USABLE SECURITY- THE WEAKEST LINK

A HUMAN COMPUTER INTERACTION APPROACH FOR USABLE AND EFFECTIVE COMPUTER SECURITY

Any Security system is only as good as the weakest link in the system.

-Schneier

In the case of human computer interaction systems, user behavior and attitude towards security serve to be the most exploitable means of compromising security. This behavior is easily exploitable and generally overlooked. Over and above personal users of the HCI, organizations are the most vulnerable entities. In general hackers are of the opinion that it is easier to trick humans into giving up passwords as opposed to actually hacking an unattended computer system. This conclusively states that the weakest link in security systems are humans.

There are several factors backing this conclusion. Humans have limited memory resources. With the number of devices/ accounts per person growing exponentially every year, they are forced to remember several passwords, most of which have stringent password guidelines. This leads to users succumbing to setting mundane, easily guess-able passwords. Most organizations require their employees to change passwords frequently. This also makes it cumbersome to remember the right password at the right times. Most financial institutions allocate 6 digit randomly generated numerical pins. These by far, perform the worst in case of recall and resetting frequency. The problems caused after a mandatory PIN change are directly in proportion to how frequently users access pin protected systems and these are inversely proportional the quality of PINs appropriated by the user to the system.

There are several good practices that need to be adhered to when setting a good password. Firstly, the password should be a pseudo random sequence of alphabets, symbols and numbers. Different systems need to be allocated different passwords that need to be unrelated to each other and they should be changed at regular intervals of time. But these practices are found to be cumbersome for the users hence they choose to ignore these tenets and flout the fact that they did. Some other reasons why users avoid adhering to the said rules are existential perception issues – their co-workers might think that they are untrusting or untrustworthy or pedantic. Accountability is another factor that's overlooked. There aren't commensurately serious repercussions to flouting laid-down password rules. Most users are ushered into a false sense of security where they feel that they aren't privy to any sensitive information that could lead them to be a target of hacking or they are simply complacent in their beliefs.

None of these problems can be solved by increasing the complexity of the password procedure. Alternative measures should primarily ensure the user that security is part of the process of using the system as opposed to a barrier. They must coalesce with the goals of every user and as such decisions regarding system and file access must be based on how the workflow is organized. Some alternatives with the disadvantage of added memory and network constraints are:

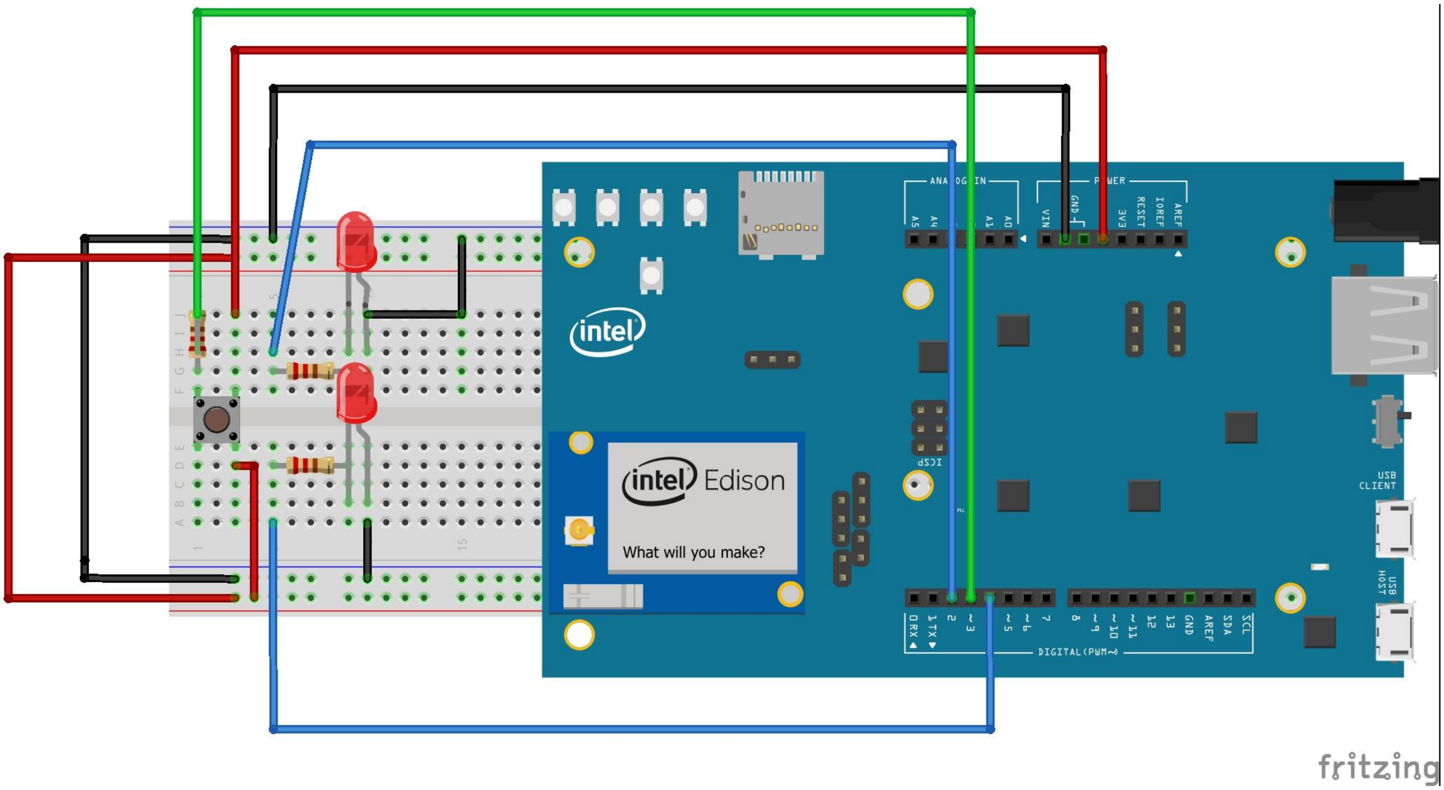
1. Composite weak authentication: it uses weak but memorable objects to verify the identity of the user.
2. Cognitive passwords: It fires a series of questions based on the users' personal preferences and history
3. Associative Passwords: word-pair or phrase associations
4. Pass Sentence Mechanisms: Prompts questions about the pass sentence so user can give a minimally required number of right words of the sentence.
5. Visual Authentication: Usually comprised of a visual scene of which user has to identify objects in the right order or select the right image from a panel of random images.

Most of these problems are usually solved by subscribing to a strict policy about security and repercussions following the breach of security while also impressing upon users their vulnerability from time to time.

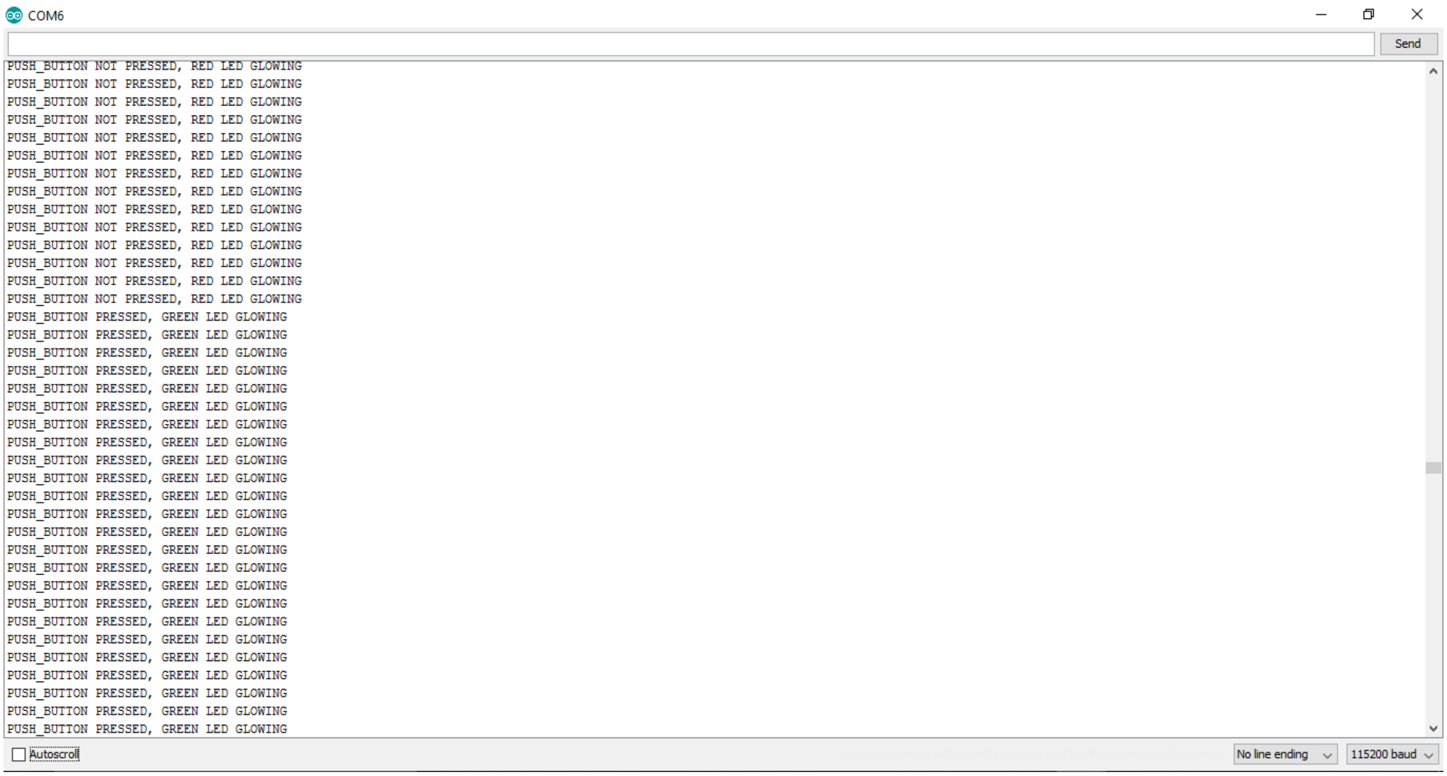
With recent developments in processor technology, biological passprints have become the norm. Thumb impressions, face recognition and voice recognition are usually the best and easiest recourses. Higher security institutions incorporate retinal scans in addition the above alternatives.

HW2

SKETCH



SERIAL MONITOR



```
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON NOT PRESSED, RED LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
PUSH_BUTTON PRESSED, GREEN LED GLOWING
```