Passwords and Biometrics Authentications

By
Fahad Alsolami
PhD in Engineering Concentration in Security
University of Colorado at Colorado Springs
Visiting Scholar at University of South Florida
Assistant Professor at King Abdulaziz University, Saudi Arabia

Abstract:
Organizations and, to larger extent governments, have in recent years become more reliant than ever on the consistent operation of their information systems (ISs), which have become critical to their success and efficacy. Even though the growing dependence on ISs has created a pressing need for gathering information and easing its accessibility, security vulnerabilities in the systems have unfortunately spawned opportunities for hackers to compromise the system’s integrity and validity. This has put information systems confidentiality at high risk. As this research shows, user authentication mechanisms, particularly passwords and fingerprint, determine confidentiality, which is an essential aspect of IS security. Passwords have been and are still a common method of securing ISs. A problem arises when users need to memorize and manage passwords that meet requirements, namely that users are more likely to use a single password across multiple accounts. User selection of passwords for use in ISs creates an impasse for the user. Furthermore, the systems progressive reliance on passwords for user authentication points to the necessity of investigating password creation policies in organizations. In spite of organizations recommendations on password choice to users, the majority do not choose to protect their passwords or even require choosing strong passwords in effect making hackers work easier. This study uses a survey questionnaire to evaluate user-generated password characteristics and present findings that prove user negligence with regards to password choice. Additionally, this study proposed a Cloud-ID-Screen scheme which considers as an alternative fingerprint authentication tool. The Cloud-ID-Screen utilizes low cost cloud storage and scalable cloud computation to improve security and privacy of fingerprint data in the cloud. Cloud-ID-Screen achieves this improvement by splitting fingerprint features into small subsets and distributing these small subsets over multiple clouds simultaneously, where no single cloud stores all subsets of a fingerprint. Our experiments show that Cloud-ID-Screen achieves comparable accuracy in matching while being statistically significantly faster as compared to the baseline.