Authentication in Online Banking Systems: Quantum Cryptography Perspective

Anand Sharma, S.K.Lenka

Abstract— Online banking systems allows consumers to access their banking accounts, review most recent transactions, request a current statement, transfer funds, view current bank rates and product information and reorder checks. These services that are offered by online banking systems are changing and being improved because of the intense competition between the banks. The major concern in online-banking is security threat specially the user authentication. Banks use either symmetric cryptography or asymmetric cryptography for this but due to the advent of sophisticated technology and cryptanalysis techniques, security solutions are not unconditionally secure. Here in this paper we are going to analyze the use of quantum cryptography for the authentication purpose.

Index Terms— Authentication ,Online banking, Privacy, Quantum Cryptography, QKD, Quantum Mechanics, Security.

1 Introduction

THE online banking has triggered massive change in the commercial banking practices since it was first introduced as "home banking" services by the four major New York banks in 1981. While there are differing definitions related to online banking found in the literature, in this study, online banking refers to performing banking transactions using electronic medium. Online banking solutions have many features and capabilities in common but traditionally also have some features that are application specific. The common features fall broadly into the following categories:

- ✓ Transactional
  - Payments to third parties, including bill payments and telegraphic/wire transfers.
  - Funds transfer between a customer's own transactional account and savings accounts.
  - Investments purchase or sale.
  - Loan applications and transactions such as repayments of enrolments.
- ✓ Non-transactional
  - Viewing recent transactions.
  - Downloading bank statements, for example in PDF format.
  - Viewing images of paying checks.
- ✓ Management of multiple users having varying levels of authority.
- ✓ Transaction approval services.

The various issues in online banking systems are as follows:

- confidentiality
- Integrity of communications;
- Non-repudiation of transactions;
- Data integrity;
- Authenticity of the parties involved in transactions;
- Protection of personal data;
- Bank secrecy;
- Traceability of transactions;
- Continuity of offered services to customer;
- Prevention, detection and monitoring of intrusion in the system;
- Restoration information system for managed and natural disasters and unforeseen events;
- Management of information system.

2 Security Attacks for Authentication

Here we are providing a list of attacks. An ideal password authentication should be secure against these attacks.

- The attacker may observe the communications channel.
- The attacker records messages he has observed and re-sends them at a later time.
- The attacker intercepts the messages sent between the user and bank server and replaces these with his own messages. He plays the role of the user in the messages which it sends to the bank server, and at the same time plays the role of the bank server in the messages that he sends to the user.
- The attacker impersonates the user or the bank server to get some useful information.
- The attacker is assumed to have access to a relatively small dictionary of words that likely includes the secret password.
- The attacker records past communications, then goes over the dictionary and deletes those words that are not consistent with the recorded communications from the dictionary. After several tries, the attacker's dictionary could become very small.
- An additional attack method targets a specific account and submits passwords until the correct password is discovered.
- Some attacks depend on patience, waiting until the logged-in workstation is unattended.

- *Anand Sharma is currently pursuingPhD degree program in Faculty of Engineering and Technology of Mody Institute of Technology and Science, Lakshmangarh, Sikar, Rajasthan, India.
  E-mail: anand_glee@yahoo.co.in*
- *S.K.Lenka is Professorand Head of Department of IT inFaculty of Engineering and Technology of Mody Institute of Technology and Science, Lakshmangarh, Sikar, Rajasthan, India.
  E-mail: lenka.sarojkumar@gmail.com*

3 Authentication with Quantum Cryptography

The major concern in online-banking is security threat specially the user authentication. Banks use either symmetric cryptography or asymmetric cryptography for this but due to the advent of sophisticated technology and cryptanalysis techniques, security solutions are not unconditionally secure. Earlier we have proposed a QKD user authentication approach [1].

As Single factor authentication in online banking is no longer sufficient to protect accounts. The supplement suggests financial institutions incorporate multi-factor authentication for their higher risk transactions, such as cash management implementations. Multi-factor authentication requires the implementation of two types of access methodologies from the customer. Typically, it incorporates something the customer knows, such as an ID and password, and one of two other choices—something the customer has, a token, or something unique. Our proposed model explained in figure 1.

The starting point is the user’s request. In the event of a request, the user is redirected to authentication service, carrying with him/her some kind of Pass code or PIN. After verifying that pass code or PIN the user will access that Quantum cryptosystem. Quantum Cryptography (QC) / Quantum Key Distribution (QKD) involvement is needed only to authenticate.
Entities involved are the user, user’s pass-code/PIN and the quantum cryptosystem. The user submit user’s pass-code/PIN for the user authentication and then quantum cryptosystem is used for QKD user authentication.

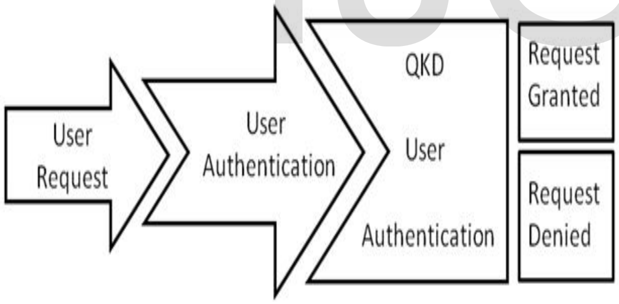

Fig1. Quantum Cryptography for User Authentication
Source: [1]

4 Authentication Issues With QC

Authentication allows user and bank to guard against authenticity of user and bank. That shows a user is communicating with right bank and its vice versa. QKD authentication must be performed on an ongoing basis after user authentication with pass code/ PIN given by bank. QKD does not remove the requirement for authentication: indeed, authentication is essential as a primary phase to the security of QKD. It described the authentication problem and sketched a solution to it based on quantum cryptography. This approach requires user and bank to already share a pass code/ PIN small secret key, which is given by bank to all its customers using online facility. Authentication in online banking environment consists of the following issues:

4.1 Security

Security of the transactions in online banking systems is the primary concern .Here the communicating parties (user and bank) must establish an authentic channel with unconditional security and use an unconditionally quantum cryptography algorithm. An unconditionally security is provided by only QKD. It ensures the highest security level of authentication because it is not possible for any third party to communicate in passive way. High security level of the QKD is ensured by means of the principles of the quantum mechanics. It meets this requirement in the best way – the quantum information is exchanged only between proper entities. In order to achieve high level of security for banking we are authenticating the user with QKD as well as normal authentication process. By combining a secure authentication scheme with a QKD authentication, user can produce a key exchange which gives a high level of security that can be established unconditionally, assuming only the validity of the laws of quantum physics. Most of attacks in online banking are based on deceiving the user to steal login data and valid pass code /PIN. By the use of QKD authentication we can easily avoid that attacks.

4.2 Privacy

The privacy of information may be one of the biggest concerns to the online banking users. Online banking users who most likely connect to the Internet via dial-up modem, Wi-Fi connection, or broadband connection are facing with a smaller risk of someone from the Internet gaining their information. The information that might be derived from the observation of network activities can be used by intruders against users or banks. Privacy directly ensures the secrecy of user’s personal information, bank details and further enhances the security of the transactions. When we have this requirement during system design process, we should consider the QKD authentication. It is designed to protect user’s account information and transaction details. Always when third party want to observe the quantum information, they change the quantum states and can be uncovered. The private information related to the online banking system is: the amount of the transaction, the date and time of the transaction, and the name of the user where the transaction is taking place. Like previous requirement – the QKD ensures the privacy by means of the principles of the quantum mechanics.

4.3 Transaction

Transaction directly shows the bank’s ability to deliver products or services. This transaction issue exists in each product and service offered. Transaction issues arise from fraud, processing errors and unauthenticated user anticipated events. A traditional bank can host meetings and call in experts to solve a specific issue. The transaction issue is mainly concern about the structure of the bank’s processing environment, including the types of authentication system, supporting technologies, services offered and the complexity of the processes. The key to controlling transaction issue lies in QKD authentication. This action means that user will be able to use their bank account to conduct transactions in online banking system as securely and easily as they use in traditional banking. QKD authentication controls, in particular, become more significant requiring additional authentication, processes, tools, expertise, and testing. The main concerns for the transaction include not only ensuring the safe transaction, but also prove the authenticity which both the user and the bank are the ones they claim to be. QKD authentication ensures the confidentiality and the authenticity of the transaction.

4.4 Performance

Performance is the overall feature of the online banking systems which is inseparably from security. It is as important as security of the online banking system. Performance is the requirement which is usually directly felt by users. Performance of the QKD authentication has not be worse than other authentication tools like traditional authentication or single factor authentication.

5 Preliminary Belief

To use and have faith in QKD authentication we have to consider some preliminary beliefs.

5.1 Quantum Mechanics is Correct

This belief shows that any third party involvement be detected and bounded by the laws of quantum mechanics, although within this realm there are no further restrictions beyond the unauthenticated user's inability to access the devices. In particular, we allow the unauthenticated user to have arbitrarily large quantum computing technology, far more powerful than the current state of the art. Quantum mechanics has been tested experimentally for nearly a century, to very high precision.

5.2 Our Devices Are Secure

Development of QKD authentication system that is verifiably secure is a substantial engineering challenge that researchers are still working on. Although the first prototype QKD system leaked key information over a side channel, it made different noises depending on the photon polarization, and thus the "prototype was unconditionally secure against any eavesdropper who happened to be deaf", experimental cryptanalysis leads to better theoretical and practical security. More sophisticated side-channel attacks continue to be proposed against particular implementations of existing systems, but so too are better theoretical methods being proposed, such as the decoy state method. Device-independent security proofs aim to minimize the security assumptions on physical devices. It seems reasonable to expect that further theoretical and engineering advances will eventually bring us devices which have strong arguments and few assumptions for their security.

6 Conclusion

Online banking is a highly profitable channel for Banks. It provides user's convenience and flexibility to use their accounts and various services at a lower cost than traditional branch banking. Online banking systems must authenticate users before granting them access to particular services. The need for stronger user authentication in an online banking environment has become necessary to ensure user security, privacy, transaction and overall performance. Quantum cryptography is often described by its proponents as "unconditionally secure" to emphasize its difference with computationally secure classical cryptographic protocols. In this paper, we analyzed the requirements of authentication from QKD point of view. We tried to show the issues which indicate that the QKD authentication will be really a good solution as multifactor authentication.

References

[1] Anand Sharma. S.K. Lenka, "Authentication in Online Banking Systems through Quantum Cryptography", International Journal of Engineering and Technology, Vol 5 No 3, pp. 2696-2700, 2013.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York), pp. 175–179, 1984.

[3] C.H. Bennett, G. Bessette, G. Brassard, L. Salvail, and 1. Smolin, "Experimental quantum cryptography", Advantages in Cryptology Eurocrypt '90 Proceedings, pages 351-366, May 1990.

[4] Anand Sharma, Vibha Ojha, Vishal Goar "Security Aspect of Quantum Key Distribution" in International Journal of Computer Applications, Volume 2 – No.2, pp. 58-62 , May 2010.

[5] Osho, G.S., "How technology is breaking traditional barriers in the banking industry: Evidence from financial management perspective." European Journal of Economics, Finance and Administrative Sciences(11), p. 15-21, 2008,

[6] A.M. Aladwani, "Online banking: a field study of drivers, development challenges, and expectations", International Journal of Information Management 21 213-225, 2001.

[7] K. B. Bignell "Authentication in an Internet Banking Environment; Towards Developing a Strategy for Fraud Detection." In: Proceedings of the International Conference on Internet Surveillance and Protection. IEEE Computer Society 2006

[8] C.S. Elizabeth Daniel, "On-line Banking: Strategic and Management Challenges", Long Range Planning 30 890-898, 1997.

[9] Muller, 1. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than lkm", Europhysics Letters, 23:383-388, August 1993.

[10] Anand Sharma, Vibha Ojha, R.C.Belwal, Vishal Goar "Quantum cryptography – The Concept and challenges" in proceeding of 2nd International Conference on Computer and Automation Engineering (ICCAE 2010) Singapore, volume 1, pp. 710-714, 2010.

[11] Lee Y. G., "The influence of security and risk perception on the reuse of internet banking", The Journal of MIS Research, Vol.17, No.1, , pp.77-93, 2007.

[12] Anand Sharma, Vibha Ojha, R.C.Belwal, Gaurav Agarwal "Transmission and System Control in Quantum Cryptography" International Journal of Computer Technology and Applications. Volume 2 (3) pp. 590-593, 2011.

[13] Gilles Brassard. "Brief history of quantum cryptography: A personal perspective." In IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security 2005, pp. 19–23. IEEE, 2005. DOI:10.1109/ITWTPI.2005.1543949. EPRINT arXiv:quant-ph/0604072.

[14] Suh, B. and I. Han, "Effect of trust on customer acceptance of Internet banking", Electronic Commerce Research and Applications, Vol.1, pp.247-263, 2002

[15] onathan Barrett, Lucien Hardy, and Adrian Kent. "No signaling and quantum key distribution." Physical Review Letters, 95(1):010503, 2005. DOI:10.1103/PhysRevLett.95.010503. EPRINT arXiv:quantph /0405101.

[16] Yu I. and So S. H., "An empirical study on the factors influencing the usage intention of internet banking systems", The Journal of Industrial Economic

Research, Vol.17, No.6, pp.2383-2404, 2004.

[17] M. Quaddus, D. Achjari, “A model for electronic commerce success”, telecommunications policy, 127-151, 2005.

[18] M. Pohjola, “The New Economy: Facts, Impacts and Policies,” Information Economics and Policy, 14, pp. 133–144, 2002.

[19] C.S. Yiua, K. Grantc, D. Edgar, “Factors affecting the adoption of Internet Banking in Hong Kong—implications for the banking sector”, International Journal of Information Management 27 , 336-351, 2007.

[20] C.S. Elizabeth Daniel, “On-line Banking: Strategic and Management Challenges”, Long Range Planning 30 890-898, 1997.

[21] B. H. Wixom and P. A. Todd, “A theoretical integration of user satisfaction and technology acceptance,” Information System Research, vol. 12, no. 1, pp. 85-102, 2005.