Access Field Communication using NFC

Prerna Padam Dhiman
Student, MCA Department Student,
Sardar Patel Institute of Technology
Mumbai, India

Mrunmai Sanjay Champanerkar
MCA Department Student
Sardar Patel Institute of Technology
Mumbai, India

Prof. Harshil T. Kanakia
Assistant Professor, MCA Department
Sardar Patel Institute of Technology
Mumbai, India

Abstract:-In today’s world, everybody is aware of the importance of the authentication process. And for this process, passwords play an important role. Many attacks on the major systems are related to passwords. It is important to understand the importance of correct usage of passwords and also how they can be used for proper authentication of the systems as well as how they can be protected from unauthorized access. This paper presents a study of different types of password attacks and a comparative analysis of the different authentication methods for awareness of attacks and selection of authentication method in a particular scenario.

Keywords: *Dictionary, Key loggers, security, brute force*

*****

1. Introduction

Password attacks are very common in today’s world. A person needs to understand different types of password attacks and understand the importance of secure authentication system. In this paper various authentication methods have been analysed and a comparative study has been presented of different methods.Here, we have tried to understand the advantages and disadvantages of different methods through their analysis. Finally, at the end we have a conclusion wherein we try to understand the various methods and how and where one can be used.

2. Password Attacks

Brute Force Attack:

In this type, all possible combinations of passwords are tried to break in a password. They are generally used for passwords which are present in encrypted format. These are very time consuming as it requires all the permutations and combinations to crack a particular password. For example, if a user enters a password which is of eight characters, all lower case then it would require (26)8 combinations to crack the correct password.

Dictionary Attack:

This type of attack tries to break in the password using the most common types of words or words of daily use.

It uses common knowledge of users because mostly people use passwords which are common to them like the names of their friends and family or some other common names. It is faster than brute force attack but it has its own limitations.

Shoulder Surfing:

Here, the attacker tries to spy the person. He/she may try to see what a user is typing and what key strokes he is using. The attacker can use closed circuit camera or video recording devices to capture the required password.

Key Logger:

The key loggers are software programs which monitor the user activities by monitoring each and every key being pressed by the users. Attacker needs to install this in the user system. He can do this by himself or by tricking the user to install the software himself. Hence, as all the information is maintained the attacker can get all the details of the user’s passwords and all the accounts. Therefore, he/she can gain unauthorized access to the system.

Video Recording Attack:

Here, the attacker tries to capture the user data using some kind of video recording device. And the user is unaware of the same.

4. Expected Outcome

Registration Process:

A Steganography key, which is obtained by embedding the encrypted passcode into the host photo using Steganography technique like Least Significant Bit, is transferred to user’s smartphone through a QuickResponse Code and will be used by the system to authenticate users. [1]

It proves to be a secure token as it does not allows unauthorized users to use the SAC (Stego Access Control) Application, without which a hacker or a third party would not be able to send the graphical password to the Middleware application even if they knew that the photo is the Steganography key.

Encoding and Decoding Process:

Users tap their NFC Enabled Smartphone in front of their NFC Reader to launch Stego Access Control Application where users will provide Graphical Password chosen during registration process, if the password is correct, users select the correct Steganography key from their smartphone. Steganography key and Graphical Password is sent to the middleware application.

System extracts encrypted passcode from the user’s steganography key based on Steganography technique and then obtains the decrypted passcode based on cryptography technique used in the encoding process from the user’s graphical password. [4]The Decrypted passcode is then compared with the access passcode stored in the server for verification. If both passcodes match, access signal is sent to unlock. [1]

5. Hardware Set up

After the Middleware successfully authenticates the user, a Control Signal is sent from Computer to Controller Board through a USB to UART interface to unlock the servo motor operated door lock. [2]If the Authentication is invalid, then the Control Signal is sent to devices such as Light Emitting Diodes or turning on of a video surveillance camera which indicates intruders.

6. Conclusion

It can be concluded that the proposed system uses the combination of existing system to build a better access control system which is more user friendly and easier to operate.

References:

[1] NFC room keys find favour with hotel guests. Retrieved from:http://www.nfcworld.com/2011/06/08/37869/nfc-room-keys-find-favourwith-hotel-guests.

[2] Fergusan, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering: Design principles and practical applications (1st ed.). Indiana, USA: John Wiley and Sons.

[3] Jain, A. K., Hong, L., &Pankanti, S. (2000). Biometric identification. Communications of the ACM, 43(2), 90–98.

[4] Raza, M., Iqbal, M., Sharif, M., &Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication.