TELKOMNIKA, Vol.12, No.3, September 2014, pp. 689~694
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v12i3.92

One-Time Password Implementation on Lego Mindstorms NXT

Barlian Henryranu Prasetio[1], Heru Nurwarsito[2], Wijaya Kurniawan[3]
[1] Computer System and Robotics Lab, Program of Information Technology and Computer Science, University of Brawijaya, Jl. Veteran Malang, Ph. Fax: +62341-577911
[2] Computer Networking Lab, Program of Information Technology and Computer Science, University of Brawijaya, Jl. Veteran Malang, Ph. Fax: +62341-577911
[3] Computer System and Robotics Lab, Program of Information Technology and Computer Science, University of Brawijaya, Jl. Veteran Malang, Ph. Fax: +62341-577911
e-mail: barlian@ub.ac.id[1], heru@ub.ac.id[2], wjaykurnia@ub.ac.id[3]

Abstract

One of the factors that affect the security of a network or system is user authentication, so that at times it can be said to be no longer safe. Brute force attacks on password systems are a dominant (static) potential way to penetrate network security or user authentication systems. One way to overcome these drawbacks is to use the One Time Password (OTP) algorithm. OTP is a password security system using dynamic passwords. The password will be valid for one session only. In this research, the author will analyse the reliability of the OTP algorithm by applying it to a LEGO Mindstorms robot. The robot will be designed as part of a system where the user will be safe to enter the default password, and then the system will change the password every session. The results of the questionnaire showed that 79% of users felt more secure, but more than 60% said it was difficult to do.

Keywords*: authentication, OTP, lego robot*

1. Introduction

Various methods have been designed or studied to improve the safety factor of a system or network associated with the user authentication problem. People tend to have a lot of accounts to ensure security [1], which can eliminate brute force and malware-based replay attacks [2]. One way which we know and have begun to implement is the One Time Password (OTP) algorithm. In this algorithm, the password will be dynamic; if there is any change in the session, the system will change the old password for a new password that follows certain rules and depends on the old password or users [3]. Along with the development of technology, embedded systems are already widely used to replace PC/desktop computers. This also encourages the implementation of the OTP algorithm not only to solve network security issues, but also to invest in embedded systems.

A good security system is important for people, so overcoming risks requires a major investment. As an analogy, valuable property is often stored in a box to protect it. Up to now, storage boxes for valuables have used mechanical keys. However, with the spread of technology a box is no longer considered to provide good security, because a replica key can easily be made. Instead a new alternative was made, using electronic keys. But this still had weaknesses.

So with these problems, we use an electronic locker box password for security systems [4]. The password used changes randomly every time. The main user password is used only as a main password. The password to open the box can alternate. The random password algorithm is known as an OTP algorithm [5]. One way to maintain password security [5] is that the saved password is not the same as the loaded password [6],[7].

This research emphasizes how to design the OTP algorithm system and how the OTP algorithm is represented using a LEGO Mindstorms robot. LEGO NXT brick uses a 32-bit ARM microprocessor that can be programmed by the user [8].

To analyse the system's reliability, the LEGO Mindstorms robots were designed into a locker system with a password using the OTP algorithm. In creating this system, the various objectives are:

Received February 27, 2014; Revised July 28, 2014; Accepted August 12, 2014

- Designing LEGO Mindstorms robots into a locker system
- Designing OTP algorithms that will be used in the system
- Programming the OTP algorithm locker system with the LEGO Mindstorms robots

2. Research Methods

The methods used in a research study greatly affect the performance of the system to be able to work optimally. In one study, a method that suits your needs is expected to run well, so that the given method or procedure can be followed. The methodology used in the research was:

1. Assembling the robots: intelligent mechanical hardware implementation that can be used - LEGO NXT Robot [9, 10]. In this section, the LEGO Mindstorms robots are assembled in order to become a locker system simulator that uses a password to open.
2. Designing OTP algorithm. OTP is created by following a certain rule that has been determined by the users [11] and is implemented to allow users to protect their accounts [12]. This section is designed to create an OTP algorithm; that is, how the rules are to be applied for the dynamic password system.
   Default password consists of three digits of which one is 0-99 decimal. The default password is stored in memory as a basic password system. When the user enters the password, then what is displayed is not the default password, but the password is a random result of a default password with a random sum. The three default password input combinations will also be created at random.
   For example:
   The default password 1 = 12
   The default password 2 = 8
   The default password 3 = 22
   Possible combinations (random) -> User Password:
   Enter the password 1 + 24 (random) = 36
   Enter the password 3 + 13 (random) = 35
   Enter the password 1 + 54 (random) = 67
3. Programming robots using LEGO-G software. In this section, OTP algorithms that have been designed in the previous stage will be implemented into the robot using LEGO-G compiler.
4. System Test. In this section, there will be a test of a locker system of LEGO Mindstorms robots already planted with an OTP algorithm for the system password.
5. Analysis. In this section, the system will be analysed based on the results of the tests that have been done in the previous stage.
6. To test the successful implementation of the research, there should be diversity in random passwords, different for each session, so as to make a security system box.

3. Results and Discussion

3.1 Hardware Implementation

Simulation of the hardware is done from a LEGO Mindstorms kit. A simulator locker password robot is shown in Figure 1.

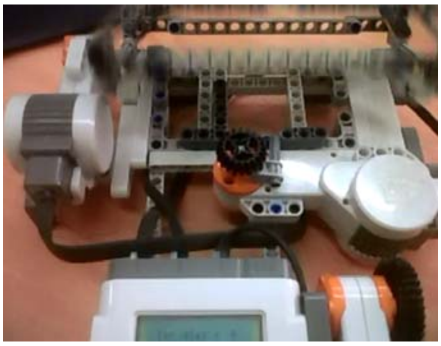

Figure 1. Simulator locker password robot

In Figure 1, the box contains an object or item; in the picture above there are two balls in the box. Then the box will be closed and locking using the OTP algorithm.

3.2 Software Implementation

The programming language used to create the OTP password locker LEGO Mindstorms is LEGO-G language. Figure 2 shows the LEGO-G code flowchart. The LEGO-S (LEGO Operating System) on top of an RCX system is an example of an operating system that enables infrared communication [13].

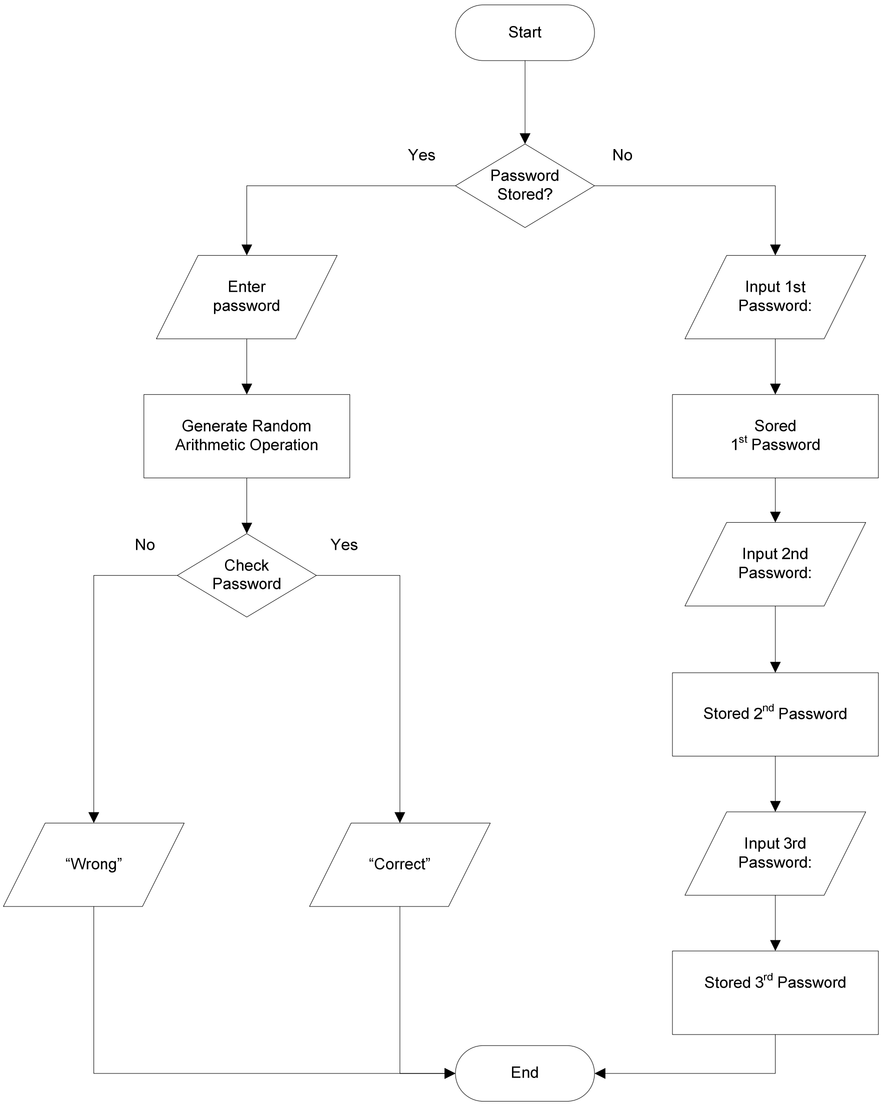

Figure 2. OTP Algorithm LEGO-G Programming

Figure 2 shows the program to create a LEGO One Time Password (OTP) using LEGO-G GUI software.The program consists of:

1. Coding section, so that each part of the LEGO motor rotation is converted into numeric data values to be changed up or down depending on the direction of motor rotation. It starts from 0 in the form of an integer number (0, 1, 2, 3, etc. or 99, 98, 97, etc.).
2. Display section: the value of the data obtained from the motor rotation to the existing display in the LEGO NXT Intelligent Brick.
3. Part branching (if-else) consisting of:

a. If the LEGO has not set a numeric value as a password, then the numerical value obtained from the motor rotation will be saved as a password to unlock the LEGO box .
b. If the LEGO has already set a password, then the numerical value obtained from the rotation of the motor will be used as the input of the user who wants to open the LEGO box. The box will open if the value of the user's number is the same as the numeric value of the password which is stored in the LEGO box.

3.2.1 OTP Generator on LEGO

1. Getting Started (Initial Step)

   There are three files that are stored in a LEGO. Each file stores a code number that is the password to open the LEGO box. So in total, there are three password numbers to open the LEGO box. The user can enter a password by turning on the motor, which functions as a LEGO rotation sensor. In LEGO displays, the first number that appears is zero (0). The number will be revised up or down according to the direction of motor rotation. How much the numbers increase or decrease is determined by using the system integer (0, 1, 2, 3, etc. or 99, 98, 97, etc.).
2. Computation Step

   An OTP is generated by applying a series of random functions to call one of the three files that store the passwords of LEGO. Each file named 1st dial, 2nd dial and 3rd dial will be displayed on the dial that LEGO displays so the user can adjust the value of the password that must be included in accordance with the instructions that appear. The process will be repeated three times.
3. Output Step

   When the user has to input the password correctly in accordance with the orders/instructions that appear three times, then LEGO will match the input from the user to the password file that is stored three times. If all three are correct, then the LEGO box will open, but if any one is wrong, then the LEGO box will remain locked.

3.2.2 One Time Password Schematics

Numbers are used to establish a series of OTPs starting from 0 up to 255; as much as three numbers value will be stored in three files with different names (1st dial, 2nd dial, 3rd dial). When the system is running, there will be a random process to call one of the three files. After a file is called, it will no longer process random numbers that add up the value stored in the file specified by a random number. In LEGO display, an injunction will appear requiring the user to add the random numbers with a numeric value and put a password into LEGO by turning the motor so it appears the numbers are the result of the sum. If the input entered by the user is correct, then the system will repeat the process twice again at random. In other words, the user must perform the above process correctly three times.

3.2.1 OTP Verification

The verification process checks whether the number entered by the user is correct. Checks are carried out three times. Suppose the first is A, the second is B, and the third is C, then LEGO will compute the true value of A and B and C. If the results obtained from the process are TRUE then the LEGO box will open.

3.3 Analysis

We use the questionnaire date to determine whether the system is working as intended. The questionnaire was given to 100 people. It contains four questions. Scores are given a value between 1 to 5, where a score of 1 represents very poor/strongly disagree and a score of 5 represents very good/strongly agree.

For a discussion and conclusion, we looked in detail at the value of each item shown on each score. For example, for statement 4, nobody gave a value of 1, 11 people gave a value of 2, eight people gave value 3, 56 people gave value 4 and 25 people gave value 5. Most of them stated that the system is safer than other similar systems. This is based on the contents stating that 56 people gave a value of 4 and 25 people gave a score of 5.

The results of a more complete analysis are presented in Table 1. The Average Score column is obtained from the total value of the score of each item multiplied by the score, divided by all respondents. In equation form, this can be expressed as the following Equation 1.

$$Hn = ((1*Cn)+(2*Dn)+(3*En)+(4*Fn)+(5*Gn))/100 \quad (1)$$

Where n is a number in every question.

For example, regarding Eq. 1 about how easy it is to remember the password combination, then the average score is:

$$\begin{aligned} H1 &= ((1*20)+(2*10)+(3*20)+(4*20)+(5*30))/100 = (20+20+60+80+150)/100 \\ &= 330/100 = 3{,}3 \end{aligned}$$

The value "3.33" of the maximum score "5" means that in general the respondents stated that the combination is pretty easy to remember passwords.

The % column is the percentage of respondent satisfaction, obtained from the average score divided by the maximum score. The equation is expressed as the following Equation 2.

$$In =(Hn/5)*100\% \quad (2)$$

For example, Eq. 1, the percentage of participant satisfaction is:

$$\begin{aligned} I1 &= (3{,}3/5) *100 \% \\ &= 66 \% \end{aligned}$$

This means that 66% of respondents felt it was easy to remember the password combination.

Table 1. Questionnaire Evaluation Analysis

No	Question	Score Average	%
1	Do you feel it easier to remember three numbers separately rather than a collection of some numbers as your password?	3.33	66.00
2	Do you feel it difficult to calculate simple arithmetic operations such as addition in your mind and remember the result?	3.26	65.20
3	Is OTP easier to use than other systems?	3.57	71.40
4	Do you feel safer with the OTP than other systems?	3.95	79.00

Overall, the average satisfaction of the respondents with the system was the lowest, at 65.2%, and the highest was 79% on the assertion that the respondents feel the system is more secure than other similar systems. The lowest value was 65.2%, for the statement that respondents find it difficult to perform simple arithmetic calculations to unlock the system. It can be concluded that this system has answered the desire of respondents to have a more secure system, but needs rethinking on how to let users easily perform calculations or bit rate if the password is to unlock the system.

4. Conclusions

The OTP system can handle a replay attack so that the password is actually safe. The One Time Password is to be used only once in the login process, so that if someone gets the password, the OTP cannot be used again for a subsequent login process. No confidential information is stored, so that if someone tries to search for stored data, that would be of no use. In the future there is the addition of extra features when a user forgets the password that has been entered into the system, and adding Artificial Intelligence in the OTP system. The results of the questionnaire showed that 79% of users feel more secure, but more than 60% said it was difficult to do because the user must perform the calculations in advance to enter the password.

References

[1] M Prakash, Viju. Eliminating Vulnerable Attacks Using One Time Password and Pass Text – Analytical Study on Blended Schema. *Universal journal of Computer Science and Engineering Technology.* 2010; 1(2): 133-140.
[2] O'Donnell, AJ. When Malware Attacks (Anything but Windows). *IEEE Transaction on Security and Privacy*. 2008; 6(3): 68-70.
[3] Huang, Chun Y. Using One Time Password to Prevent Password Phising Attacks*. Journal of Network and Computer Applications*. 2011.
[4] Sung-Ming Yen. Security of a One-Time Password Signature. *IEEE Transaction on Electronics Letters*. 1997; 33(8): 677-679.
[5] Hiltgen A, Kramp T, Weigold T. Security Internet Banking Autentication. *IEEE Transaction on Security and Privacy*. 2006; 4(2): 21-29.
[6] Yampolskiy, Roman V. Secure Network Autentication Using Passtext*. IEEE on Information Technology ITNG*. 2007: 831-837.
[7] Inayatullah. Analisis Penerapan Algoritma MD5 untuk Pengamanan Password*. Jurnal Iimuah STMIK MDP Palembang*. 2007.
[8] Trussel M. *Engaging with the NXT Prototype Board*. Spring Term. Swiss Federal Institute Technology of Zurich. 2009.
[9] Lund HH. Adaptive LEGO robot. A robot=human view on robotics. *Systems. Man and Cybernetics. IEEE*. 1999; 2: 1017-1023.
[10] Hayes GM, Hallam JCT. *Teaching robotics with Lego Robots.* Conference on Robotics and Education IEE Colloquium. 1997; 2(1-2).
[11] Chen C. *Ubiqutous One Time Password Service Using Generic Authentication Architecture.* School of Computer Science and Engineering, South China University of Technology. 2009.
[12] Harris JA. *OPA: a one-time password system*. Parallel Processing Workshops. 2002.
[13] Daesung Lee, Kim KJ. *Enabling Lego Robot Communicate Routing.* Conference on Information Science and Applications (ICISA). 2010.