Security professionals almost universally recognize that the UserID/Password system of authentication is fatally flawed. Sheer numbers of accounts and passwords make it impossible for users to remember. Varying complexity requirements and rules further complicate passwords. Password manager tools can help, but are not widely used or accepted. Mobile devices changed the game – entering a long, complex password from a mobile phone can be tedious. PINs and patterns to unlock devices have limited effectiveness.

Considering these factors, develop a short essay (approx. 500 words) on what you believe is the greatest challenge to developing a more secure and manageable authentication process. Here are some questions to consider when developing your position:

How difficult is it to enroll new identities?

How does the user registration process affect the authentication process?

How does the sign in process actually validate who is signing in?

How does the sign in process map authorization to the authenticated user?

How can I defeat the authentication process?

How can I defeat federated authentication?

Is there a better way to authenticate users than passwords?

What are common password risks?

What authentication risks do wifi and public networks create?

What about 2-factor authentication?

What about risks posed by the device(s) you access (storing passwords, session management, etc.)?

What about the use of default credentials?

And a couple interesting “on the horizon” ideas:

<https://nakedsecurity.sophos.com/2018/07/18/could-semantic-icons-replace-passwords-and-pins/>

<https://gfycat.com/PointedOptimalFrog>

There is no right/wrong for this discussion. The exercise seeks to determine a level of understanding related to authentication issues. We will discuss some of the topics and issues mentioned in the responses.

Todays 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 were few. With the creation of the internet and with it the innovation of web based 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 mainly because of the number of ID’s and passwords that users have to remember today according the a 2017 report by LastPass, an identity management company, an average business user has to keep track of 191 passwords! Which it is not humanly possible to remember all your passwords, add to the fact that each requirement for ID and password is different just exponentially complicates the issue.

The entire system of creating (enrolling) and ID and password to the authentication of the users is riddled with weaknesses that expose many systems to security issues and breaches. The current authentication mechanisms have several weaknesses, the most obvious is that they rely on users providing information that may or may not be valid or true for the purposes of identifying the user. The other big problem is that due to the incredible number of id’s and passwords users have to maintain, users will try invariably reuse ID’s and passwords invariably increasing the likelihood that a breach can easily spread to multiple systems.

The greatest challenge in developing a more secure and manageable authentication system is the dependence on human memory to remember user ID’s and passwords. User ID’s and Passwords are not the natural way humans identify each other. Systems need to move to more natural ways to identify users essentially expanding the use of biometric methods. The natural way we identify each other is by a the use of a combination our senses, the 2 most common ways we identify each other is visually and through voice recognition, so the use artificial intelligence and machine learning to increase the accuracy of facial and voice recognition can greatly increase the accuracy and 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.