Anthony Gimei

Assignment: Authentication Assignment

Greatest Challenge to Developing Secure And Manageable Authentication Process

Today’s computer systems and applications depend largely on User ID and Password to authenticate users. whereas this seems like the logical and most sensible way to secure a system from unauthorized use, it worked well as long as the number of id’s and passwords that a user had only a handful user ID’s and Passwords to remember. However, with the advent of the internet and with it, the innovation of web based distributed systems and ultimately the invention of the smartphone and smart devices, the issue of User ID’s and passwords has become an antiquated way for authenticating users due the complexity of these new distributed systems and the sheer number of ID’s and passwords that users have to remember today. According to a 2017 report by LastPass, an average business user has to keep track of 191 passwords! It should be obvious that it has become humanly impossible to commit to memory all these ID’s and passwords, and to add to that fact, there is the other issue of each system having different requirements for these credentials and that exponentially complicates the issue.

The current processes of creating and or enrolling users to create ID’s and password’s is riddled with weaknesses that expose many systems to security issues and breaches, these include, man in the middle attacks where a hacker can essentially intercept the process and thereby steal the credentials. The other issue with the current enrollment mechanisms is that they depend on the users providing information that may or may not be valid or true for the purposes of identifying the user. The biggest problem is that due to the incredible number of id’s and passwords users have to maintain, users will try invariably to reuse ID’s and passwords thus increasing the likelihood that a breach on one system can easily spread to multiple systems.

I believe that the greatest challenge in developing a more secure and manageable authentication system is that current systems largely depend on humans to both create the identity then commit these to their memory. It is a fact that in the real world, ID’s and passwords are not natural attributes that identify a human or entity, biometric attributes are what I can call true identifiers. Systems need to expand the use of biometrics if we are to create more secure authentication systems. The natural way we identify each other is by the use of a combination our senses, at the top would be visually and through vocally, so the use artificial intelligence and machine learning to increase the accuracy of facial recognition or other unique human features and voice recognition can greatly increase the accuracy of authentication mechanisms and greatly reduce breaches. These can be incorporated into 2-factor authentication where if a system may request for either of these in addition to the user ID’s and passwords.