An Idealistic Study of Passwords

Shweta Ohri
Jagannath International Management School, Vasant Kunj, New Delhi-70

Abstract

In this paper we discuss an idealistic study about passwords. We actually attempt to address the problems related to password. In addition, we demonstrate the earlier attempt of problems. We also, take a careful look at the weakness and strength points of the process of passwords. Finally, we redefine the password problem to ensure the authentication and improvement.

Keywords: Password problems, Redefinition of the password problem

I. INTRODUCTION

As we know that the word “Password” is composed of two words i.e. pass and word so we can pass if we have the right word. Even before the advent of computers watchwords existed in the form of secret codes, agents of certain command for their respective authorization or administration used watchword e.g. for identifying other agents and the underlying concept is essentially the same today. In this paper we take a deep look into both the theory and philosophy of passwords; in short we will be addressing a fundamental question: can password semantics enable them to mimic Nature’s way of keeping secrets and providing security.

Due to the critical nature of information, be it personal information on someone’s personal computer or information systems of large organizations, security is a major concern. There are three aspects of computer security: authentication, authorization and encryption. The first and most important of these layers is authentication and it is at this layer that passwords play a significant role. Most common authentication mechanisms include use of an alphanumeric based word that only the user to be authenticated knows and is commonly referred to as passwords. The SANS Institute indicates that weak or nonexistent passwords are among the top 10 most critical computer vulnerabilities in homes and businesses. Philosophical analysis of passwords can lead to the refinement of the authentication process. This approach has rarely been adopted in the exploration and design of computer security. Passwords too are entities having an existence of their own and this lead us to study them under a philosophical context.

In the remaining of this paper, there are six more sections. In Section II, we provide an attention about the password problem. Also, we attempt to address the problem in section III. The problems in earlier attempts, redefinition of the password problems are discussed in section IV AND V. Finally, conclusions and references are provided in Section VI and VII.

II. THE PASSWORD PROBLEM

When it comes to the area of computer security there is a heavy reliance on passwords. But the main drawback of passwords is what is termed as the “password problem” for text-based passwords. We will refer to this problem as the “classical password problem.” This problem basically arises from either two of the following facts:

1) Human memory is limited and therefore users cannot remember secure passwords as a result of which they tend to pick passwords that are too short or easy to remember. Hence passwords should be easy to remember.

2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user. They should not be written down or stored in plain text.

III. ATTEMPTS TO ADDRESS THE PROBLEM

Current authentication techniques fall into three main areas: token-based authentication, biometric-based authentication and knowledge-based authentication. Token-based authentication techniques use a mark or a symbol for identification which is only known to the authenticating mechanism and it is under the possession of the user just like a coin which has no meaning other than that known to the mechanism. An example is that of key cards and smart cards. Many token-based authentication systems also use knowledge-based techniques to enhance security. For example ATM cards are generally used together with a PIN number. Biometrics systems are being heavily used; biometric authentication refers to technologies that measure and analyzes human physical and behavioral characteristics for authentication purposes.
IV. SOME PROBLEMS IN EARLIER ATTEMPTS

- The token-based passwords though secure but require a token (permit pass) which could be misplaced, stolen, forgotten or duplicated and the biggest drawback is that the technique can only be applied in limited domains not within the reach of common user.
- The biometric passwords are efficient in that they are near to a human’s science and do not require remembrance rather they are closely linked with humans but they are expensive solutions and cannot be used in every scenario.
- Knowledge based passwords require remembrance and are sometimes breakable or guessable. Ensure the establishment of a link between system and specific human mind from domain set.

V. REDEFINITION OF THE PASSWORD PROBLEM

We can redefine the password problem as follows:

- Introducing variety into the domain set of password is a task that must be given due consideration and any attempt to implement the philosophical concepts explored in this paper must address the question: How and in what ways can variety be introduced into the passwords so that \( N^K \) formulation sustains more with \( N \) than with \( K \) where \( N \) is single input or action and \( K \) is length of input.
- We have stated that password recognition is a process in itself but the details and phases of that process have to be identified. To accommodate philosophical ideas one must carefully model the process of evaluation (i.e. input and validation).
- By exploiting senses to ensure variety does not mean to exhaust user both physically and mentally but means to enhance level of comfort and freedom to choose from variety that lead in securing system sensibly.
- Randomization in password should follow the common sense rather than heavy mental exercise in a way that senses tell computer system “Yes, I am the right person. Please let me pass!”
- In security critical zones, heavy investment is made to ensure protection at the level of authentication but lacks to decide level of quality achieved.

VI. CONCLUSIONS

In this paper we discussed the philosophy of passwords and their study in connection with the human mind. Although the points that we have mentioned in the paper have been noted by different researchers at different times but there’s no single place where the entire “password philosophy” has been defined. Thus we have laid out the constitutional terms for any study of intelligent and smart passwords. The two main points that we have identified in this “Constitution of Passwords” are as follows:

1) Password is not just a unit of work; rather it is a complete process.
2) Password should incorporate common sense of humans.
3) There must be quality assurance at the level of authentication mechanism.

This philosophy can play vital role for immediate practitioners if they keep tradeoff of in their mind before producing a secure solution and as well as for researchers to dive into challenging problems that have been left open for them.

REFERENCES