Security Notes

Jack

September 27, 2024

1 Ideas

- Asymmetric
- Factoring Prime Numbers
- User has to encypt their password with cipher
- Box can only accept hashed/encrypted password,

  This will help with any kind of passcode leak. The adversary will have to have knowledge of cipher scheme.
- Enigma Machine and R2D2 Puzzle. The Idea is the user has to figure out the propper sequence of rotaions like r2d2 to connect the cypher circuit properly like the engima machine. If the rotation sequence is wrong the system will still operate, but even if adversary gets readable passcode, the sytem will decipher incorrectly like the enigma machine.
- once the cipher is rotated into position and the password properly authenticated, the system will reveal the key for unlock.
- The seed for the cypher can be determined by measuring a specific voltage across a complicated and potentially nonlinear circuit.

  The rotor wheels will connect the circuit in different ways changing the current/voltage of the measured line.

  The frequency response of the waveform can determine the arrival rate of poissons distribution, as a way to create the map. We can utilize more basic elements to construct the circuit. series and parallel resistors can create different currents or voltages that can create the cipher.

1.1 Process

- User approaches the box and inserts the cypher key into the ring array (R2D2 Lock). The user will turn and push the key accordingly just like a user of the enigma machine would set the rotors.

  There are many possible combinations, at least 256, of the rotor settings. All of them will power on the device, indicating to an unknowing adversary that the are "correct".

  Since only the proper rotor setting decodes the pass code properly, any attempt on the improper settings will fail.

- Proper rotor settings and password will reveal the true lock for the user to access with a key.

1.2 Questions

- Can we lax the size requirement to have fun with this locking mechanism idea?