CHAPTER 8

CONCLUSION

There are many authentication schemes that are in practice today. If they are categorized based on usability and security then most of them fall into the category of security that ensures the safety of the user’s account using second factor, but they lack proper usability. The remaining are the authentication schemes that are designed to achieve better usability, but lack proper security to protect the user from communication channel attacks and masqueraded server attacks.

This research was aimed at providing authentication schemes that shall bridge the gap between security and usability. It was also aimed that the security be achieved using smart card as the second factor whereas the usability using graphical passwords.

8.1 PRESENT WORK

The work started with the survey of current research in smart card based Two-Factor Authentication schemes that resulted in identifying various schemes on dynamic ID. These schemes generate a dynamic ID at each user login, thus resisting the threat of identity theft. Though the security analyses of the schemes were presented through theoretical intuition, but none of them were evaluated for security using formal methods. Moreover, most of these schemes are found to be vulnerable to
the common authentication attacks such as Replay Attack, Guessing Attack, Stolen Verifier Attack, Insider Attack, Server Spoofing Attack etc.

Therefore, an enhanced dynamic ID based scheme was proposed that provides better security strength comparing to existing schemes. The distinguishing features of the proposed scheme are (i) The use of secret random numbers (against time stamps) for resisting the replay attack, (ii) Diffie-Hellman Key Exchange Protocol for secret sharing of random number, (iii) Successful Mutual Authentication, (iv) Authenticated Key Agreement, (v) Security against common attacks on authentication systems besides achieving the desirable features such as User Anonymity and Explicit Key Authentication.

The security analyses of the proposed scheme was presented through theoretical intuition, in addition to validating the scheme using automated formal analysis tool called scyther [80]. The proof of concept of the proposed scheme is implemented to evaluate the practicality and usability of the said scheme. The screen shots of the verification result and the POC can be found in the last section of this document.

Graphical Password based Authentication Scheme: Since usable authentication is an important area of usable security, this research also focused on the usability aspect of the authentication schemes. Most of the existing graphical password based schemes requires verifier table. Therefore, the research objective was to propose a graphical password based Two-Factor Authentication scheme that does not require verifier
The graphical password used in the proposed scheme is similar to existing works.

To validate the claims about the security, firstly the security analysis of the scheme was presented, followed by the formal verification of the said scheme using Scyther. The proposed scheme is also implemented along side other proposed schemes.

**Text-o-Graphic Password based Authentication Scheme:** While designing the Graphical Password Scheme, it was found that the recognition based graphical password could be susceptible to guessing, therefore, to overcome this; a novel graphical password called text-o-graphic password with two variations namely S-27 and S-16 was proposed. The user password in text-o-graphic method is the combination of image and its tag. S-27 presents three grids (each having nine images) to the user for password selection. The user has to choose one image from each grid and write a description called tag about the image so that the concatenation of three images along with their tags makes the user’s password. S-16 presents one grid of sixteen images of which the user has to choose one image and associate a tag to it.

As per the research objective, the Smart Card based Authentication Schemes were proposed for S-27 and S-16. S-27 scheme utilizes the DHKE protocol to achieve the desired security strength, whereas, S-16 employs PKI for secure authentication. PKI is used in the scheme to have the legal validation of authentication as per the IT Act
2000 of India [31]. Both the schemes were formally analyzed using Scyther.

To prove that the schemes without verifier table are realizable, a proof of concept named ‘STARS’ is implemented employing Java technologies. STARS provides a platform where the user is provided with the option of choosing any of the four schemes. It is designed such that, at run time the user cannot figure out which scheme is running in the background. Moreover, the design allows the registered user to switch to any other scheme using change password option. To check the security of implementation, the security analysis of the STARS against some expected threats is also presented. The screen shots of the formal verification results of all schemes and STARS are given below.

To give completeness to the work, a usability study of STARS is conducted with 394 participants having varied background. The result of the study indicated that despite STARS being a Two-Factor solution, the usability of i-27 and S-16 is more than conventional text password solutions where as the security of STARS variants is better than existing graphical password methods.

8.2 FUTURE ENHANCEMENTS

This research contributed to Secure and Usable Authentication, but there are some areas that need further extension to the existing work. These are discussed below:
**Attack Analysis of STARS:** The proof of concept is implemented using Java Technologies and the security analysis of the POC is carried out for possible threats, but a concrete attack analysis and vulnerability assessment of STARS is to be done for proving its credibility against common attacks such as SQL Injection, XSS, Phishing Attack, Guessing attack etc.

**Implementation using Valid Certificate:** The S-16 protocol which requires digital certificate is implemented as part of STARS using the certificates generated by a demo tool. Therefore, to get the feel of real online transactions and to have the legal recognition of the transactions made through STARS, the digital certificates issued by the certifying authorities are to be used. Moreover, the server side implementations of all the schemes require private key of the server which was again taken from the certificate created using OpenSSL. Hence, the certificates required by the schemes are to be replaced with the valid CA certificates.

**Field Study of STARS:** As discussed in 7.1.1, many people were invited for usability study by way of giving demo presentations but only 394 turned up of which the maximum were from C-DAC. Therefore, it is strongly felt that firstly, STARS is to be integrated with any existing e-commerce or e-banking application and then conduct the field study so that it reaches the wider audience which therefore gives the correct usability of the system.
In addition, the authentication schemes can be enhanced to achieve greater efficiency than the currently achieved efficiency by way of reducing the number of computations.

Also, the possibility of a Secure & Usable Authentication using one-time password without maintaining verifier table can be explored by taking the current work further. Moreover, as the proposed schemes are broader enough to be integrated with any type of password (be it graphical password / textual password / biometric etc.), these concept of these schemes can be utilized to modify the existing authentication schemes used in industry to achieve greater security, efficiency and usability.