Available online at www.ijiere.com

International Journal of Innovative and Emerging Research in Engineering

e-ISSN: 2394 - 3343 e-ISSN: 2394 - 5494

Study of Anti-Phishing on Internet Banking

Gunjan Pathak, Riddhi Nishar, Harnish Shah, Pooja Gajera
Department of Information technology, University of Mumbai, Mumbai, INDIA

ABSTRACT:

Internet banking is increasing day by day at very high speed. For this increasing technology it is important to provide a higher level security, the present technology used for the security purpose is the OTP(one time password) this technology is based on mobile connection to avoid using other medium we have used the same internet medium using Email. The system will send a mail to the email-id given by the customer. She/he has to download that the image which will be in the .png format and give the path to the bank website for the authentication purpose. The image will be less than 2^64 bits in length. The last 16 bits of the image will be used to pass the security code for verification. This security code will be generated using MD5 (Message Digest 5) algorithm. Internet banking anti phishing system provides the higher security by busing the two factor authorization i.e. one by login id and password authorization and the other authorization done with the help of email id given by the customer.

Keywords: phishing, security, Internet banking, Two factors Authentication, stenography.

I. Introduction

Internet banking system is developed to make a higher security internet banking process. In this system, authorization will be done on two factors, first is using the login id and the password given by the bank at the Time of opening account and the other type of the authorization will be done using the email id. As we are using the same Internet medium an email will be sent to the customer, the customer then will receive an image. He/she must download the image and give the path where exactly the image has been downloaded for the verification process. Every time the customer login's he/she will receive a different image with the different encrypted code in the image. Even if the customer gives the path of the last received image then he won't be given access to his account. As we know phishing technique takes place for hacking the login id and password so if the hacker tries phishing on the account he won't be given an access to the account because of the email id verification which is more secured.

II. REVIEW OF LITERATURE

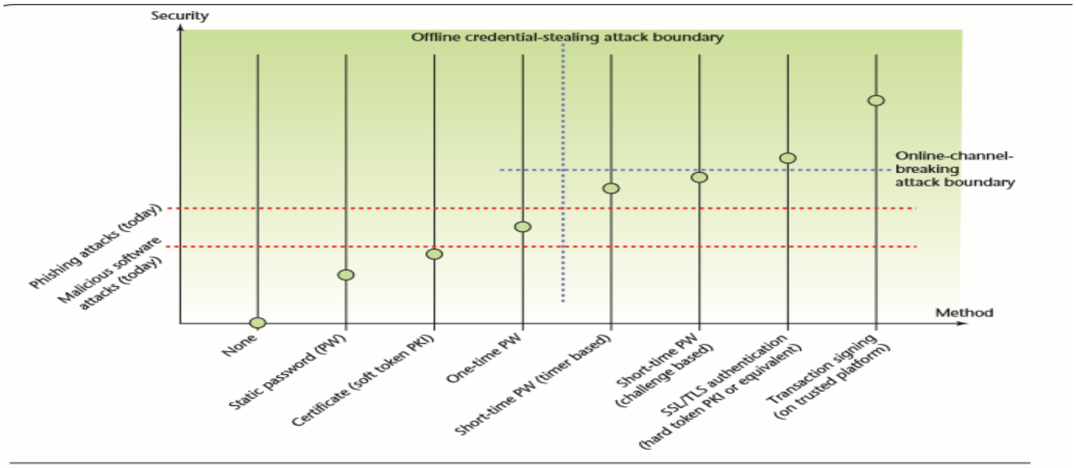

Figure 3. Taxonomy of Internet banking authentication methods. Methods are classified according to their resistance against offline credential-stealing and online channel-breaking attacks.

Figure 1. An Attack Taxonomy[3]

This diagram shows the technologies that are presently used and how they can be hacked or the problem that can be face.

Internet banking is a very popular now-a-days, and hacking is done on a large scale. We need to control this by adding more security level to the internet banking websites. After studying different papers and technology, some technologies used now-a-days are OTP, cache memory, certificates, digital signature used for higher security. This technique has some or the other disadvantage like no network coverage for OTP, cache can be used by the hackers to gain information and others similarly. So to overcome this disadvantage the group members of this project have come up idea of using two factor authentication using internet as medium for higher security. The use stenography concept has been used for hiding data in images.

III. REPORT ON THE PRESENT INVESTIGATION

The authentication schemes and attacks introduced in the main article represent the standard of knowledge discussed in various publications dealing with user authentication[1]. However, most of them provide just an overview of schemes and corresponding attacks and don't attempt to draw a security landscape by relating them to each other in a sensible way.

Short-time password solutions based on a password-generating hardware token are available from various manufacturers such as RSA Security (www.rsasecurity.com), Actividentity (www.actividentity.com), or VeriSign (www.verisign.com). RSA's SecurID solution2 is the most prominent example. It consists of a small device (with an LCD display and an internal timer) that continuously calculates the next short-time password. In contrast to the solution presented in the main article, SecurID is timer-based and doesn't use a smart card to ensure tamper resistance and scalable vendor-independent device personalization. Furthermore, because it generally isn't equipped with an alphanumeric or numeric keypad, the short-time password-generation functionality can neither be private identification number (PIN) protected nor can it be extended to transaction signing. Challenge–response-based solutions such as the one described in the article are available, too, but they're rarely used on a large scale. Clearly, convenience comes before security at this point. Only a few banks have decided to use public-key cryptography for their Internet banking systems, mostly to avoid setting up and maintaining a public-key infrastructure (PKI). One example in which a PKI solution is in production is Migrosbank (www.migrosbank.ch/de/Private/KartenZahlungsverkehr/MCardMCardSmart.htm). Here, the e-banking customer uses a smart card to securely store an RSA private key and sign data in the context of a challenge–response authentication protocol. In contrast to the Financial Transactional IC Card Reader- (FINREAD-) based solution presented in the article, this type of PKI solution relies mostly on simple card-reader devices; it's not equipped with a secure keypad, display, or cryptographic capabilities. Advanced solutions that use FINREAD are slowly emerging. Within the EU-funded Trusted FINREAD project,3 a remote banking pilot recently demonstrated the FINREAD platform's basic functionality and interoperability. However, most of today's solutions use keypad-equipped readers; solutions compliant with the home banking computing interface (HBCI; www.hbci-zka.de/english/index.html) use the reader mainly to implement secure PIN entry. With both SSL/TLS client authentication and double signatures authenticating the card as well as the reader device, the solution we've presented in the main text is vastly superior [2].

IV. PROPOSED SYSTEM

Internet banking customers only need a computer with access to the Internet to use Internet banking services. Customers can access their banking accounts from anywhere in the world. Each customer is provided a login ID and a password to access the service. It is indeed easy and convenient for customers.

However, the use of password does not provide adequate protection against Internet fraud such as phishing. The problem with password is that when it has been compromised, the fraudsters can easily take full control of online transactions. In such cases, the password no longer works as an authentication taken because there is no surety of who is standing behind the customer and tracing the password. This new authentication factor would be very easy for the customers for better security and to freely access their accounts. The transaction which takes place would take hardly a few seconds to process and give out successful result. However, easy access and convenience should not be at the expense and mercy of the security of information. This is important in order to ensure the confidentiality of information and that it is not being manipulated or compromised by the fraudsters. Hence this software has the higher security then the present working system.

V. CONCLUSION

Internet Banking Anti-Phisher is a useful application. It provides more security then any of the present working system. It provides more security by providing two factor authentications i.e. one by checking login id and password and other by using email id verification and the image verification. By using the MD5 algorithm system can generate unique code by encrypting the code and sending in image. This provides more and more security and anti-phishing for the internet banking. Thus to give more security to the customers by implementing it to present working system was the main goal of this project.

ACKNOWLEDGMENT

We wish to express our gratitude to our principal Mr.V.C.kotak for allowing us work with this project and giving us the chance to explore this domain. We would also like to thank our Head of Department Mrs. Swati Deshpande for our constant encouragement and support towards achieving this goal.

We would also like to thank the Review Committee for their invaluable suggestions and feedback without whom our work would have been very difficult.

We take this opportunity to express our thankfulness and deep regards to our guide Prof. SmitaBansod for her continuous guidance, monitoring and constant encouragement throughout the working of this project. Her time to time constant guidance shall help us in every aspect of our lives.

We would like mention our college teachers, who have already mastered or expertise in this domain helped us throughout the project. Without their blessings and correct path guidance the project would not been completed.

We would like to thank our parents and friends for their support throughout the project.

REFERENCES

[1] M.Arathi, Jagan Naidu, " Securing transaction using two factor authenticaton",international Journal of andvances in Engineering and Applied Science(IJAEAS)vol-1 Iss-1,Feb2014

[2] Rahul kale, Neha Gore, "Two factor authentication using mobile phone", International journal of innovative & studies, Vol2 Iss-5, May2013. www.ijirs.com

[3] Alain Hiltgen, Thorsten Kramp and Thomas Weigold,"Secure Internet Banking Authentication", Published By The IEEE Computer Society 1540-7993/06/$20.00 © 2006 IEEE

[4] PetrHanaeek, KamilMalinka& Jiri Schafer Brno University of Technology, "e-Banking Security- A Comparative Study", IEEE A&E SYSTEMS MAGAZINE, January 2010

[5] NeeteshSaxena, Member, IEEE, and Narendra S. Chaudhari, Senior Member, IEEE, "EasySMS: A Protocol for End-to-End Secure Transmission of SMS", IEEE Transactions on Information Forensics And Security, Vol. 9, No. 7, July 2014

[6] "Survey of steganography", 1556-6013 © 2014 IEEE.

[7] BablooSaha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No. 1, January 2012.