Introduction

The foundational principals of achieving information and data security in the realm of digital systems is based on the CIA (Confidentiality, Integrity, and Availability) triad. However, to fully understand the security requirements of a particular system or an application, a much in depth assessment would be required that incorporates the implementation of relevant security policies and procedures. Thus, when narrowing down to an application that encompasses a distributed system, the exact requirements might vary depending on the required set of functionalities in the application. Nonetheless, the most crucial aspect that should always be taken into account is the process of authentication in such a system. Furthermore, a typical distributed system involves a client (might server as an end-user) that requests services from a remote host, also known as a server. When taking into consideration the vast network facilitated by the Internet, the task of achieving authentication between these two entities can be quite cumbersome. How can a server make sure that some client, requesting from it a service or data, is actually genuine and not someone else and vice versa? Moreover, this is only one of the myriad lenses that the problem of authentication might be viewed from. It is also imperative that the entities do remain authentic throughout the established communication. (Stallings, 2011)

In order to achieve authentication, one of the first steps would require the client to prove themself as authentic. This may be accomplished by client and server agreeing on some credentials that might comprise of a type of identification along with a password, smart card, and or biometrics. Upon establishing a communication and requesting access to services or data that a client is eligible, the latter can use these credentials to gain access. However, the major obstacle to overcome in this endeavour is to make sure that the client submitting these credentials is in fact who they claim to be. This is where multi-factor authentication might come into play, that requires a client to not just input their password but more information. Other additional steps to take can also include the secure storage of a cryptographically strong password. (Lutkevich, 2022)

In addition, the process of authentication involves other major side of the coin, that puts spotlight on the problem of the server being authentic and not a malicious entity that the client is trying to communicate with. Or even worse, both honest entities come under the assumption that they have authenticated each other but instead they are communicating with an intruder. A classic case is analogous to the attack on the Needham Schroeder protocol, in which the authentication principals are violated by an intruder performing a man-in-the-middle-attack. (DS Lecture 2)

The methods and techniques involving the security that ensures the regulation of authenticating genuine users to some resources is covered using access control mechanisms (Lutkevich, 2022). This will be covered in much detail later in this report.

Furthermore, a comprehensive study of several security mechanisms will be addressed in this paper that touches upon the problem of secure storage and transportation of a password and making the process of authentication more secure. The solution proposed in this paper focuses on countermeasures for aforementioned complications that typically arises in a distributed system comprised of a client and a server. Moreover, the developed software puts in practice, part of the solution to the vast array of problems revolving around authentication. In essence, the client's password is stored as a one-way hash in a database management system that the server then uses to authenticate the latter.

References.

William Stallings. NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS FOURTH EDITION 2011

Ben Lutkevich 2022. https://www.techtarget.com/searchsecurity/definition/access-control#:~:text=Access control is a security,access control: physical and logical.