IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

Controlling Attacks and Intrusions on Internet Banking using Intrusion Detection System in Banks

Pritika Mehra

P.G. Department of Computer Science, Khalsa College for Women, Amritsar

Abstract: Internet usage has increased exponentially and has managed to cover all geographical areas across the world. Business-to-business (B2B), business-to-consumer (B2C), Internet-based e-commerce transactions, and Internet banking have come of age and are facing serious threats of attack, penetration or intrusion, despite the best available firewalls. Efficient and modern security tools are required to prevent information loss during internet banking and e-commerce transactions. One such tool that provides protective mechanism during internet based e-commerce transactions and banking is Intrusion Detection System. This paper discusses the types of attacks and how Intrusion Detection Systems can detect and prevent those attacks and intrusions during internet banking and other e-commerce based transactions.

Keywords: Intrusion, Intrusion detection system, Phishing, Pharming, MitM, MitB, Trojan horse virus, NIDS, HIDS.

I. INTRODUCTION

With the rapid growth of Internet, computer attacks and intrusions are increasing and can cause financial loss to an organization or an individual. The number of malicious applications targeting internet banking transactions has increased severely in recent years. This represents a challenge not only to the customers who use such facilities, but also to the banking institutions which offer them. Detection of intrusions and attacks is an important issue during internet banking and e-commerce transactions. Intrusion Detection Systems have been proposed as an efficient solution to protect online financial systems against intrusions and attacks.

II. TYPES OF ATTACKS AND INTRUSIONS

An attack can be defined as an intended or planned visit to the system by an uninvited visitor who sneaks and spoils or defaces the system or web site. Several types of electronic fraud specifically target internet banking. Some of the more popular types are described below:

A. Phishing attacks

Phishing attacks use fake email messages from an agency or individual pretending to represent one's bank or financial institution. The email asks to provide sensitive information (name, password, account number, and so forth) and provides links to a counterfeit web site. If one follow the link and provide the requested information, intruders can access personal account information and finances. In some cases, pop-up windows can appear in front of a copy of a genuine bank web site. The real web site address is displayed; however, any information one type directly into the pop-up will go to unauthorized users.

B. Pharming

Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. In pharming, larger numbers of computer users can be victimized because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim. In one form of pharming attack, code sent in an e-mail modifies local host files on a personal computer. The host files convert URLs into the number strings that the computer uses to access Web sites. A computer with a compromised host file will go to the fake Web site even if a user types in the correct Internet address or clicks on an affected bookmark entry.

C. Man-in-the-middle attack (MitM)

It allows the hacker to see or even to modify the communication between the client and the bank. The attacker needs to have a trojan horse virus on the victim computer

D. Man-in-the –browser attack (MitB)

A MitB attack is carried out by infecting a user browser with a browser addon, or plug-in that performs malicious actions. In principle, as soon as a user's machine is infected with malware, the attacker can do anything the user can, and can act on their behalf. If a user logs into their bank account while infected, the attacker can make any bank transfer that the user can. By the virtue of being invoked by the browser during Web surfing, that code can take over the session and perform malicious actions without the user's knowledge.

E. Spyware

Spyware is another way through which online banking credentials are stolen and used for fraudulent activities. Spyware works by capturing information either on the computer, or while it is transmitted between user's computer and websites. Often times, it is installed through fake "pop up" ads asking users to download software.

DOI 10.17148/IJARCCE.2015.41176

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

F. Viruses

Viruses are designed to compromise your computer systems, and allow others to gain access to your files, etc. This is different than spyware in that a virus may search for information considered to be of value, where spyware will wait for input or action from whomever is using the computer. A system that is compromised may be used to attack other systems, denying people legitimate access to services. These types of attacks are called "denial of service" attacks. One of the most common scenarios with viruses is where they will discover financial data such as payroll files, bank account information, and credit card information.

G. Keylogger Trojan attacks

These 'keyboard spying' programs will monitor activity on the victim's computer and wait for the user to connect to an actual banking website. As soon as the user accesses a banking website – that is on the Trojan's list of bank sites – the Trojan virus will start to capture the keystrokes that the user types on their keyboard. This enables the cybercriminal to steal data – including login, username, and password – which then enables the criminal to access the user's account and transfer funds.

III. INTRUSION DETECTION SYSTEM

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or forthcoming threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet during Internet Banking, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized.

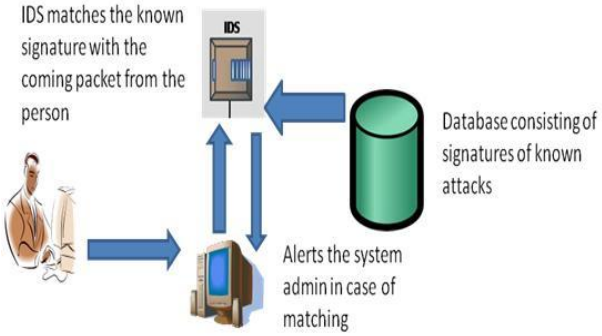
Intrusion Detection System (IDS) is a hardware or software or combinational system, with defensive-aggressive approach to protect information, systems and networks. It is usable on host, network and application levels. It analyzes the system or network traffic or controls the incoming connections to different ports, and then it detects the occurring attacks. It can detect known attacks, unusual traffic, harmful data, misuse and unauthorized access to the systems and networks by internal users or external intruders. It informs and notifies to the security manager by different types of warnings or notifications; sometimes, it disconnects the suspicious connections or blocks malicious traffic. In general, three main functionalities of IDSs include monitoring (evaluation), analyzing (detection) and responding (reporting) to the occurring attacks on computer systems and networks. IDSs use many methodologies to detect attacks.

A. IDS Classification based on Detection Method

IDSs can be classified into two types based on detection method.

a. Signature Based or Misuse Detection Method

Signature-based detection is the process of comparing signatures against observed events to identify possible attacks. In this method, IDS gathers the properties of attacks and abnormal behaviors and then, make database of them. Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a database of signatures using string comparison operations. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, detection software is only as good as the database of intrusion signatures that it uses to compare packets against.



b. Anomaly based Detection Method

An Anomaly-Based Intrusion Detection System is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature based systems which can only detect attacks for which a signature has previously been created.

B. IDS classification based on Architecture

IDS are classified into two types depending on information gathering source or input data supplier.

a. Network Intrusion Detection Systems(NIDS)

Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, works in a promiscuous mode, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

b. Host Intrusion Detection System (HIDS)

Host-based IDS systems consist of software agents installed on individual computers within the system. HIDS analyze the traffic to and from the specific computer on which the intrusion detection software is installed on. HIDS systems often provide features one can't get with network-based IDS. For example, HIDS are able to monitor activities that only an administrator should be able to implement. It is also able to monitor changes to key system files and any attempt to overwrite these files. Attempts to install Trojans or backdoors can also be monitored by a HIDS and stopped. These specific intrusion events are not always seen by a NIDS.

DOI 10.17148/IJARCCE.2015.41176

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 11, November 2015

C. IDS classification based on response method

Based on response method, IDS are classified into two types.

a. Passive System

In a passive system, the intrusion detection system (IDS) sensor detects a potential security breach, logs the information and signals an alert on the console or owner.

b. Reactive System

In a reactive system, also known as an intrusion prevention system (IPS), the IPS auto-responds to the suspicious activity by resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source.

IV. USING INTRUSION DETECTION SYSTEM IN INTERNET BANKING

Intrusion detection System offers security solutions that protect against Trojan viruses, phishing, pharming, Man-in-the-middle attack, Man-in-the-Browser attack, computer viruses, and other intrusions and attacks. IDS can be deployed in bank's servers and at crucial network points so that customer can benefit from more secure online banking.

V. CONCLUSION

With the growth in popularity of online banking services, the theft of banking information has become one of the most common types of criminal activity on the Internet. Internet banking continues to present challenges to financial security and personal privacy. This paper suggests using Intrusion Detection System in Internet Banking security infrastructure for increasing the security of Online banking transactions. The most important advantages of using IDS as security solution for banks is that they increase safety and reliability of Internet Banking services and decrease the damages of fraud events.

REFERENCES

[1] https://www.uscert.gov/sites/default/files/publications/Banking_Securely_Online07102006.pdf.
[2] http://www2.safenet-inc.com/email/2010/MITB2010/WhitePaper_Top-Threat-to-Financial-Service-Providers-in-2010_FINAL.pdf.
[3] Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131.
[4] Thomas Tjostheim and Vebjorn Moen; Vulnerabilities in Online Banks;European Committee for Banking Standards, Norway; 2003.
[5] Wang, Ke. "Anomalous Payload-Based Network Intrusion Detection". Recent Advances in Intrusion Detection. Springer Berlin. doi:10.1007/978-3-540-30143-1_11.
[6]http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf
[7]https://www.homefederal.com/news/article/common_threats_to_business_online_banking_security/
[8] http://usa.kaspersky.com/internet-securitycenter/ threats/online-banking-theft#.VPfrM_mUexU

DOI 10.17148/IJARCCE.2015.41176