Password Complexity Evaluation Instruments in Access Control Components of Cyber-Physical Systems

Anatoliy Ihnatovych[1], Vitaliy Pyvovar[2]

1. Department of Computer Engineering, Lviv Polytechnic National University, UKRAINE, Lviv, S.Bandery street 12, E-mail: ignatovicha@gmail.com

2. Department of Specialized Computer Systems, Lviv Polytechnic National University, UKRAINE, Lviv, S.Bandery street 12, E-mail: vitalya.pyvovar@gmail.com

Abstract – This paper describes usage of password complexity evaluation instruments as a part of access control components of cyber-physical systems. In particular, as password-based authentication remains the most widespread method of access control components today, we propose an instrument for password complexity evaluation, which can be used as a component of access control system of Cyber-Physical Systems.

Keywords – Password, Password Complexity, Cyber-physical system, Computer security.

Introduction

With recent developments of cyber-physical systems (CPS) assurance of cybersecurity of CPS during the process of their functioning in various subject areas is an actual task with growing importance. Security issues are particularly important at those CPS levels, where interaction with an individual takes part. As a rule such interaction happens at fifth level, where personal services usage has to be provided [1].

CPS architecture trends suggest that modern cyber-physics systems are created on the base of modular architecture. Besides, security components, as a rule, consist of several independent parts that can be connected and interact. Access control components are an important part of CPS cybersecurity infrastructure.

Significant approaches of access-control systems creation use identification methods based on biometrics – the recognition biological and/or behavioural characteristics of individuals. Although biometric and other innovative technologies are developing, password-based authentication is still considered to be the standard authentication mechanism for many services and components of CPS [2]. However, access control components based on password authentication are a weak point in cybersecurity despite many efforts [3]. Consequently, it is essential to use, create, modernize and explore tools for evaluation of passwords complexity for the access control components of CPS.

Formulation of the problem

We aim to develop a software solution for evaluating the complexity of passwords, which can be used as a component of access control in cyberphysical systems that are based on modular architecture.

Password Complexity Evaluation Module

For the purpose of solution of the described problem we propose to use password complexity evaluation module (PCEM) as a part of access control components of CPS. For calculating password complexity we are going to use a framework of threshold scores by checking whether password meets or does not meet a specific criterion. To define a set of criterions we explored existing systems for evaluation of complexity of passwords such as SeaMonkey Password Exporter, Password Strength Meter (jQuery plugin), Password Strength Checker (Cornell University), and Password Strength Tester (Rumkin.com project).

After analyzing disadvantages of the above mentioned services of password evaluation, we decided to create PCEM based on evaluating following set of criterions:

- password length;
- number of different types of characters (Latin and Cyrillic letters, numbers, special characters etc);
- absence of a specific word and/or its variations in the dictionaries and among widely used passwords (including checking the symbol replacement table, i.e. when "@" symbol will be interpreted as "a");
- in case of presence of other input fields, searching for matches of text there and password, for example comparing with individuals personal information;
- exploring time to find the password by brute force method;
- absence of repetitions or sequences of characters on the keyboard.

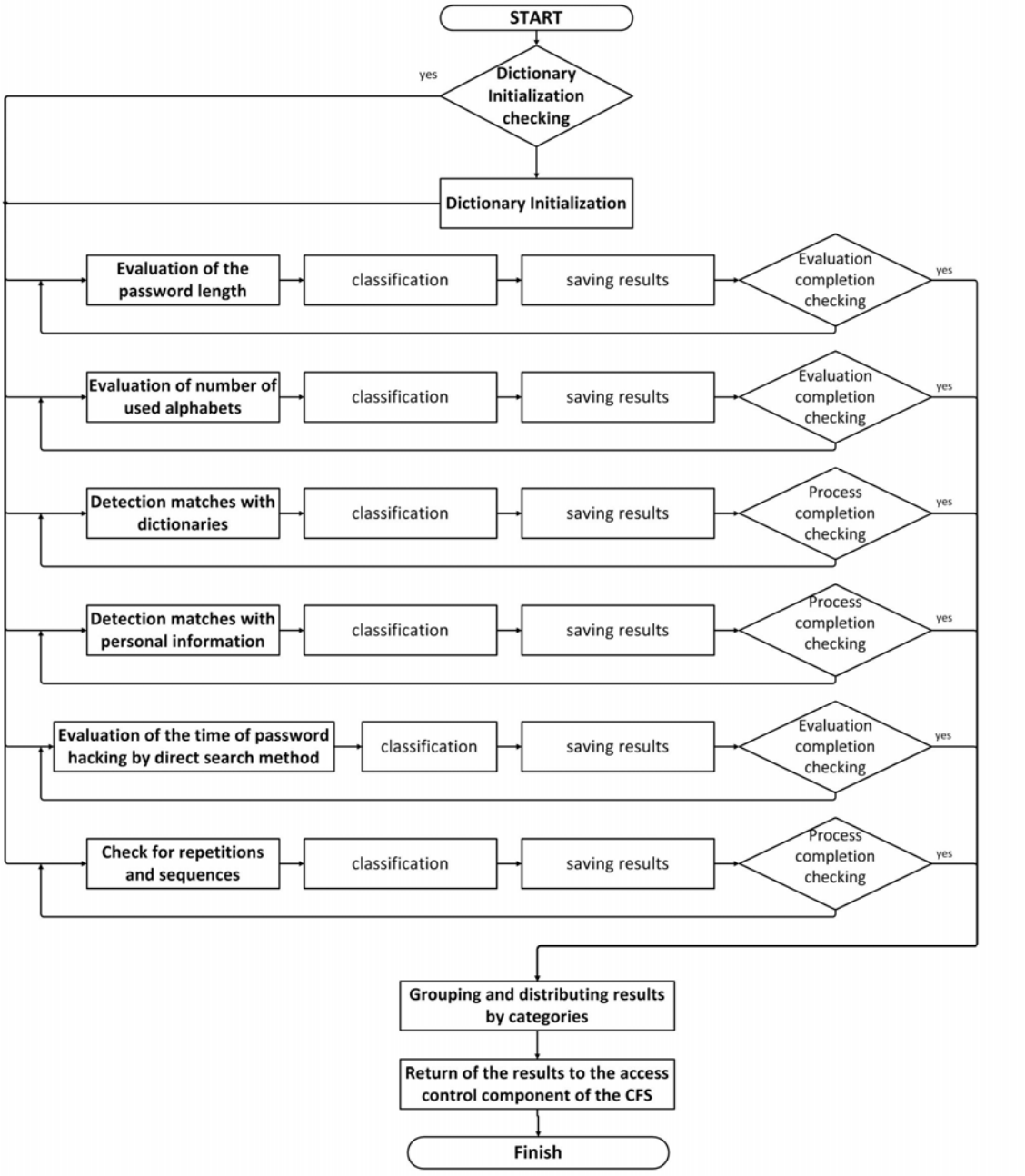

Fig.1. Block diagram of the functioning algorithm of password complexity evaluation module.

According to the given criterions PCEM will:

- evaluate password length;
- evaluate number of used alphabets;
- detect matches with dictionaries;
- detect matches with individuals personal information;
- evaluate time necessary for hacking password by the exhaustive search method;
- search for repetitions and sequences.

Thus, according to the proposed set of criterions created PCEM will sort passwords into several groups of complexity. The result of the evaluation given by PCEM will also include statistical information and will indicate number of characters, number of types of alphabets, similar word from the dictionary or other input fields if there are any, time required for password hacking by the direct search method and all replies and the sequence on the keyboard that the password contains.

Block diagram of the functioning algorithm of proposed password complexity evaluation module is presented on Fig. 1.

It is necessary to mentioned that PCEM consist of separate modules, so in case user has other criteria, they can be easily integrated to the system. Such PCEM allows you to evaluate passwords for as many features as possible. Also each developer has a possibility to set his own threshold scores according to critical parameters of CPS.

The system consists of two main blocks: the Angular2 framework test application (main CFS Access Control Component - MACC) and an independent Password Complexity Evaluation Module (PCEM), algorithm of which is proposed. Interaction process and ways of linking of MACC and PCEM is given on Fig. 2.

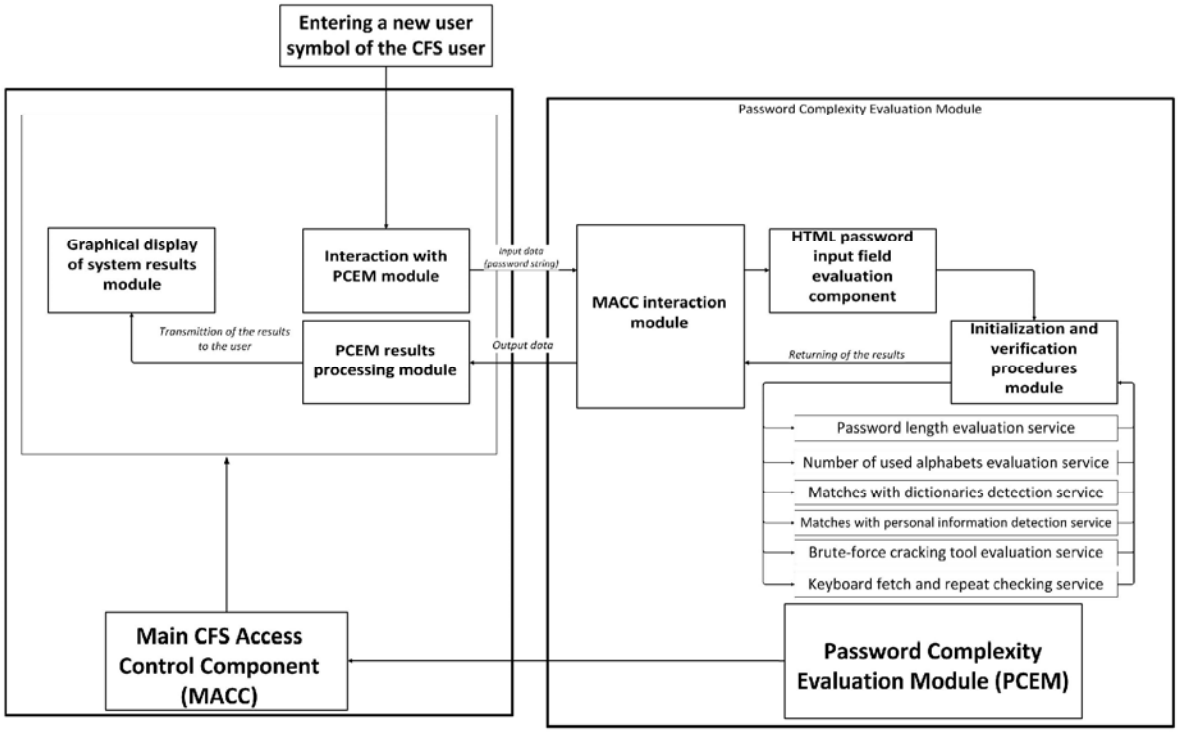

Fig.2. Structural scheme of the CFS access control component with the password complexity evaluation module.

Calling scheme procedures for the PCEM of CFS is presented on Fig. 3.

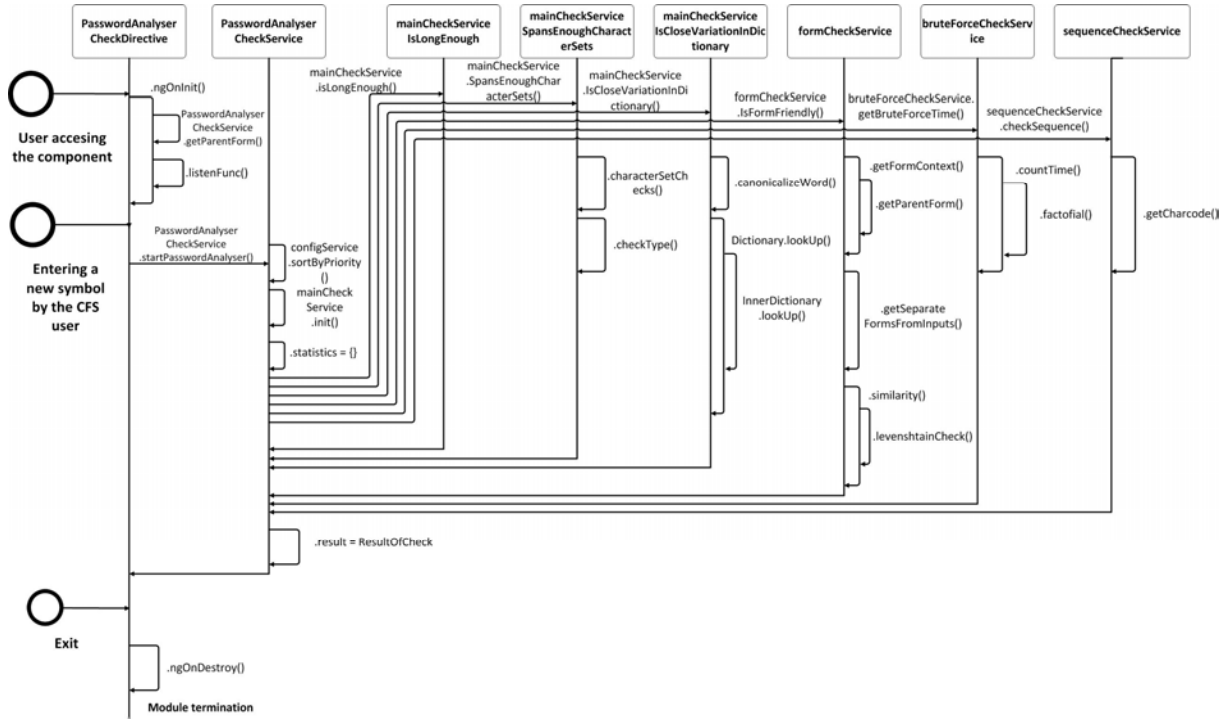

Fig.3. Calling scheme procedures of the PCEM.

As it is shown on the diagram, the system interacts with users through 3 events. Initialization takes place when the user logs in to the connection page. Not to slow down the system in the future the memory is cleared when the user leaves the PCEM. Entering each next character of the password a new password processing cycle is started. All evaluations are performed separately for each category of defined criteria.

Prototype window of the designed PCEM is presented on Fig. 4.

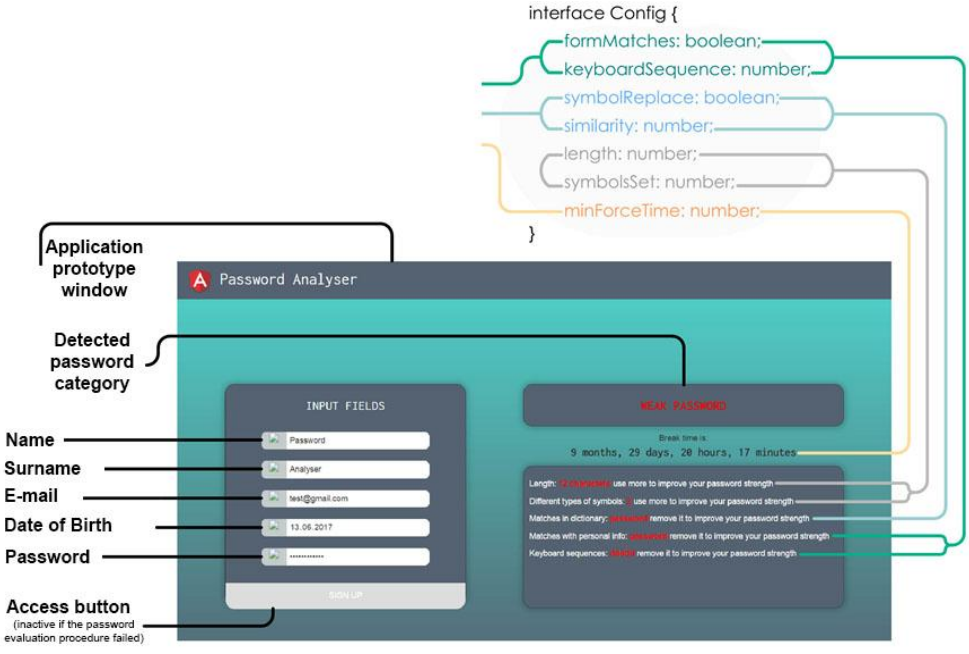

Fig.4. Prototype window of the created module.

Conclusion

Securing CPS is an important problem that is often sold by password protection. Users of CPS agree that good passwords are important, but they often choose bad passwords. Proposed in the paper PCEM software instument helps to achieve better password complexity by evaluation of passwords using threshold scores. Those scores and evaluation criteria can be changed by user of CPS and adapted to user requirements. Such PCEM allows user to evaluate passwords for as many features as possible. Furthermore, our module can be used separately or linked with other security modules to increase CPS protection.

References

[1] Melnyk A. O. Bahatorivneva bazova platforma kiberfizychnykh system// Kiberfizychni systemy: dosiahnennia ta vyklyky // Materialy pershoho naukovoho seminaru. – Lviv, 2015. – S. 5–15.

[2] IBM Security: Future of Identity Study [Electronic resource] // IBM Security. – 2018. – access mode: https://www.ibm.com/security/identity-access-management (applying date: 16.10.2018).

[3] Dell'Amico M., MichiardiI P., Roudier Y. Password strength: An empirical analysis. [Electronic resource]// Proc. IEEE INFOCOM – 2010. – access mode: https://ieeexplore.ieee.org/document/5461951 (applying date: 14.10.2018).