Conrad Buerger

Developing Secure Software

SE 4930

More Security Equals Possibly Less Security

For: Dr. Schilling

January 25th, 2012
In review of the article “Using Fingerprint Authentication to Reduce System Security: An Empirical Study” there are many interesting topics that this paper discusses. One of the main points of the paper talks about a study done that shows how less secure people are when they are confronted with using multiple types of security.

The study discussed in the paper laid out a fake account registration system that took users through two account creations. One was protected just by a password while the other was protected by both a fingerprint and a password. To make sure that the process was totally random, they made the account creation orders random for the users so that the data recorded would have no random trends. The volunteers were told that their accounts would have five dollars total inside them. If the accounts were broken into, the hackers would get the money, this was incentive to make conditions realistic so people would take this more seriously rather than put in bogus passwords. To measure the amount of confidence that the users had in each of their accounts’ security, they were allowed to allocate five dollars split any way between the two accounts. The period they had to wait to see if their accounts got hacked was one week. This was bogus information since there are no hackers, so no matter how the users put the five dollars in their accounts, they were going to get the money they were promised. The results that were gathered from this experiment gave many results. To test the strengths of the passwords for both accounts, the study used a program named Jack the Ripper with the plugin Markov. The program was ran on the user’s passwords over twenty-four hours and during this time only 16.8 percent of passwords for password only accounts could be hacked, while 28.4% passwords could be hacked of finger print accounts. Another interesting topic brought up was the education of the users in comparison to the length of the passwords used on their accounts. People without a GED tend to have long passwords when the password was the only object protecting the account, while when their fingerprint was also protecting the account the respective password was just over half the length of the password protecting the account without the finger print security. Also researched was the age of the
user in comparison to their password. The age group that had the longest passwords for both accounts was ages 35-44. Another interesting bit of information is that all the age groups had shorter passwords for their fingerprint accounts, thus providing evidence that a second security measure does not necessarily mean more secure. Overall, the results of the study show that when there are more than one security measure taken to protect an account, the account may not be more protected and could be even less protected depending what the security precautions taken are.

In conclusion, we have learned that even though some security systems may have in place multiple types of security methods, the information being protected may be at a higher stake than before. This was shown through a study that showed a trend that when people are confronted with multiple ways to protect an account, the user will not put as much effort into each security method. That is, passwords will be weaker and if the second security measure taken is also easy to bypass, then the sensitive information being protected could be put at a higher risk than if the information was protected by just a password.