Using Two-factor Authentication Systems to Prevent Social Phishing & Man-In-The-Browser Attacks for Internet Banking

Zhe SUN (Zsun012)

Zsun012@aucklanduni.ac.nz

Department of Computer Science, University of Auckland

Abstract

Social Phishing and Man-In-The-Browser are two new efficient ways to steal victims' important information. Social Phishing use public gatherable information lure user to a spoofed website to get their secure information. [2] Man-In-The-Browser uses a new Trojan horse inside user's browser to modify a victim's requests and responses during the transaction. It's hard for unprofessional people to detect or prevent and easy for attackers to get valuable information from victims. With huge benefits, Internet Banking users' details are the most attractive for attackers, like bank account passwords, credit card details and etc. As personal password protection is the weakest link of Security Chain [1], simply ID and password protection does not work well against the above threats. Some new Two-factor authentication systems with Mobile Device have been developed to fight against them. This paper will analyse and compare how they can anti current threats and protect personal security for normal Internet Banking users.

1 Introduction

1.1 Background

Internet Banking becomes more popular in our society now for its great positive features, such as easy to use, saving transport to the bank and queue time on the counter and some

other extra benefits. However, as every coin has its pros and cons, Internet banking is not an exception. Since it was born, attackers around the world have been working on breaking it and stealing online banking users' money from their accounts, which looks more safe and easy than robbing a bank. On the contrary, Online Banking users would not like to be free ATM machines for hackers. Thus, banks and their security experts have been keeping developing new technology to protect their customers' Internet banking accounts. The wars between them never stop. An accent Chinese general Sun Tzu said in his "Art of War": "If you know both yourself and your enemy, you can come out of hundreds of battles without danger". We will start to analyse our enemies first and discuss how to defeat them in the next following chapters.

1.2 Secure Threat for Internet Banking

1.2.1 Social Phishing

Social Phishing is a form of deception in which attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity using victim's public gatherable information. [2]

Normally, a Social Phishing attacker pretends to be a friend, relative or important person of the victim (e.g. a victim's bank manger) sends an email related with the victim's account to the victim and asks him to enter a bank URL provided in the Email. If the victim clicks this URL in the email, he will enter a web page looking like the Bank's Internet Banking login page which is indeed a fake website run by the phisher. When the victim uses his Internet banking user name and password to login this page, his user name and password will be recorded and sent to the phisher. With this information, the phisher can login to the real rank's website and transfer the victim's money to his own account.

For normal customers, it is hard to identify that the current Email is from their bank manger or the phisher, and also the webpage is genuine or not. Scrupulous users may use their browser to input their banks' website addresses manually to avoid this

phishing attack; while the majority of the Internet Banking users prefer just clicking the addresses attached in emails if the phisher pretends to be a bank manger they trust.

1.2.2. Man-In-The-Browser

Man-In-The-Browser (MitB) is structurally as a new kind of Man-In-The-Middle (MitT) attack. It works between the user and the security mechanisms by attacks browsers with new Trojan horses. The new Trojan is technically more advanced than prior generations by the way of combining Browser-Helper-Objects, Browser Extensions, and direct Browser manipulation techniques. [6] It can modify the transactions in browsers to gain benefits or redirect users' requests to fraudulent phishing websites to steal their passwords.

As Philipp Gühring mentioned in his article, a man in the browser attack is more difficult to prevent and disinfect, for attackers can intercept messages in a public key exchange and substitute bogus public keys to request party. [6]

A simple illustrate figure can be seen as below:

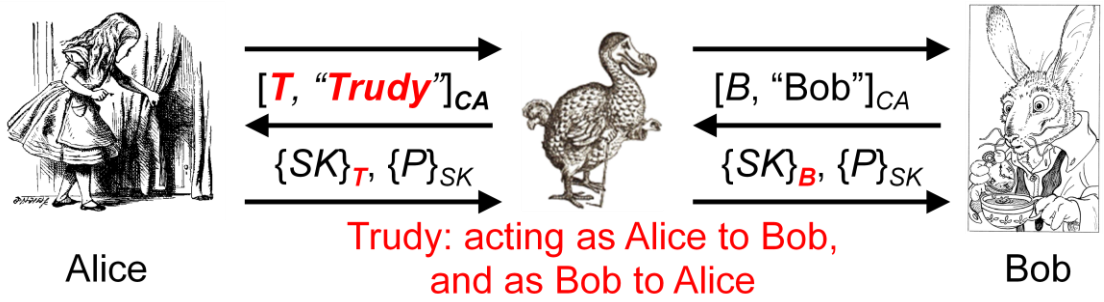

Figure 1 [8]

From Figure 1, we can see that it works in the following steps:

1. The attacker (Trudy) distributes Trojans to infect the victim (Alice) computer's software and installs extension into her browser, so that the attack will take off when the browser starts next time.

2. When the victim (Alice) starts the browser and wants to contact with Internet banking server (Bob) after Trojans infection, it will automatically register handler for each page-load and check whether it's URL in the target lists.

3. When Trojan finds that the target URL has been loaded, it will register a button event handler in the current page. When the submit button is pressed, all the data in the form field will be extracted and remembered. It can record and even modify the value and make the browser continue submitting it (whether modified or not) to the server. (Trudy, standing in the middle, transfers his certificate to Alice as Bob and encrypts Alice's message with his certificate sent to Bob as Alice.)

4. The server receives the form and trusts its value, for it does not know if it has been recorded / modified or not. Then it performs the transaction and returns with a receipt. (Bob receives Trudy's message and trusts it is from Alice. Trudy receives Bob's reply before Alice.)

5. The browser receives and displays the receipt (the data on the receipt needs to be converted back to the user's real request before being displayed to the user if it has been modified). (Trudy modifies Bob's message and sends it to Alice.)

6. The attack completes, while the user trusts that the server has performed the right traction as he requested. [6] (Alice knows nothing about what Trudy has done and trusts it is from Bob.) [8]

1.3 Two-Factor Authentication System Solution

There are 3 basic "factors" involved in existing authentication methodologies. Something the user ***knows*** (e.g., ID, password, PIN);

Something the user ***has*** (e.g., ATM card, mobile phone); and

Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint). [5]

As FFIEC mentioned that, properly designed and implemented multifactor authentication methods are more secure than single-factor methods and has more reliable and stronger fraud deterrents. [5]

Security Device can be a second factor that user ***has*** for authentication based on the above definitions. To prevent phishing attacks, Secure-ID Token and Mobile Phone are the most popular security devices for Internet Banking at this moment. As the MitB solution concepts talked by Philipp Gühring, the external authorization device

and secure communication over insecure systems both have their pros and cons. [6] A two-factor authentication system using secure devices combining their advantages seems operative.

2, Two-factor Authentication System Analyse

As FFIEC mentioned, the success of a particular authentication method in Internet Banking environment depends on more than this technology, two-factor authentication. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans. [5]

There are several different ways to setup an exercisable two-factor authentication system. Secure-ID Token, Mobile Phone with Phoolproof protocol and Mobile Phone with MP-Auth protocol are the three main useful systems that will be discussed in this paper.

As usability is a great concern for any protocol supposed to be used by general users and security is the main topic need to be discussed, this paper will measure and discuss security devices by these two factors. In Usability part, it is evaluated based on implementation requirements and costs for work / study; in Security part, it is estimated against Social Phishing and Man-In-The-Browser attack, the main threats mentioned in this paper.

2.1 Secure-ID Token

Figure 2 [9]

The Secure-ID Token as we can see from Figure 2 is called Password-Generating Token [5]. It also has some other names and features in different areas, for example "Online Security Device" which HSBC bank uses as a One Time Password generator, and "Net Security Device" used by Royal Bank of Scotland and NatWest bank with a bank card reader inside.

Whatever, all these devices have a similar feature that is One Time Password generating function. This token produces a unique pass-code each time. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if the regular password matches and the OTP generated by the token matches the password in the authentication server. A new OTP is typically generated normally every 60 seconds. [5] This very brief period is the life span of that password and make it secure for authentication.

2.1.1 Usability

2.1.1.1, Deployment Requirement

1, The user need press the button to generate a security ID and input it to the web form with his user name and password.

2, The user need change the device or its battery when it runs out of energy. Normally, this kind of device can run continuously for 36 to 42 months or even longer. [7]

3, The bank need set a scheme on Internet Banking Server side cooperating with User's Secure-ID Token.

4, The bank need train its staffs and customers to use this Token.

2.1.1.2, Cost Requirement

It costs banks or customers to propose Secure-ID Tokens.

2.1.2 Security

2.1.2.1, Against Social Phishing

Result: 90%Yes, 10%No.

(Some smart phishers can steal money from stupid users.)

Simple Social phishing attacks can be avoided by this device for its randomness, unpredictability and unique OTP with synchronize and time-sensitive features. [5]

Even if a phisher successfully gets a user's Internet Banking ID and password with his spoof website, he can do nothing with the user's account because he cannot get the OTP generated by the user's Secure-ID Token.

Some smart phishers will add a new input field in his spoof website to gather users' OTP. However, mostly it is useless, for OTP is time-sensitive and expires in 60 seconds. Even a lucky phisher got the OTP and used it within the expire time, a one more confirm OTP from the Bank website during the transfer would make his trail fail. It's really hard for the phisher to ask the victim input his OTP several times without any reason. There is only one possible successful way for the phisher, which is the phisher telling the victim that there is something wrong with his input and asking him to re-input. The phisher can use these OTPs simultaneously on the real bank's website and transfer the funds. [2] This is possible only if the victim really trusts the phisher's website and would like to input his OTPs as many times as the phisher needs without doubt.

2.1.2.2, Against MitB

Result: No.

In Gühring's opinion, all authentication systems using the PC as the single channel for data transaction are circumvented, [6] and Secure-ID Token is one of the insecure authentications under MitB attacks. During attacks, Trojans grab users' requests and

alter them before sending to the bank server in real time and modify the server's reply to the users. That means, even during account summary check, the hacker can ask the user to input his OTPs as many times as he needs to do funds transfer.
Whatever, if the Trojans in MitB take users' input as records only, Secure-ID Token can also fight against MitB, as OTP will expire in 60 seconds.

2.2 Mobile Phone

Mobile Phone is a good authentication device that can be used as a second factor between user and server in FFIEC. [5] This part will discuss how it works with different protocols for Internet Banking. One is called Phoolproof and the other is called MP-Auth. They will be analysed and estimated with their usability and security against Social Phishing and MitB attacks.

2.2.1 Mobile Phone with Phoolproof Protocol

Phoolproof protocol was designed by Bryan Parno, Cynthia Kuo, and Adrian Perrig in early 2006. They proposed to use mobile phone-based authentication to prevent Phishing and MitM attacks for Internet Banking with less reliance on users. Below is the working process for PhoolProof protocol:

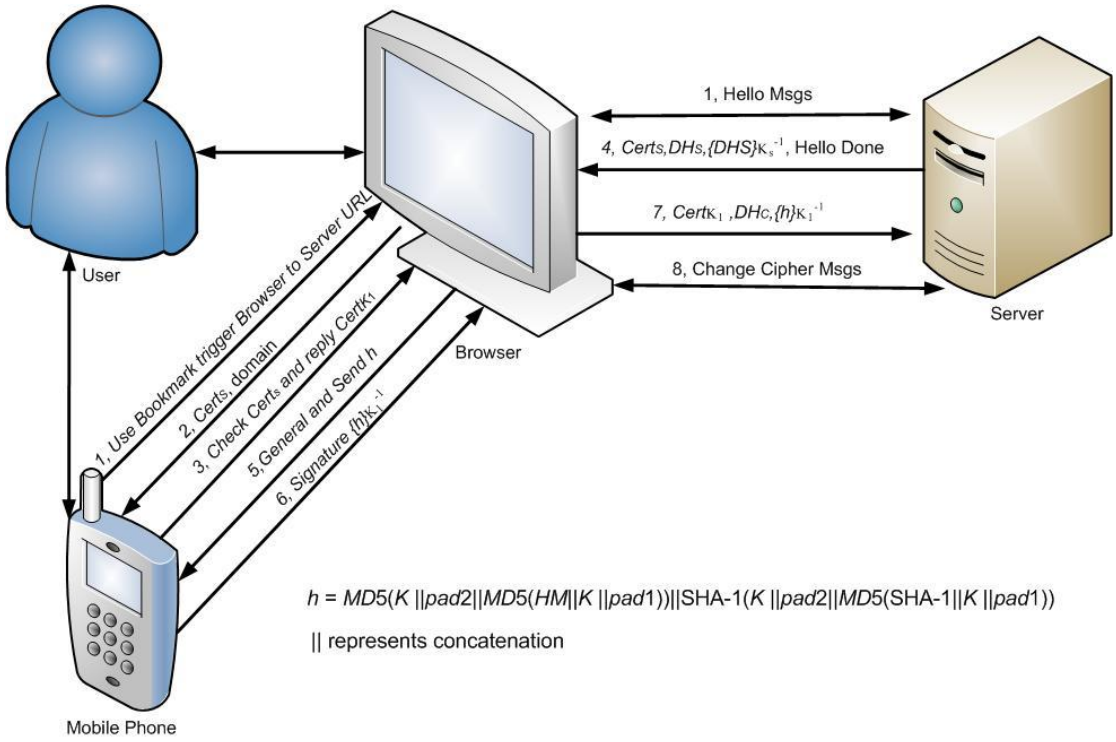

Figure 3 Phoolprool Login processes

Firstly, a shared secret is created between the user and the bank server with sufficient length e.g. 80-128 bits to avoid brute force attacks. It is generated from an out-of-band channel, e.g., postal mail, bank counter setup, etc. After that, user will set up an account with corresponding bank server and receive server's certificate. The user's mobile phone needs to generate a key pair $\{K_1, K_1^{-1}\}$ stored with server's certificate for logins afterward and send the public key (K_1) to the server. The mobile phone will create a bookmark with server's name and domain name. [3] After setting up, the user can communicate with the server through it.

Figure 3 illustrates the login process:

1, The user uses the bookmark in his mobile phone to trigger the browser to the server's URL via Bluetooth.

2, The browser sends server's certificate and domain name to the mobile phone.

3, The mobile phone authenticates the server's certificate with the pre-stored one. If it is approved, mobile phone will send his certificate to the browser, otherwise warning the user.

4, The browser and server then establish an SSL/TLS connection. The server will send the browser a message encrypted by his certificate.

5,The browser retrieves the message. It generates the necessary Diffie-Hellman key material and calculates a secure hash of the SSL/TLS master secret *K* (which is based on the derived Diffie-Hellman key) and all of the previous handshake messages *h* and sends *h* to the mobile phone.

6, The mobile phone encrypts *h* to make a signature and sends it back to the browser.

7, The browser sends user's certificate and the client's Diffie-Hellman key material with the signature to the server.

8, The server authenticates the user and the SSL/TLS connection has been established, so that the user can use the browser to do his Internet Banking as usual. [3]

2.2.1.1 Usability

2.2.1.1.1, Deployment Requirement

1, The user needs to install server's certificate and his own key generating script into the mobile phone and generate a key pair. He also needs to reinstall server's certificate and revoke his key pair in case of public key updating, replacement, lost or malfunctioning the mobile phone. Additionally, the user's mobile phone needs a script to check server's certificate, domain name and etc. Experienced technical staffs are necessary for non-technical users to complete this procedure. [4]

2, The server needs to install 2 simple Perl scripts and make some configuration. [3]

3, To make the Local channel between the browser and mobile phone (Bluetooth) secure, a camera-phone may be required. [4]

4, The browser may need to be modified (e.g. script for generating *h*) to comply with this protocol. [4]

2.2.1.1.2, Cost Requirement

This system requires a smart phone with a camera. In another word, if the user does not have it in hand, he may need to purchase a suitable mobile phone.

2.2.1.2 Security

2.2.1.2.1, Against Social Phishing

Result: Yes.

In case of a phishing attack, even if the user inputs his ID and Password into spoofed website, it is not enough for the phisher, for the absence of the user's public key which is setup when the user open an account and stored in the bank's server. The phisher can do nothing with the user's account without the user's mobile phone. On the other hand, if the phisher gets the user's mobile phone but without the use's ID and Password, it is still meaningless to login into the user's account. [3]

2.2.1.2.2, Against MitB

Result: No.

Bryan et al. said that Phoolprool can prevent MitM attacks because the server stored the user's public key and his mobile phone stored the server's certificate; while Mohammad et al. was against this and indicated that when the browser received the client's public key from the mobile phone, attackers might hijack account setup or (user) public key re-establishment through MitB. [6]

2.2.2 Mobile Phone with MP-Auth Protocol

MP-Auth was designed by Mohammad Mannan and P. C. van Oorschot at Carleton University in late 2006 and refined in early 2007. The following is the setup and working process for MP-Auth protocol:

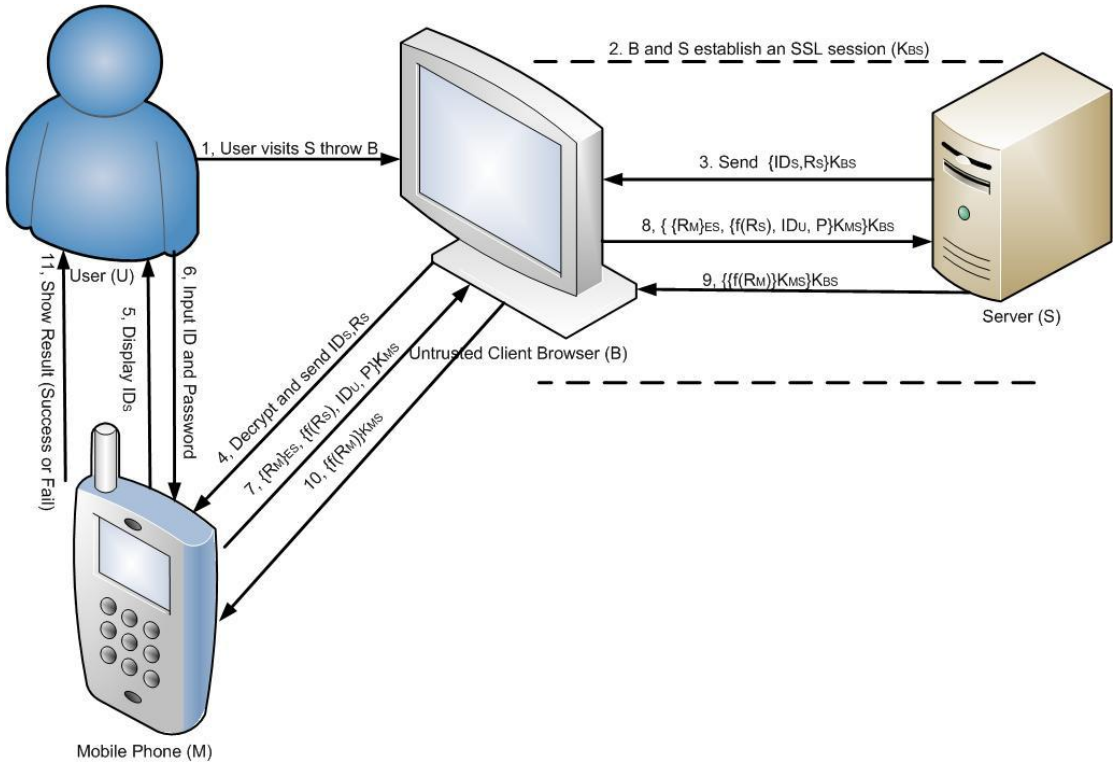

Figure 4 MP-Auth Protocol steps [6]

1, 2, The User utilizes browser B to visit the bank server S and establishes an SSL session using SSL secret key: K_{BS}.

3, The Server generates a random nonce Rs and sends its ID and Rs encrypted with K_{BS} to the browser B.

4, The browser B decrypts this message and forwards IDs and Rs to the mobile phone M via Bluetooth.

5, 6, The mobile phone M displays IDs to the User and asks him to input his ID and Password for the bank server S. The Password will not be stored in the mobile phone.

7, The mobile phone M generates a random secret nonce R_M and calculates session key K_{MS} from Rs and R_M. M encrypts user ID: ID_U, Password P and message f(Rs) by using K_{MS} and encrypts R_M by using Server S public key Es, and then sends them to the browser B via Bluetooth.

8, The browser B encrypts the message from M with K_{BS} and sends it to Server S via SSL.

9, The server S decrypts the message from B and verifies ID_U, P and Rs. If it is successful, S will encrypt f (R_M) with K_{MS}, which will be encrypted with K_{BS} later, and then sends it to the browser B.

10, The browser B uses K_{BS} to decrypt the first shell of the message and sends the rest to mobile phone M.

11, The mobile phone M decrypts the message to get f (R_M) and verifies it with the local stored R_M. M displays success or failure message to the user U.

2.2.2.1 Usability

2.2.2.1.1, Deployment Requirement

1, The user needs to install the server's public key system into the mobile phone from the secure channel (ATM, bank counter, post mail etc.). [4] He also needs to reinstall the server's public key in case of public key updating, replacement or lost the mobile phone. Experienced technical staffs are necessary for non-technical users to complete this procedure.

2, The browser side needs to install a Firefox Extension to communicate with the server. [4]

3, The mobile phone needs to install a MIDlet script for encryption/decryption. [4]

4, The server side needs to add PHP scripts to the login page with PHP OpenSSL functions and mcrypt module. [4]

2.2.2.1.2, Cost Requirement

This system requires a smart phone or PDA, so that if the user does not have it in hand, he may need to purchase a suitable mobile phone.

2.2.2.2 Security

2.2.2.2.1, Against Social Phishing

Result: No.

Mohammad et al. thought that MP-Auth can prevent from phishing attacks. On the contrary, from my point of view, a smart social phisher's email could prompt users to enter their IDs and Passwords into a spoofed Internet Banking website other than their mobile phones in real life. [4] The phisher can use his own mobile phone which stores the bank's certificate to communicate with the real bank server by using the victims' IDs and Passwords. For the bank server does not store any other information of the users except their IDs and Passwords, disclosed IDs and Passwords to the smart phisher will cause disasters without additional protection from the bank. As we all know, personal password protection is the weakest link of Security Chain, [1] we cannot simply ascribe to users' behaviors. Instead, it is the technical staff's duty to avoid it.

2.2.2.2.2, Against MitB

Result: Yes.

In MP-Auth, there is no authentication between the mobile phone and the browser. MitB attack fails against MP-Auth if session ID verification is used, because the session IDs displayed on the browser and the mobile phone will be different.
Some users cannot detect this difference. Fortunately, transaction integrity confirmation step also can prohibit the attackers' actions except viewing even without session ID verification.

3. Result

From above overall analyse, we can draw a conclusion that, Security Device using two-factor authentication methods may make the collection of passwords less useful

to attackers and thus help restrict phishing attacks. [4] However, their usability issue, such as additional study / work on deployment, cost of the token / smart phone, recovery of the token / mobile phone; and security issue like social phishing, MitB attack and so on [4] have to be considered as important developing conditions.

Secure-ID Token is the most simple security device in two-factor authentication system for Internet banking. It's easy to use and deploy together with trusted PCs in the environment with low security requirement. It does avoid the most phishing attacks and even some kinds of MitB attacks. Nevertheless, as it is an additional device that needs to be carried on and cannot work well in high-level security systems, it may disappear in no far future. Some banks have already developed the new technology, utilizing SMS messages in mobile phones, to take the place of it. [6]

Mobile phone is a good security device can be used in untrusted PC environment. Bryan et al. and Mohammad et al. stated that mobile phones with Phoolproof or MP-Auth work well against security threats in untrusted PC environment.

For usability, Phoolproof is difficult to control by normal users, especially in key pair generating and certificate installation. As for security, a mobile phone with Phoolproof protocol has outstanding performance against phishing attacks. The author insisted in his paper that it can prevent MitM attacks, while it is not true especially for MitB in the case of session hijacking attacks. In addition, it is unconvincing that the author assumed that the local channel for mobile phone and PC browser is secure. Another secure problem is that the user's key pair and server's certificate both are stored in the user's mobile phone permanently, which may cause information leaking when the phone is lost or changed. Combining its usability and security, Phoolproof protocol only suits some particular security environment, and requires users with some security technique experience.

As Mohammad et al. mentioned in his paper, a mobile phone with MP-Auth protocol has better usability and security than Phoolproof. [6] However, installing the server certificate and script into the user's mobile phone is still not easy for normal users. MP-Auth has higher security level in local communication with session ID checking through either direct connection or Bluetooth. It is important that MP-Auth has really

good protection from MitM attacks and even MitB attacks, but user's misusing may lead to phishing attacks successful. General speaking, compared with Phoolproof, MP-Auth has easier deployment and similar security control. In another word, MP-Auth is currently a better choice for normal users and can be used in the environment with high security requirement if the phishing attacks caused by the user's misusing can be avoided.

Overall, the following table describes features for the above 3 security devices:

	Usability (Requirement)						Security	
	Deployment	Cost	On-device secret	Trusted PC OS	Malware-free mobile		Social Phishing	MitB
Secure-ID Token	×	×		×			√#	
Phoolproof	×	×*	×		×		√	
Mp-Auth	×	×*			×			√

Figure 5 Security Device Comparisons

×* cost takes place if users do not have smart mobile phones
√can be avoided
×requirement
√#conditional avoiding apply

4, Conclusion and Discussion

After analysing and comparing these different secure devices and protocols for Internet Banking users, I can draw a conclusion that: for the user's computer it is not safe enough, we cannot rely on it. Secure ID Token, mostly relying on the security of the user's computer, is not a good choice in this situation. Additionally, both Phoolproof and MP-Auth rely on Malware-free mobile phones, so that malware in mobile devices will be a potential problem for them. As Tom et al. said social phishing is so successful for normal users [2] that users' behaviours are not reliable.

[1] Therefore, a mobile phone with Phoolproof or MP-Auth protocol looks not secure enough for normal users. In my opinion, an authentication system in Internet Banking disregarding user's device (PC or Mobile Phone) security level and users' behaviours will be more efficient and secure.

5, Acknowledgement

Thank Professor Clark Thomborson (University of Auckland) for his guidance on the research topics and recommendation to the relevant materials.

6, Reference

1, [GC07] Gilbert Notoatmodjo and Clark Thomborson, Exploring the weakest link: A study of personal password security, presentation at New Zealand Information Security Forum, Auckland, 20 December 2007.

2, [JA07] T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, "*Social Phishing*", Commun. ACM 50(10), pp. 94-100, October 2007.DOI: 10.1145/1290958.1290968

3, [PB06] Parno, B. Kuo, C. and A. Perrig, "*Phoolproof Phishing Prevention*". Proceedings of the Financial, Cryptography and Data Security 10th International Conference, February 27 - March 2, 2006. Anguilla, British West Indies.

4, [MP07] M. Mannan, P.C. van Oorschot. *Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer. Financial Cryptography and Data Security (FC'07)*, Lowlands, Scarborough, Trinidad and Tobago, Feb.12-15, 2007. *Extended version: Technical Report TR-07-11* (Mar 2007).

5, [FF05] Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, October 2005. http://www.ffiec.gov/pdf/authentication_guidance.pdf

6, [Gu07] P. Gühring, "*Concepts against Man-in-the-Browser Attacks*", 15 pp., web manuscript, published circa January 2007. Available: http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf, 23 July 2008. A preliminary version of this article was announced in *Advances in Financial Cryptography, Number 3 (FC++3)*, 25 June 2006.

7, http://www.thefind.com/computers/browse-rsa-securid-sid700-hardware-token

8, [CT07] Clark Thomborson, *Cryptography and Steganography* CompSci 725 (Handout 10) University of Auckland, 10 September 2007

9, http://en.wikipedia.org/wiki/Image:RSA-SecurID-Tokens.jpg