A CASESTUDY ON PASSWORD SECURITY EVOLUTION

M. SANDIRIGAMA AND N.S WERAGAMA

Department of Computer Engineering, Faculty of Engineering
University of Peradeniya

As the Internet and Mobile applications have been increasing in the recent past, the need for authentication over remote servers and telephones has become very important. The need of authentication is essential as the private data sent over the Internet have risk of being wiretapped. Existing password authentication schemes can be divided into two types, one requires only the weak password and the other must use the strong password.

The main objective of this case study is to present a review on the evolution of the strong password protocols. Starting with the earliest password authentication protocols such as Lamport I, CINON and the PERM, the study comprehensively analyzes the most recent protocols such as SAS-2 and SPAPA. The newest protocol SPAPA stands for hash-based Strong Password Authentication Protocol with user Anonymity. The user's anonymity is highly required in a hostile environment as it prevents observing the user's activity. Also, the SPAPA protocol is very simple and contains only hash functions and XOR operations as compared to the earlier versions, which are suitable for power and computation constrained smart card applications. The SPAPA protocol is tested and verified to be secure from Stolen Smart Card or Online Guessing Attack, Offline Guessing Attack, Stolen Verifier Attack, Replay Attack and Denial of Service (DoS) Attack.

In addition, all the attacks performed on each of these protocols are covered in this case study as well. The common pattern in evolution and the details of the attacks that compromised the security measures in each of the protocol are taken into account.