BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 63, No. 2, 2015
DOI: 10.1515/bpasts-2015-0062

Analysis of QKD multifactor authentication in online banking systems

A. SHARMA* and S.K. LENKA

Faculty of Engineering and Technology, FET, Mody University of Science and Technology, MUST, Lakshmangarh, Sikar, Rajasthan, 332311 India

Abstract. In the present scenario internet usage and the online banking sectors are experiencing spectacular growth. The Internet is the fastest growing banking channel today, both in the fields of corporate and retail banking. Banks prefer their customers to use the online banking facility as it reduces their cost, primarily through labour costs. The online banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. Online fraud has become major source of revenue for criminals all over the globe. The challenges that oppose online banking are the concerns of security and privacy of information. This has made detecting and preventing these activities a top priority for every major bank. The use of single-factor authentication, such as a user name and the password, has been inadequate for guarding against account fraud and identity theft, in sensitive online banking systems. In this paper we are going to analyze the QKD multifactor authentication in online banking systems.

Key words: online banking, authentication, multi-factor authentication, quantum cryptography, QKD, security.

1. Introduction

Online banking that allows people to interact with their banking accounts via the Internet from virtually anywhere in the world provides enormous benefits to consumers in terms of the ease and cost of transactions. This online banking system permits consumers to request information and carry out most of banking services such as balance reports, inter-account transfers, and bill payment. This means that online banking has a very large potential for use since many people expect that electronic checks will substitute paper checks. While online banking offers enormous advantages and opportunities, it faces different kinds of risks that are specific to conduct sensitive business over the Internet. The online banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The basic architecture of online banking system consists of three major components

- User
- Application server
- Database, which stores user and bank data.

Since online banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The use of online banking systems has brought many concerns from different perspectives: government, businesses, banks, individuals and technology.

By strengthening the privacy technology, this ensures the secrecy of user's personal information and further enhance the security of the transactions. The examples of the private information relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place. Presently, online banking users only need a computer with access to the Internet to use online banking services. Users can access their banking accounts from anywhere in the world. Each user is provided a login ID and a password to access the service. It is indeed easy and convenient for users.

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 token because we cannot be sure who is behind the keyboard typing that password in.

Authentication aims to prevent fraudsters from accessing online banking accounts that do not belong to them, and subsequently viewing confidential information, causing malicious damage and stealing funds. In general, the solutions to the online banking authentication issues require the use of multifactor authentication mechanism.

In this paper we first discussed the motivations and ventures in online banking. Secondly, it talks about the multifactor authentication. Thirdly, this paper discusses the Quantum Cryptography concept used for multi-factor authentication in online banking systems. Fourthly, the security issue and attacks are also discussed, with analysis of Quantum Key Distribution (QKD) and finally the conclusions with some thoughts.

2. Multi-factor authentication

The process by which a user proves his association with an electronic identity to a computing system is called authen-

*e-mail: anand_glee@yahoo.co.in

tication. An authentication factor is used to produce some evidence that an entity at the end of the communication channel is the one which it claims to be. Authentication factors are grouped into classes according to how they are linked to their owners. Authentication keys are called multi-factor when they use more than one of the factors of authentication. Traditionally, all authentication mechanisms can be placed into one of the following three categories:

- Something you know – a secret, such as a password.
- Something you are – a biometric, such as a fingerprint.
- Something you have – a device or object or some kind, such as a credit card.

Multi-factor authentication is either two-factor or three-factor. Note that using two types of the same factor is not multi-factor authentication. For example, a password and personal information are both what you know, so using them together would still be single-factor authentication. In a multi-factor authentication, multiple authentication secrets of complementary natures, such as a long-term password and a one-time response value, are combined securely to provide mutual authentication. Multi-Factor Authentication provides very strong protection for secure communication and has been recommended by many banking systems for use in highly sensitive banking services. The authentication secrets must be combined so that the user can convince the bank-server that he knows all the authentication secrets and that the bank - server can convince the user that it knows all the authentication secrets: this provides mutual authentication.

Multi-factor authentication can improve security. However, this usually comes with an increase in cost and system complexity. For these reasons, the authentication key must be selected based on the risks to be addressed.It should be taken care that the multi-factor authentication mechanisms chosen should be interoperable,reliable, scalable for future growth, and readily accepted by the user.

3. Quantum cryptography for Multi-Factor Authentication

Previously we have proposed a Quantum cryptography authentication mechanism for multi-factor authentication in online banking system [1]. In that system we have proposed an authentication mechanism as follows:

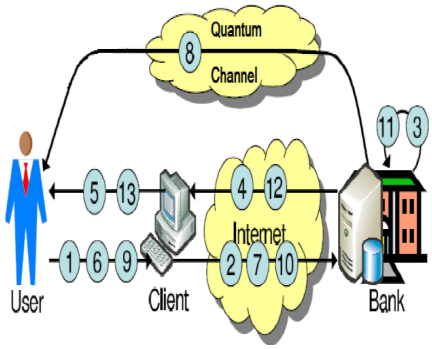

Fig. 1. User authentication through quantum cryptography: source (after Ref. 1)

Here we are having step by step scheme for our proposed authentication mechanism. In this proposed model we have introduced quantum cryptography concept for authentication. Figure 1 shows the steps for authentication. The two levels of authentication we have used in an online banking system to stronger the authentication.

1. Produce Login Id and Pass-code
2. Transmit Login Id and Pass-code
3. Verify Login Id and Pass-code
4. Transmit service options
5. Present service options
6. Transaction request
7. Transmit transaction request
8. Quantum Key Distribution
9. Produce Quantum code
10. Transmit Quantum code
11. Verify Quantum code
12. Transmit transaction confirmation
13. Present transaction confirmation

This scheme of authentication is an enhancement of the standard authentication scheme which authenticates the customer to the online banking system. Strength of this Quantum authentication is that it allows the user to have a higher level of trust in any communication they receive from the banks and it allows users to feel safe when logging into their accounts.

4. Security attacks and analysis

In parallel with this growth in attack volume, there has been a parallel rise in the variety and complexity of attacks. Banking security experts must now be familiar with a bewildering, array of techniques and terminology: phishing, pharming, spear phishing, session hijack, man-in-the-middle, man-in-the-browser, Trojans, Rock Phish... the list goes on.

4.1. User fraud attacks. Where the user deliberately compromises his or her authentication key or computing environment to enable them to deny subsequent authentication events.

4.2. Eavesdropper attacks. Where an attacker obtains information from an authentication exchange and recovers data, such as authentication key values, which then may be used to authenticate.

4.3. Insider attacks. Where verifiers or systems managers deliberately compromise the authentication system or steal authentication keys or related data.

4.4. Key logger attacks. Malicious code or hardware attacks that capture keystrokes of a customer with the intention of obtaining any password typed in by the customer or other manually entered authentication key data.

4.5. Malicious code attacks. Attacks that are generally aimed at the customer's computing environment. They vary in their sophistication from simple key loggers to advanced

Trojan programs that can gain control of the customer's computer. Malicious code attacks may also be aimed at verifier systems.

4.6. Man-in-the-middle attacks. Where an attacker inserts himself between the customer and the verifier in an authentication exchange. The attacker attempts to authenticate by posing as the customer to the verifier and the verifier to the customer.

4.7. Password discovery attacks. This covers a variety of attacks, such as brute force, common password and dictionary attacks, which aim to determine a password. The attacker may try to guess a specific customer's password, try a few commonly used passwords against all customers, or use a pre-composed list of passwords to match against the password file, in their attempt to discover a legitimate password.

4.8. Phishing attacks. Social engineering attacks that use forged web pages, emails, or other electronic communications to convince the customer to reveal their password or other sensitive information to the attacker.

4.9. Replay attacks. Where the attacker records the data of a successful authentication and replays this information to attempt to falsely authenticate to the verifier.

4.10. Session hijacking attacks. Where the attacker takes over (hijacks) a session following successful authentication.

4.11. Shoulder-surfing attacks. Social engineering attacks specific to password systems where the attacker covertly observes the password when the customer enters it.

4.12. Social engineering attacks. Attacks that are aimed at obtaining authentication keys or data by fooling the customer into using an insecure authentication protocol, or into loading malicious code onto the customer's computer. Attacks may also be aimed at the verification process, for example by trying to trick help desk staff into accepting a false story.

4.13. Verifier impersonation attacks. Where the attacker impersonates the verifier to the customer to obtain authentication keys or data, which then may be used to authenticate falsely to the verifier.

Quantum Cryptography is a particularly good method for producing long random keys. Quantum Cryptography is often described by its proponents as "unconditionally secure" to emphasize its difference with computationally secure classical cryptographic protocols. Quantum Cryptography using Quantum Key Distribution is a new tool in the cryptography. It allows for secure key agreement over an untrusted channel where the output key is entirely independent from any input value, a task that is impossible using classical cryptography. A property of quantum key distribution is that a relatively short input can be used to generate perfectly secure random key material.

Any secure key agreement protocol must make a few minimal assumptions, for security cannot come from nothing: we must be able to identify and authenticate the communicating parties, we must be able to have some private location to perform local operations, and all parties must operate within the laws of physics. In QKD Multifactor Authentication a secret key is shared between user and Bank to authenticate the very first quantum exchange. They obtain some quantum states and measure them. They communicate to determine which of their measurement results could lead to secret key bits; some are discarded in a process called sifting because the measurement settings were incompatible. It has been shown that using part of the output of this QKD session to authenticate the user means that this communication is perfectly secure. They perform error correction and then estimate a security parameter which describes how much information an eavesdropper might have about their key data. After that they perform privacy amplification for the authentication purpose and got that final authentication for online banking transaction.

QKD is just one part of this overall information security infrastructure: two parties can agree upon a private key, the security of which depends on no computational assumptions, and which is entirely independent of any input to the protocol. Quantum key distribution does not remove the need for authentication: indeed, authentication is essential to the security of QKD, for otherwise it is easy to perform a man-in-the-middle attack. The unconditional security of QKD systems has been mathematically proven: even in the face of an adversary with infinite supplies of time and processing power, the security simply cannot be broken.

5. Conclusions

In this paper, we have analyzed a number of attacks for multifactor authentication and find that the use of QC/QKD for authentication is safe for online banking systems.

The introduction of additional authentication provides an added level of security. The QKD Multifactor authentication provides an effective protection against a wider variety of security threats without increasing the burden on the end user. This enables banks to implement much more effective security measures, reducing their financial risk of online banking threats without adding significant maintenance cost for the online transaction and other online applications. Banks, nevertheless, have a dilemma in introducing more layers of authentication as it leads to more difficulty for users in accessing and utilizing their bank accounts and services.

QKD does not eliminate the need for other cryptographic primitives, such as authentication, but it can be used to build systems with new security properties. Experimental research on quantum key distribution continues to improve the usability, rate, and distance of QKD systems, and the ability to provide and certify their physical security. As public key cryptography systems are retooled with new algorithms and standards over the coming years, there is an opportunity to incorporate QKD as a new tool offering fundamentally new security features. As experimental research continues, we

expect the costs and challenges of using QKD to decrease to the point where QKD systems can be deployed affordably and their behaviour can be certified.

REFERENCES

[1] A. Sharma and S.K. Lenka, "Authentication in online banking systems through quantum cryptography", *Int. J. Engineering and Technology* 5, 2696–2700 (2013).

[2] Federal Financial Institutions Examination Council, "Authentication in an internet banking environment." *FFIEC* 11, www.ffiec.gov/pdf/authentication_guidance.pdf (2008).

[3] *PCI Data Security Standard*, http://www.pcisecuritystandards.org/ (2010).

[4] *NIST Special Publication* 800-63, http://csrc.nist.gov/publications/ (2011).

[5] A. Sharma and S.K. Lenka "Authentication in online banking systems: quantum cryptography perspective", *Int. J. Engineering and Technology* 5, 561–564 (2014).

[6] D. Pointcheval and S. Zimmer, "Multi-factor authenticated key exchange", in *ACNS of LNCS* 5037, 277–295 (2008).

[7] D. Stebila, P. Udupi, and S. Chang, "Multi-factor password-authenticated key exchange", *Eighth Australasian Information Security Conf. AISC* 105, 56–66 (2010).

[8] C.H. Bennett, G. Bessette, G. Brassard, and L. Salvail, "Experimental quantum cryptography, advantages in cryptology", *Eurocrypt 90 Proc*. 1, 351–366 (1990).

[9] C.H. Bennett and G. Brassard, "Quantum cryptography: public key distribu-tion and coin tossing", *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* 1, 175–179 (1984).

[10] A. Sharma, Vibha Ojha, R.C. Belwal, and V. Goar "Quantum cryptography – the concept and challenges", *Proc. 2nd Int. Conf. Computer and Automation Engineering (ICCAE 2010)* 1, 710–714 (2010).

[11] A. Sharma and V. Ojha, and V. Goar, "Security aspect of quantum key distribution", *Int. J. Computer Applications* 2, 58–62 (2010).

[12] F. Nancy, "The final countdown – as the ffiec online banking authentication deadline looms, banks work through the confusion to select their solutions", *Bank Systems & Technology* 43, 11 (2006).

[13] B.-Britz, "FFIEC rules making a difference – javelin study finds more banks using multifactor authentication", *Bank Systems & Technology* 44, 17 (2007).

[14] C. Steve, "Read this before you take Multi-factor Plunge", *American Bankers Association, ABA Banking J.* 98, 54–55 (2006).

[15] G.S. Osho, "How technology is breaking traditional barriers in the banking industry: evidence from financial management perspective", *Eur. J. Economics, Finance and Administrative Sciences* 1, 15–21 (2008).

[16] Y.G Lee., "The influence of security and risk perception on the reuse of internet banking", *J. MIS Research* 17, 77–93 (2007).

[17] A.M. Aladwani, "Online banking: a field study of drivers, development challenges, and expectations", *Int. J. Information Management* 21, 213–225 (2001).

[18] J. Cleens, V. Dem, and J. Vandewalle, "On the security of today's online electronic banking systems", *J. Computers & Security* 21 (3), 257–269 (2002).