COMPATIBLE RESILIENT TWO SERVER PASSWORD AUTHENTICATION WITH TRADITIONAL SINGLE SERVER

T.S.Thangavel,
Assistant Professor, Department of M.Sc(IT),
K.S.Rangasamy College of Technology,
Tiruchengode – 637 215

Dr. A. Krishnan,
Dean
K.S.Rangasamy College of Technology,
Tiruchengode – 637 215

ABSTRACT

The authentication systems which uses passwords to authenticate their systems stores their password in a central server which is easily prone to attack and if they are being compromised by the intruder, it is possible for the intruder to obtain the password and gain access to the contents of the user. To overcome this problem, the multi-server systems were being proposed in which the user has to communicate in parallel with several or all of the servers for the purpose of authentication. Such system requires a large communication bandwidth and needs for synchronization at the user. The system is not easy to deploy and maintain or it requires the protocols which are quite expensive.

To overcome these problems the two server authentication system is being proposed which uses only the passwords and the session keys rather than performing any cryptographic techniques. The system consists of two servers, the front end service server which interacts directly to the user and the back end control server which is only visible to the service server. The users contact only the service server but these two servers are responsible for the authentication of the user. The user has a password which is transformed into two long secrets which are held by service server and control server. Both the system using their respective shares validate user during the login. The system also overcomes the online and offline dictionary attacks that are prevailing in the single and multi-server systems. The system is particularly suitable for resource-constrained users due to its efficiency in terms of both computation and communication. It is also possible for the servers to associate with multiple clients. The system is compatible with the single server systems that are available today such as FTP and web application.

Keywords **-** Password-Authentication, Two Servers password, Cryptosystem, Secure Password, Service sever, control server.

1. INTRODUCTION

The multi-user systems require the users to provide their passwords along with their user identification. The password serves to authenticate the ID of the individual logging on to the system. This is required to determine if the user is authorized to gain access to the system. This ID also determines the privileges accorded to the user. The short secrets are convenient, particularly for an increasingly mobile user population. Many users are interested in employing a variety of computing devices with different forms of connectivity and different software platforms. Such users often find it convenient to authenticate by means of passwords and short secrets, to recover lost passwords by answering questions, and to make similar use of relatively weak secrets.

Most password-based user authentication systems place total trust on the authentication server where passwords or easily derived password verification data are stored in a central database. These systems could be easily compromised by offline dictionary attacks initiated at the server side. Compromise of the authentication server by either outsiders or insiders subjects all user passwords to exposure and may have serious problems. To overcome these problems in the single server system many of the systems has been proposed such as multi-server systems, public key cryptography and password systems, threshold password authentication systems, two server password authentication systems.

The proposed work continues the line of research on the two-server paradigm in [10], [11], extend the model by imposing different levels of trust upon the two servers, and adopt a very different method at the technical level in the protocol design. As a result, we propose a practical two-server password authentication and key exchange system that is secure against offline dictionary attacks by servers when they are controlled by adversaries. The proposed scheme is a password-only system in the sense that it requires no public key cryptosystem and, thus, no PKI. This makes the system very attractive considering PKIs are proven notoriously expensive to deploy in real world. Moreover, the proposed system is particularly

suitable for resource constrained users due to its efficiency in terms of both computation and communication. The paper work, generalize the basic two-server model to architecture of a single back-end server supporting multiple front-end servers and envision interesting applications in federated enterprises.

2. LITERATURE REVIEW

Public key techniques are absolutely necessary to make password systems secure against offline dictionary attacks, whereas the involvement of public key cryptosystems under a PKI (e.g., public key encryption and digital signature schemes) is not essential. There are two separate approaches to the development of secure password systems one is a combined use of a password and public key cryptosystem under a PKI, and the other is a password only approach. In these systems, the use of public keys entails the deployment and maintenance of a PKI for public key certification and adds to users the burden of checking key validity. To eliminate this drawback, password-only protocols (password authenticated key exchange or PAKE) have been extensively studied, e.g., [2], [3], [4]. The PAKE protocols do not involve any public key cryptosystem under a PKI and, therefore, are much more attractive for real-world applications. Any use of public key cryptosystem under a PKI in a password authentication system should be avoided since, otherwise, the benefits brought by the use of password would be counteracted to a great extent.

Most of the existing password systems were designed over a single server, where each user shares a password or some password verification data (PVD) with a single authentication server (e.g., [2], [3], [4]). These systems are essentially intended to defeat offline dictionary attacks by outside attackers and assume that the sever is completely trusted in protecting the user password database. Unfortunately, attackers in practice take on a variety of forms, such as hackers, viruses, worms, accidents, mis-configurations, and disgruntled system administrators. As a result, no security measures and precautions can guarantee that a system will never be penetrated. Once an authentication server is compromised, all the user passwords or PVD fall in the hands of the attackers, who are definitely effective in offline dictionary attacks against the user passwords. To eliminate this single point of vulnerability inherent in the single-server systems, password systems based on multiple servers were proposed. The principle is distributing the password database as well as the authentication function to multiple servers so that an attacker is forced to compromise several servers to be successful in offline dictionary attacks.

The system in [6], believed to be the first multiserver password system, splits a password among multiple servers. However, the servers in [6] need to use public keys. An improved version of [6] was proposed in [7], which eliminates the use of public keys by the servers. Further and more rigorous extensions were due to [8], where the former built a t-out-of-n threshold PAKE protocol and provided a formal security proof under the random oracle model [5] and the latter presented two provably secure threshold PAKE protocols under the standard model. While the protocols are theoretically significant, they have low efficiency and high operational overhead. In these multi-server password systems, either the servers are equally exposed to the users and a user has to communicate in parallel with several or all servers for authentication, or a gateway is introduced between the users and the servers.

Recently, Brainard et al. [1] proposed a two-server password system in which one server exposes itself to users and the other is hidden from the public. While this two-server setting is interesting, it is not a password-only system: Both servers need to have public keys to protect the communication channels from users to servers. As we have stressed earlier, this makes it difficult to fully enjoy the benefits of a password system. In addition, the system in [1] only performs unilateral authentication and relies on the Secure Socket Layer (SSL) to establish a session key between a user and the front-end server. Subsequently, Yang et al. [9] extended and tailored this two-server system to the context of federated enterprises, where the back-end server is managed by an enterprise headquarter and each affiliating organization operates a front-end server. An improvement made in [9] is that only the back-end server holds a public key. Nevertheless, the system in [9 is still not a password-only system.

3. MODES OF SERVER PASSWORD AUTHENTICATION MODELS

In the single-server model, where a single server is involved and it keeps a database of user passwords. Most of the existing password systems follow this single-server model, but the single server results in a single point of vulnerability in terms of offline dictionary attacks against the user password database.

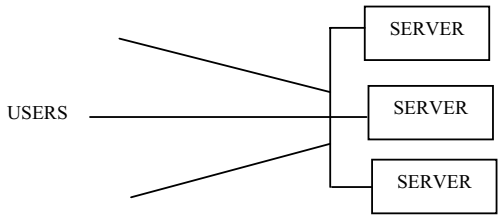


Figure 1. Multiple Server Password model

In the multi-server model as shown in Fig1, the server side comprises multiple servers for the purpose of removing the single point of vulnerability, the servers are equally exposed to users and a user has to communicate in parallel with several or all servers for authentication. The main problem with the plain multi-server model is the demand on communication bandwidth and the need for synchronization at the user side since a user has to engage in simultaneous communications with multiple servers. This may cause problems to resource-constrained mobile devices such as hand phones and PDAs.

Figure 2. Gateway Augmented Multi-server model

In the gateway augmented multi-server model as shown in Fig2, gateway is positioned as a relaying point between users and servers and a user only needs to contact the gateway. Apparently, the introduction of the gateway removes the demand of simultaneous communications by a user with multiple servers as in the plain multi-server model. However, the gateway introduces an additional layer in the architecture, which appears "redundant" since the purpose of the gateway is simply to relay messages between users and servers, and it does not in any way involve in service provision, authentication, and other security enforcements. From security perspective, more components generally imply more points of vulnerabilities.

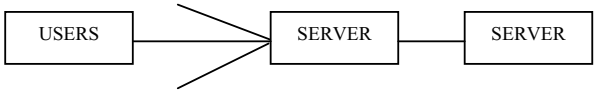


Figure 3. Two server model

The two-server model comprises two servers at the server side, one of which is a public server exposing itself to users and the other of which is a back-end server staying behind the scene; users contact only the public server, but the two servers work together to authenticate users. The differences between the two-server model and the earlier multi-server models are

a) In the two-server model, a user ends up establishing a session key only with the public server, and the role of the back-end server is merely to assist the public server in user authentication, while in the multi-server models, a user establishes a session key (either different or the same) with each of the servers.

b) From a security point of view, servers in the multi-server models are equally exposed to outside attackers (recall that the gateway in the gateway augmented multi-server model does not enforce security), while in the two-server model, only the public server faces such a problem. This improves the server side security and the overall system security in the two-server model.

In two server model, different levels of trust upon the two servers with respect to outside attackers can be made. The back-end server is more trustworthy than the public server. This is logical since the back-end server is located in the back-end and is hidden from the public, and it is thus less likely to be attacked. Two-server model has successfully eliminated drawbacks in the plain multi-server model (i.e., simultaneous communications between a user and multiple servers) and the gateway augmented multi-server model (i.e., redundancy) while allowing us to distribute user passwords and the authentication functionality to two servers in order to eliminate a single point of vulnerability in the single-server model. As a result, the two-server model appears to be a sound model for practical applications.

The existing systems upon the two-server model are not suffice, in turn motivated to present a password-only system over the two-server model. In the proposed system, the public server acts as a service server that provides application services, while the back-end server is a control server whose sole purpose is to assist the service server in user authentication (the service server, of course, also participates in user authentication). In the plain multi-server model and the gateway augmented multi-server model, several or all servers equally participate in service provision as well as user authentication, which is implied by the fact that a user negotiates a session key with each server. The two-server model is generalized to an architecture that a control server supports multiple service servers.

4. FUNCTIONAL ARCHITECTURE OF TWO SERVER PASSWORD AUTHENTICATION SYSTEM

Three types of entities are involved in our system, i.e., users, a service server (SS) that is the public server in the two server model, and a control server (CS) that is the back-end server. In this setting, users only communicate with SS

and do not necessarily know CS. For the purpose of user authentication, a user U has a password which is transformed into two long secrets, which are held by SS and CS, respectively. Based on their respective shares, SS and CS together validate users during user login. CS is controlled by a passive adversary and SS is controlled by an active adversary in terms of offline dictionary attacks to user passwords, but they do not collude (otherwise, it equates the single-server model).

A passive adversary follows honest-but-curious behavior, that is, it honestly executes the protocol according to the protocol specification and does not modify data, but it eavesdrops on communication channels, collects protocol transcripts and tries to derive user passwords from the transcripts, moreover, when an passive adversary controls a server, it knows all internal states of knowledge known to the server, including its private key (if any) and the shares of user passwords. In contrast, an active adversary can act arbitrarily in order to uncover user passwords. Besides, we assume a secret

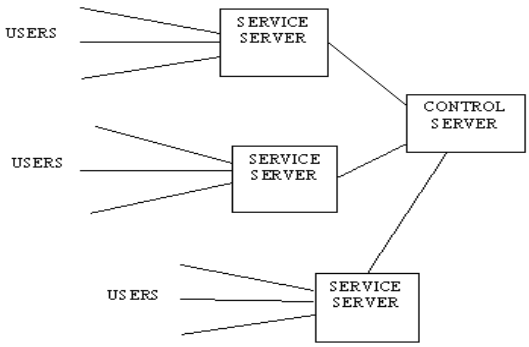
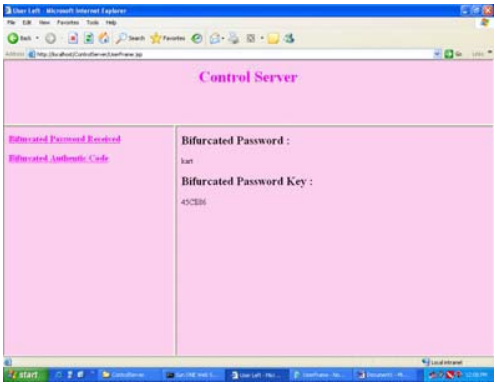


Figure 4. Generalized Two Server Architecture of a Single Control Server with Multiple Service Server

communication channel between SS and CS for this basic protocol. This security model exploits the different levels of trust upon the two servers. This holds with respect to outside attackers. As far as inside attackers are concerned, justifications come from our application and generalization of the system to the architecture of a single control server supporting multiple service servers, where the control server affords and deserves enforcing more stringent security measurements against inside attackers. The back-end server is strictly passive and is not allowed to eavesdrop on communication channels, while CS in our setting is allowed for eavesdropping.

5. EXPERIMENTAL RESULT AND DISCUSSIONS

The user contacts only the service server but both the control and service servers are responsible for the authentication of the user. The user has a password which is transformed into two long secrets which are held by service server and control server. Both the system using their respective shares validate user during the login. The servers compute function to verify the user and finally a session key is being established between the user and service server for the confirmation of the user and the server. The service server (Fig 6) which is an active adversary acts arbitrarily to uncover the passwords and could control the corruption of the password, the control server which is a passive adversary acts according to



the protocol specification. (Fig 5)

Figure 5. Control Server Key Generation for User Password (bifurcated)

In the offline dictionary attacks, where the successful logins between the user and the server is recorded by the intruder and it tries the passwords in the dictionary against login transcripts and this is overcome in the system by control server as passive adversary and service server as active adversary. In the system, the communication and the computations are more efficient. The user can use the same password to register to different service server, the service server connect either to distinct control servers or to the same control server. This is a highly desirable feature since it makes the system user friendly. The system could be adapted to any existing FTP and web applications that are available today by adding a control server to it where these are managed by the administrative domain.

In our experimental implementation, a password is split into two random numbers. Therefore, a user can use the same password to register to different service servers; they

connect either to distinct control servers or to the same control server. This is a highly desirable feature since it makes the system user friendly. A big inconvenience in the traditional password systems is that a user has to memorize different passwords for different applications. The system has no compatibility problem with the single-server model. This is of importance, as most of the existing password systems use a single server.

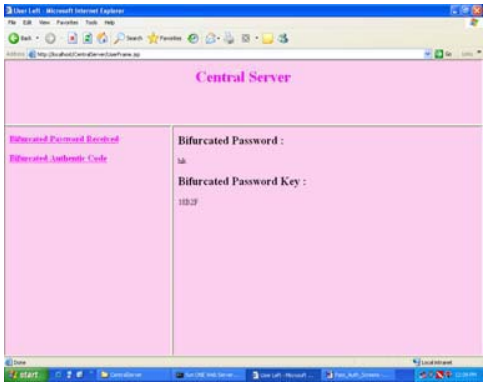


Figure 6. Service Server Key generation for user password (bifurcated)

The generalization as well as the applications of the two-server password system well support the underlying security model, in the sense that the enterprise headquarter naturally assume adequate funds and strong security expertise and, therefore, affords and is capable of maintaining a highly trustworthy control server against both inside attackers and outside attackers. Without the concern of a single point of vulnerability, affiliating organizations that operate service servers are offloaded to some extent from strict security management, so they can dedicate their limited expertise and resources to their core competencies and to enhancing service provision to the users. From the perspective of users, they are able to assume the higher creditability of the enterprise while engaging in business with individual affiliating organizations.

Performance Measure

The exponentiations dominate each party's computation overhead, the two server password authentication system only count the number of exponentiations as the computation performance. The digits before "/" denote the total number of exponentiations performed by each party, and the digits following "/" denote the number of exponentiations that can be computed offline. One round is a one-way transmission of messages. The proposed two protocols demonstrate performance quite efficient in terms of both computation and communication to all parties. Take U, for example, it needs to calculate 3 and 4 exponentiations in the two protocols, respectively, and 2 of them can be performed offline. This means U only computes 1 and 2 exponentiations in real time in the respective protocols, the communication overhead for U is particularly low in terms of both bits and rounds. The table 1 listed below indicates the computation performance in terms of time and success rate (number of rounds) of the two server password authentication and single server authentication

Table 1: Performance Measure on Two Server and Single Server Password Authentication Scheme

Scheme	Time of Authenticity	Success rate
	(milliseconds)	%
Two server password authentication	10	96
Single server	8	87

Discussions

With two-server password system, single point of vulnerability, is totally eliminated. Without compromising both servers, no attacker can find user passwords through offline dictionary attacks. The control server being isolated from the public, the chance for it being attacked is substantially minimized, thereby increasing the security of the overall system. The system is also resilient to offline dictionary attacks by outside attackers. This allows users to use easy to remember passwords and still have strong authentication and key exchange. The system has no compatibility problem with the single-server model. The generalization of the two-server password system well supports the underlying security model. In reality, adversaries take on a variety of forms and no security measures and precautions can guarantee that a system will never be penetrated. By avoiding a single point of vulnerability, it gives a system more time to react to attacks. The password-based authentication and key exchange system that is built upon a novel two-server model, where only one server communicates to users while the other server stays transparent to the public. Compared with previous solutions, our system possesses many advantages, such as the elimination of a single point of vulnerability, avoidance of PKI, and high efficiency.

6. CONCLUSION

The developed two-server password authentication architecture has control server and service server. The control server is controlled

by a passive adversary while the service server is controlled by an active adversary. A single point of vulnerability, as in the existing password systems, is totally eliminated. Without compromising both servers, no attacker can find user passwords through offline dictionary attacks. The control server being isolated from the public, the chance for it being attacked is substantially minimized, thereby increasing the security of the overall system. The system has no compatibility problem with the single-server model.

In the system, a password is split into two random numbers. Therefore, a user can use the same password to register to different service servers, they connect either to distinct control servers or to the same control server. This makes the system user friendly. The two-server password system well support the underlying security model, in the sense that the enterprise headquarter naturally assumes adequate funds and strong security expertise and, therefore, affords and is capable of maintaining a highly trustworthy control server against both inside attackers and outside attackers. The end users are able to assume the higher creditability of the enterprise while engaging in business with individual affiliating organizations. In contrast to existing multi-server password systems, the two server system has great potential for practical applications. It can be directly applied to fortify existing standard single-server password applications, e.g., FTP and Web applications.

REFERENCES

[1] J. Brainard, A. Juels, B. Kaliski, and M. Szydlo, "A New Two Server Approach for Authentication with Short Secrets," Proc. USENIX Security Symp., 2003.

[2] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password Based Protocols Secure against Dictionary Attacks," Proc. IEEE Symp. Research in Security and Privacy, pp. 72-84, 1992.

[3] S. Bellovin and M. Merritt, "Augmented Encrypted Key Exchange: A Password-Based Protocol Secure against Dictionary Attacks and Password File Compromise," Proc. ACM Conf. Computer and Comm. Security, pp. 244-250, 1993.

[4] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks," Advances in Cryptology (Eurocrypt '00), pp. 139-155, 2000.

[5] M. Bellare and P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. ACM Computer and Comm. Security, pp. 62-73, 1993.

[6] W. Ford and B.S. Kaliski Jr., "Server-Assisted Generation of a Strong Secret from a Password," Proc. IEEE Ninth Int'l Workshop Enabling Technologies, 2000.

[7] D.P. Jablon, "Password Authentication Using Multiple Servers," RSA Security Conf., pp. 344-360, 2001.

[8] P. Mackenzie, T. Shrimpton, and M. Jakobsson, "Threshold Password-Authenticated Key Exchange," Proc. Advances in Cryptology (Eurocrypt '02), pp. 385-400, 2002.

[9] Y.J. Yang, F. Bao, and R.H. Deng, "A New Architecture for Authentication and Key Exchange Using Password for Federated Enterprises," Proc. 20th Int'l Federation for Information Processing Int'l Information Security Conf. (SEC '05), 2005.

[10] Yanjiang Yang, Robert H. Deng, and Feng Bao, "A Practical Password-Based Two Server Authentication and Key Exchange System," IEEE Transaction on Secure and Dependable Computing,Vol.3, No.2,April-June 2006

BIOGRAPHY

T.S.Thangavel received the B.Sc., Degree in Computer Science (Bharathiyar University) in 1991 and the Msc Degree in computer science (Bharathidasan University) in 1993 and the Mphil Degree in Computer Science (Bharathidasan University) in 2003. He is pursuing the PhD Degree in department of science and humanities (Anna university). He is working as an assistant professor in MSc (IT) Department at K.S.Rangasamy College of Technology, Tiruchengode

Dr. A. Krishnan received his Ph.D degree in Electrical Engineering from IIT, Kanpur. He is now working as an Academic Dean at K.S.Rangasamy College of Technology, Tiruchengode and research guide at Anna University Chennai. His research interest includes Control system, Digital Filters, Power Electronics, Digital Signal processing, Communication Networks. He has been published more than 156 technical papers at various National / International Conference and journals.