Multi Server Authentication System using PKI and Kerberos

Parvathi R [1], Shanthi Saravanan[2], Sankar M [3]

1. Assistant Professor , Department of Information Technology,
PSNA College of Engineering and Technology, Dindigul,Tamilnadu,India.
2. Professor, Department of Computer Science and Engineering,
PSNA College of Engineering and Technology, Dindigul, Tamilnadu,India.
3. Assistant Professor , Department of Electrical and Electronics Engineering,
RVS College of Engineering and Technology, Dindigul Tamilnadu,India.

[1] 2005.parvathi@gmail.com
[2] dshan71@gmail.com
[3] shankarlaaal@gmail.com

Abstract -- Password-based user authentication systems place total trust on the authentication server where clear text passwords or easily derived password verification data are stored in a central database. This system provides heterogeneous authentication services and single sign on in a network environment. In addition, the system hides the heterogeneity. Compromise of authentication server by either outsiders or insiders subjects all user passwords to exposure and may have serious legal and financial repercussions to an organization. Recently, several multilevel password systems were proposed to circumvent the single point of vulnerability inherent in the single-server architecture. In this paper, we present a secure multifactor authentication service for multi server in network. This system has a number of appealing features. In this system, only a front-end service server engage directly with users while a control servers stays behind the scene; therefore, it can be directly applied to strengthen existing two-server password systems.

Key words —Password system, network security, PKI, Kerberos, user authentication, .

I. INTRODUCTION

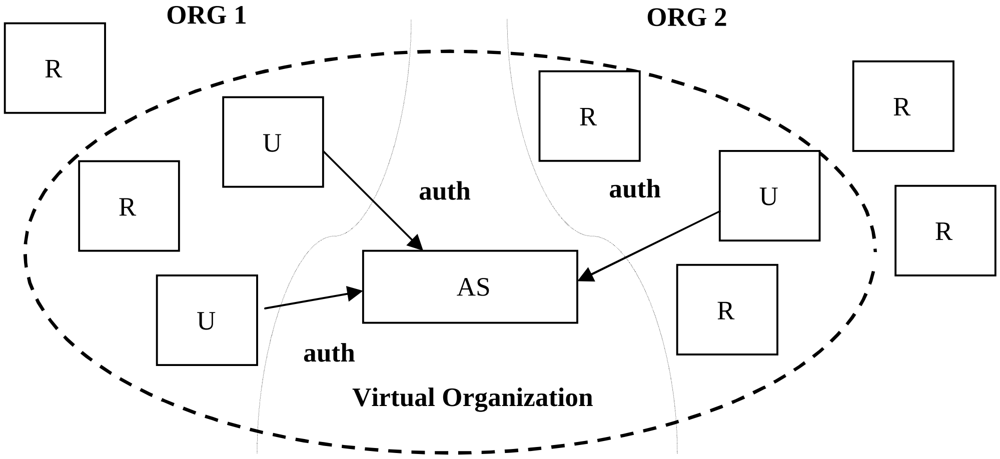
. The computational network provides a collaborative infrastructure with easy, consistent and inexpensive access to diverse computational resources belonging to heterogeneous administrative domains through a unified view of single virtual resource. Distributed computing infrastructure thus involves integrated and collaborative sharing of computing resources forming Virtual Organization[2].

Computational resources sharing between different organizations in an untrusted environment arises several issues related to information security. This is especially true on computational networks where members of different organizations join a Virtual Organization (VO) for resources can be dynamically added to or removed from a VO [5].

The Security services can be easily deployed for creating a computational network which allows secure utilization of resources shared by members. In this scenario, the configuration of the Security service is managed by the VO administrator and each non-virtual organization which wants to allow access to the network to some of its members, or make some of its resources available, will have to join the Security infrastructure which transparently provides, among other services, mutual authentication, integrity and confidentiality for network communication

Globus Toolkit version 4(GT4) implemented various security services by using different security protocols[3]. GT's security services heavily rely on the availability of PKIs and using different security mechanisms. This system has a service for scalable and flexible management of authentication policies governing access to resources shared by members of a Network, by improving on the Authentication Service distributed with the Globus Toolkit [5].

Password-based user authentication systems in a network are low cost and easy to use. A user only needs to memorize a short password and can be authenticated anywhere, anytime, regardless of the types of access. By and large, password has been the most pervasive user authentication means since the advent of computers and is still gaining popularity even in the presence of several alternative strong authentication approaches, e.g., Multi factor authentication which uses combination of user ID & password with some form of tokens.



Notations:

R – Resource , U – User , AS – Authentication Server, ORG – Organization , auth – Authentication request

Figure 1. The collection of Private Organizations configuring the Virtual Organization.

A. Earlier Work

Security of network resource is very important. Many platforms like Avaki [1] , Legion[4], Foster et al [3] are the possible network middleware choices. They are all support authentication and coarse grained security [7]. Earlier work [8] was on security protection through hierarchical administrative servers and single sign on across several administrative domains. The applicability of security issues and its protection in ubiquitous environment was investigated by Jana et al [7].

Security Model of Service Oriented computational network was explored by Jana et al [7]. They used dynamic user credential management by using dynamic token generation during session establishment and ongoing communication. The scheme for dynamic token generation in a network environment ensures more security because of the dynamic changing of the token, used in all transactions. The dynamic token thus generated forms part of the private key and the user id of the client provides the public key in terms of PKI.

Public Key Infrastructure (PKI) is the most widely adopted security infrastructure used in Network environments[3]. In addition to PKI based security tools, traditional security issues have been managed through well-known identity management and access control technologies, e.g. X.509 certificates[9], Secure Sockets Layer (SSL) communication protocol etc.

B. Virtual Organization

A Virtual organization is a dynamic set of individuals or institutions defined around a set of resource sharing rules and conditions. All these virtual organizations share some commonality among them, but may vary in size, scope, duration, sociology and structure. The sharing is controlled with resource providers defining what is shared ,who is allowed to share, and the conditions under which sharing occurs. The set of individuals or institutions defined by the sharing rules form the virtual organization [5].

Authentication policies can be dynamically managed by the server. In the initial state of the considered scenario, i.e. when a Virtual Organization is created, the only interactions allowed by the Security Services are authentication requests from the users to the VO's authentication server which accepts authentication requests, evaluates authentication policies and replies with authentication decisions (see Figure.1).

For issues of reliability, the VO authentication server may be replicated on different level of servers. In this case, members should be allowed to send authentication requests to all authentication servers used by VO and standard replication techniques should be used for ensuring overall consistency of the authentication servers. In this approach one can dynamically modify the set of authentication policies granted to server of a VO.

II. THE N-SERVER ARCHITECTURE

The Password systems are normally built over the following five types of architectures shown in Figure 2.

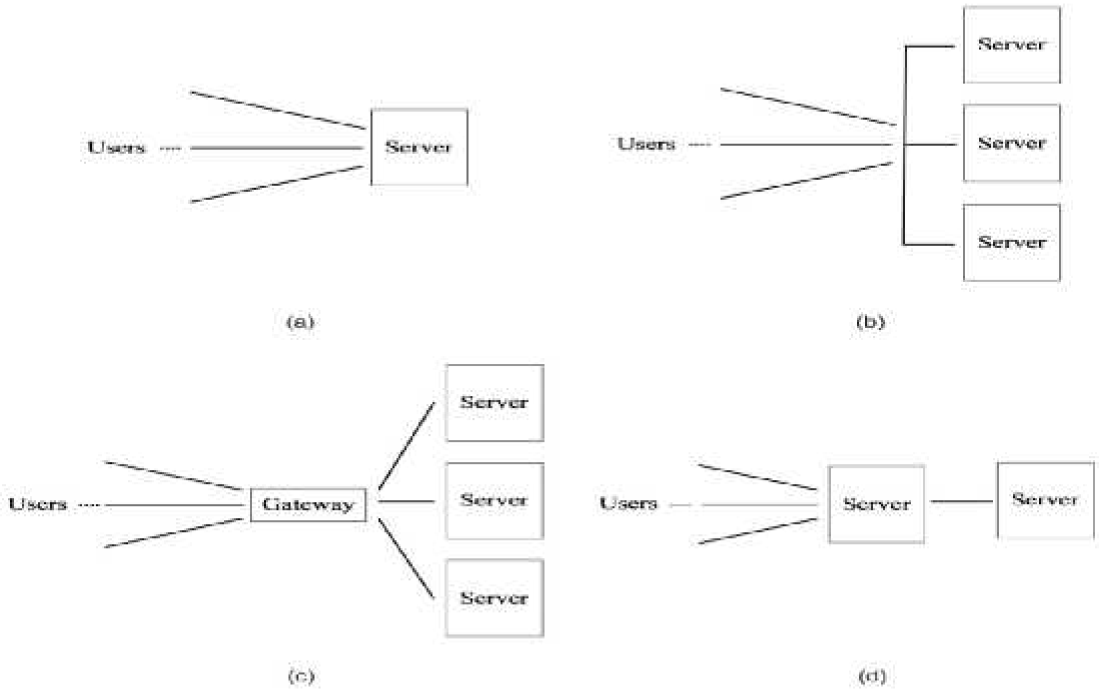


Figure 2a. Models of password systems. (a) Single-server model. (b) Plain multiserver model. (c) Gateway augmented multiserver model. (d) Two-server model.

The first type is the single-server model given in Figure. 2a, 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.

The second type is the plain multi server model [6] depicted in Figure. 2b, in which the servers are equally exposed to users and a user has to communicate in parallel with several or all for authentication. The main problem with the plain multi server model is the need for synchronization at the user side since a user has to engage in simultaneous communications with multiple servers.

The third type is the gateway augmented multi server model [6] shown in Figure.2c, where a gateway is positioned to relay the messages between users and servers, and it does not in any way involve in service provision, authentication, and other security enforcements.

The fourth type is the two-server model[10] (outlined in Figure. 2d), that 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.

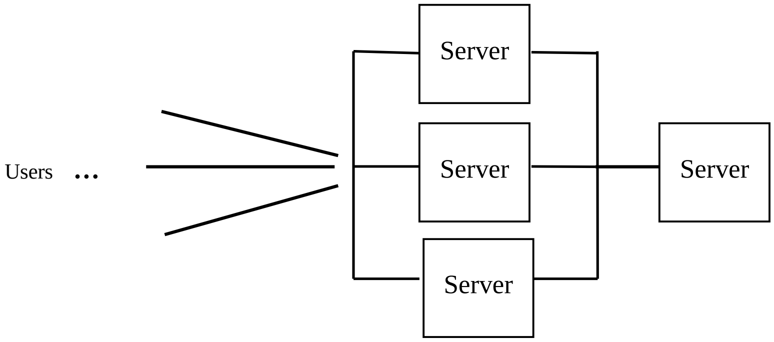
The fifth type is the combination of both two servers Model & gateway augmented multi server model shown in Figure. 2e This system models also has redundant control server. The system model consists of four service servers and one control server.

III. N-SERVER PASSWORD AUTHENTICATION

In this system, each machine is considered as a private organization (PO). This System model has five private organizations. Their policies may differ with each other. These private organizations are combined together to form a Virtual Organization.

A. System Model

The System model (shown in Figure.3) comprises two levels of servers at the server side, one of which is service servers (SS) and the other of which is a back-end server called control server (CS).



(e)

Figure 2b. Models of password systems. e) 'n'-server model

Three types of entities are involved in this 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 .This system model consists of four service servers and one control server. One service server use PKI policy, whereas another service server uses Kerberos authentication service and remaining two of service servers follows primitive password authentication service.

CS authenticates user only in three ways. They are Public Key Infrastructure, Kerberos authentication service and primitive password authentication service. When user directed to access with service server which uses PKI, then CS creates certificate to the user and allows to access with corresponding SS. When user directed to access with service server which uses Kerberos, then CS generates ticket to the user and allows to access with corresponding SS. The creation process of both certificate and ticket is kept transparent to the user. When user directed to access with service server which follows normal password authentication service, then CS only verifies user's password and allows to access with corresponding SS.

B. User Registration

In any password system, to enroll as a legitimate user in a service, a user must register with service provider by establishing a shared password with the provider. In this system, User needs to register not only to the service server SS but also to the control server CS.

User has already successfully identified himself to SS, e.g., by showing his identification card, User splits his password p into two long random numbers. User then registers in a secure manner p1 and p2 to SS and CS, respectively. SS stores the account information to its secret database, and CS stores to its secret database. CS completes the user registration phase. User registers p2 to CS and the CS is supposed hidden from User.

C. Key generation public and private server:

User enters into the System by using One Time Password (OTP) key. Once the User login with this key, user cannot again use this same key.OTP has to be valid up to the completion of current work. When the work is completed, the key will be discarded.

D. Authentication and key exchange:

We retrieve encrypted passwords from the server and verify the password using DES key exchange algorithm. DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key. It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher. Using DES algorithm we combined and decrypt the password, and then finally password is verified. If the password is correct, the user will be authenticated.

IV. THE MULTI FACTOR AUTHENTICATION SERVICES

It uses combination of user ID & password with some form of tokens. It is difficult to spoof, impersonate and easy to use. The deployment can be difficult, tokens can be stolen and management of tokens can be challenging especially in the event of stolen tokens. There is a variety of technologies in multi factor authentication to protect data are PKI (Public Key Infrastructure), Kerberos and so on.

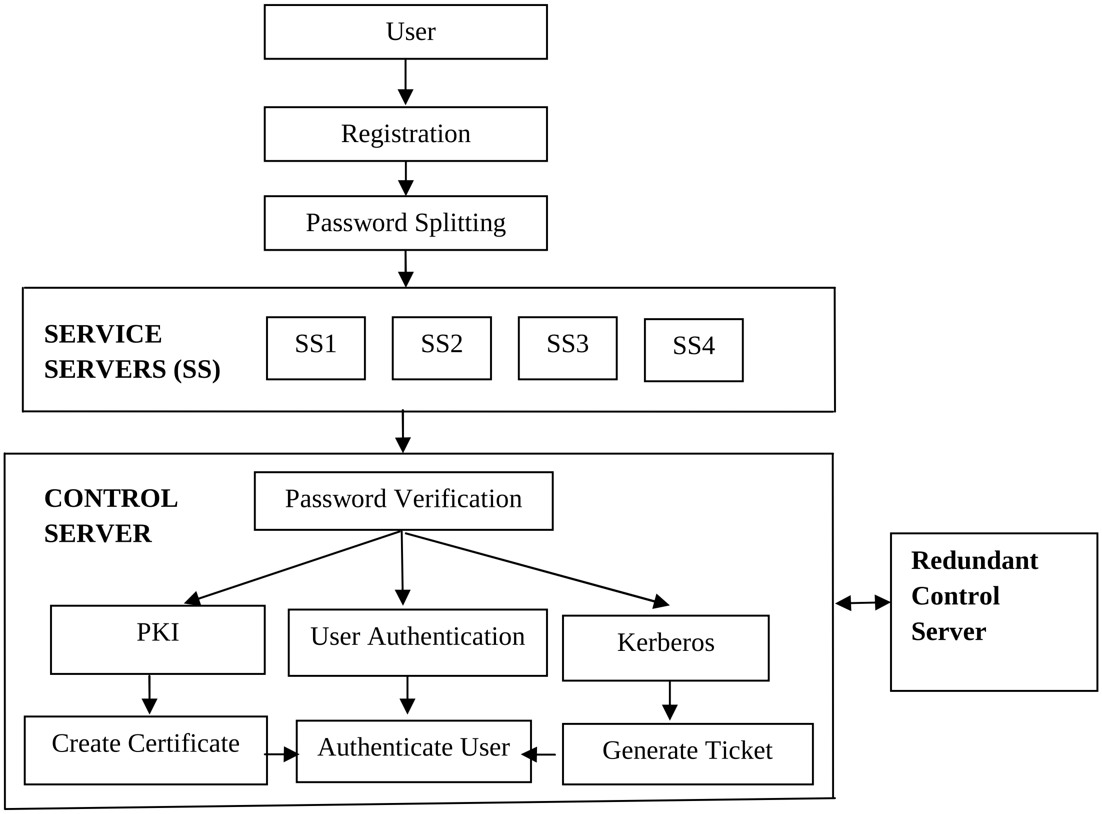


Figure 3. The N-Server model Architecture diagram

A. PKI (Public Key Infrastructure):

Public key infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete enterprise-wide network security architecture.In Public key infrastructure, digital certificate will be created by control server at the time of user registration. When the user enters username and password, certificate will be verified. If the certificate is valid, the user will be allowed to access the site. Otherwise the user will not be allowed to access the site.

B. Kerberos:

Kerberos is a authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It consists of two logically separate parts: an Authentication Server (AS) and a Ticket Granting Server (TGS). Kerberos works on the basis of tickets which serve to prove the identity of users.In Kerberos, encrypted ticket will be created by control server at the time of user registration. When the user enters username and password, ticket will be decrypted and verified using secret key. If the ticket is valid, the user will be allowed to access the service. Otherwise the user will not be allowed to access the site.

V. APPLICATIONS

The major contribution of Network is to enable the collaboration among wider entities. Network has enhanced this capability to a higher scale incorporating very heterogeneous systems. In Network users can be dynamically grouped into Networks (VOs) with their own policies. Thus these VOs can share their resources in larger network.

This architecture model is the next generalization of the basic two-server model. In this architecture, the control server and the service servers are managed in different administrative domains

More interesting applications can be envisioned for this architecture. A good example of such applications is in a federated enterprise, where many divisions, branches, and affiliations unite under a single enterprise authority. Each of the affiliating organizations that serve different aspect of a business continuum and service coverage has its own business interest and provides service to a distinct group of users.

VI. DISCUSSIONS

The N-server password system together with its practical applications offers many appealing features:

1. Without compromising both servers, no attacker can find user passwords. 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. This feature allows users to use easy to remember passwords and still have strong authentication.

2. 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.

3. In this system, a password is splitted 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.

4. From the perspective of users, they are able to assume the higher creditability of the enterprise while engaging in business with individual affiliating organizations.

VII. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed Secure Multifactor Authentication service for ‘n’ servers in Network 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, this system possesses many advantages, such as the elimination of a single point of vulnerability, avoidance of PKI, and high efficiency.

In contrast to existing password systems, this system has great potential for practical applications. It can be directly applied to fortify existing two-server password applications. It can also be applied in the federated enterprise setting, where a single control server supports multiple service servers. The security model underlying the proposed protocols assumes that the control server can only be controlled by the attacks. This assumption is quite logical while considering the positioning of the two levels of servers in the n-server model and the applications of the model to federated enterprises. It is clear that weakening of this assumption should be of both practical and theoretical significance, which will take as future work.

VIII. REFERENCES

[1] Avaki: Avaki Compute Network. (2003). http://www.avaki.com/products/acg.html, Apr. 2003.

[2] Debasish jana,Amritava chaudhuri, and Bijan bihari bhaumik,”Privacy and anonymity protection in computational network Services”, International Journal of Computer Science and Applications, 2009 Vol. 6, No. 1, pp. 98–107,1998.

[3] Foster I. and Kesselman C. (1999): Globus: A Toolkit-Based Network Architecture. Foster, I. and Kesselman, C. (eds.), The Network: Blueprint for a New Computing Infrastructure. Morgan Kaufmann, 1999. pp. 259—278.

[4] Grimshaw A., Wulf W., French J.,. Weaver A and Reynolds P. (1994): Legion: The Next Logical Step Toward a Nationwide Computer. Tech. Report,University of Virginia, UMI Order Number: CS-94-21, Jun. 1994.

[5] Ian Foster, Carl Kesselman, and Steven Tuecke. The anatomy of the network: Enabling scalable network. International Journal of Supercomputer Applications, 15(3):200.222, 2001.

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

[7] Jana Debasish, Chaudhuri Amritava, Datta Abhijit and Bhaumik Bijan Bihari. (2007): A Fine- Grained Hierarchical Role Based Network Access Control. IEEE India International Conference, Proceedings of the IEEE INDICON 2007, September 06-08, 2007, Bangalore, pp. 1-5.

[8] Jana Debasish, Bhaumik Bijan B. (2004): Single SignOn for Network Services. Proceedings of the First IEEE India Annual Conference(INDICON 2004), IIT Kharagpur,Dec 20-22, 2004 pp. 513-516.

[9] Tuecke S., Welch V., Engert D., Pearman L., and Thompson M. (2004): Internet X.509 public key infrastructure proxy certificate profile. The Internet Engineering Task Force (IETF), RFC 3820,June 2004.

[10] Yanjiang Yang, Robert H. Deng, Senior Member, IEEE, and Feng Bao A “Practical Password-Based Two-Server Authentication and Key Exchange System” IEEE Transactions on Dependable and Secure computing, vol. 3, no. 2, April-June 2006.