Cory Bryan

SE4930

January 9, 2012

Article Summary 2

Using Fingerprint Authentication to Reduce System Security: An Empirical Study

This article, written by Hugh Wimberly and Lorie M. Liebrock from the New Mexico Institute of Mining and Technology, covers a study performed with 96 mostly undergraduate volunteers on password security with and without a fingerprint reader as a second authentication factor. The point of this research was to determine how users' password behavior changes when additional levels of security are added to a system.

Participants were asked to create two accounts, one of which was protected by both a password and a fingerprint reader, and the other with just a password. They were then given $5 to split between the accounts as they desired. Participants were told that they could keep the money from the accounts that weren't compromised during the study. Accounts were created through a guided desktop program which randomized the creation order, and then asked each participant a series of questions as to how secure they felt each account was.

The researchers used several techniques to determine the strength of each password entered. John the Ripper was used against the hashes to assess the strength of the chosen passwords, and left to run 24 hours in each mode (mangling, iterative, and markov). The passwords were also recorded in plain text to estimate the amount of time needed to break them using offline attacks.

The passwords participants used in this study were significantly stronger than expected. The researchers believe this to be the case due to several factors. The first is that the participants were largely more familiar with computers than the people who have historically had their passwords leaked onto the internet. The second is that the participants were told that their accounts would try to be hacked, so they used stronger passwords because of this knowledge. They also only needed to log into their accounts a couple times, so the inconvenience of stronger passwords wasn't important. The third factor is that the participants believed they were in a password strength competition.

Based on this study, the researchers determined that people almost always use a weaker password when they feel there are additional security measures keeping their information safe, in this case the fingerprint scanner. The participants tended to put more money in the fingerprint-using account due to this sense of extra security. The researchers also noticed that as participants' faith in the security of the account grew, the weaker their passwords became.

In their conclusion, the researchers determined that while the passwords participants used in this study were stronger than what they expected, they feel that a similar decrease in password strength would occur with real user passwords. They conclude the paper saying that studying user behavior should be a more significant focus in the field of computer security, and that anticipating this behavior will become more important as systems become more secure and users become the weakest link.

Source:

Wimberly, Hugh and Lorie M. Liebrock, "Using Fingerprint Authentication to Reduce System Security: An Empirical Study", IEEE Symposium on Security and Privacy, 2011.