International Journal of Information & Network Security (IJINS)
Vol.2, No.3, June 2013, pp. 203~206
ISSN: 2089-3299

Quantum password sharing scheme using trusted servers

Gabriela Mogos*,
* Department of Computer Science, Stefan Procopiu Technical College, Romania
Departement of Electrical and Computer Engineering, University of Oradea, Romania

Article Info

Article history:

Received Nov 23th, 2012
Accepted Dec 28th, 2012

Keyword:

Quantum computing
Quantum security
Secret sharing

ABSTRACT

The main purpose of the sharing schemes based on trusted servers is to obtain a password. The threshold cryptography aims the secret cryptographic protection, and is based on the distribution of the key on several servers, with the purpose to tolerate the attacks. In this work I will present a quantum version of the password sharing protocol, using a number *n* of trustful servers, to assure its security. The model I propose approaches the issue of the distribution of the authentication key between a client and *n-1* servers.

Corresponding Author:

Gabriela Mogos,
Department of Computer Science,
Stefan Procopiu Technical College,
Calea Chisinaului 132bis, Iasi, 700179, Romania.
Email: gabi.mogos@gmail.com

1. INTRODUCTION

Many of today's real world systems are based on password authentication in order to verify the identity of a user before allowing the user to realise certain functions, as the creation of a private virtual network or downloading secret information. There are many concerns related to the security associated to the authentication password, mainly due to the fact that most of the users' passwords are extracted from a rather small and easily generated dictionary. Consequently, when the information is sufficient in order to verify if an alleged password leaked, the password can be found by realising an offline dictionary attack: a dictionary can be searched for possible passwords, with the purpose to determine the right password.

When the authentication password is realised through a network, no leak of information should be allowed for the intruders, or for those who attack the network actively. This was worked out after SSL was provided with a secured channel to prevent the leak of information. The problem becomes more difficult when the public server key cannot be verified by the user. Authentication protocols with strong password were invented to solve this problem. They have the property that the probability of an active attacker (for example, an intruder who would insert, erase, or modify the messages in a network could pretend he is a user) is negligible as compared to a simple attack of on-line guessing type, where the intruder is guessing passwords iteratively, as well as the functioning of the authentication protocol.

The research related to authentication password protocols resisting to offline attacks started with the work of Bellovin and Merritt. A formal model was proposed by Halevi and Krawczyk, who developed a secured protocol applicable when the authentication server has a certified public key, known by the client. The first security protocol (and the only one known at present) which does not use any further configuration is the one proposed by Goldreich and Lindell. This protocol is based on general hypotheses (trapdoor permutations), and should be regarded as a proof of feasibility of obtaining the password. Unfortunately, it is very inefficient, and it cannot be used in practice.

Ford and Kaliski introduced the idea of sharing the information of the password by several servers, with the purpose to prevent the leak of the passwords to an attacker who would be capable to enter the authentication server. They present a solution of *n-out-of-n* solutions, i.e. the password is shared by *n* servers

and all these should cooperate to authenticate the user. Though this solution guarantees that the password is secured against an attacker who breaks *n-1* servers, it is also tolerating less the random defects.

Jakobsson, MacKenzie and Shrimpton presented a password authentication protocol, with *t-out-of-n* threshold, demonstrating the security through a random model of an oracle.

In this paper I will present a quantum version of the password sharing protocol, using a number *n* of trustful servers, to assure its security. The model I propose approaches the issue of the distribution of the authentication key between a client and *n-1* servers. The purpose is that, when the client engages himself in an authentication protocol, he can obtain the authentication key by putting together all the *n-1* sub-keys distributed along with the one he has. Any *n-2* servers would conspire together, and finding the password would be impossible.

2. QUANTUM PASSWORD SHARING

The secret sharing was proposed for the first time by Blakley et al in 1979. The easiest way to describe it is as a secret shared by the sender in two parts for two receivers. The secret can be reconstructed only if both receivers act together, having either no knowledge about the original message. In 1999, this concept was generalized for the quantum case by Hillery, Buzek and Berthiaume, who introduced the notion of quantum secret sharing (Q.S.S.). Quantum secret sharing plays an important role in the protection of secret quantum information. The last scheme of secret sharing was introduced by Lance et al in 2004, and is called quantum state sharing (Q.ST.S). In 1999 it was presented the first scheme, using the three-qubit or four-qubit state Greenberger-Horne-Zeilinger (GHZ) for sharing securely an unknown random single-qubit state. Later, Cleve et al described the general case of the scheme. In 2000, Bandyopadhyay proposed a new Q.St.S. scheme, using optimal methods, and in 2003, Hsu proposed another method based on Grover's algorithm. In conclusion, all these methods are analysing the case of a single-particle qubit or multi-particle qubit state.

The distribution scheme of the authentication key between a client and *n-1* servers also has applicability in the quantum case, starting from the quantum secret sharing scheme among *n* participants.

The authentication key is made of *n* qubits prepared in quantum state with maximal entanglement, or, in other words, in a GHZ state. This is emitted by an Authentication Centre, and for surety, it distributes parts of the password to *n-1* servers, and for the authentication, the client will receive a single qubit.

The multiple GHZ state is as follows:

$$\left|\Psi\right\rangle_{GHZ} = \frac{1}{\sqrt{2}}(\left|000...0\right\rangle + \left|111..1\right\rangle)$$

We will use a sequence $b_1(j), b_2(j), ..., b_n(j)$ to note the measurement bases of the information for client, server1, ... for the *j* state of GHZ.

The number 1 is client's particle, the number 2 server2's particle, and so on.

In general, in order to establish the password sharing scheme, we need to realise a detailed table containing all the possible combinations of the measurement bases, and the possible results for all the parts. When the number of participants is high, the realisation of such a table is very difficult, and difficult to use.

If $b_i(j) = 0$, then for the *i* group it is used the *x* basis, and *if* $b_i(j) = 1$, it means that the *i* group uses the *y* axis.

The component $\left|00...0\right\rangle$ can be written:

$$\left|00...0\right\rangle = \prod_{i=1}^{n}(\sqrt{\frac{1}{2}}(\left|0\right\rangle_{b_i} + \left|1\right\rangle_{b_i}))$$

and the component $\left|11...1\right\rangle$:

$$\left|11...1\right\rangle = \prod_{i=1}^{n}(\frac{-i}{\sqrt{2}}(\left|0\right\rangle_{b_i} - \left|1\right\rangle_{b_i})$$

When the *y* basis is chosen by an odd number of servers, the representation of $\left|00...0\right\rangle$, can be extended as follows:

$$\left|11...1\right\rangle = \frac{\pm i}{(\sqrt{2})^n}\prod_{i=1}^{n}(\left|0\right\rangle_{b_i} - \left|1\right\rangle_{b_i})$$

where the sign "+" is for $n = 2k + 1$ and the sign "-" is for $n = 4k + 1$, where *k* is integer and positive. The GHZ state can be re-written:

$$|\Psi\rangle = \frac{\pm i}{(\sqrt{2})^{n+1}} \prod_{i=1}^{n} (|0\rangle_{b_i} + |1\rangle_{b_i}) \pm i \prod_{i=1}^{n} (|0\rangle_{b_i} - |1\rangle_{b_i})$$

for an odd number of servers who choose the *y* basis. In other words, for a set of measured values $i_2,...,i_n$ in the bases $b_2,...,b_n$ by the server1, server2 and so on, the results of client's measurements will have two alternatives.

If the number of the parties choosing the y basis is equal, then:

$$|\Psi\rangle = \frac{\pm i}{(\sqrt{2})^{n+1}} \prod_{i=1}^{n} (|0\rangle_{b_i} + |1\rangle_{b_i}) \pm i \prod_{i=1}^{n} (|0\rangle_{b_i} - |1\rangle_{b_i})$$

Due to the fact that some terms from the second product have negative sign, they are cancelling each other with the terms from the first product, obtaining only the terms 2^{n-1}. Among the terms 2^{n-1}, the values of the first bit, the result of client's measurement is uniquely determined by the *n-1* values remained. In this case, when *n − 1* parties are gathered together, and the result is measured, they can determine uniquely the value of client's bit. If not all the *n − 1* servers are present, the determination of the value of client's bit is impossible.

To conclude, the general rules for secret sharing among *n* parties are as follows:

1. The number of parties using the same basis must be equal;

2. When the number of parties using the *y* basis is equal to *2(2k +1)*, where *k* - is a non-negative integer, the value of client's bit is the sum modulo 2 of the bit values of the *n-1* parties, plus 1:

$$i_{Alice} = i_1 = i_2 \oplus i_3 \oplus ... \oplus i_n \oplus 1$$

3. When the number of parties choosing the *y* basis is *4k*, then the value of client's bit is the sum modulo 2 of the bit values of the *n − 1* parties:

$$i_{Alice} = i_1 = i_2 \oplus i_3 \oplus ... \oplus i_n$$

The scheme of password sharing for *n* parties is as follows:

1. The client and the Authentication Centre prepare the GHZ state of the *n* particles;

2. The client keeps a particle and sends the rest *n − 1* particles to the *n* − 1 servers, receiving each one particle;

3. Each party chooses randomly one of the *x* or *y* measurement bases to measure the particle. They keep the measurement result and the information related to the measurement basis they used.

4. The procedures 1 − 3 are repeated several times until a sufficient number of results were obtained. This could be at least twice the desired number of shared bits;

5. After the procedure 4, every server, using a classical communication channel, sends information to client and Centre regarding the measurement basis they chose. The client together with the Center counts the number of parties that have chosen the y basis.

The client announces publicly the nature of this number for each round: an odd or even number of the form *2(2k + 1),* or an even number of the form *4k.* The exact number of *k* must not be revealed.

If the number is odd, then this round of measurements is cancelled, and if the number is even, all the participants will keep the values they measured, as well as the information concerning the basis used in this case.

6. The client selects a sufficiently big set of such cases, and asks the servers to reveal the measurement results. This information is necessary in order to determine the existence of potential intruders. If the error ratio is high, client concludes that there are intruders, and the session is cancelled. If the error ratio is low, the session of is considered secure, obtaining in the end, the row of bits of the authentication password.

3. THE PRESENCE OF INTRUDERS

An intruder can attack from inside and outside.

External attack - if an intruder captures and measures parts of the password, this will lead to the destruction of the correlation of the three GHZ particles. The client and the Center will realize this at the end of the process, when servers reveal publicly the parts in their possession.

Internal attack- can happen when one or more servers become untrustworthy, this can be found easy at the end of the process when the client reconstructs the password.

4. CONCLUSION

The integration of quantum techniques bring an advantage in what concerns the security of the method, the no-cloning theorem, and the principle of irreversibility of quantum systems measurement, guaranteeing for it. The main purpose of the methode based on quantum password sharing is the fact that it offers a different conceptual way to solve some of the problems related to client-server authentication. The advantages consist in the improvement of the efficiency of the classical authentication methodes, the detection of the intruders implying the comparison of a smaller number of bits as compared to the high probability that the intruder modifies the result expected by the parties involved in communication.

ACKNOWLEDGEMENTS

This work was cofinanced from the European Social Fund through Sectoral Operational Programme Human Resources Development 2007-2013, project number POSDRU/89/1.5/S/56287 "*Postdoctoral research programs at the forefront of excellence in Information Society technologies and developing products and innovative processes*", partner University of Oradea.

REFERENCES

[1] D. C. Feldmeier, P. R. Karn – UNIX Password Security – Ten Years Later, Advances in Cryptology – CRYPTO '89, Springer-Verlag, Berlin, 1990
[2] D. V. Klein – "Foiling the Cracker": A Survey of, and Improvements to, Password Security, Proceedings of the USENIX UNIX Security II Symposium, USENIX Association, Berkeley, 1990
[3] M. Burrows, M. Abadi, R. Needham – "*A Logic of Authentication*", ACM Operating Systems Review, Vol. 23, 1989
[4] L. Gong, R. Needham, R. Yahalom – "*GNY Logic Fill In*", Proceedings of the IEEE Symposium on Security and Privacy, 1990
[5] L.Xiao, G.L.Long, F.-G.Deng, J.W.Pan, *Efficient Multi-Party Quantum Secret Sharing Schemes*, Phys. Rev. A 69, 052307, 2004
[6] W. Ford and B. S. Kaliski, *Server-assisted generation of a strong secret from a password*, Proceedings of The 5th IEEE International Workshop on Enterprise Security, 2000
[7] M.A.Nielsen and I.L.Chuang, Quantum Computation and Quantum Information, UK, 2000.

BIOGRAPHY OF AUTHOR

Gabriela Mogos . Postdoctoral studies, Area of Specialization: Informatics, *University of Oradea*, Romania, 2010 – present. She holds Ph.D. in Computer Science, Area of Specialization: Informatics, M.Sc. in Computer Science from and B.Sc. in Physics, Area of Specialization: Solid-State Physics, Al.I. Cuza University, Iasi, Romania