Online Banking Security

Faheem Ramzan Tehman Pervaiz
Email: {fahra840, tehpe747}@student.liu.se
Supervisor: Anna Vapen, {annva@ida.liu.se}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

In this paper we have studied a variety of authentication solutions that online banks offer their customers. We have analyzed and compared the different solutions from both security and usability perspective. We have also performed a risk analysis based on the presented authentication solutions.

1. Introduction

Online banking is being accepted and gaining trust of many customers with the passage of time [11]. Pay bills while traveling, transfer funds in other accounts, viewing mortgage balance etc. are some of the advantages of the online banking. One of the reasons of the increasing use of the online banking system is its availability. There exists many techniques for authentication in online banking but there is a strong need to increase the security and usability of these techniques. Security is important in the sense that customers will become free from threats like fraudulently loss of money. Security is important not only for banking organizations but also for their clients. More secure the online banking authentication, more satisfied will be their customers, and their revenue will also increase. Usability is also an important perspective in online banking authentication. With usability we mean how much usable is the online banking authentication system for their customers. In this report we will study variety of authentication solutions, both from security and usability perspective.

1.1 Methodology

In this section we have discussed how we have arranged the data for the report from different sources, our working strategy in a group, and also the questions/problems addressed in the report related to our topic.

1.1.1 Data collection

To accomplish our objective we have studied different online banking authentication solutions by taking references from the course literature and research papers. We have analyzed and compared the security of online banking solutions from both security and usability perspective.

1.1.2 Group Working

We have adopted very systematic and professional approach for attaining our goal for this project. Roles and responsibilities have been assigned to both group members from the beginning of the project. Internal group meetings have held twice a week to get the overview of the work and to evaluate that each group member is going in the right direction.

1.1.3 Questions/Problems

Our report will answer the following questions:

- What are different online banking authentication techniques?
- What kind of security issues are there with online banking authentication?
- What is the usability of different online authentication techniques?
- What are the risks associated with different authentication solutions and their assessment?

2. Background

Online banking security is becoming seriously important in recent years due to increasing amount of internet users. Now a day's almost every bank is offering online banking solutions to their customers. Higher security standards are required as banking activities are by nature more sensitive than most other Internet activities. Most banks employ two-factor authentication to increase security, which involves two basic factors: [5]

- Something user knows, like password, PIN, pass phrase etc.
- Something user has, like smart card, hardware token etc.

2.1 Online banking security

Web has become the only medium for an increasing amount of business and other sensitive transactions for online banking. Almost all browsers and servers deploy SSL/TLS protocols to address concerns about security. But, even the usage of SSL/TLS by browsers still allows Web spoofing, that is, misleading users by impersonation or misrepresentation of identity or of credentials. [1,7]

There are different types of risks associated with online banking. Security for user credentials has become much more important than anything. Indeed, there is an alarming increase in the amount of real-life Web-spoofing attacks, usually using simple techniques. Often, the attackers fraudulently redirects the user to spoofed Web site by sending her spoofed e-mail messages that link to the spoofed Web sites; this is often called phishing attack. The goal of the attacker is often to obtain user-IDs, passwords/PINs, and other personal and financial information. Some of the risks associated with online banking are as following: [4,7]

- Web Spoofing and Phishing Attacks.
- DNS Cache Poisoning (Pharming).
- Malware: Trojan-horses, backdoors, root-kits, key-loggers.
- Credential stealing attacks.
- Channel breaking attacks.
- Nigerian 419 and other scams.

2.2 Authentication methods

There are different authentication methods used for online banking security with involve different authentication factors like password, PIN, pass phrase. Most banks conduct two-factor authentication one of which being based on the knowledge of some data (i.e. something the user knows). The actual implementations may vary, still username-password combination, pass phrases or PIN numbers are the most commonly applied. In order to increase security, most banks employ a second authentication factor – a token that user possesses. The implementations of the authentication factor can be classified as follows: [4,5]

- **One-time password approach:** Tokens in form of one-time passwords are very popular in Scandinavian countries. Main advantage of one-time passwords is the fact, that they can be used only once and become invalid afterwards.
- **Certificate based approach:** Certificates are software tokens that require PKI (public key infrastructure). In the case of certificate based approach a certificate is used as the second authentication factor. They can be stored either on the hard drive or another storage device e.g. USB stick, smart card. Usually banks employ the combination of a certificate together with username-password, pass phrase or PIN number.
- **Timer based (short) password approach:** Timer based one-time-password is generated using hardware generators (e.g. Secure-ID). Additionally, a PIN or password is used together with one-time-password. Once the password is generated, it is valid only for some specific time interval. This approach is not only used by banks, but also employed by providers of other services like PayPal or eBay.
- **Certificate - smart card based approach:** In online-banking smart cards can be used to store certificates or as devices for generating one-time-passwords. When using smart cards, card reader is essential.

3. Different authentication solutions from security and usability perspective

In this section we have analyzed and compared the different solutions from both security and usability perspective. Applications which concerns with major security and usability problems, especially in online banking solutions are being used by customers who are less familiar with the threats and issues related to these applications. These solutions are being used by almost all banks which make possible for them to serve far more customers at the fraction of cost [8].

3.1 Security

From the security point of view the first step is to look more closely at the things that make online banking authentication methods too much susceptible to attacks. Offline credential-stealing attacks are only harmful for those methods in which secured data is valid for long time period, for example static passwords (fixed passwords) and data is entered on un-trusted devices such as a user's computer that has no antivirus or firewall. Static password can easily be obtained by malware like Trojan horses and key loggers which record the input entered by the user via the keyboard. A static password once obtained by the attacker can be useful for him until user notices that the password has been stolen [4].

One of the solutions of the previous problem is One Time Passwords (OTP). As previously discussed there are several types of one time passwords. One of the forms of OTP is scratch list which is issued to the user by the bank each password on the scratch list is valid for only one time login. There may be a problem with such method, that some users store these passwords on their computers for convenience in this way these passwords may be exposed to offline credential stealing attacks. This scheme may be slightly more secure because banking server may specify which password will be used in the scratch list next. So the security of this scheme requires that the passwords are not stored to insecure devices like computers etc. This problem is overcome by another technique that every time generates new password either based on time-synchronized OTP, non time-synchronized OTP or challenge based passwords (depending on the method used). In these methods user must manually copy the password from microprocessor based hardware token to web form. So the authentication in these methods i.e. hardware token public key infrastructure, there is less chance for offline credential

stealing attacks in unsecured computers. But these methods are susceptible to online channel breaking attacks. In these schemes the bank assign users with a matching private and public key and a trusted authority issues a digital certificate. This certificate verifies the username is corresponding to the given public key and the respective private key is valid. On the basis of the private key and certificate an authenticated SSL/TLS connection is established between bank server and user's computer. In this case the issue is with the protection of private key of user from different malwares. One of the possibilities is to store the key as soft token which is basically an encrypted file stored on user's computer, but in this case the key is vulnerable to offline credential attacks. In order to avoid this ambiguity the tamper resistant hardware like smart cards and USB sticks etc are used. These devices expose private key related functionality only [4]. Figure 1 shows the taxonomy of Internet banking authentication methods. These methods are classified according to their resistance against offline credential-stealing and online channel-breaking attacks [2].

3.2 Usability

The usability of the system is that how feasible is for the user to use the system. In [2] are defined some security usability principles. These principles explain different types of user involvement with security applications like online banking.

- **Security action:** Security action is when user enters credentials to elicit some secured information. One of the examples of security action is entering and submitting user password.
- **Security conclusion:** Security conclusion is to observe the security state of the system. One of the examples of security conclusion is to observe whether communication is protected by SSL.

There are usability principles regarding to security action and security conclusion.

Usability principles regarding security action are [2].

- Users have understanding of the security actions required.
- Users can implement the right security actions.
- The load of security actions must be acceptable.

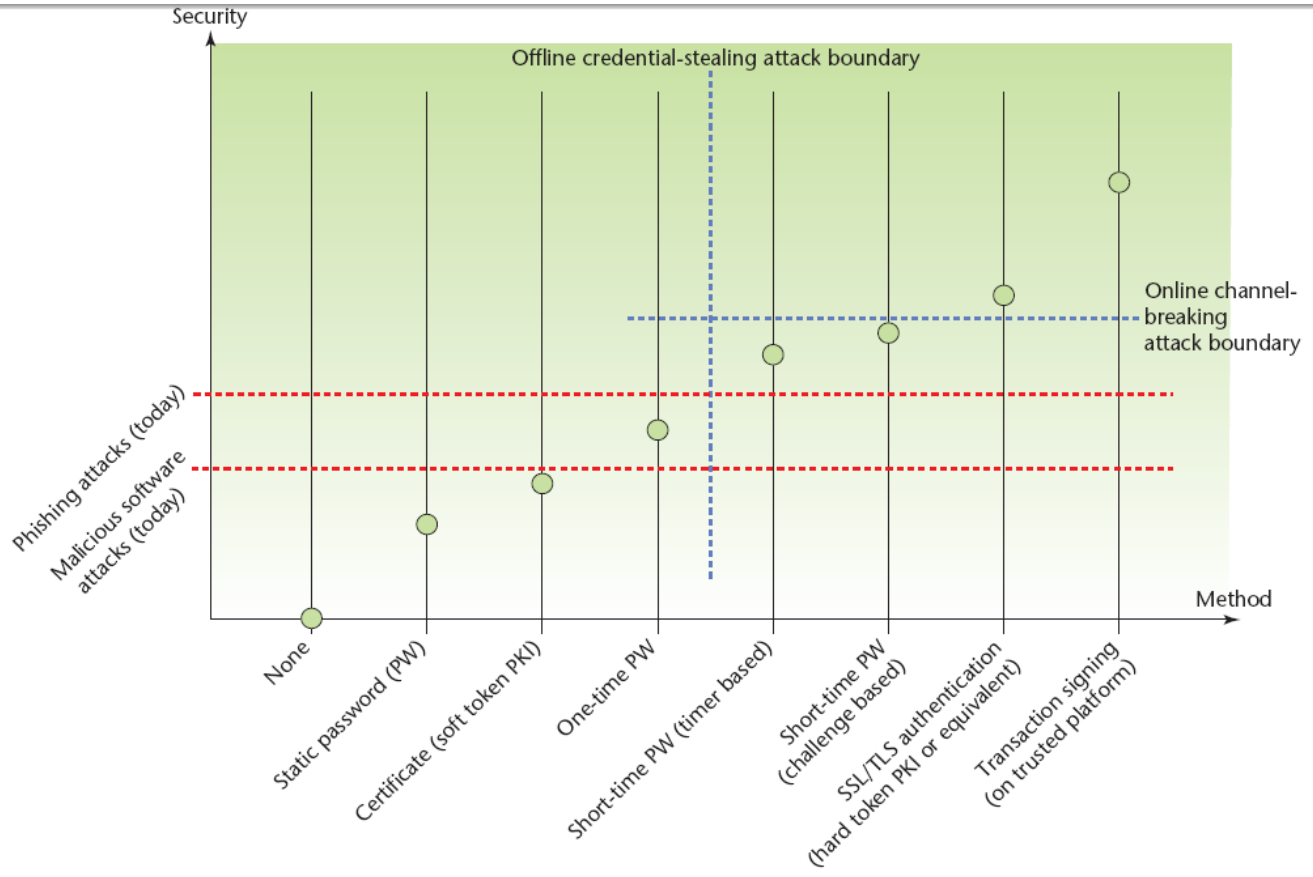

Figure 1: Taxonomy of Internet banking authentication methods [2]
(Methods are classified according to their resistance against offline credential-stealing and online channel-breaking attacks.)

- The load of repeating the security actions for practical transactions must be acceptable.

Usability principles regarding security conclusion are [2].

- User must have proper understanding of the precautions to make safe transactions.
- System must provide the detailed information for deriving the security conclusion.
- The load of security conclusion must be acceptable.
- The load of repeating the security conclusion for practical transactions must be acceptable.

In [1] the usability issue with the fixed passwords system was tinted whereas this was not an issue with the security box users.

"… 12 digits or something which you cannot remember so you need a bit of paper with you…" (Fixed password users) "I have the box and I have my own code to the box" (Security box user) [1].

In [2] the usability of push button token, card activated token, pin secured token techniques is experimentally measured. The result was that the push button token was having the high usability while card activated token was having medium and pin secured token was having low usability. If we see in the terms of security the pin secured token was having high while card activated token was having medium and push button token was having low security. In [3] here are suggested a variety of solutions to improve the usability of SMS based authentication by providing better user interface. In certificate based authentication approaches like USB and smart card, usability issue with smart card is that is order to make online transaction user must have card reader to make online transaction while USB device is simple plug and play having no special device requirement.

4. Risk assessment

Measuring credit risk for banks is particularly challenging because of the importance of financial linkages in the banking system. The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in following perspective: [6]

- Type of customer e.g. retail or commercial.
- Customer transactional capabilities e.g. bill payment, wire transfer, loan origination.
- The sensitivity of customer information being communicated to both institution and the customer.
- The ease of using the communication method.
- The volume of transactions.

Risk assessment is the process by which businesses and organizations focus on critical areas of concern and prioritize their use of resources in order to maximize response and recovery efforts. Risk assessment is extremely important in online-banking security [9]. The process should: [6]

- Identify all transactions and levels of access associated with Internet-based customer products and services.
- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access.
- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

5. Discussion

Security and usability both are important aspects which need to be considered in online banking authentication solutions. Online solutions are not just to be designed from security perspective but usability must also need to be considered. In simple words we may say that we need usable security. System must not be designed just to fulfill requirement of the banks but also to satisfy its users (customers) requirements. On the other hand, In order to securely use online banking authentication average user must have some technical expertise to maintain the system. User must be aware of the issues like failure of auto update etc. But these tasks are challenging for an average computer user [13].

6. Future work

Most of the banks which provide online services are using two-factor authentication methods. Two-factor authentication methods have been introduced by banks in response to the traditional phishing attacks, and these methods are indeed effective in stopping such attacks. Apart from benefits there are some issues associated with these methods. One of the major issues is two-factor authentication solutions are very costly. Cost is not only associated with the implementation of the solutions but expense for maintenance of the system, and training the user to adopt the new system.

Research is currently going on to make possible personal electronic devices such as mobile phones, and personal digital assistants (PDAs) to be highly secure for online banking transactions. One method is to generate cipher text representation of their PIN. In cipher text data has been encrypted, and is unreadable until it has been decrypted into plain text with a key. The functionality is unlike the electronic token, and seeks to use existing technology that may already be in the possession of potential users, to reduce costs [14].

There is also research going on for deploying voice-authentication technologies for banks to add an extra layer of security for their online and telephone banking customers. Voice authentication is reliable, but should be used with other forms of authentication so that if one method creates a question, other method helps resolve uncertainty a bank may have in authenticating user. [12,15]

Continuous research is required to meet the growing needs for security of the online service providers like banks. Service providers need such a system which is highly user friendly but with no compromise on security of the system. Finally, in order to evaluate the performance of the new scheme an investigation and research is needed.

7. Conclusion

In an environment where users are continually affected by the risks associated with online banking, it is important that user must be aware of the factors which influence their trust. Two-factor authentication methods have been introduced by banks in response to the traditional phishing attacks, and these methods are indeed effective in stopping such attacks. One of the big challenges for online banking is to maintain the balance between the security and usability of the solutions provided. In this paper we have analyzed and compared the different solutions from both security and usability perspective. We have also performed risk analyses based on the presented authentication solutions. Identity management and authentication systems need to provide adequate usability and security. We are quite hopeful that the two-factor authentication methods have been providing online banks and other online service providers to be better prepared for emerging risks, which need utmost security and usability.

References

[1] Maria Nilsson, Anne Adams and Simon Herd (2005). *Building security and trust in online banking*. Communications of the ACM.

[2] Mohammed AlZomai, Audun Jøsang, Adrian McCullagh and Ernest Foo (2008). *Strengthening SMS based authentication through usability*. IEEE Computer Society.

[3] Catherine S. Weir*, Gary Douglas, Martin Carruthers and Mervyn Jack (2008). *User perceptions of security, convenience and usability for ebanking authentication tokens.* Computers & Security, Science Direct.

[4] Alain Hiltgen, Thorsten Krampand and Thomas Weigold (2006). *Secure internet banking authentication*. IEEE Computer Society.

[5] Marko Hölbl (2008). *Authentication approaches for online-banking*. CEPIS LSI Secretary

[6] Federal Financial Institutions Examination Council (2001). *Authentication in an Internet Banking Environment*. http://www.ffiec.gov/pdf/authentication_guidance.pdf (Visited: 2009-04-15)

[7] Amir Herzberg and Ahmad Jbara (2008). *Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks*. Communications of the ACM.

[8] A. Adams and M. A. Sasse. *Users are not the enemy.* Communication of the ACM, 42(12), 1999.

[9] Rachna Dhamija, *Security Usability Studies: Risk, Roles and Ethics*, 2007

[10] One-time password. http://en.wikipedia.org/wiki/One-time_password (Visited: 2009-04-17).

[11] *Online Banking: Personal Loans Online: Finance a Mouse Click Away.* http://www.wholebanking.com/2009/03/online-bankingpersonal-loans-online-finance-a-mouse-click-away/ (Visited: 2009-04-17)

[12] *Banks inch towards voice authentication.* http://www.zdnet.com.au/news/security/soa/Banks-inch-towards-voice-authentication/0,130061744,139210410,00.htm (Visited: 2009-04-23)

[13] Mohammad Mannan, P. C. van Oorschot (2007). *Security and Usability: The Gap in Real-World Online Banking.* Communications of the ACM.

[14] *Factor Authentication in Online Banking : The New Banking Factor: Online Security*. http://www.tomsguide.com/us/factor-authentication-in-online-banking,review-678.html (Visited: 2009-04-23).

[15] *Voice Authentication in the Future for Online Banking.* http://www.bankinfosecurity.com/articles.php?art_id=254 (Visited: 2009-04-23)