End User Authentication (EUA) Model and Password for Security

George S. Oreku, Harbin Institute of Technology, China
Jianzhong Li, Harbin Institute of Technology and Heilongjiang University, China

ABSTRACT

Authentication is one among a set of services that constitute a security subsystem in a modern computing or communications infrastructure. End User Authentication flexibility model proposed in this article will allow the user to have multiple authentications with varying levels of guarantee, and for suppliers to request and rely on mechanisms appropriate to the service requested. We describe the ticket used by clients, servers, model and algorithm to achieve authentication toward prevention of unauthorized access to in sourced data on applications level. An authentication to end-user proposed in this article is a simple three level ticket request model solution in an open distributed environment. We also develop an analytical password for the proposed mechanism and validate this approach through experiment. Furthermore, we explore this approach to end user authentication and demonstrate the conception of a textual password which in many cases improves the security. We analyze Diffie-Hellman exchange weakness and present how it can be made robust against attacks. Our approach is based on the use of the Kerberos authentication technique and the Diffie-Hellman Key exchange. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: Authentication; Authorization; End User; Kerberos; Tickets

MOTIVATIONS

The frontline of defense against intruders is the password system. Virtually all multiuser systems require that a user provide not only a name or identifier (ID), but also a password. The password serves to authenticate the ID of the individual logging on to the system. To understand the nature of the threat to password-based systems one should consider a scheme that is widely used on UNIX, in which passwords are never stored in clear text. The problem is that many users choose a password that is too short or too easy to guess. At the other extreme, if users are assigned passwords consisting of eight randomly selected printable characters, password cracking is effectively impossible.
Our goal, then, is to eliminate guessable passwords while allowing the user to select a password that is memorable.

If a set of users is provided with dedicated personal computers that have no network connections, then a user’s resources and files can be protected by physically securing each personal computer. When these users instead are served by a centralized time-sharing system, the time-sharing operating system must provide the security. Currently these requirements are being overridden in the interests of efficient, standardized commercial arrangements. Thus, a corporate IT infrastructure would want to authenticate that the user of a certain requested online service is authorized for certain services prior to granting privileged sensitive access (perhaps by means of a user password and a smartcard). However the operating system can enforce access control policies based on user identity and use the logon procedure to identify users.

Today neither of these scenarios is typical. More common is a distributed architecture consisting of dedicated user workstations (clients) and distributed or centralized servers. In an unprotected network environment any client can apply to any server for service. The obvious security risk is that of impersonation. An opponent can pretend to be another client and obtain unauthorized privileges on server machines. To counter this threat we would like to minimize the number of times that a user has to enter a password by a sign on password. The second problem is that the earlier scenario involved a plain text transmission of the passwords which may cause an eavesdropper to capture the password and use any service accessible to the victim. To solve this problem we introduce a scheme for avoiding plain text passwords and a new server model.

In our DBMS model key exchange tickets storage for communication authentications, we would only want to grant access to those users whose accounts are (current). For example we would not permit users to access the system using a stolen credit card.

Many systems currently lack the expertise in an increasingly distributed environment (i.e., Internet services) in which it is likely to become harder to provide users with understandable and effective controls over their data use. With that idea in mind, three approaches to security can be envisioned:

1. Rely on each individual client workstation to assure the identity of its user or users and rely on each server to enforce a security policy based on user-based identifications (ID).
2. Require that client systems authenticate themselves to servers, but trust the client systems concerning the identity of their users.
3. Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.

Raising questions to e-commerce security, this article presents authentication and authorization service model algorithms to an end user by the use of textual passwords and authentication. We extend the use of the last models by Diffie-Hellman, “Key Exchange A Non-Mathematician’s Explanation” (Palmgren, 2005) and Kerberos authentication model (Steiner, Neuman, & Schiller, 1988) quoting at length to place authentication in proper systems context use.

LITERATURE REVIEWS

Since the introduction of public key cryptography in the 1970’s (Deffie & Hellman, 1976), many cryptosystems have been proposed and many cryptographic schemes have been broken. The most used cryptosystems rely on a number of theoretical problems like the factorization problem (Rivest et al, 1978) and the discrete logarithm over suitable group (ElGamal, 1985). For the vast majority of computer systems, authentication for users and passwords are the method of choice for access control security.
Measuring the Impact of Information Systems on Organizational Behavior
[www.igi-global.com/chapter/measuring-impact-information-systems-organizational/4439?camid=4v1a](www.igi-global.com/chapter/measuring-impact-information-systems-organizational/4439?camid=4v1a)

A Composite Framework for Behavioral Compliance with Information Security Policies
[www.igi-global.com/article/a-composite-framework-for-behavioral-compliance-with-information-security-policies/81297?camid=4v1a](www.igi-global.com/article/a-composite-framework-for-behavioral-compliance-with-information-security-policies/81297?camid=4v1a)