COMPUTER SECURITY REPORT

Junsong Yang

School of Computer Science
University of Nottingham

1. PASSWORDS

In this section, the designed password and authentication policy will be proposed and justified. First, the password policy will be explained in detail with additional authentication measures. Then, mechanisms of storing passwords will be entailed.

1.1. Password Policy

The design of the policy is the result of balancing complexity and overall security. As Gollmann [1]suggested, the overall security may be diminished if one security mechanism is overstated. Users tend to bypass the mechanism if it is too inappropriate for them to properly work with, hence the overall security of the system may be weakened. By considering that, the following password policies are proposed.

1.1.1. Password Length

This policy enforces the minimum number of character required to use as a valid password. Generally, the short the password, the more like and easily to be cracked by brute-forcing. Hence, by setting the minimum password length to ten, the difficulty for brute-forcing password cracking would be noticeably increased.

1.1.2. Password Format

This policy intended to accumulating the strength of the valid password by requiring what and how many kinds of character must be included in a password. By requiring the password to contain at least one lower and upper letter, one number, and one special character, combining with password length policy, the possibility of successful brute-force cracking would significantly decreasing.

1.1.3. Password Ageing

This policy requires users to change their password periodically. The likelihood of password breaching would increase as time goes by, hence this is a appropriate approach to eliminate the risk of potential breaching.

1.1.4. Password Use

To further diminishing the risk of potential password breaching over time, additional mechanism need to be employed to block users from using the same password twice. This policy is essential to assist the password ageing policy to fulfil its purpose.

1.1.5. Login Attempts

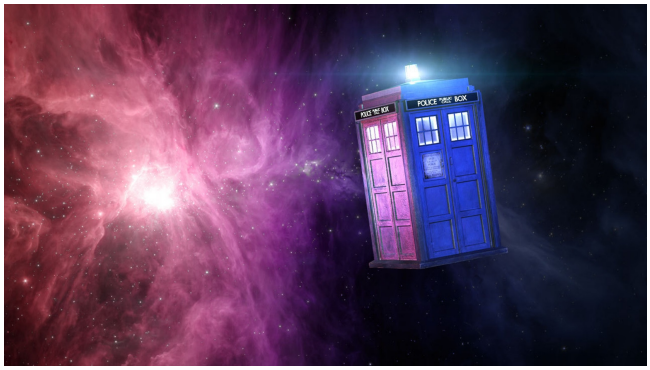
1.2. Additional Authentication Measures

TOCTTOU and Biometrics

1.3. Storing Passwords

2. FIREWALLS

3. SERVER SECURITY



(a) Result 1

(b) Results 3

(c) Result 4

Fig. 1. Example of placing a figure with experimental results.

4. REFERENCES

[1] Dieter Gollmann, *Computer Security*, Hoboken, N.J., 3rd ed. edition, 2011.