Morse Passwords Based Authentication System

Jyotsana Raut
4th yr/ 8th sem I.T
D.B.A.C.E.R, Nagpur

Nikita Agashe
4th yr/ 8th sem I.T
D.B.A.C.E.R, Nagpur

Suchita Somkuwar
4th yr/ 8th sem I.T
D.B.A.C.E.R, Nagpur

Trupti Sapate
4th yr/ 8th sem I.T
D.B.A.C.E.R, Nagpur

Pranali Doifode
4th yr/ 8th sem I.T
D.B.A.C.E.R, Nagpur

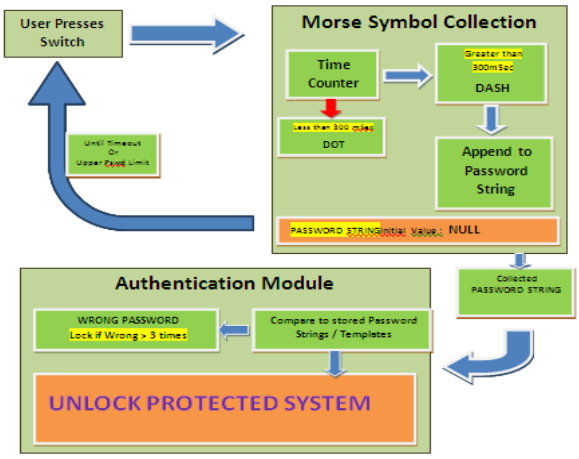
Ms.Minal Domke
Asst.Prof. (IT)
D.B.A.C.E.R,

Abstract-In this project, we are trying to develop a new kind of security system, which hasn't been seen before. We are trying to use the concept of Morse Codes, used as a communication method in emergency situation, and integrate it into an authentication security device. The project is both a combination of hardware and software that receive the Morse inputs from the user, decode them, and authenticate based on this information.

To develop a system that is immune to shoulder surfing and simple 'observe and guess' techniques of cracking passwords. To develop a system that uses such passwords that cannot relate to dates or instances relating to or belonging to a person's life, thus ensuring no resemblance between a person's chosen passwords and their life events or relations. To develop a system that is immune to fluroscent dye hack, by scorning the attack itself, by creating a system consisting of a single switch. To develop a system that is so minimalistic in design, that it causes confusion in a first time user. To develop a system that uses such low tech, and algorithms, that it is immune to attacks by high tech brute force gadgets and devices. To develop a system that abstracts its very input mechanism to a new and first time user.

I. Introduction

We are aiming to develop a minimal system, which is highly simplified in the context of its interface with the user. For the new, or novice user, such a system, due to its highly simplified and minimalistic nature, poses a strange, confusing, and hence a system that is difficult to understand and crack. We will present the user with a the minimal design and interactive device, a SINGLE SWITCH. This may be a push button switch or a bell switch as found in most homes. The actual use of this switch will be to provide Morse Style Inputs, in the form of combinations of DOTS (•) and DASHES (—). These combinations may not be from the standard Morse Codes table, and may be any sequential combination set by the user, and may be any length long. It may be noted that the system does not decode them as symbols of the Morse Table, but as a combinational entity, serving as a DOTS and DASHES string for the purpose of authentication. Following diagram illustrate the working.



User Presses Switch

Functional response begins when the user initiates action with the system by interacting with the switch i.e. the single switch dedicated for input of morse codes. This single switch is the only interacting input device given to the user.

Morse Symbol Collection

The input of the switch pressed by the user is given to the Morse Symbol Collection Module i.e. a functional unit that retrieves and decodes the Morse Symbols as per the duration for which the user pressed the switched. A Time Counter keeps

incrementing for as long as the switch is pressed. As soon as the switch is released by the user, the Time Counter would have attained a value. This value represents the time in milliseconds for which the user had pressed the switch. Based on this time duration, the current input symbol must be decoded as either a DOT or a DASH.

If the user had pressed the switch for under 300 mSec as is shown in the diagram, it is decoded as a DOT. However, this is only a representation and the actual threshold time value will be different and rather will be a defined range instead of a simple 'less than 300' condition. The range, in the real life implementation of the project will be decided based on an analysis of the

switch pressing behaviours of various users. A range between 250-550 mSec seems an appropriate choice for most people.

Similarly, a DASH is decoded when the switch is pressed for a duration longer than 300 mSec. However, this will also have to be a defined range rather than just a condition. A range of 800-1400 mSec seems like an appropriate value.

Password String

The Password string is actually a String type variable in the Morse Symbol Collection Unit. This string is initially empty thus having a NULL value. As and when each symbol is decoded, it is appended to this password string variable. Thus the password string is appended with dots and dashes as the user enters his password.

Timeout Condition

A timeout condition is defined to reset the received and decoded password string and start from beginning again, if the user stops interacting with the system for a specified minimum amount of time.

It is important to provide such a timeout reset mechanism as the user can only interact with a single switch, i.e. there is no separate cancel button to cancel the operation, hence there arises the need to have a resetting or cancelling mechanism involving the only switch he has. Hence, non-interaction with the switch for a specified amount of time leads resetting of currently gathered password symbols and system begins to wait for the user to enter new password from the beginning.

Collected Password String

The collected password string is the set of decoded morse symbols i.e. the password entered by the user in the current authentication session. This Password must be authenticated and hence is given to the authentication module for authentication.

Authentication Module

The authentication module compares the entered password with the set of stored Password(s). If a match is found, it is assumed that the user whose password it belongs to is the one trying to log in. This assumption is done because there aren't two input fields of 'user name' and 'password' for the user to log in, but rather he is determined by the password he enters

If the entered password IS A match to a stored password, the System Validates the authentication and access is granted. When we have attached our Morse Security System to a

Prototype Demo Vault or a Door, the system causes the vault or door to get unlocked upon entering the correct password.

Wrong Password

If the user enters a wrong password, the authentication module increments a wrong password counter, for consecutive wrong attempts. If a password is entered after a wrong attempt, the wrong password counter is reset to 0, thus ensuring that only consecutive attempts are logged via incrementing. A system lockdown occurs when the user enters a specified no. of consecutive wrong passwords in succession. This lockdown mode locks the target system, and cannot be unlocked even if the correct password is now entered. Such a lockdown can only be reset using a super user password which can also be called as an administrator password.

II. Problem statement

Security is a major concern in any authentication system. It is the goal of any authentication system to make the system impenetrable, un-hackable, and immune to attacks. Most of the conventional systems available however, fail to deliver on some if not all of these counts. Consider the most common types of attack. May it be the low tech shoulder surfing, where a person tries to obtain the password by simply prying in and trying to look when the person is entering his or her password. Some people who yhhave a rather modest experience with such techniques, gain expertise in obtaining the sequence and digits of the passwords, say in a numeric keypad by simply observing the hand motions of the person who is entering the password. A professional low tech technique is to use fluorescent dye in powder form to be sprinkled over a recently used keypad, which makes the buttons that were pressed glow, as the fluorescent dye highlights the body oils that stick on to the buttons while they were pressed. Such techniques, although cannot determine the sequence of how the digits were pressed, can at least identify which digits form the password. To a casual observer, one who knows some personal details of the user, can in most cases simply yet correctly guess the password even by looking at only a partial sequence of digits of the user's password. This is because of the tendency of most users to set their passwords same as a date, entity, event or such related material that is part of their life. Most common tendencies include setting the ATM password same as their vehicle registration number, last four digits of mobile number, or ddmm of a ddmmyy date of significance in their life. Or a high tech professional can use a custom built brute force attack gadget, which can be easily programmed to apply all possible combinations belonging to a given symbol set. Such devices can apply hundreds of passwords per second and are usually successful in cracking the password especially in a numeric password system. Thus, all existing systems have flaws and shortcomings that can be easily exploited by someone who intends to crack a user's password. It is therefore important that a new, better system be developed that can offer protection to the above discussed vulnerabilities.

III. Proposed scheme

Morse System

Beginning in 1836, the American artist Samuel F. B. Morse, the American physicist Joseph Henry, and Alfred Vail developed an electrical telegraph system. This system sent pulses of electric current along wires which controlled an electromagnet that was located at the receiving end of the telegraph system. A code was needed to transmit natural language using modern international morse code.

a. Keystroke dynamic

Keystroke dynamics is part of a larger class of biometrics known as behavioural biometrics; their patterns are statistical in nature. It is a commonly held belief that behavioural biometrics are not as reliable as physical biometrics used for authentication such as fingerprints or retinal scans or DNA. The reality here is that behavioural biometrics use a *confidence measurement* instead of the traditional pass/fail measurements. As such, the traditional benchmarks of False Acceptance Rate (FAR) and False Rejection Rates (FRR) no longer have linear relationships. The benefit to keystroke dynamics (as well as other behavioural biometrics) is that FRR/FAR can be adjusted by changing the acceptance threshold at the individual level. This allows for explicitly defined individual risk mitigation–something physical biometric technologies could never achieve.

Another benefit of keystroke dynamics: they can be captured continuously—not just at the start-up time—and may be adequately accurate to trigger an alarm to another system or person to come double-check the situation. In some cases, a person at gun-point might be forced to get start-up access by entering a password or having a particular fingerprint, but then that person could be replaced by someone else at the keyboard who was taking over for some bad purpose.

In other less dramatic cases, an employee might violate business rules by sharing his password with his secretary, or by logging onto a system but then leaving the computer logged-in while someone else he knows about or doesn't know about uses the system. Keystroke dynamics is one way to detect such problems sufficiently reliably to be worth investigating, because even a 20% true-positive rate would send the word out that this type of behaviour is being watched and caught.

.

Following Projects were referred

- Auto Disabling Security System for Speed Based Authentication
- Morse Coding System for Rapid Emergency Signalling
- Sample Durations Based Voice Passwords for Singing Unlock Systems.

IV. References

1) **https://instruct1.cit.cornell.edu/courses/ee476/FinalProjects/**

Cornell University ECE Final Semester Submissions

2) ***Advanced Human Computer Interfaces for New Age Security challenges.***

by John Piccirillo, Univ of Alabama, Feb '09

