FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

THE PATENTS RULES, 2003

COMPLETE SPECIFICATION

(See Section 10; rule 13)

Title of the Invention

OPERATING SYSTEM INDEPENDENT AND FILE INDEPENDENT COMPUTER SYSTEM AND METHOD FOR AUTHENTICATING A USER

APPLICANTS:

Name in Full	Country of Residence	Address of the Applicant
Cialfor Research Labs Pvt Ltd	India	ODC-4, 4th Floor, Panchshil Tech Park, Hinjewadi Phase 1, Pune–411057, Maharashtra, India
Quantum University	India	Quantum University, Roorkee-247167, Uttarakhand, India

The following specification particularly describes the invention and the manner in which it is performed.

TECHNICAL FIELD

The present disclosure relates generally to user authentication method which is OS (operating system) independent and file independent system, and more specifically relates to preventing data theft by ensuring high level of security with strong passwords.

BACKGROUND ART

[0001] Password cracking is the process of trying to gain unauthorized access to locked systems using widely used passwords or password-guessing algorithms. In other words, it's an art form to discover the right password that grants access to a system that uses authentication.

[0002] In order to accomplish its objectives, password cracking uses a variety of strategies. During the cracking process, passwords can be checked against word lists or algorithms can be used to create passwords that match. Using input from a random or pseudo-random number generator, a random password generator is a software program or hardware device that creates passwords automatically. Using simple randomness generators like dice or coins, or by using a computer, one can create random passwords by hand or automatically.

[0003] The minimum length of a secure password is ten characters. In order to create an unpredictable string of characters that doesn't resemble words or names, strong passwords combine letters, numbers, cases, and symbols. To limit susceptibility in the event of a hack, a strong password should be specific to each account.

[0004] With the knowledge they obtain from password cracking, malevolent actors are able to carry out a variety of illegal operations. These include obtaining financial login information or utilizing the data for fraud and identity theft.

[0005] Nowadays, there are techniques that exists which can help generate

passwords. For example, reference can be made to US7698564B2 which discloses generating a single password for a plurality of different applications. Further, reference can be made to US8468598B2 which discloses password protection using false passwords. However, none of the conventional techniques disclose techniques for generating a list of passwords to be chosen from based on various preferences of the user extracted from multiple sources.

OBJECTS OF THE INVENTION

[0006] The principal object of the present invention is to provide OS (Operating system) independent and file independent computer system for authentication of the user.

[0007] Another object of the present invention is to provide OS (Operating system) independent and file independent computer system technique for creating secure passwords.

[0008] Another object of the present invention is to provide techniques for generating passwords based on preference of a user.

[0009] Another object of the present invention is to provide techniques for suggesting a list of passwords to user when the current password of a user is weak.

[0010] Another object of the present invention is to provide techniques for helping a user to crack password easily.

SUMMARY OF THE INVENTION

[0011] In one embodiment, an OS (Operating system) independent and file independent computer system for generating secure passwords is disclosed. The computer system comprises a memory, a preference generator configured to

extract preferences of a user from a plurality of sources, wherein a password generator configured to generate a list of passwords for the user based on the preferences of the user, a processor configured to compare password currently entered by the user and a password chosen by the user from the list of passwords, allow access to a secure file/folder based on the result of comparison.

[0012] In another embodiment, a method for generating secure passwords is disclosed. The method comprises extracting preferences of a user from a plurality of sources, wherein generating a list of passwords for the user based on the preferences of the user, comparing password currently entered by the user and a password chosen by the user from the list of passwords, and allowing access to a secure file/folder based on the result of comparison.

BRIEF DESCRIPTION OF DRAWINGS

[0013] Figure 1 illustrates a block diagram of a computer system for authenticating a user, in accordance with one embodiment of the present invention.

[0014] Figure 2 illustrating a flowchart of a method for authenticating a user, in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0015] While the present invention is described herein by way of example using embodiments and illustrative drawings, those skilled in the art will recognize that the invention is not limited to the embodiments of drawing or drawings described and are not intended to represent the scale of the various components. Further, some components that may form a part of the invention may not be illustrated in certain figures, for ease of illustration, and such omissions do not limit the embodiments outlined in any way. It should be understood that the drawings and the detailed description thereto are not intended to limit the invention to the particular form disclosed, but on the contrary, the invention is to cover all modifications, equivalents, and alternatives falling within the scope of the present

invention as defined by the appended claim.

[0016] As used throughout this description, the word "may" is used in a permissive sense (i.e. meaning having the potential to), rather than the mandatory sense, (i.e. meaning must). Further, the words "a" or "an" mean "at least one" and the word "plurality" means "one or more" unless otherwise mentioned. Furthermore, the terminology and phraseology used herein are solely used for descriptive purposes and should not be construed as limiting in scope. Language such as "including," "comprising," "having," "containing," or "involving," and variations thereof, is intended to be broad and encompass the subject matter listed thereafter, equivalents, and additional subject matter not recited, and is not intended to exclude other additives, components, integers, or steps. Likewise, the term "comprising" is considered synonymous with the terms "including" or "containing" for applicable legal purposes. Any discussion of documents, acts, materials, devices, articles, and the like are included in the specification solely for the purpose of providing a context for the present invention. It is not suggested or represented that any or all these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention.

[0017] In this disclosure, whenever a composition or an element or a group of elements is preceded with the transitional phrase "comprising", it is understood that we also contemplate the same composition, element, or group of elements with transitional phrases "consisting of", "consisting", "selected from the group of consisting of, "including", or "is" preceding the recitation of the composition, element or group of elements and vice versa.

[0018] The present invention is described hereinafter by various embodiments with reference to the accompanying drawing, wherein reference numerals used in the accompanying drawing correspond to the like elements throughout the description. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiment set forth herein. Rather, the embodiment is provided so that this disclosure will be thorough and complete

and will fully convey the scope of the invention to those skilled in the art. In the following detailed description, numeric values and ranges are provided for various aspects of the implementations described. These values and ranges are to be treated as examples only and are not intended to limit the scope of the claims. In addition, several materials are identified as suitable for various facets of the implementations. These materials are to be treated as exemplary and are not intended to limit the scope of the invention.

[0019] Referring to **FIG. 1**, a block diagram of an OS (Operating system) independent and file independent computer system 100 for authenticating a user is disclosed. The computer system 100 comprises a memory 102, a password generator 104, a user preference generator 106, a display 108 and a processor 110 coupled to the memory 102, the password generator 104, the user preference generator 106 and the display 108. In one embodiment, the computer system 100 may be connected with a server 112 via a network 114. In this embodiment, the computer system 100 may, in addition to, storing the data in the memory 102, also store the data in the server 112. Further, the computer system 100 constantly transfers and receives the data from the server 112 via the network 114.

[0020] The password generator 104 is responsible for generating secure and hack proof password for a user. The password generator 102 takes input from the user preference generator 106 section of the computer system 100. Thus, the password generated by the password generator 104 is based on the preference of the user. The preferences of the user can be obtained from multiple sources as explained below. The password generated by the password generator 104 is stored in the memory 102 which can be fetched by the processor 110 for comparison. Thus, when the password is generated based on the preference of the user, it is easy for the user to remember.

[0021] In one embodiment, the password generator 104 generates a list of passwords to be stored in the memory 102. The list of passwords can include all the possible combination of passwords which can be possible based on the

preferences of the user extracted from the preference generator 106. Further, the password generator 104 suggests different password to user if it is observed that the password generated by the user appears to be weak. The suggestion may be presented to the user on the display 108 of the computer system 100. The presentation of the suggestions can be based on different styled text presented to the user on the display 108. For example, an error message mentioning that the password chosen by the user is weak can be displayed on the display 108.

[0022] In one embodiment, the reason for weak password may be presented to the user on the display 108. For example, an OS (Operating system) independent and file independent computer system 100 may receive a list of weak passwords from the server 112 and store the list in the memory 102. The list of weak passwords may be generated by the server 112 over a period of time by learning the various passwords chosen by the user which have been compromised in the past. Thus, for example, if the password chosen by the user is simply his name and date of birth combination as “amit@31”, the server can inform the computer system 100 that “amit@31” is a weak password since it has been compromised in the past. Thus, next time if the user with same password and date of birth combination chooses such password, the computer system 100 can inform the user that this password appears to be weak with a reason that it has been compromised in the past.

[0023] The preference generator 106 can take input about preferences of the user from a plurality of sources. The plurality of sources may include, but not limited to, user’s likes and dislikes on the social media accounts, user’s choice of passwords on the other accounts and emails, user’s phone number, user’s name including formal and informal/nicknames, user’s date of birth as extracted from social media, user’s social security number as present on any website run by the government, any other details about the user which can indicate preferences of the user. The details can be included from any other platform except the social media platform (for example, user’s food delivery platforms, cab booking platforms, etc.). Thus, the input sources are not limited to the one mentioned here and can include any source which user’s preferences in any way.

[0024] In one embodiment, sentiment analysis may be performed on text present on the social media account of the user to determine preferences of the user. The text can be taken from the comments or the social media posts of the user. For example, if the user has commented on a picture of mountains that he likes Himalayas, the user preference generator 106 can store that mountains/Himalayas as the preference of the user.

[0025] In one embodiment, likings of the user can be considered as preferences of the user. For example, if the user has liked a photo of his friend having roll, the user preference generator 106 can store rolls as preference of the user. Similarly, the dislikes of the user can also be stored in the user preference generator 106. The dislikes can help the password generator 104 while generating a password for the user.

[0026] In one embodiment, the preference generator 106 can learn preferences of the user over a period of time. For example, the preference generator 106 use machine learning algorithms to learn the preferences of the user from various input sources. For example, if the user likes photos of Himalayas over a period of time, it can be learnt that the user prefers Himalayas, and the word “Himalayas” can be added to the preference generator 106. Similarly, if the user expresses his interest on the social media about his likings of “strawberry” a number of times, the preference generator 106 can learn that the user likes “strawberry”.

[0027] The password thus generated by the password generator 104 is a combination of ASCII characters, which includes alphabets, numbers and special characters. Thus, when the user desires to set the password of any folder/file, the computer system 100 suggests a list of passwords to the user. The list of passwords includes a combination of all preferences which can together make up a password. The combination can include names, likings, comments, date of birth, etc. All the preferences will be taken from the list of preferences stored in the memory 102 by the preference generator 106. The memory 102 may store the passwords in a form of a table. An illustration of the table is shown below,

however, the table is not limited to the one shown here, but can include other fields as well:

User Name	User DOB	User preferences from comments	User preferences from likings
Amit	31/01/1990	Himalayas	Arabian sea

[0028] The password generator 104 may then extract the preferences of the user from the memory 102 and generate a password. For example, the password generator 102 may parse each of the fields of the table 1 and generate a list of passwords using the combination of entries in each of the fields. The list of possible passwords may include, but not limited, to the following:

A. Amit@3101

B. Amitinhimalayas@1990

C. Amitinarabiansea@01

D. Himalayasandarabian@31

E. Amit@31himalayas

[0029] Thus, the passwords are generated in a way that it is easy to crack for the user. For example, as shown in the above list, the passwords are easy to remember for the user since the passwords are generated from the preferences of the user. Hence, in addition to having a secure password, the users can also have a password which is easy to remember.

[0030] A password can be chosen by the user from the list of passwords displayed to the user by the password generator 104. The chosen password is then set as the password of the user for securing a file or a folder. The next time, a user tries to access the secure file/folder, the user enters a password. The processor 110 compares the password currently entered by the user and the password previously

chosen by the user. If the password matches with the password chosen by the user before, the access is granted, or else, the access is denied.

[0031] Referring to **FIG. 2** now, a flowchart of a method for authenticating a user is shown. At step 202, the step comprises extracting preferences of a user from a plurality of sources. At step 204, the method comprises generating a password from the extracted preferences of the user. At step 206, the method comprises suggesting a list of passwords to the user based on the generated passwords. At step 208, the method comprises comparing the password with the password entered by the user. At step 210, the method comprises allowing access to the secured file if there is a match of the password. At step 212, displaying a list of weak passwords to the user.

[0032] The various actions, acts, blocks, steps, or the like in the flow diagram may be performed in the order presented, in a different order or simultaneously. Further, in some embodiments, some of the actions, acts, blocks, steps, or the like may be omitted, added, modified, skipped, or the like without departing from the scope of the invention.

[0033] Although particular embodiments of the invention have been described in detail for purposes of illustration, various modifications and enhancements may be made without departing from the spirit and scope of the invention.

I/We Claim:

1. An OS (Operating system) independent and file independent computer system (100) for authenticating a user, comprising:

    a memory (102);

    a preference generator (106) configured to extract preferences of a user from a plurality of sources, wherein:

    a password generator (104) configured to generate a list of passwords for the user based on the preferences of the user;

    a processor (110) configured to:

        compare password currently entered by the user and a password chosen by the user from the list of passwords;

        allow access to a secure file/folder based on the result of comparison.

2. The OS (Operating system) independent and file independent computer system as claimed in claim 1, wherein the list of passwords generated by the password generator is stored in the memory.

3. The OS (Operating system) independent and file independent computer system as claimed in claim 1, wherein the preferences of the user include name, date of birth, likings of the user.

4. The OS (Operating system) independent and file independent computer system as claimed in claim 1, wherein plurality of sources includes social media account of the user.

5. The OS (Operating system) independent and file independent computer system as claimed in claim 1, further comprising a display for notifying the user if the user has chosen a weak password from the list of passwords.

6. A method for authenticating a user using the computer system (100) of the claim 1 wherein the method comprising:

extracting preferences of a user from a plurality of sources, wherein:

generating a list of passwords for the user based on the preferences of the user;

comparing password currently entered by the user and a password chosen by the user from the list of passwords; and

allowing access to a secure file/folder based on the result of comparison.

7. The method as claimed in claim 6, wherein the list of generated passwords is stored in a memory.

8. The method as claimed in claim 6, wherein the preferences of the user include name, date of birth, likings of the user.

9. The method as claimed in claim 6, wherein plurality of sources includes social media account of the user.

10. The method as claimed in claim 6, further comprising notifying the user if the user has chosen a weak password from the list of passwords.

Dated this: 23rd Sept, 2022

Name:
TAPASYA DUA
IN-PA/1634

ABSTRACT

OPERATING SYSTEM INDEPENDENT AND FILE INDEPENDENT COMPUTER SYSTEM AND METHOD FOR AUTHENTICATING A USER

An Operating system independent and file independent computer system and a method for authenticating a user are disclosed. The computer system comprises a memory (102), a preference generator (106) configured to extract preferences of a user from a plurality of sources, wherein a password generator (104) configured to generate a list of passwords for the user based on the preferences of the user, a processor configured to compare password currently entered by the user and a password chosen by the user from the list of passwords, allow access to a secure file/folder based on the result of comparison.

[Figure 1]