Volume 5, No. 4, April 2014 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Strong Authentication for On-line Transactions

J.V.R.S. Sriharsha[1], S.S.Alekhya[1], M. Akkalakshmi[2]
Dept. of CSE[1], Dept. of CSE[2], Dept. of IT[2]
[1,2]GITAM University, Hyderabad

Abstract: On-line transactions are cost effective and convenient to customers. But this benefit is accompanied by diversified attacks by unscrupulous users. A Strong Authentication mechanism is essential before any on-line transactions is performed like online shopping, internet banking. Various authentication mechanisms are available and are in use for different situations. In this paper we are going to give a detailed description of various existing authentication techniques, attacks and their suitability to online transactions. Comparison of these techniques is made that helps in devising a strong authentication mechanism.

Keywords: Strong Authentication, Phishing, Man-in-the-Middle, OTP, session hijack.

I. INTRODUCTION

Many business organizations like banking sector, sales and purchases sector are adopting on-line transactions as it is easy, convenient to use and cut down the cost of business process. The first step in these transactions is to ensure the identity of user or customer. Due to lack of face-to-face interaction, fraudulent users are attempting to spoof the legitimate users by stealing personal information resulting in financial losses and attack on personal credentials of the user. Financial services industry has been the primary target of all the cyber attacks on a global scale.

Online transactions are convenient and easy to use alternative for the customer. Speed of transaction is very much faster than use of ATM or direct transaction. It does not involve the risk of handling heavy amount of cash physically. In addition to the benefits offered to the customers, it is also beneficial for organizations as large maintenance of staff and constructing large offices will not be there as everything will be taken care by the server intended for that. It has moved a step further allowing transactions using mobile devices.

In spite of so many benefits offered, it is faced with following challenges. The biggest problem is data security where anyone can grab our credentials like username and password and try to impersonate mostly for financial benefits. The attacks can be in the form of Phishing, Pharming, Man-in-the-Middle etc. The problem of spam is more in the online transactions where the user will get a mail to give his account details etc and the chances of getting attacked through them will be more. Sometimes, slow internet connections results in incomplete transactions. According to the popular review on kaspersky anti-virus, countries affected by online attacks are

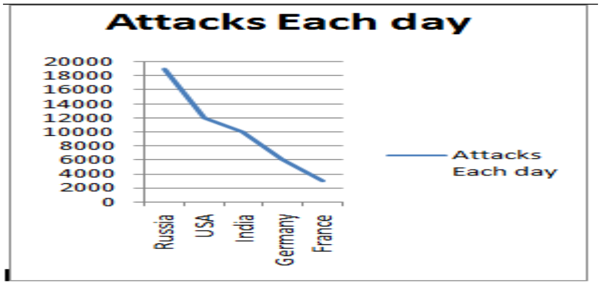

Figure: 1

The organizations that provide on-line transactions should also focus on ensuring the safety and protection of customer's personal information. Offering online services will cut down business cost, but it is effective only when it is accompanied by safety measures to gain customer trust and confidence. Security breaches will have far reaching impact not only on company's finance but to their reputation as well. It invites lawsuits, negative publicity, loss of sales and customer confidence. Without protection and security to their information, customers are less likely to use online services.

In addition to premier defence mechanisms like Firewalls, Intrusion detection systems, Anti-virus software, strong authentication mechanism is required to ensure the identity of users. According to ITRC (Identity Theft Resource Centre), a breach is an event in which an individual name plus Social Security Number (SSN), driver's license number, medical record or a financial record/credit/debit card is potentially put at risk – either in electronic or paper format.

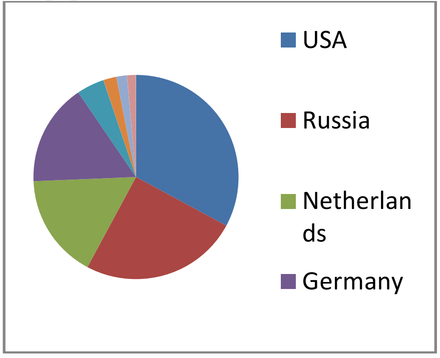

Figure: 2

II. POPULAR ATTACKS ON ON-LINE TRANSACTIONS

A. Identity theft/ phishing:-

In this attack [4], the imposter obtains key pieces of personal information like user Id, passwords, Social security number, credit card information, banking data and use it to commit fraud or crime. It is easy to do and happen especially when you least expect it. It is sometimes called as phishing.

The graph below explains the yearly statistics of the phishing attacks from the year 2010 to 2013

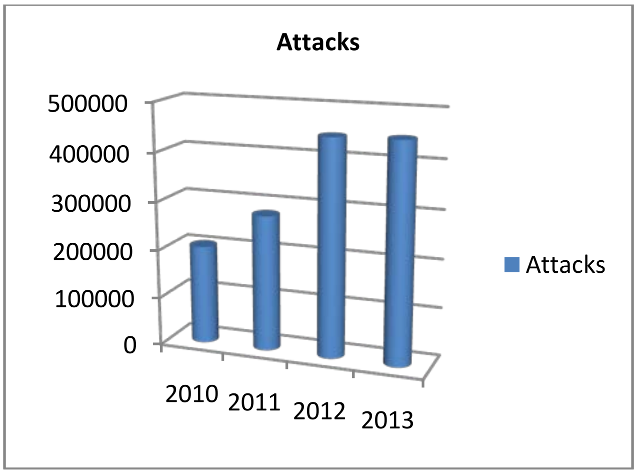

Figure: 2

Identity theft is categorized in two ways: true name and account takeover. In True name identity theft the thief uses personal information to open new account, establish cellular phone service or open a new checking account in order to obtain blank checks. Account takeover identity theft means the imposter uses personal information to gain access to the person's existing accounts and typically changes the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem. It can be easily performed as transactions can be made without any personal interaction.

According to the sources obtained from the kaspersky labs there is a total increase of 102,100 users all over the world in the year 2012-2013 which is just double the victims in 2011-2012. The table below will show us the number of people affected by phishing in those countries.

Table: 1

Country	2011-2012 (In millions)	2012-2013 (In millions)
Russia	4.47	6.98
United States	1.9	4.5
India	1.62	3.7
Germany	1.15	2.3
China	0.76	0.85
Vietnam	0.48	1.2
U.k	0.6	1.0
Ukraine	0.4	0.6
Italy	0.5	0.8
France	0.6	0.9

Simple measures to protect yourself from this threat are

a. Check the misspelling of you names, address in your credit reports
b. Avoid using public wireless access in airports, coffee shops etc
c. Dumpster-Diving is increasingly common occurrence hence destroy the papers containing sensitive information
d. Do not entertain people who claim to be bankers or from Govt agencies and communicate with you over phone or mails.

B. *Man-in-the-middle attack: -*

Man in the middle attack is defined as the attacks which occur when an attackers attempt to intercept communications between two nodes like sender and receiver in spite of their knowledge. For example when A wants to communicate with B and meanwhile C wants to intercept i.e C wants to send a false message to B. Firstly, A asks B for his public key if he sends to B meanwhile C is able to intercept the he sends a forged message to A that claims to be B but instead includes C public key. A thinks the public key to be B's, encrypts her message with C's key and send the enciphered message back to B. C again intercepts, deciphers the message using her private key, possibly alters it if she wants, and re-enciphers it using the public key B originally sent to A, when B receives the newly enciphered messages, he believes it came from A.

C. *Password database theft: -*

This is the process where the password will be stolen from the database where it is stored and the attacker will misuse our account with our password he got from the database. SQL injection attack is also the most possible one to steal the password from the database.

D. *Man in the browser attack: -*

In this attack the hacker will steal all the details of the users entered in the web browser and it will also modify the web pages and alter the transactions by including the additional transactions. We can state this as a proxy to Trojan horse. The man will breach through our user un-authorized and will take down all the important credentials that have been entered by the user like credit card numbers and bank account numbers for performing online transactions.

E. *Pharming: -*

It is the attack that will redirect the user from the website he is operating to the one created by the hacker. This technique was mostly targeted by the hackers on the personal computers of the users instead of the servers so that whatever the transaction that is being performed by the user will be redirected to the fraudulent website of the user and will grab all the credentials of the user. It can best be explained as the "Phishing without lure" . The attack that can be done by the is known as DNS poisoning where the DNS table will be modified where automatically it will be directed to the IP address of the website entered by the hacker in the DNS table which is going to be fraudulent.

III. FACTORS OF AUTHENTICATION

Three general factors used for Authentication are

a. Something a person 'has' like Key, swipe card, access card, badge, etc [5].
   But the things can be lost. It is commonly used to access facilities.
b. Something a person 'knows' like password, PIN, response to a challenge etc [5].

This is usually the least expensive to implement. User name coupled with reusable password is the most common form of system identification and authorization mechanisms. At the same time, Passwords are also considered one of the weakest security mechanisms available.

Common techniques used to attack passwords are

a) Attacker Listens to network traffic to capture users personal information especially when a user is sending her password to an authentication server. The password can be copied and reused by the attacker later called replay attack.

b) Password file on an authentication server is accessed to get Identity information of all the users. The file should be protected with access control mechanisms and encryption.

c) *Brute Force Attacks*: Performed with tools that cycle through many possible character, number and symbol combinations to uncover a password.

d) *Dictionary Attacks*: Files of thousands of words are used to compare to the user's password until a match is found.

e) *Social Engineering*: An attacker falsely convinces an individual that she has the necessary authorization to access specific resources.

If passwords are properly generated, updated, and kept secret, they can provide effective security. Some simple techniques to make it effective are

i. If users can choose their own passwords, then the operating system should enforce certain password requirements.

ii. An audit trail can also be used to track password usage and successful and unsuccessful login attempts.

iii. A password's lifetime should be short but practical. Forcing a user to change passwords on a more frequent basis provides more assurance that the password will not be guessed.

(a). OTP One time password [1], [6] – it consists of generating a different password that is only valid for one session or transaction, and it is also referred as dynamic authentication. This password can be event-based, time-based or challenge-response based. OTP can be communicated to the user using SMS, Hardware Token, and Software Token etc.

(b). Something a person is – it is based on a physical attribute called *Biometrics* [5].

Biometrics is the most expensive method of verifying a person's identity. Popular biometrics used are

i. Fingerprint – common in most of the organizations for attendance

ii. Iris Scan - Scans uniqueness in the characteristics of in individual's iris. Used by Govt agencies as voter identity. But user needs to be aware of proper placement of optical unit for scan.

Other biometrics includes, Palm Scan, Hand Geometry, Retina Scan, Signature Dynamics, Keyboard Dynamics, Voice Print, Facial Scan, and Hand Topography.

Biometric systems accuracy is measured by false rejection rate, false acceptance rate, Crossover Error Rate. Biometrics faces hurdles to common use that includes user acceptance, enrollment timeframe and throughput.

Using a single factor for authentication is simple to break. A combination of two or more factors will provide multiple levels of protection and more difficulty to compromise called Strong Authentication. For example

i. Combination of Swipe Card and PIN number. Used in Banking, Sales & Purchases

ii. combination of Id card and Iris scan used in Voter Identity

iii. Finger print & password for employees attendance in companies

Higher the security required, greater the cost and user inconvenience. It is all the more critical when using mobile devices. As per the ITRC report, major categories of data loss methods are when data is on move.

Any technique chosen should be in accordance with industry & govt regulations and user acceptance.

IV. COMPARISON OF AUTHENTICATION TECHNIQUES

Table: 1

Authentication Technique	Uses	Advantages	Limitations
Username	For creating an id to the user	He cannot forget the identification of his account	The username can only be used for only once and it cannot be used by other in the database
Password	A security measure for the user account	Ensures security for protecting the account	Can be risky if the password is being stolen or known to the attacker.
Two factor authentication	TFA as stated in paper [2],[4] was used as an authentication technique in banking where we can take an ATM as the best example which comprises of both username, passwords and hardware security token	-It provides security by establishing two independent types of information. -It reduces the risk raised by weak user passwords which can easily be cracked. -It reduces the time administrators by providing a strong authentication which is simple, secured and automated.	-The two factor authentication comprises the use of a third party authentication service. -The administrator configures user names, assigns token and manages authenticated related tasks. -Tokens are given to the administrator gives the user to display temporary token codes
Phone Based Authentication	Used as an authentication technique in cloud computing[3] as well as in banking transactions where we can send OTP to the user mobile phone through SMS or Call	-It comprises of software that is to be installed in the mobile and it generates an OTP every time the user asks. -The Administrator will send an SMS to the user mobile every time the user logs into his account.	-The end user who is using the phone must be in a position to use the software that is deployed on phone and the staff who is designing it must be trained well in order to reach it clearly and works efficiently for end user. -The user must wait after he entered the username and the pin to occur in the form of sms and it will be inconsistent as it will get suffered from network delays at peek time.

Multi Factor Authentication	It is a security approach which requires more than one form of verification of a person in order to prove their identity and allow to access the system	Multi factor authentication involves three major factors which include verification of the information which the user 'knows' like password, information which the user 'has' like smart card, security token, and the information which the user 'is' like biometrics	It also consists of simple device identification. Simple identification device is the device which can easily replicated by the fraudster, such as identifying IP address.
One Time Password (OTP)	Used in banking as well as in cloud computing[6]	These are the passwords that were valid for only one transaction and once the login was completed then it will not be used for the next time. We can avoid replay attacks by using this technique	The main disadvantage of this technique rather than static passwords is that they were difficult to remember for a user every time, the remedy for this problem is using some randomized mathematical algorithms.
Tokens	Used in Online banking and cloud computing and also as gateway passes[3]	-Token is a hardware object that ensures security to the user to say that he is the authenticated person in performing that service. -The object may be anything such as smart card or a key fob. -Along with the security tokens there is also a personal identification number (PIN) associated	If the token was lost then there is a problem of misuse of the Token by some un-authorized user. The Randomized algorithms used in the token may sometimes be known to the user which results in manufacturing of duplicates.
Static Tokens	Used for logging into account	The static password tokens comprises of a password for authenticating the user each time when he logs in he must type the password in order to perform the authentication process.	-If the attacker steals the password and if the user has not noticed it then the attacker will grab all the confidential data. -It will come to User notice only after the loss has been occurred.
Dynamic Tokens	Used for generating OTP	The main thesis behind these tokens were to provide the password each time the user logs in and the password usually changes every time the user logs in	How the password will be generated is a big issue over her. Because if the generated password is through mobile then the user
Asynchronous Password Tokens	Generating Password	Same as the dynamic password tokens but doesn't have any time interval for generating the password. It will generate at a regular time interval and the time interval may vary	As there is no particular time for generating the password the chances of man-in-middle attacks are very high.
Challenge Response Tokens	Generates challenging questions where every user must answer	The user will send the challenge to the system and the system will generate a challenge response. The user will then generate the response to the system and the authentication will be proved	If the user forgets to answer the question or if the attacker randomly answers the users question then the system will authenticate the attacker assuming that he is the authenticated user.

V. CONCLUSION

This paper gave a detailed survey of various challenges and threats faced by on-line transactions. It also gives various existing techniques and its suitability to on-line transactions. A comparison of these techniques helps in devising a strong mechanism for various applications.

VI. REFERENCES

[1] SANS Institute Info Sec Reading Room "An Overview of Different Authentication Methods and Protocols" a White paper.

[2] Andrew Kemshall, Phil Underwood "Options for Two Factor Authentication" White paper

[3] Christopher Mallow "Authentication Methods and Techniques" White paper

[4] Cryptomathic White paper on "Two-Factor Authentication for Banking" .

[5] Federal Financial Institutions Examination Council "Authentica tion in an Internet Banking Environment " White paper

[6] Maninder Singh, Sarbjeet Singh "Design and Implementation of Multi-tier Authentication Scheme in Cloud" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 201

[7] Wassim Itani, Ayman Kayssi, Ali Chehab "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures" 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[8] Jaejung Kim, Seng-phil Hong " A Consolidated Authentication Model in Cloud Computing Environments" International