CHAPTER 1

INTRODUCTION

One of the most important attributes of Information Security is Authentication. It is the act of proving to someone that you are the one who you claim to be. This process is dependent on identity validation. Generally speaking, authentication practices are quite old and are not just restricted to computers and cryptography. The importance of authentication was demonstrated long back in the tales of Ali Baba and Forty Thieves where they used to chant some secret known only to them to enter the cave.

In daily life, people have been practicing authentication for quite sometime; it was not a serious issue earlier as it is today because previously people used to trust each other highly. It is often heard from elders that in earlier days a person’s reputation was built over time as he or she becomes known in the community; and thereon a handshake was good enough to finalize a deal. However, as the communities became larger, and distance greater, it became necessary to provide formal documents such as passport, driving license etc. that prove the identity and character of a person.

As the Internet community is too large for people to know everyone else directly, a mere e-mail ID or other digital ID’s are not enough to validate a person or freeze an online financial deal. Moreover, because of the lack of availability of face-to-face methods on Internet, it is very
difficult to ascertain who someone is, how reliable they are, how to validate them etc.

One way to ascertain identity of a person over Internet is the use of Password based Authentication wherein the claimant provides his identity and a secret called password to the verifier to get access to the restricted resources. The increase in the user base for web based services in recent years has raised concerns about security & privacy of user’s personal information. Most of the websites protect this sensitive information with mere username and password which makes the user authentication more critical in combating threats such as unauthorized access and identity theft.

The increasing number of online services has raised another serious issue of number of web accounts a user has to maintain. As every website requires the user to register before accessing its resources, the user has to register with each website separately and maintain multiple login accounts. Remembering several password pairs are difficult for the users due to human memory limitations with alphanumeric passwords. Therefore, for easy recall of passwords, the users either set simple passwords (sometimes same) for all their accounts or set alphanumeric passwords and write it on piece of papers. But such practices suffer from various online attacks such as guessing, dictionary, phishing etc. and often lead to compromise of user’s accounts.
Since, authentication is the entry point for any network including Internet for accessing a resource on the server, there has been an increasing focus in recent years on strengthening the authentication methods to ensure utmost safety of web based accounts. Strengthening the authentication includes the proper level of assurances of security at client, transmission channel and server, besides offering strong password methods to web users.

1.1 MOTIVATION

In the last decade, a section of researchers, dedicated their work in improving the strength and memorability of text passwords and therefore proposed methods such as Pass phrase [1][2] (considered to be stronger than passwords [3]), Mnemonic-based Password [4],[5],[6], Pass text[7], Pass thought [8] etc. Another alternative to improve the text passwords is the use of Graphical password [96] (discussed in detail in sections 2.3 and 2.4). These methods gained significance because of the use of images as passwords which help the user to easily recognize and recall his password. Though all these methods provide better security than conventional text passwords, they still fall in the category of Single Factor Authentication (SFA) which is vulnerable to various online attacks. This has lead to the introduction of Multi-factor Authentication to ensure safety of online accounts.

In 2005, Federal Financial Institutions Examining Council (FFIEC) of US, had released a document [9] in which all the financial institutions
were strongly recommended to implement Multi-Factor Authentication, layered security, or other controls to mitigate online threats and attacks. The council set the deadline of December 2006 to all online financial service organizations for implementing the recommendations. Consequently, the online banks and financial institutions in US have upgraded the authentication to Two-Factor or Multi-Factor methods. As per the design guidelines, the second factor device could be Smart Cards, USB Tokens, Biometrics etc. for user authentication.

However, it is increasingly recognized that security is often designed and implemented without users in mind. For example, a study conducted into human vulnerabilities of system security [10], commented that “Most security mechanisms are currently chosen to protect the technology, with little or no consideration of the impact on individuals. Many existing mechanisms create a high workload for individual users”. Hence, designing a secure and usable authentication requires bridging the gap between the graphical passwords and Multi-Factor Authentication. The literature survey of the existing Graphical Password based Multi-Factor Authentication Schemes resulted in few schemes [124][128][131] that address the above discussed issue. But none of these works provide security against stolen verifier attack (section 2.3.2). These schemes will be discussed in section 2.5.

The wider recognition of these issues has motivated the initiation of the current research. The aim of this work is to propose Multi-Factor Authentication Schemes using Text and Graphical Passwords without
Verifier Table. The research work started with an in-depth survey of existing textual password based Two-Factor Authentication schemes using smart cards that resulted in an idea that the current schemes focused only on strengthening the authentication systems against various security attacks; whereas survey on graphical password techniques resulted in the understanding that most of the current work currently focuses more on usability of the system and strengthening the password. The literature survey did not find any authentication scheme that provides the usable security that provides the best of graphical password and smart card based Two-Factor schemes. Therefore, the current research acknowledges through this work, the requirement of a proven secure and usable authentication system that can readily be deployed for current web based services.

1.2 MAJOR RESEARCH OBJECTIVES

The aim of this research is to design, analyze and implement Secure and Usable Authentication Schemes. To achieve better usability the focus is to provide the users with memorable passwords; and to achieve security, the focus is to design Two-Way Two-Factor Authentication Schemes without Verifier Table at Server.

The major objectives of this work identified are as follows:

- Design a Secure Two-way Two-Factor Authentication and Key Agreement Scheme that does not maintain verifier table at server.
• Catalogue the existing Graphical Password based Authentication Schemes and identify the most suitable method that focuses on security and usability.

• Design a Graphical Password based Two-Way Two-Factor Authentication and Key Agreement Scheme without Password table.

• Propose a Graphical Password that provides better strength than the existing image based password methods. Consequently design the scheme for the proposed graphical password.

• Analyze the security of all the proposed schemes against common attacks on authentication schemes.

• Validate the proposed schemes through formal analysis methods.

• Implement the proof of concept for all the proposed schemes to suite web based services.

• Determine the usability of the POC through usability study and evaluate it using empirical methods.

1.3 ORGANIZATION OF THESIS

The rest of the thesis is organized as follows. Chapter 2 outlines the background literature including Basics of Cryptography, Types of Authentication, Smart Card based Authentication. It further presents the previous research in Smart Card based Two-Factor Authentication Schemes, Graphical Password methods, Security Attacks on Authentication Schemes and Usability and Security Analysis of Graphical Passwords. Chapter 3 discusses the first proposal on
Two-Factor Textual Password based Authentication. It also outlines the security strength and functionalities of the proposed scheme. The formal analysis of the said scheme is discussed at the end of the chapter. Chapter 4 introduces the proposal on Two-Factor Graphical Password based Authentication Scheme. It also presents the detailed security, efficiency and formal analysis of the said scheme. Chapter 5 discusses the proposal of Text-o-Graphic Password with two variations (S-27 & S-16). This chapter also discusses the Two-Factor Authentication Scheme for the proposed password. It then discusses the security, efficiency and formal analysis of the same. Chapter 6 explains the Proof of Concept Implementation named STARS, of all the proposed schemes. It also presents the security analysis of the STARS. Chapter 7 analyses the Usability of STARS and discusses the results. Finally, Chapter 8 presents the conclusion and future work in the current area of research.