ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

Review: Location Based Authentication to Mitigate Intruder Attack

Dr. A.L.N Rao, Silky Puri, Shalini Rana
Professor, Department of CS/IT, Amity University, Noida, India,
Department of Information Technology, Amity University, Noida, India
Department of Information Technology, Amity University, Noida, India

Abstract — Recently the use of online banking has been increased to perform various online banking transactions. On the other hand, it is been targeted by various attacks found at the client side. Lately, traditional security methods were not capable enough to tackle these attacks such as intruder attacks, phishing attacks, etc. Presently remote authentication is the most efficient technique used to protect various services, resources, security for the unauthorized use. In this paper we use three-factor authentication and upgrade this method by including the fourth factor. The main three factors are (a) password (b) smart-card, and (c) biometrics. The newly introduced fourth factor is "Where you are" (Location), which mainly consist of REAL TIME LOCATING SYSTEM technique and instant generated pin code mechanism for the verification of the user performing the transaction.

***Index Terms* — Authentication, security, password, biometrics, smart-card, intruder, RTLS.**

I. INTRODUCTION

In today scenario, online baking is getting more prone to unauthorized attacks in many ways. Among these attacks, the most popular threat is the INTRUDER attacks. An intruder attack has been architectured to get hold of the data as it passes over a secure communication link between a client and an online application. Once Trojan is activated it can stop and manipulate any type of information that a client pass-on in real time. These Trojans are responsible for hijacking the session which means to pervert an authorized user active session.

Various authentication methods are used to identify the identity of a client. Presently main three authentication factors used are:

1) What you have i.e. smart-card
2) What you know i.e. password
3) What you are i.e. biometrics

The first-factor authentication is human generated password which was easily memorable and could be predicted by the attacker. This eventually makes all the information available to the hijacker, thus compromising the user security. This limitation leads to the two-factor authentication which included a "smart-card" security in addition to a valid password. But later on, the intruders were successfully able to retrieve and store the data in the smart-card and the password. Another limitation of this authentication factor is that the smart-card can easily be lost or stolen. Due to which the third factor authentication came into existence. This authentication mechanism is biometrics, where users are identified by their unique human characteristics, such as fingerprint, voice and scanning of eyes. These characteristics are proved to be a reliable authentication factor because they are a source of high-entropy based information and this cannot be easily lost or forgotten.

Instead of all these advantages there are some loop holes in this technique, as its characteristics could be easily obtained without the consent of the user. The final authentication factor which overcomes the limitation of these three factors is "Where You Are". While location has been previously been suggested for localized access control and authentication systems [1]–[3].Location traced by accurate RTLS has several features such as system can provide contiguous and smooth tracking of target location. Thus main advantage of this authentication system is that it provides an attacker to initially gain physical access so that an attacker can perform a cyber attack.

II. INTRUDER ATTACK

This part of our paper includes all the details about the Intruder attacks and how this attack is performed.

There are various protocols which have already been implemented to mitigate this attack. These protocols are:

Secure Socket Layer (SSL)
Transport Layer Security (TLS)

The Trojans which are responsible for these attacks are Zeus/Spy Eye, URLzone, Silent Banker and Gozi [4].These Trojans are used to get access of data transferred between a user and a browser and can also manipulate it. The basic flow of Intruder attack is as follows:

1. Firstly, the user login for online transaction and gets infected with a Trojan which is responsible for initiating an Intruder attack.
2. The Trojan then triggers into action and perform its Intruder functionality.
3. The user continues with its usual online transaction process including authentication process (two-factor or three-factor). During this whole process the Trojan waits silently in background for user's successful login.
4. The Trojan then manipulates the details of the transaction by the user such as the amount transferred, the destination of the transaction etc.
5. After performing these manipulations the Trojan then display false information and fake pages to the user, so that user remains unaware of the changes and it considers that details as the original.

The Intruder attack has the following chronology:

1. Firstly, the targeted browser of the user is infected by the vicious browser extension. This vicious gets entry in the browser and remain there until the user

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

visit various websites based on electronic commerce.

2. When this vicious extension discover details related to transaction while scanning through the user's history it records the information which user enters such as login details. These details could also be later on be manipulated by the vicious extension without the consent of the user.
3. For example, suppose a user wants to perform an online transaction of Rs.100 to bank account A. The vicious extension manipulates the amount information mentioned by the original user to Rs.1000 and it also changes the destination bank account to B. The server will not be able to discover the difference between the original details and the changed details because the information comes from a valid user and the IP address are also the same.

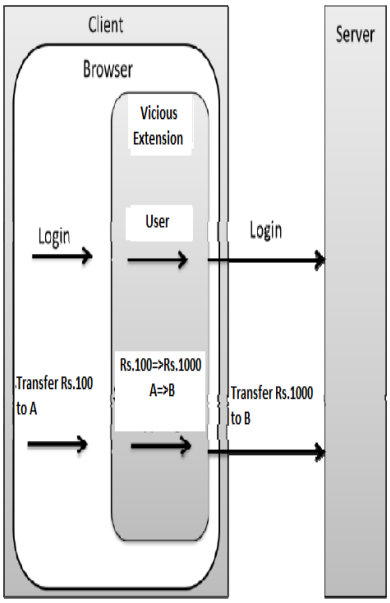

Fig 1: Intruder Attacks. [6]

A. Attestation Based On the Trusted Platform Module

When dealing with online transactions such as electronic commerce and online banking the relationship between communicating machines has been an important factor which is responsible for user reliability. For example, users may confirm that during their transaction they are interacting with the valid merchants and vice versa. In order to overcome this problem we have considered the Trusted Platform Module (TPM) because of its potential of providing attestation which is based on the information regarding the platform and also can ensure the integrity of the platform is not tampered [5].The Attestation Identity Key (AIK) is used to ensure the validity of the integrity measurement for TPM, by signing the integrity measurement. This asymmetric key has been derived from the unique Endorsement Key (EK), which is manufacturer certified and can identify the TPM identity [6]

Fig2. Describes the process of remote attestation where a client initiates the attestation process by sending a request for the service to the host. In respond to which the host will send back a challenge respond. The client will then check its integrity information which is then stored in a non-volatile memory in the TPM known as Platform Configuration Register (PCR) [7], [8]. On the basis of this stored information the client sends an integrity report to the host for verification. After this the host permits its services to access by the client as soon as the client's platform integrity has been verified.

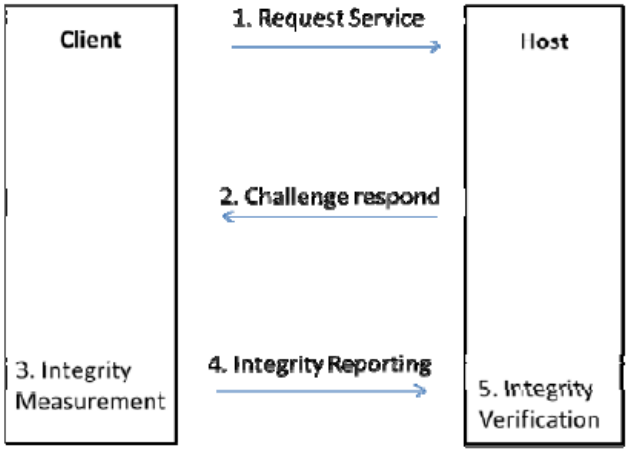

Fig 2: Remote Attestation. [6]

III. THREE - FACTOR AUTHENTICATION

Due to some limitations in two-factor authentication the third factor has been included. The three-factor authentication includes password, smart-card and biometrics. Several authentication protocols have been introduced to incorporate biometrics in the password and smart-card authentication. Lee [9] proposed an authentication system which does not require any password database to authenticate already registered users. Whereas, allotted smart-card and fingerprints are only required. Later on, it was discovered that this analysis technique is not secure under conspiring attack.

Lin and Lai [10] proposed that Lee's technique is also prone to intruder attack. This term signifies that a registered user has an option to make a successful login on behalf of another registered user. To overcome this problem Lin and Lai proposed an improved authentication protocol which had other sort of security issues.

In [11], Kim introduced a new authentication technique based on two ID-based passwords which was later on reviewed by Scott. He showed that an intruder can successfully break-in by logging onto the server claiming any registered user identity after passively eavesdropping only one valid login. Fan and Lin [12] introduced a three-factor authentication scheme which further increases the level of security on biometrics. The approach under this scheme is as follows:

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

(1) When a user sign-up on to the server for the first time, it chooses a random string of its own choice and encrypts its details using his/her biometric template.
(2) This encrypted information known as sketch is further stored on the user's smart –card; and
(3) Whenever this user login again on the server he must try to convince the server by decrypting the already stored sketch, giving correct biometric template.

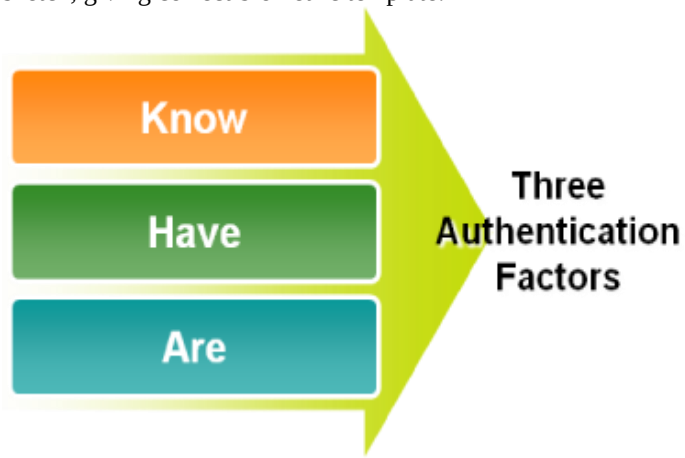

Fig 3: Three Factors used during Authentication

IV. LIMITATIONS OF THREE - FACTOR AUTHENTICATION

1) The password based authentication is used for providing countenance and for providing the authorization. But still it suffers from many limitations related to security and utility. The basic limitation related to the password is that the user always creates their passwords in such a way that can easily become memorable, hence due to which the complexity of the password reduces. The users always prefer to choose string of short characters which leads to low entropy and thus easier to crack by the attackers. When the client solely depends on password authentication for security, he/she may become a victim of password guessing technique and spear phishing.
2) The second authentication factor based on smart-card, which an item belonging to the user technically is referred to as "token". This token act as an identity proof of the user carrying unique photo identification or a unique id. This technique enforces the user to always carry this token physically whenever an transaction is performed. The most frequent drawback related to this authentication factor is that the item can be lost or easily stolen which compromises the security issues.
3) The final authentication factor which uses Biometrics further has some vulnerability. The server which are used to compare the stored biometric data and compare it with the current input data are not 100% secure and trusted. As while taking the input data natural features such as noise distraction may not produce accurate result. One another issue related to this authentication factor is that the review process should be done by the server instead of remotely located devices.

Unlike password which can be easily renewed or revoked, biometric data once compromised either disclosed accidently or compromised by the user itself cannot be re-issued easily. The biometric features are further divided into two parts:
(1)Physical characteristics: fingerprints, iris scan etc.
(2)Behavioral Patterns
These factors vary with time, and hence lead to various vulnerabilities, spoofing and natural or accidental variations.

Fig 4: Biometric-Authentication

V. ENABLING FOURTH-FACTOR AUTHENTICATION

To overcome the above mentioned limitations observed in three-factor authentication, "Where You Are" (location) is proposed as a fourth authentication factor which further increased the level of security for the clients performing online transaction. This authentication can also be implemented in banking transactions performed through ATM's. This method can not only validate the user's identity but can also trace its location of transaction using "Real Time Locating Systems" (RTLSs). RTLS Systems use tags attached to people or objects, which can function as recipients and senders of location information used to determine the location of the tracked object [13].

Today, various RTLS vendors and products enable to track devices and people that form the foundation of forth factor authentication. Local positioning system is one of the basic applications of RTLS which is used to track the current and precise location of objects or people in real time. This technique has been classified under four physical phenomena: (1) electromagnetic waves; (2) sound waves; (3) the Earth's magnetic waves; and (4) IMU-based measurement of velocity, orientation, and gravitational force. Further this technique is distributed using two different methods: self-positioning and infrastructure-based positioning. In self-positioning system the targeted object is itself responsible for collecting all the location related information from the surroundings or the location infrastructure. Whereas in infrastructure positioning system, the infrastructure is responsible for sensing the mobile target and provide all the relevant information required for the estimation of targeted location.

The three factors that govern the RTLS usage are listed below [14]:

(1)Unless required by established security policies or safety rules, authentication may not obstruct operational tasks at hand.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 9, March 2013

(2)Unless it violates the first rule, the integrity of authenticated data must be persistent and available throughout the authenticated state.
(3)Authentication may not violate the loss of physics:
a. A person cannot be in two different places at once;
b. There is a limit to how fast a person can move through space and time;
c. A person's identity may not be interchanged.

VI. CONCLUSION

This paper focuses on several prominent issues of three-factor authentication and makes a step forward to overcome its limitations. This is done by implementing the "Where You Are" as the fourth factor. This technique includes real time locating system techniques which helps in tracking the current location of object. Hence increases the level of security at client side.

REFERENCES

[1] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing, vol. 2802, pp. 201–212, 2004.

[2] A. Juels, "Rfid security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[3] M. Safkhani, N. Bagheri, and M. Naderi, "Vulnerabilities in a new rfid access control protocol," in Proc. of International Conference for Internet Technology and Secured Transactions (ICITST), 2011.

[4] RSA Lab, "Making Sense of Intruder Attacks" http://viewer.media.bitpipe.com/1039183786_34/1295277188_16/INTRUDER _WP_0510-RSA.pdf.

[5] A. Sadeghi, "Trusted Computing – Special aspects and challenges" SOFSEM 2008. LNCS, vol. 4910, pp. 98—117, 2008.

[6] Fazli Bin Mat Nor, Kamarularifin Abd Jalil and Jamalul-lail Ab Manan,"An Enhanced Remote Authentication Scheme to Mitigate Intruder Attacks", Cyber Security, Cyber Warfare and Digital Forensic(CyberSec), 2012 International Conference, 26-28 June 2012.

[7] S. Kinney, "Trusted Platform Module Basics: Using TPM in Embedded System", NEWNES, 2006.

[8] D. Challener, K. Yoder, R. Catherman, D. Safford, L.V. Doorn, "A Practical Guide to Trusted Computing", IBM Press, 2008.

[9] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-Based Remote User Authentication Scheme Using Smart Cards," Electron. Lett., vol.38,no.12, pp. 554-555,Jun. 2002.

[10] C.H. Lin and Y.Y.Lai, "A Flexible Biometrics Remote User Authentication Scheme," Comput. Standards Interfaces, vol. 27,no.1, pp. 19-23, Nov.2004.

[11] H.S. Kim, J.K. Lee, and K.Y. Yoo, "ID-based Password Authentication Scheme Using Smart Cards and Fingerprints," ACM SIGOPS Operating Syst. Rev., vol. 37, no. 4, pp. 32-41, Oct. 2003.

[12] C-I. Fan and Y-H. Lin, "Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics," IEEE Trans.Inf.Forensics Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.

[13] ISO/IEC 19762-5, International Organization for Standardization Std.

[14] Sung Choi and David Zage, "Addressing Insider Threat using "Where You Are"as Fourth Factor Authentication", Security Technology (ICCST), 2012 IEEE International Carnahan Conference, 15-18 Oct. 2012.

AUTHOR BIOGRAPHY

Dr. A.L.N Rao did his B-Tech, M-Tech, Ph.D in Computer Science & Engineering. He is having 15 years of teaching experience in India & Abroad. At present he is working as a Professor in IT department and Incharge, Research: Projects & Patents at Amity University, Noida – India. He has published his research Papers in Various National and Inter National Journals.

Silky Puri born in 1990.She has done her bachelors from Punjab Technical University, Jalandhar in year 2012. Now currently pursuing M.Tech in Information Technology from Amity University, Noida, India.

Shalini Rana born in 1990.She has done her bachelors from Rajiv Gandhi Proudyogiki Vishwavidyalaya University, Gwalior in year 2012. Now currently pursuing M.Tech in Information Technology from Amity University, Noida, India.