**EMCS2020: Advanced Topics in Computer Security**

Post-Work Assignment: Personal Knowledge Questions for User Authentication

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

***Why are statistical attacks against personal knowledge questions effective?***

Statistical attacks are most effective when the application’s / site’s personal knowledge questions are too common. In cultures where people share many of the same experiences and qualities, can as common last names, the answers to personal knowledge questions tend to be the same. For example, questions about a person’s favorite things in America ( ie favorite food, color, etc ) tend to be the same things over and over again and don’t present any unique qualities. The Google researchers offer a number of different compelling statistics that should how easy it would be for an attacker to “play the odds” and guess the answers to these questions when the questions are not special enough.

**Does providing untruthful answers to personal knowledge questions (that is, potentially valid answers that are not accurate such as entering “New York” as your city of birth when you were instead born in “San Francisco”) increase user security?**

From a practical standpoint, my gut tells me that providing false answers to personal knowledge questions is a bad idea, especially since these questions are generally used to retrieve or reset a password that has been forgotten. Since the user is likely to forget their lie(s), or in an attempt to not forget them may write the answers down in a place where it may be exposed, lying is a bad idea. I think of the personal knowledge questions as reminder of identity like if you met a friend on the street that radically changed their hair. To verify they are who you think they are you would most likely wait to hear their voice, look into their eyes, take notice of their mannerism, etc. If those things seemed fake too, you might walk right past them and not recognize them at all.

***Does providing random answers (e.g., entering “4%oS8--RXh;=” as your city of birth) increase user security?***

A better approach ( versus lying or making up the answers to personal knowledge answers ) is to be smarter about obfuscating truthful answers if the questions are too common. For example, the answer to the city of birth question might be “ILNYC2019!” where the I and the L stand for “I Love”. The approach here may be considering “salting” the answers with a unique key that only the user understands: IL = I Love, IWBI = “I was was born in”, TMT = “Take me to”, and so on.

**As untruthful and random answers are more difficult to remember than truthful ones, which methods and/or tools could be deployed to make them more usable?**

“In cryptography, a salt is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase”, but in this case, it serves as a way of turning common answers into more unique keys. By salting the answer a user can create a way to obfuscate the answer without having to totally “make up” that they can’t remember.