Password Strengthening: Using Multi-Lingual Passwords

Suman Bhoi*
https://orcid.org/0000-0002-9514-8088
Mir Residence, Telengasahi, Balasore, Odisha, India-756001

Correspondence Address:- Suman Bhoi*

Abstract:-

- ➢ ***Current Scenario:***

Passwords are required and used to secure cyber systems. Currently, cyber systems of decent security use passwords comprising of minimum eight characters which comprises of upper-case letters, lower-case letters, numbers and symbols from one language. Hence, all password-based systems are currently using monolingual passwords. Experimentally monolingual passwords can be broken within a matter of few seconds under given conditions, with given tools.

- ➢ ***Proposed Scenario:***

Here, we investigate (a) different factors of password strength and (b)compare the strength of monolingual password to multilingual password.

- ➢ ***Conclusion:***

The novelty of multilingual password lies in the increasing of password strength over monolingual passwords by factor of 100s to 10,000s or more. Hence, we conclude that multilingual passwords are better than monolingual passwords.

Keywords:- *Password Strength, Multilingual Password.*

I. INTRODUCTION

Passwords are ubiquitous. They are used to secure computers and other information processing systems. Cryptography and cryptanalysis go hand-in-hand. As systems got more complex, so are the passwords used to secure them. In the present era, it is required to use a minimum of eight-character password which comprises of uppercase letters, lowercase letters, numbers, and symbol. Currently, most systems have passwords that contain characters from one language, i.e. they are monolingual passwords. These passwords can be broken in just few days if not within seconds (Bošnjak, Sreš, & Brumen, 2018).

Password strength is an estimate of the efficacy of a password, which is the first line of defense against guessing or brute force attacks (Chanda, 2016). Password strength estimators measure the efficacy of password in terms of its bit strength and complexity. Password strength determines how many trials would be done in brute-forcing the password. The strength of a password is determined by its length, complexity and its unpredictability. In the following text, we also list some other factors on which the strength of a password-based security system depends.

- ➢ *Password Strengthening: Using Multi-Lingual Passwords*

The strength of a multilingual password is far greater than a monolingual password. When the language used in password is increased, it increases the character set used in the password. The increase in character set increases the number of possible entries for each character in the password, thereby increasing the password complexity itself.

Even then there are a few hurdles to the password strengthening method described in this paper as it requires the software handling the login-password module to be internationalized, i.e.- to have multilingual support enabled in the login module itself.

- ➢ *The following are the Determining Factors of Password Strength: -*

- *Password Encryption Type*

- ✓ Irreversible encryption
- ✓ Reversible encryption

- *Password Encryption Algorithm*

- ✓ AES
- ✓ Two-Fish

- *Password Storage*

- ✓ Plaintext
- ✓ Password and hash
- ✓ Password, salt and hash

- *Password Complexity*

- ✓ Bit strength
- ✓ Character set
- ✓ Randomness
- ✓ Character Encoding Scheme

- *Cryptanalysis Type*

✓ Password complexity
✓ Brute-Force

- *Human Factor*

✓ HUMINT level
✓ HUMINT strength
✓ Enforced password policy

- *Software Tools*

✓ Runtime debugging tools
✓ Password cracking tools
✓ Disassembler tools
✓ Rainbow tables

- *System (Hardware) Used in Decrypting (Brute Forcing)*

✓ CPU versus GPU versus ASIC
✓ Single threading versus multithreading processor
✓ Personal vs Cloud vs mainframe vs Super

- *Further Exploration*

✓ Heterogeneous platform architecture with CPU, GPU & ASIC.
✓ e.g.- HC-2ex Heterogeneous Computing platform

➢ *Determinant 1 ➔ Password Encryption Type*

The password protection strength primarily depends on the encryption mode used in password storage, i.e. whether the encryption is reversible or irreversible.

- *Case A:* When encryption is reversible — Password can be retrieved from storage in clear text thereby causing security breach.
- *Case B:* When encryption is irreversible— the security strength depends upon the encryption algorithm used in password storage.
- n.b.- Asymmetric encryption algorithm is stronger than symmetric algorithm.

➢ *Determinant 2 ➔ Password Encryption Algorithm*

The password encryption algorithm also determines the strength of security as the strength depends upon the encryption algorithm as well. e.g.: –

- AES encryption algorithm is stronger than Two-fish encryption algorithm
- AES-2048-bit is stronger than AES-256-bit
- JSH algorithm (Churi, 2014) is a newer and improved algorithm

➢ *Determinant 3 ➔ Password Storage Type*

The password protection strength primarily depends on how the password is stored, i.e. whether the password is stored as plaintext or hashed using a hash function and salted or not. A hash function is a cryptographic algorithm that is used to encode data into hash values.

- *Case A:* Password in stored as plaintext – A dump of the Login-Password database can reveal the passwords.
- *Case B:* Password is hashed through a hash function – A mere dump of passwords database does not reveal the password, it reveals the hashes. Further, the use of a honeyword password hash can make it difficult to decrypt the real password from the hash, if stolen.

➢ *Determinant 4 ➔Password Complexity*

The password protection strength also depends on the password complexity, which itself depends on the following factors: -

- Bit-Strength➔ This is the number of bits that the password comprises of.
- Character Set (ISO/IEC_8859-1, n.d.) ➔ This is the set of all possible characters that can be used in the password
- e.g.- Latin character set consists of 191 number of characters.
- Randomness ➔ It is the entropy value of the password, i.e., randomness of the password
- e.g.- Non-dictionary word is more complex than dictionary word.
- Character Encoding Scheme ➔ It is the encoding type of the password.
- e.g.- ANSI vs. UTF

➢ *Determinant 5 ➔Cryptanalysis Type*

The next factor affecting the password-based protection is the type of Cryptanalysis attack vector used. Various cryptanalysis attacks include the use of debugging tools, cracking tools, brute forcing, disassembling, etc.

However, we will consider only *brute-force attack* type in the discussion in this paper for comparing the password strength as brute force attack is the most common form of cryptanalysis.

➢ *Determinant 6 ➔Human Factor*

The next determining factor in security of any cyber physical system is human factor. The human sector involved in security administration determines the enforced security policies such as password policy, security policy, group policy, etc.

Here, we can also consider human-factor based attacks such as phishing, social engineering attacks, shoulder-surfing, catfishing, vishing, etc.

Hence, we can say that HUMINT strength also determines the strength of any cyber-physical system.

➢ *Determinant 7 ➔Software Tools*

The security required in a cyber-physical system depends on the threat matrix, which in turn is determined by the technology available to the adversary. Here, we will consider the software to available for cryptanalysis, e.g.-

Runtime debugging tools, password cracking tools, disassembler tools, rainbow tables, etc.

➢ *Determinant 8 ➔Hardware Tools*

The ability to break into a secured cyber physical system is heavily impacted by the hardware technology (Bošnjak, Sreš, & Brumen, 2018)being used in the cryptanalysis process. e.g.-

- Single threading vs multithreading
- CPU vs GPU vs ASIC vs FPGA
- PC vs Cloud vs Mainframe vs Super

A multithreading processor can process instruction at a faster rate than single threading processor. CPU is less efficient than GPU (Eun-Jin Im, 2011), which is in turn less efficient than ASIC or FPGA. The computing capability increases when we move from PC to cloud to mainframe to super, where a pc computes at a few gigaflops and supercomputers compute at a few teraflops.

➢ *Determinant 9 ➔Further Exploration*

When used to brute force a CPU used alone is lower than CPU used in conjunction with the GPU. An ASIC Specifically designed for the same task will be exorbitantly faster than a CPU used in conjunction with the GPU.

- *Hence, in Terms of Computation Speed:*

[CPU] < [CPU+GPU] < [CPU+ASIC] < [CPU+GPU+ASIC] < [CPU+GPU+ASIC+FPGA] (Liu, 2018)

➢ *Comparing the Strength of Monolingual Password to that of Multilingual Password*

Now that we have understood the different factors determining the password strength, we will proceed to comparing the strength of monolingual password to that of multilingual password.

A monolingual password in the English language consists of characters from the Latin script containing 191 characters. Currently, most enterprise systems run with 'Password Policy' of minimum eight characters including alphabets, numbers and symbols.

- *So, with 191 characters spanning an 8-character password, it's complexity value will be—*

$$191^8 = 1.7711973\text{e}+18 \text{ bits}$$

Proposedly, when using Tamil and English to form bilingual password, there would be an increase in the characters in character set of the password as English consists of 191 Latin characters and Tamil consists of 156 non-Latin characters. So, combined character set is 191+156=347 characters.

- *Then, with 346 characters spanning an 8-character password, it's complexity value will be—*

$$346^8 = 2.0540395\text{e}+20 \text{ bits}$$

When using Greek, Tamil and English to form a multilingual password, there would be an increase in the characters in character set of the password as Greek consists of 255characters (htt), English consists of 191 Latin characters and Tamil consists of 156 non-Latin characters. So, combined character set is 255+191+156=602 characters.

- *Then, with 602 characters spanning an 8-character password, it's complexity value will be—*

$$602^8 = 1.7249318\text{e}+22 \text{ bits}$$

II. CONCLUSION

Table 1 Comparison of Monolingual Password to Multilingual Password

No. of Languages in Password	Total no. of characters in Char-Set	Bit-Strength of Password (in bits)
1	191	1.7711973e+18
2	346	2.0540395e+20
3	602	1.7249318e+22

From the previous section, the finding of comparison of monolingual password to multilingual password is shown in table 1.

So, a bilingual password is 100 times stronger than a monolingual password, and a trilingual password is 10,000 times stronger than a monolingual English password. To sum it up**,** *the use of multilingual password increases the bit-strength of the password by a factor of 100 to a factor of 10,000.* It is wise to conclude that multilingual passwords are stronger than monolingual passwords. **The more the no. of languages in your password, the stronger your password is.**

REFERENCES

[1]. (n.d.). Retrieved from www.ascii-codes.com/ cp869.html

[2]. Bošnjak, L., Sreš, J., & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1161-1166). Opatija, Croatia: IEEE. doi:10.23919/MIPRO.2018.8400211

[3]. Chanda, K. (2016). Password security: an analysis of password strengths and vulnerabilities, 8(7). International Journal of Computer Network and Information Security.

[4]. Churi, P. K. (2014). JSH algorithm: a password encryption technique using Jumbling-Salting-Hashing. International Journal of Computer Applications, 92.2. doi:10.5120/15982-4900

[5]. Eun-Jin Im, Y.-M. K.-A.-I.-D. (2011). A homogeneous parallel brute force cracking algorithm on the GPU. ICTC 2011. Seoul, Korea (South): IEEE. doi:10.1109/ICTC.2011.6082661

[6]. ISO/IEC_8859-1. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/ISO/IEC_8859-1

[7]. Liu, P. L. (2018). An energy-efficient accelerator based on hybrid CPU-FPGA devices for password recovery. IEEE Transactions on Computers, 68(2), 170-181.