journal of critical reviews Vol. 7, No. 4.

[5] M. Bhasin (2007) Mitigating cyber threats to banking industry, The Chartered Accountant, Vol. 50 No.10. Pp. 1618 – 1624.

[6] M. L. Bhasin (2015) Menace of frauds in the Indian Banking Industry. An empirical study, SSRN Electronic Journal Vol.4 No.12, Pp.1-13, Banking & Insurance e-Journal, Malaysia.

[7] S.V. Ramana, G. Krishna (2017) A study on the impact of fraud in the Indian Banking sector. International Journal of Academic Research and Development, Vol.2 No. 6, Pp. 544, 547.

[8] S. Kundu, N. Rao (2014) Reasons of Banking Fraud – A case of Indian Public Sector Banks. International Journal of Information systems, Management Research and Development (IJISMRD), Vol. 4 No. 1, Pp. 11 – 24.

[9] M.J.Prem,M.Karnan (2014) Business Intelligence Hybrid Metaheuristics Techniques, International Journal of Business Intelligence Research (IJBIR) Vol.5 No.1, Pp. 64 – 70.

[10] J.K. Yego (2016) The impact of Fraud in the banking industry. A case of Standard Chartered Bank (Doctoral Dissertation). United States Internal University – Africa.

[11] L.K. Pani, S.Swain, S.Swain (2014) FDI in Indian Banks and foreign banks in India – Study of the recent changes and the implications, International Journal of Management IT and engineering, Vol. 4 No.3, Pp. 247 – 253.

[12] Aaron M. French (2012) A case study on E-Banking security- when security becomes too sophisticated for the user to access their information, Journal of Internet Banking and Commerce, Vol.17, No.2,South Korea.

[13] K. Tuma, G. Caliki, R. Scandariato (2018) Threat analysis of software systems: A systematic Literature review, Journal of Systems and Software, Volume 144, Elsevier Pages 175 – 294, Department of Computer Science and Engineering, University of Technology, Vasaparken Gothenburg, Sweden.

[14] M. Ashish, Shaji (2020) Cybersecurity in Digital Banking. Threats challenges and Solution, Finance Business, enterslice.com.

[15] A.Mustafa et.al (2019) E-Banking Fraud Detection: A Short Review, International Journal of Innovation, Creativity and Change, Vol.6, No.8, International Business School, University Technology Malaysia, Kuala Lumpur, Malaysia.

[16] M. Mannan, P.C.V.Oorchot (2008) Security and Usability: The Gap in Real – World Online Banking. Carleton University, Ottawa, Ontario, Canada.

[17] F.F. Council (2001) Authentication in an internet Banking Environment, Arlington: Federal Financial Institutions Examination Council.

[18] K. Eriksson, K. Kerem, D. Nilsson (2008) The adoption of commercial innovations in the former Central and Eastern European markets. The case of internet banking in Estonia. International Journal of Bank Marketing, Vol.26, No. 3, Pp. 154-69.

[19] Sayar, Ceren, Wolf Simon (2007) Internet banking market performance: Turkey versus the UK. International Journal of Bank Marketing, Vol. 25 No. 3, Pp.122-141.
[20] Amato-McCoy (2005) Creating virtual value, Bank Systems and Technology, Vol.1 No.22.
[21] E. Danial (1999) Provision of electronic Banking in UK and the republic of Ireland. International Journal of Bank Marketing, Vol.17 No. 2, Pp. 72-82.
[22] D. Chou and A.Y.Chou (2006) A Guide to the Internet Revolution in Banking. Information Systems Management, Vol. 17 No.2, Pp. 47-53.
[23] E. Garbarino, Strahilevitz, (2004), Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation, Journal of Business Research, Elsevier, Vol. 57 No.7, Pp.768-775.
[24] T.B. Joewono et al (2017), Influence of Personal Banking Behaviour on the Usage of the Electronic Card for Toll Road Payment, Transportation Research Procedia, Vol. 25, Pp. 4454-4471, Elsevier.