Computer Science and Engineering 2012, 2(6): 92-97
DOI: 10.5923/j.computer.20120206.02

Secure Web Financial Transaction Methods and Smart Authentication with a Focus on Mobile Devices

Basant Kumar

Department of Computer Science MCBS, Muscat,Sultanate of Oman

Abstract In the preceding few years, new form of security threats has appeared to alter the confidential data between the user and the navigation program's security mechanism. Man-In-The-Browser ("MITB") and Man-In-The-Middle ("MITM") are new form of Internet intimidations, typically a Trojan horse program; interpolate itself between the user and the navigation program like Internet Explorer or Firefox. They take over user access to the bank's web site despite of the sound and emphatic authentication method. In the current scenario of security threats extra up-to-the-minute protections are required to avoid security breach of financial data transaction on web. These attacks emphasize the need for financial organizations to securely authenticate users and ensure the integrity of web transactions in the face of a growing threat environment. In this paper we analyze the "Man In the Browser" and "Man In the Middle" attacks and propose a solution based upon Digitally signing a transaction and using the mobile phones as a software token for Digital Signature code generation which pioneers an avenue of carrying out secure authentication from a mobile device to verify an authentic user to carry out financial transactions in a secure way on the WWW.

Keywords MITB, MITM, Digital Signature, WWW, Trojan Horse Program

1. Introduction

The first social engineering technique has been used as Phishing in which potential victims are convinced to provide their confidential information, such as usernames, passwords, and bank account details. In the current scenario there are some different spying techniques used to track the user's banking information claimed by Ståhlberg[8], such as screenshot and video capture, code injection of fraudulent pages or form fields, redirecting website, and keystroke logging.

Consequently, a newer and more perilous facet to phishing technology such as a Trojan horse has been confined. Man in the browser is also called a proxy Trojan or a password pinching Trojan[9] throws in itself between the user and the navigation program's safety mechanism. Both Firefox and Internet Explorer has been the target of successfully MITB attacks[1].Consequently, an MITB attacks can intrude verification, modify web assembly, and begin fake web transactions. In the similar fashion Man-In-The-Middle ("MITM") intrude can alter web transaction of the customer or create new web transactions; phishing deviates the customer to counterfeit server that integrates the connection[2]. Strong authentication to protect against all types of identity theft and fraud, additional safeguards and transaction verification, are required. Transaction verification provides a means to confirm as legitimate those transactions that transaction anomaly detection has identified as risky.

Transaction authentication using a digital signature derived from public- key infrastructure (PKI)[3] credentials (with or without smart tokens) is vulnerable to Trojan attacks on Windows-PCs, unless implemented with stand-alone tokens or handheld device(Mobile Phone) using universal Two-Factor authentication[5].

In this paper we take a brief look into how the MITB and MITM attack take place? How it is capable of modifying an online transaction? We propose a solution based on using mobile phones as software token for Digital Signature code generation. Digital Signature is known to ensure the authenticity and integrity of a transaction.

Mobile-commerce, also known as the next generation e-commerce, can be defined as any electronic transaction or interaction conducted using a mobile device such as a mobile phone or personal digital assistant (PDA)[4]. The fact that our mobile devices are always with us and rarely turned off makes m-commerce an attractive field for businesses.

Thus we can use the mobile phone as software token to generate Digital Signature code.

2. Man in the Browser Attack Scenario

A new threat is emerging that attacks browsers by means of Trojan horses. The new breed of new Trojan horses can

* Corresponding author:
basant.info@gmail.com (Basant Kumar)
Published online at http://journal.sapub.org/computer
Copyright © 2012 Scientific & Academic Publishing. All Rights Reserved

modify the transactions on-the-fly, as they are formed in browsers, and still display the user's intended transaction to her. Structurally they are a man-in-the-middle attack between the user and the security mechanisms of the browser.

Distinct from Phishing attacks which rely upon similar but fraudulent websites, these new attacks cannot be detected by the user at all, as they are using real services, the user is correctly logged-in as normal, and there is no difference to be seen.

It combines the use of phishing approaches with a Trojan horse technology, inserted into a customer's browser, to modify, capture, and/or insert an additional information on web pages without the customer's and the host's knowledge[10][11]. Once connected to the legitimate site and 'piggybacks' on a legitimate authenticated session between the user and the financial institution, the MITB attack alters the appearance of transactions in the user's browser. As the alteration occurs in real-time, the MITB prevents the user from detecting the fraudulent activity. For example, the user thinks he is transferring funds between accounts to pay bills, and the browser displays the transfer, when in fact the MITB attacker is actually transferring the user's funds into the account of a third party. The user views and confirms what he thinks are his intended transactions, only to become an unknowing accomplice to raiding his own account.

An example of how an MITB attack would succeed(see Figure:1)

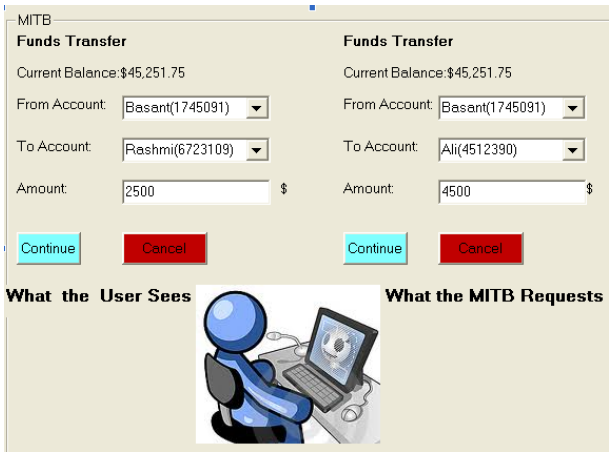

Figure 1. How an MITB attack

1. Basant requests transfer of $2500 to Rashmi
2. MITB alters transfer request to transfer $4500 to Ali
3. MITB submits fraudulent request to bank
4. Bank requests confirmation of transfer of $4500 to Ali
5. MITB alters confirmation page to present user with original request
6. Basant reviews the transaction details and confirms request
7. Bank transfers $4500 to Ali

3. Man-in-the-Middle

MITM attacks rely on customers divulging their credentials on a fraudulent Web site. The attacker then forwards the legitimate credentials to sign onto the legitimate site (such as a bank portal), and then acts as a relay between the legitimate user and the legitimate site.

What is unusual about the MITM attacks is that they succeed in spite of customers using "one-time password" (OTP) tokens that generate a unique password every minute. The attacker immediately forwards the customer's credentials to the bank portal, signing in before the token-generated onetime password can expire.

An example of how an MITM attack would succeed (see Figure: 2)

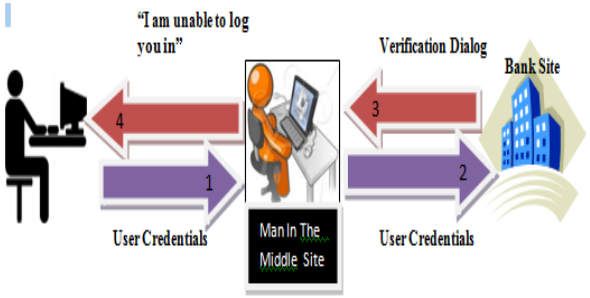

Figure 2. How an MITM attack would succeed

1. User clicks on link in a phishing email, goes to goes to MITM site and enters credentials (including token generated one-time password)
2. MITM site connects with Bank site and impersonates legitimate user using phished credentials
3. Bank site grants MITM account access
4. MITM displays phony page stating system is unavailable, or waits until user wants to log off, then displays phony page confirming log-off

By intercepting the traffic between the customer and the portal, an MITM attacker has the freedom to:

- Capture the user's credentials and use them to gain repeated access to the portal posing as the genuine user (when the credential is a fixed password)
- Log into the system while presenting a "System temporarily down" or "I am unable to log you in" message to make the user think the portal is not available (when the credential is dynamic, such as with an OTP token)
- Log into the system and simply relay all activity between user and the portal until the user tries to end his session.

Then provide a "You are now logged off" message while remaining logged into the user's account (when the credential is dynamic, such as with an OTP token)

4. Fake Sense of Security

The achievement of the MITB and MITM attacks highlight the fake sense of security that many types of authentication solutions can give IT/Security teams within organizations. In the case of MITB, deploying advanced authentication solutions like smartcards or PKI have long

been considered sufficient protection against identity theft techniques. However, since the MITB attack piggybacks on authenticated sessions rather than trying to steal or impersonate an identity, most authentication technologies are incapable of preventing its success. In the case of MITM attacks, the real-time relaying of legitimate credentials by the MITM to the legitimate bank site defeats the security of OTP generated by hardware or software tokens. The validity of such a password token is between 30 to 60 seconds, sufficient time for the fraudulent user to capture the temporary password and forward it on to the portal, while the password is still alive. The root problem in an MITM attack is that a user has no way of verifying who is asking for his authentication information. Consequently, most two-factor credentials, including OTP tokens, risk analysis engines, personal assurance messages and so forth are vulnerable to this type of attack.

5. The Solution against Both MITB and MITM

This paper offers a unique approach to protecting online customers from sophisticated attacks like "Man-In-The-Bro wser" and "Man-In-The-Middle" intrudes.

Defeating Man-in-the-Browser

There are two fundamental problems exploited by MITB attacks

1) How to make sure the integrity of the data in t ransacti on between a legitimate user and financial institution

2) How to offer additional authentication of the transaction itself to allow the user and financial institution to have a high degree of assurance in the transaction ensuring data integrity is fundamental to preventing a MITB attack from succeeding, as there will be no indicator to the user that the MITB attack is underway and altering the

transaction. Any successful approach to combating MITB will need to abolish the browser as means with which to conduct transactions, as well as detect any variance between the transaction originally submitted by the user and the transaction as reported to the financial institution.

Digital signing of forms to both bypass any browser-based Trojan or helper application as well as detect when there has been tampering with the transaction data. Digital signing of forms works as follows: when a user initiates a transaction, he is presented with a PDF-based form. It is this PDF form, rather than an HTML form, into which he enters all transaction details. Upon completing the form, the user then clicks on the 'submit' button which causes the user to digitally sign the PDF, enabling the completion of the transaction. The form data is never exposed to an MITB attack as it takes place outside of a browser environment.

Another technique used to defeat MITB is the creation of a Virtual Private Session (VPS). VPS creates a virtual session with the end-user, exposing any changes in the transaction made by malware in the browser, or any browser helper objects. The secure in-band authentication provided by the VPS allows the server to send a confirmation to the user that includes an OTP that the user must enter to approve the transaction. The OTP is time-sensitive, and its short life (e.g., 30 seconds) prevents the attacker from intercepting, altering, and resending the confirmation to the user before the embedded OTP expires.

Defeating Man-in-the-Middle

Public Key Infrastructure (PKI) technology is used to defeat MITM attacks[7] .PKI uses a challenge/response protocol to ensure a secure, authenticated communication session between the client and the application or portal.

The PKI is able to automatically verify that the site requesting the authentication credentials is in fact the site that issued them. If the site requesting the credentials did not issue them, it will not respond to requests for username or password, automatically preventing identity theft and fraud.

6. Proposed System

6.1. Digital Signature Solution

A digital signature ensures integrity and authenticity of a transaction[6].

Digital Signatures enables an extension of PKI based authentication technology to the Mobile

Phone environment (WPKI) and positions the SIM (UICC) card and thus the mobile phone as the central device in the service chain (shown in figure 3).

6.1.1. Process Flow

The following gives a simplified example of the steps in the process flow of a user accessing a

virtual resource, for example an on-line banking Internet site, from the perspective of the end user.

User invokes access to the service via a computers Internet browser.

Internet service requests the user to input account name or similar account identifier.

Internet service identifies that the user has a digital Signature and initiates an authorization request to the relevant

Managed Security Service Provider(MSSP).

MSSP messages the SIM client on the user's mobile phone, via SMS, which requests adigital Signature (typically a 4 digit code) from the user.

User enters signature code.

MSSP sends a request to the Certification Authority, which validates the electronic signature.

MSSP return a positive confirmation to the Application.

User is allowed to enter the banking Internet site.6.1.2. Additional Counter Measures

- A virtual scrambled keypad to foil key loggers and mouse-click loggers
- Dynamic content such as a "Personal Assurance Message," customized by each user, to confirm that they in fact are on the correct site before entering their credentials

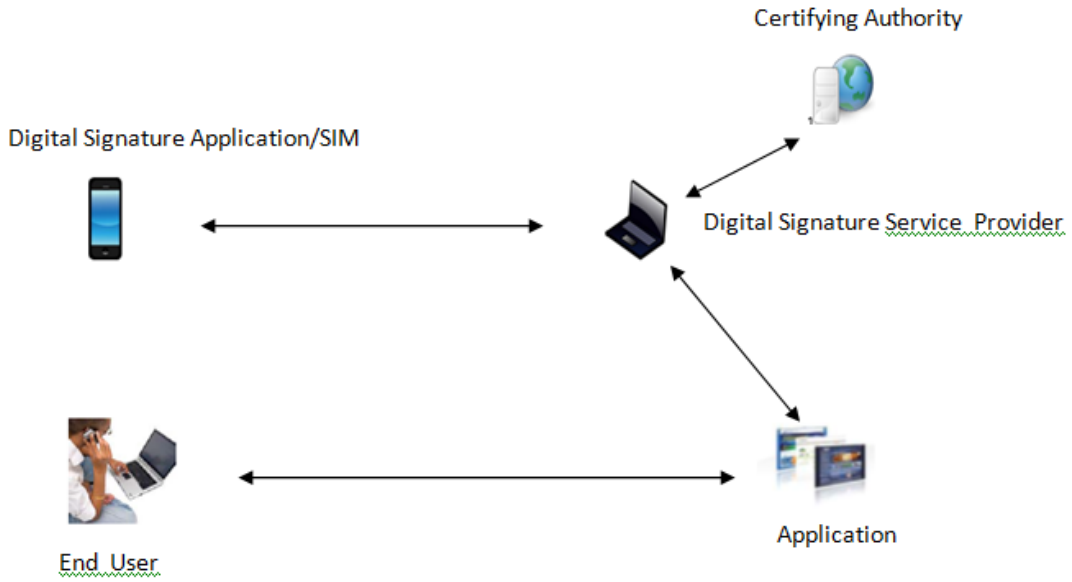

Figure 3. System Schematic

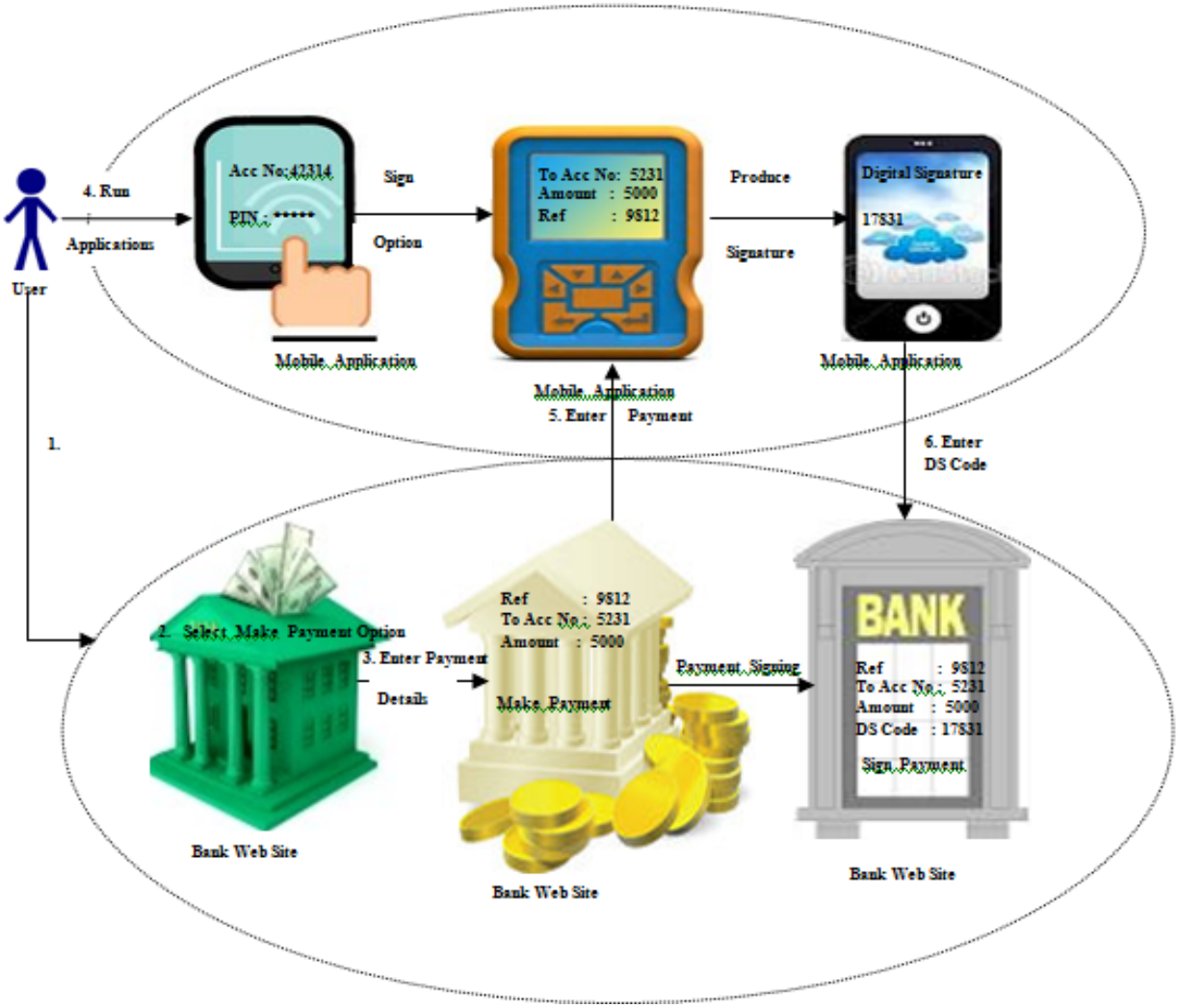

Figure 4. Block Diagram Representing user interface with Mobile Application and Banks Web Site

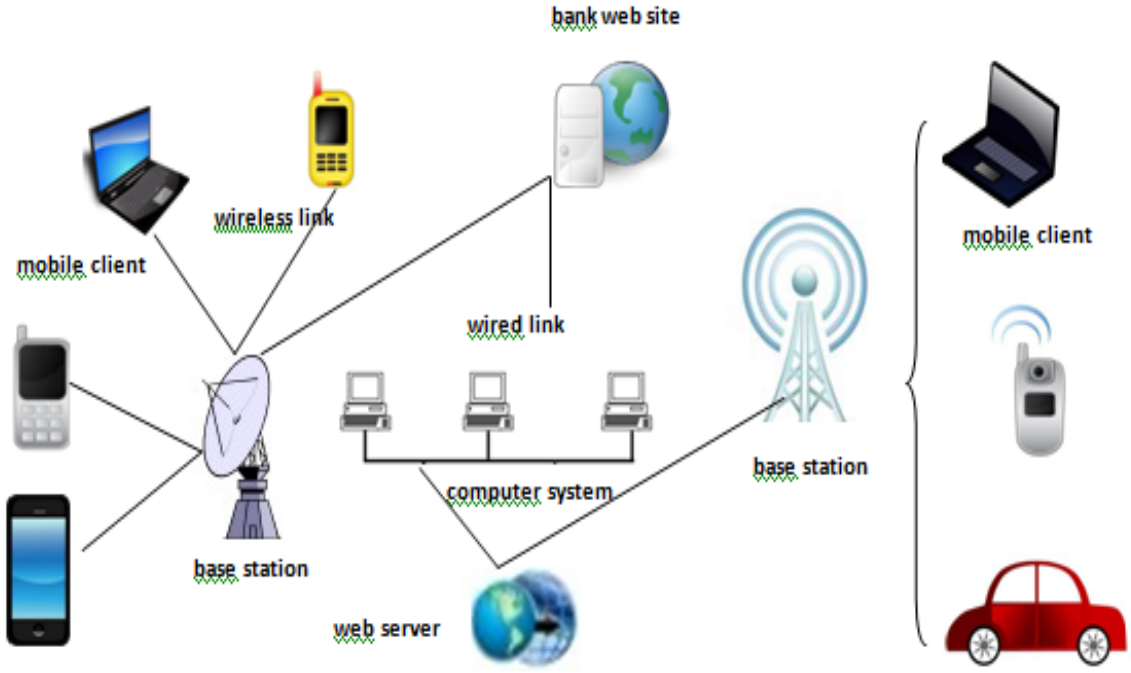

Figure 5. A typical mobile environment for web transaction

- Install the anti-browser toolbars that have ability to analyse the URLs, imagery on a site, text and various heuristics to ensure a safety of a website[12].
- Customers must check their bank account balances regularly and be aware of bank privacy policies and practices[13].
- The TriCipher Armored Credential System (TACS) enhances the device for client authentication to protect the initial

login web applications and transaction authentication used to verify the authenticity of online transactions[14].

- Apply virtual signing technology that uses the camera in the customer's mobile phone or a dedicated optical token. It removes the need for the awkward authenticators and time consuming re-keying of the challenge codes or the transaction details. The large capacity allows more transaction details to be authenticated, and these can be changed rapidly, in response to adaptation in criminal behaviour[15].

6.2. Client Interface

A J2ME program is developed and can be installed onto the user's hand held device like a mobile phone as a .jar file. The .jar file is run and the application gets installed onto the mobile phone. It is platform independent and can be applied on any J2ME-enabled mobile phone. In order for the user to apply the Digital Signature Code generation application, the user has to enter his username and PIN on the mobile phone interface and authenticate himself and select the Digital Signature generation option. The user then enters the transaction details from the banks website onto the mobile phone and the application generates a Digital signature code corresponding to the particular transaction (see Figure 4). The username, PIN, and generated Digital Signature

Code is never stored on the mobile phone even if the mobile device is stolen; a third party cannot run the application as proper authentication is required to run the application

7. Conclusions

Man-In-The-Browser ("MITB") and Man-In-The-Middle ("MITM") are sophisticated threats that can succeed in spite of organizations deploying multi-factor authentication soluti ons. These two attacks are representative of an emerging class of threats that accomplish identity theft and financial fraud by exploiting technology previously thought to be secure. For financial institutions to have confidence in the identity of their users and the transactions their users conduct, they must deploy security tools that can stay abreast of evolving threats. The transaction details are hashed; that is, a hash value is calculated using a cryptographic hash function, and the hash value is encrypted with the customer's private key to create the signature. The signature is validated by the bank's system-the bank generates its own hash of the transaction details, and it compares this against the customer's hash that it obtains by decrypting the signature with the user's public key.

Consumer and business facing financial organizations can benefit from this study to deploy multi-factor authentication and digital signing solutions that protect against MITB and MITM attacks while retaining ease of use, ease of management, and ease of deployment.

REFERENCES

[1] Philipp Guhring,"Concepts against Man-In-The-Browser Attacks",White Paper, Advances in Financial Cryptography,vol.2, 2006.

[2] Avivah Litan,"Phishing Attacks Leapfrog Despite Attempts to Stop Them",Source Gartner RAS Core Research Note G00144337,2007.

[3] Silke Holtmanns, Valtteri Niemi, Philip Ginzboorg,Pekka Laitinen and N. Asokan,"Cellular Authentication for Mobile and Internet Services", Wiley, A John Wiley & Sons, Ltd, Publication, Nokia Research Center, Helsinki, Finland,2008.

[4] Wen-Chen Hu, Jyh-haw Yeh, Hung-Jen Yang and Chung-wei Lee ,"Mobile handheld devices for mobile commerce, Encyclopedia of E-Commerce",2006.

[5] Mehdi Khosrow-Pour, "Encyclopedia of E-commerce , E-government and Mobile Commerce", Idea Group Publishing, David Coffin, Expert Oracle and Java Security,Apress,2006.

[6] Ian Curry, "An introduction to cryptography and digital signature", Version 2.0,March 2001.

[7] Tom Davis , "Information Security: Status of federal Public Key Infrastructure Activities at Major Federal Departments and Agencies", GAO report no GAO-04-157,USA,2004.

[8] Ståhlberg, M. ,"The Trojan Money Spinner",Paper presented at the Virus Bulletin Conference, Helsinki, Finland, 2007.

[9] John Leyden, J.," Firefox plug-in Trojan harvests logins", TechSupport FORUM, 2008.

[10] Tmothy Dougan,Kevin Curran,"Man in the Browser Attacks",University of Ulster,Volume 4, Isuue 1,UK,2012

[11] Andrew Trantola,"Man in the Browser" Attack Bypasses Bank's Two-Factor Authentication Systems",2012

[12] Akwukwuma, V. V. N., & Egwali, A. O.."E-Commerce: Online Attacks and Protective Mechanisms", Asian Journal of Information Technology, pp. 394-402,2008.

[13] US-CERT, "Banking Securely Online", 2008.

[14] Ant Allan, Avivah Litan,"Transaction Verification Complements Fraud Detection and Stronger Authentication", 2006.

[15] Nigel Walsh,"Beyond Phishing - De-Mystifiying The Growing Threat of Internet Banking Fraud",Cronto Limited,Cambridge, England,200