Effectiveness of Two Factor Authentication for Preventing Fraudulent Transactions During Session Hıjacking Attacks on Online Business

Şen ÇAKIR, Fatih UÇAR

Abstract—**Session hijacking is an important bottle-neck on online business; especially internet banking suffers fraudulent transactions. Two factor authentication provides much stronger authentication than simply username and password authentication. One of the most popular two factor authentication involves hardware tokens that enable constantly changing session strings at set intervals. In this method to authenticate users, a password presented and used with these constantly changing strings. However, Sophisticated attacks can steal session id even within the shortest window opportunity. But besides authenticating session, if the transaction is authenticated before it is completed with one time password, the hijacker can be thwarted. The success of the two factor authentication depends on encryption strategies and application logic. We discuss the effectiveness of two factor authentication for preventing fraudulent transactions during session hijacking attacks on online business.**

Index Terms—**Fraud, Session Hijacking, Two Factor Authentication.**

I. INTRODUCTION

The main cause of fraudulent credit card transactions on online business is “identity theft”. Identity theft is the wrongful taking of someone else’s “real world” identity for the purpose of committing fraud. Typically the thief gets their hands on enough information to pretend to be someone else. Unlike ones fingerprints, which are unique to him or her and cannot be given to someone else for their use, one’s personal data especially his or her Social Security number, bank account or credit card number, phone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at his or her expense [1].Fraudsters use techniques like phishing attack, session hijacking, spoofing for identity theft. Internet users’ identity is mainly stolen from unsecure web services on the internet.

There are three categories of identity: (1) attributed identity – includes ones parents’ names and his or her place of birth; (2) biographical identity – includes ones interactions with society as recorded in public and private databases; and (3) biometric identity – includes ones unique physical characteristics such as fingerprints, voiceprints, iris pattern and facial geometry [2].

To combat identity theft fraud, products are being developed to provide identity authentication. One such recent product is named URU, an automated, on-line identity-verification service for organizations that need to check that their customers are who they say they are and live where they claim to live theft…. URU utilizes the voiceprints biometric. The advantage of voiceprints is that they can be remotely registered, verified over a phone, and a low-cost alternative [3].

Another application of biometrics is facial recognition. Until recently, the cost of this technology frequently outweighed the benefits. However, the combination of increased portability and affordability of hardware have contributed towards making face recognition a viable identity authentication method. Relatively inexpensive miniature cameras, coupled with neural network technology, can now be deployed in corporate environments to replace the familiar user ID/password authentication method to access systems [4].

II. CONTEXT

In this document we proposed examine the effectiveness of two factor authentication for preventing fraudulent transactions during session hijack attacks on the internet applications. We used the methodology, developing strategies for preventing session hijack attack with the use of hardware tokens.

III. SESSION HIJACKING

Session hijacking is defined as stealing the users’ session to get authenticated. Session Hijack Attacks generally fall into three categories, Man in the Middle, Blind Hijack, Session theft…In a session theft attack, the attacker neither intercepts nor injects data into existing communications between two hosts. Instead, the attacker creates new sessions or uses old ones. This type of session hijacking is most common at the application level, especially Web applications [5]. In this work we will deal mostly with web application side session attacks.

Şen ÇAKIR, Department of Computer Engineering, Dokuz Eylül University *Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği Bölümü, Tınatepe Kampüsü İZMİR,sen@cs.deu.edu.tr*
Fatih UÇAR, R&D Department, Postglobal Ltd.Şti. Anafartalar Mah. Arabacı Sok. No:7 Manisa, *fatihu@postglobal.com*

There are three techniques hijacking sessions on web applications:

Brute force - the attacker tries multiple IDs until successful.

Calculate - in many cases, IDs are generated in a non-random manner and can be calculated.

Steal - using different types of techniques, the attacker can acquire the Session ID [6].

Some techniques can be used to prevent this attacks. One method is the use of long random number or session key. This reduces the risk of guessing session key during brute force attacks. Another method is regenerating session id after successful login. The attacker doesn't know the session id because it is changed after login. Some services check the request IP with previous one whether it is changed between requests. This method doesn't prevent attacks, if attacker is in the same local area network with the legitimate user. It may be better way to store and check a hash value. Another method is to change the value with each and every request. This will reduce the time interval in which the attacker can operate. This method can make management of web application harder e.g. browser back button must be disabled.

IV. TWO FACTOR AUTHENTICATION

There are three universally factors of authentication:

- "Something you know"

- "Something you have"

- "Something you are"

Two factor authentication means leveraging at least two of the authentication methods mentioned above. The most popular two factor authentication implementations use "Something you know" and "Something you have" factors together. We used secure dongle as hardware key for the factor "Something we have" and PIN for the factor "Something we know" to implement two factor authentication.

V. USE OF HARDWARE TOKEN FOR TWO FACTOR AUTHENTICATION

The use of hardware tokens for two factor authentication is very popular especially internet banking against fraudulent transactions. As a simple solution the use of USB interfaced secure dongles is very popular. The system works as follows: When the user needs to log into a server, the server sends a random based request. The user must connect the USB-dongle and to type in a personal PIN code. The server request, the users PIN and some kind of other data blocks will be encrypted inside of the secure dongle. The encrypted result token is then send back to the server. Sensitive information such as encryption key is stored safely in the dongle and on the server. Only users who have the valid dongle and the corresponding PIN code will be allowed to log into the server application/web site. Figure 1 shows the state diagram of authentication to web application. Figure 2 shows the state diagram of credit card payment.

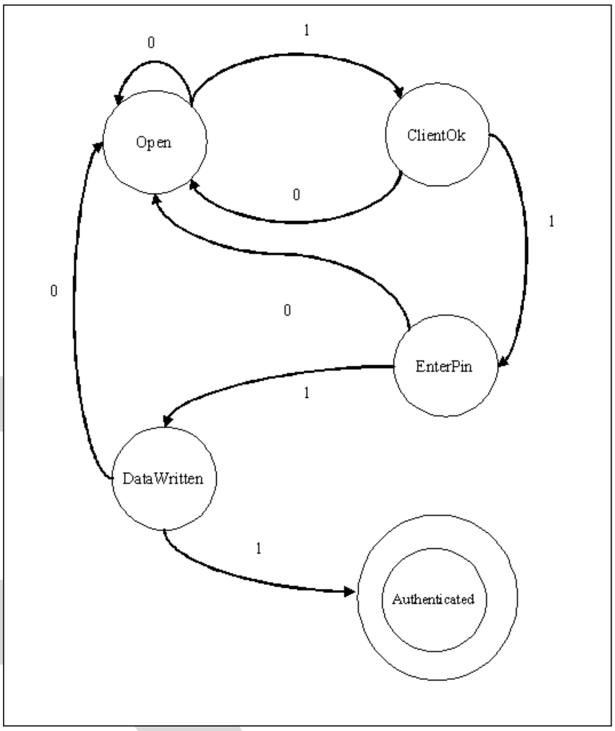

Figure1: Authentication on web application using hardware token

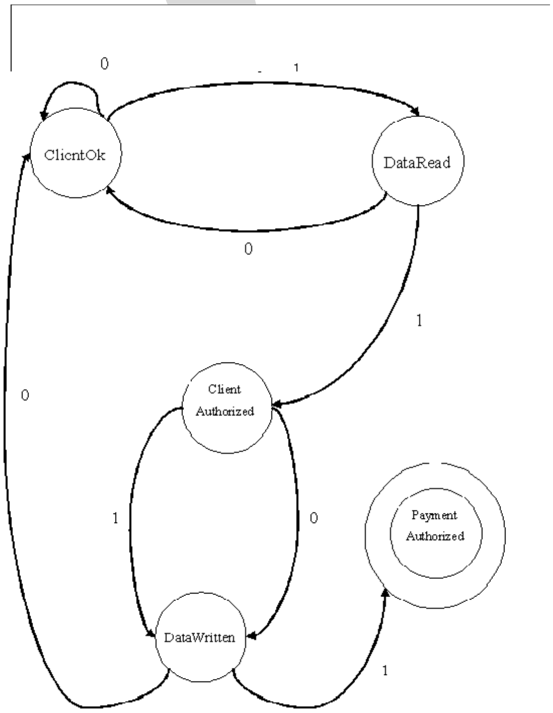

Figure2: Credit card payment using hardware token authentication

VI. INTEGRATION WITH SSL BASED SECURITY

The exchange of information between client and servers in a secure way based on encryption is confidentiality of data. Integrity function is holding the data elements original as transferred from sender. SSL can provides confidentiality and integrity of data itself. But doesn't provide client's strong authentication. Simply a Trojan on clients' computer can make a fraudulent transaction inside SSL encrypted session. Using hardware token authentication before the transaction, can prevent session hijacker to guess session token within the specified time interval.

VII. CONCLUSION

Two factor authentication is a better solution than simple user and password authentication. It can be also a way preventing session hijacking attacks. As opposite to opinion "Use of Secure ID card, or other token based secondary authentication is useless as protection against hijacking, as the attacker can simply wait until after the user authenticates, then hijack the session." [7] , we offer transaction authentication after session authentication. Sadly, a phishing attempt in 2006 against Citibank contained a field for the entry of a two-factor authentication token value. The window of opportunity (when the value on the token was known to the user) was a mere 60 seconds [8]. This shows there is still threat to online web applications even with the use of two factor authentication.

VIII. REFERENCES

[1] B. Ranjit, "Intelligent Technologies for Managing Fraud and Identity Theft", Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), 2006, pp 1

[2] B. Ranjit, Intelligent Technologies for Managing Fraud and Identity Theft, Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), 2006, pp 4

[3] C.J. Gahan, "URU – Online Identity Verification," BT

[4] Technology Journal, Vol. 22, No. 1, January 2004, pp. 43-51.

[5] Y. Gao, S.C. Hui, and A.C.M. Fong, "A Multiview Facial Analysis Technique for Identity Authentication," Pervasive Computing, January-March 2003, pp. 38-45.

[6] K. Lam, D. LeBlanc, and B. Smith, "Theft On The Web: Prevent Session Hijacking", Microsoft TechNet Magazine, January 2005.

[7] Ananonymous, "Session Hijacking" http://www.imperva.com/application_defense_center/glossary/session_hijacking.html.

[8] D. Dittrich, "Anatomy of a Hijack", http://staff.washington.edu/dittrich/talks/qsm-sec/script.html, April 1999.

[9] Z. Ramazan, "Phishing and Two-Factor Authentication", http://www.symantec.com/enterprise/security_response/weblog/2006/07/phishing_and_twofactor_authent.html, July 2006.