FURMAN COMPUTER SCIENCE

Prove Yourself:

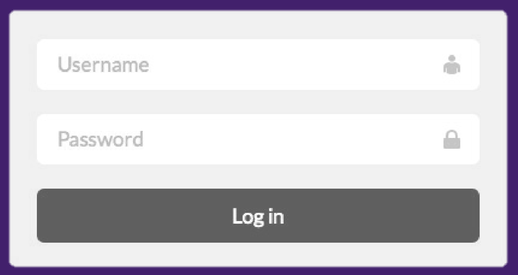
Zero-Knowledge Password Authentication

Johnathon Schultz

Introduction

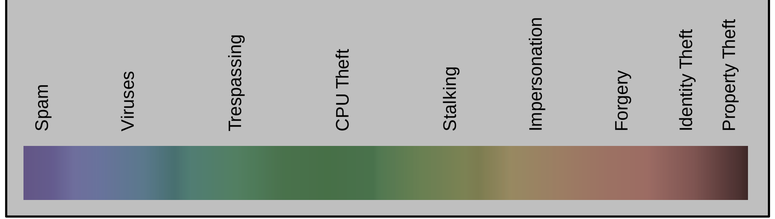
In an Internet driven society, authentication (ensuring an individual is who they claim to be) is a major conundrum. Providing the ability to discern and verify genuine users amid mistyped passwords and hackers, while protecting their security and trust from data breaches, appears seemingly insurmountable. Does authentication *require* the transmission and storage of users' passwords? What if a user's identity could be verified within a statistically insignificant margin of error? Zero-Knowledge Password Authentication (ZKPA) provides a method for verifying users with a server without revealing or passing along any information regarding the users other than the fact that the users know their password.

Figure 1: Application Interface



Why Should You Care?

Compromised credentials open a spectrum of threats:

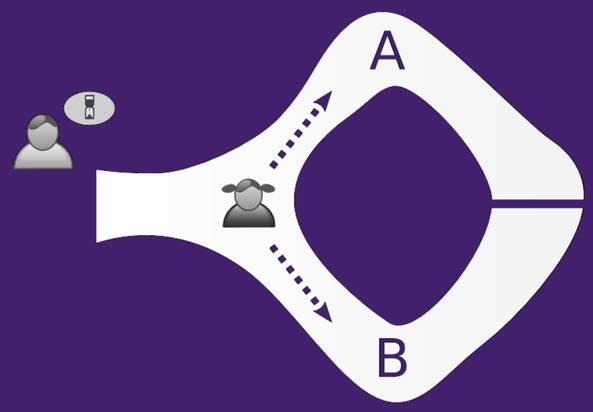


ZKPA Requirements

By definition, ZKPA must satisfy:

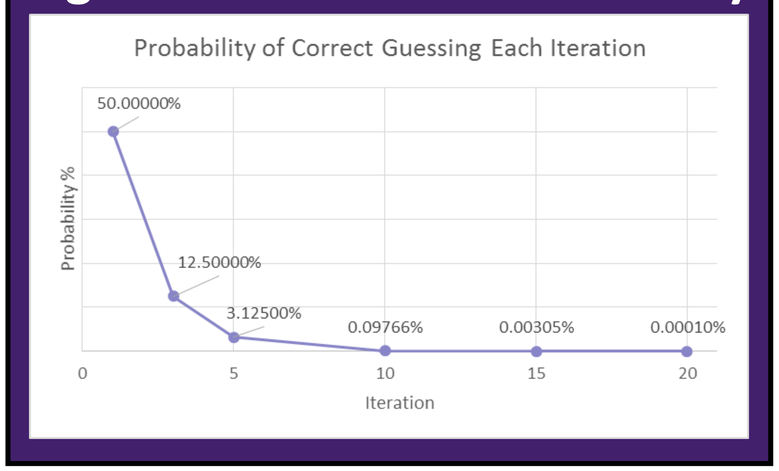
- Completeness – an observer will be convinced by an honest client possessing the password.
- Soundness – an honest observer will not be convinced by a cheating client not possessing the password (aside from a small probability).
- Zero-knowledge – a cheating observer doesn't learn anything from a honest client possessing the password other than the fact that they possess it.

Figure 2: Basic ZKPA Concept



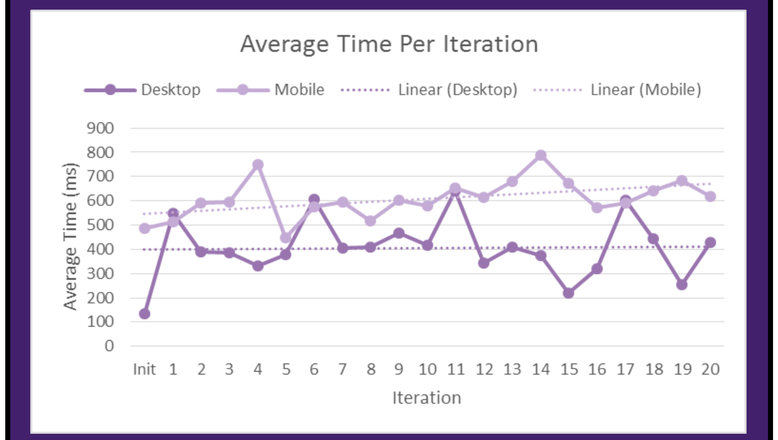
In Figure 2, a user is given two paths, A and B. At the intersecting termination of the paths is a locked door. To begin ZKPA, a user arbitrarily choses an initial path. Then, for several iterations, an observer issues the user a challenge by requesting the user appear on a particular path, A or B (chosen at random), potentially by means of the locked door. If the user fails to appear in the requested path, the observer can be confident the user does not have the password. To the contrary, if the user does, in fact, appear in the requested path, the observer can become more confident that the user has the password to the door. By asking a series of challenges and analyzing the results, an observer is able to determine whether or not the user has the password to the door with confidence.

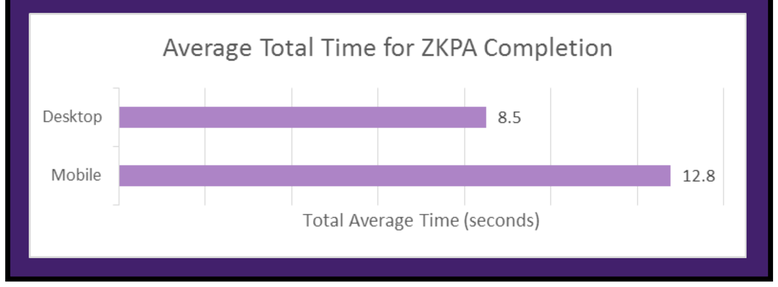
Figure 3: Basic ZKPA Probability



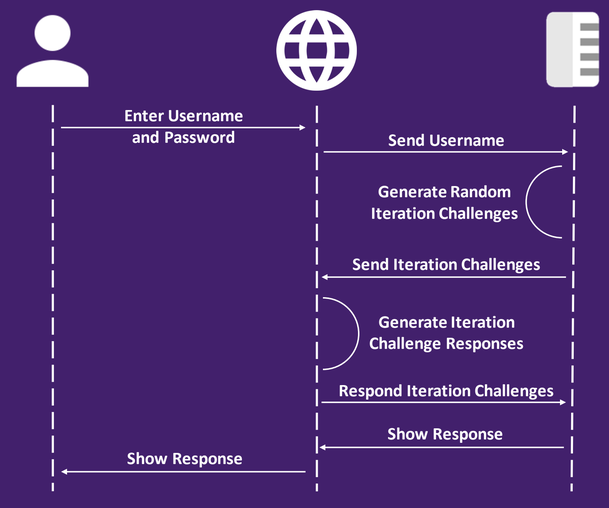
In any particular single instance, a cheating user has a 50% chance of guessing correctly, however, with each additional iteration, the overall probability of simply guessing all correct answers becomes increasingly small (Figure 3). Therefore, if a user repeatedly shows up on the requested side for enough iterations, an observer can conclude with great certainty that the user possesses the password within a statistically insignificant margin of error.

Figure 4: ZKPA Performance





Conclusion



Due to the prevalence of password-based authentication and current authentication protocols throughout the Web, as it stands, a large trust is placed on Web applications to securely store user information. ZKPA offers the ability to discern and verify genuine users without transmission or storage of users' passwords. However, the limiting factor for ZKPA is the amount of time required to obtain confident authentication of a user, Figure 4. A proposed protocol to reduce communication time by concatenating challenges is shown above. Future work in reducing computation and communication costs in an effort to minimize average total time for ZKPA will allow ZKPA to rival conventional authentication protocol methodologies.