Carson Stevens

HASS475

Summary Paper 1

September 5, 2019

The current problem with user authentication lies in the acceptance of security or usability, but not both. As passwords need to get stronger to deal with increasingly complex attackers, usability suffers as users “hate” having these more complicated passwords. The development in new techniques such as biometrics or others have created new ways to administer passwords, but they all compromise some security lacking the true security of the “original” password schemes. Due to the diversity found in all these schemes, comparison and consensus between what’s best is undecided. To try and solve this problem, the paper discusses a benchmark test containing 25 properties pertaining to security, usability, and deployability that all schemes can be compared against to highlight their different strengths and weaknesses. Despite thorough analysis, it was noted that not all websites employ these schemes correctly and that not all users follow the policies set by these schemes. This seems to be the biggest problem regardless of the scheme. Users want a fast and easy to use scheme that isn’t difficult to remember, but compromising for those aspects places strain on security and deployability. One particular insight describing the average amount of passwords and accounts reveals the reuse of passwords giving more vulnerability. Another fault shown from this is that users can’t even remember all the sites they have accounts with meaning that the password for it is surely forgotten. With the internet growing rapidly and the amount of accounts that users have, it is

becoming even more important to find a way to secure accounts. Multiple accounts with reused passwords is a weak link. Seeing that “50%” of websites don’t employ schemes correctly or to their fullest extent leads to the conclusion that if the user signs up for one site that is lacking, their accounts on more secure sites could also be compromised. Since users are often unaware of the exact security implementations (which is how it should be for security reasons), the user has no concept about what sites are safe and which ones are secure. Without knowing this, the most secure solution would be to use different passwords for everything, but this falls victim to the usability category discussed. An interesting aspect of the researchers found was that developers of these security schemes are often bias towards their own schemes and are blind to their faults. They focus more on one of the 3 categories than the others leading to poor schemes. Through their comparison, schemes can be compared to show marginal improvements for increasingly complex authentication or a compromise in security for better usability. In the end, it might be up to the user to protect their own information by employ secure passwords and strictly following policies. Although there is hope for stronger schemes that fit more of the discussed benefits, in the meantime, it seems that it should be the user’s job to abhere to the policies in places and that by reducing incorrect practices regarding security, a drop in vulnerability with current standards could be seen. Educating users about what good practices are might better help the situation too since uninformed users are probably the most at risk. I found it interesting that the paper failed to mention any notion of educating users about how to properly use schemes, though this might have been touched in the *Easy to Learn* section. I think there is a clear distinction in learning how to use and learning proper safety procedures. In the end, increasing the user’s understanding

about how things are vulnerable will make users more accepting of less usable schemes in favor of things to protect personal information.