Asian Journal of Information Technology 14 (4): 117-121, 2015
ISSN: 1682-3915

On Some Suggested Applications of Sudoku in Information Systems Security

[1]H.I. Okagbue, [2]Z.O. Omogbadegun, [2]F.A. Olajide and [1]A.A. Opanuga
[1]Department of Mathematical Sciences, [2]Department of Computer and Information Sciences,
Covenant University, Canaanland, Ota, Nigeria

Abstract: This study suggested different ways the application of Sudoku can be used in defending information systems against unauthorized access, abuse, spy or disclosure. This research showed how some simple mathematical and logical manipulations of Sudoku can generate passwords or one term passwords OTP. The enormous benefits of the research and possible applications are discussed.

Key words: Sudoku, information system, security, authentication, challenge response, passwords, one time passwords, stochastic challenge response mechanism

INTRODUCTION

The ever increasing threats to information systems inspired by unforeseen or yet to be identified vulnerabilities of information systems have led to upsurge in researches to reduce the ugly trend. Constantly, custodians of information systems are tasked with the responsibility to protect, defend or guide information systems against unauthorized access, spy, abuse, hijack, view, retrieval, modification, use, disclosure, copying, corrupting, monitoring, illegal transacting, or destruction. This huge mandate of securing information assets have yielded positive development in the information security as researchers have innovated many ways to tackle the threat posed by the increasingly motivated and sophisticated attackers.

This study exploits the stochastic and probabilistic nature of Sudoku puzzle to generate some passwords. Passwords are used in the authentication process before access is granted to an information system. Sudoku is a number puzzle and there are billions of them available online with different levels of difficulty. This study makes use of post filled 9×9 Sudoku and because the implementation of the recommendations of this research depends mainly of post filled Sudoku. It then means that some literature on ways of solving Sudoku is included for reference. Maire and Prissette (2012) designed an algorithm to solve Sudoku puzzle with different level of difficulty. Lewis (2007) advocated the use of Meta heuristics technique. Gunther and Moon (2012) solved Sudoku as an optimization problem. Santos-Garcia and Palomino (2007) solved Sudoku with rewriting rules using Maude.

The concept of Sudoku has been applied to some areas of computer and information security. Wu and Ren, Becker and Zou investigated different ways the Sudoku puzzle can be used in image authentication. Khalid *et al.* (2013) proposed the use of Sudoku as a watermarking scheme against corruption of digital image. Saisrikanth showed that Sudoku can be useful in access control. Shirali-Shahreza illustrated how to conceal a file in SMS using Sudoku to prevent unauthorized access to the phone. Agaian and Jassim developed an algorithm for image encryption using Sudoku. Because of the sensitivity and privacy of biometric data, Maji and Pal recommended some ways to secure biometric data using the Sudoku puzzle.

MATERIALS AND METHODS

This study identified different ways Sudoku can be used in information systems security. This methodology and choice of Sudoku is because it is cheap, readily available can be solved manually or with some cheap algorithms, unique with each solution, the chances of getting the same Sudoku is slim and can easily be mange using database management systems DBMS. Basic and some advance knowledge of mathematics were used to generate passwords which can also be one time passwords OTP or token using post filled Sudoku. This is important because passwords are used for authentication. The implementation of this challenge response mechanism using Sudoku will be in line with the organizations' information security policies, guidelines and procedures. Algorithms and flowchart may be developed by the security administrator for implementation. Challenge responses (passwords) are vital to access control which may be mandatory, discretionary or role based. The different suggested methods of using mathematical and

Corresponding Author: H.I. Okagbue, Department of Mathematical Sciences, Covenant University, Canaanland, Ota, Nigeria

logical techniques on Sudoku to generate passwords used for authentication. This means that during routine login by users, the system displayed a post-filled Sudoku and from the decision rule given by each user, he may be able to generate password for login and the details on how to generate the passwords are summarized in the result section.

RESULTS

Using this particular post-filled 9×9 Sudoku, we are going to demonstrate the various techniques on which Sudoku can be apply in securing information systems. All examples used in this study are from the data of this Sudoku (Fig. 1).

Generation of one time password OTP for routine login: An OTP can be generated from the given Sudoku together with other like the date of birth to attain strong authentication. This password changes at each login.

Example 1: Decision rule: {Date of Birth followed by first row of the last grid of the Sudoku}. The password is 18121987856 or 18DEC1987856.

Example 2: Decision rule: {The first column of the second grid of the Sudoku followed by your pet name}. The password is 941 the boy.

Example 3: Decision rule: {Maiden name followed by second row of the last grid of the Sudoku}. The password is Jones437.

Generation of passwords for Single Sign-on SSO access control: Generation of extra passwords can help in effective management of SSO by providing extra authentication to tackle the effects of reduced sign-on RSO. Single sign-on which is usually accomplished using the Lightweight Directory Access Protocol LDAP is vulnerable to misuse and abuse once the authentication is completed but with the help of Sudoku, an extra security features that require application of some assigned decision rules. This is in line with the merit of SSO as it reduces password fatigue. Those extra security features can be the use of a simple Sudoku to generate one time passwords to checkmate the abuse of security levels and to reduce the effects of service denials occasioned by non-availability of systems authenticated by SSO. These can be configured on authentication servers whether the SSO is Kerberos, smart card based, integrated window authentication, Security Assertion Markup Language SAML or mobile computing based. The user needs only to remember the decision rules after the initial authentication.

7	4	6	9	5	8	1	2	3
5	1	3	4	2	6	7	8	9
8	9	2	1	7	3	5	6	4
3	6	1	5	9	7	2	4	8
4	2	7	8	3	1	6	9	5
9	8	5	6	4	2	3	7	1
2	7	9	3	1	4	8	5	6
1	5	8	2	6	9	4	3	7
6	3	4	7	8	5	9	1	2

Fig. 1: The 9×9 Sudoku

Example 4: Decision rule: {For access to the applications, use the second row of any grid of the Sudoku}:

- Password for application 1: 513
- Password for software 1: 426
- Password for billing app : 695

The password strength can be increased by increasing the number of digits. This is based on the sensitivity of the information systems for example biometric database, healthcare database, missile launch codes, billing applications, terrorism and covert ops applications, etc.

Generation of passwords for multi-level access control: Sudoku can be applied to security level management where access to information systems are granted based on levels of responsibilities or role based (need to know) basis. Each level has a clear and distinct responsibility. The given examples illustrate how a security administrator can assign decision rules to different levels based on the organization's security policies. The assignment of these rules is different between and within the levels. Higher levels require stronger authentication.

Example 5: To logon to the system, a 9×9 post-filled Sudoku comes up.

Decision rule (For level 1): {the first 2 columns of the sixth grid of the Sudoku}, password: 263497.

For level 2: {The first 2 Rows of the last grid of the Sudoku followed by the user initials}, password: 856437h.i.o.

For level 3: {The first number that appears on each grid of the Sudoku}, password: 791352238.

For level 4: {The last number that appears on each grid of the Sudoku followed by the user initials}, password: 234521452g.e.j.

For level 5: {The user date of birth followed by the second number that appears on each grid of the Sudoku}, password: 0401199245269 4715 or Jan41992452694715.

Example 6: Assignment of decision rules between different levels were shown in example 5 and this example is about assigning different decision rules within the same level. This is necessary for accountability, audit and non-repudiation. Each decision rule is unique within and between all the levels. There are sub decisions rules within Level 1. All the users here are of level 1.

Decision rule for user A: {The last 2 columns of the third grid of the Sudoku}, password: 286394.

Decision rule for user B: {The last 2 rows of the third grid of the Sudoku}, password: 789564.

Decision rule for user C: {The first 2 rows of the third grid of the Sudoku}, password: 123789.

Decision rule for user D: {The first 2 columns of the third grid of the Sudoku}, password: 175286.

Decision rule for user E: {The first and third columns of the third grid of the Sudoku}, password: 175394.

Decision rule for user F: {The first and third rows of the third grid of the Sudoku}, password: 123564.

Generation of passwords using mathematical and logical means: In a search for strong authentication, Sudoku can be manipulated by mathematical and logical means to generate unique passwords.

Sequences or series: A mathematical series or sequences can be applied to Sudoku to generate passwords.

Example 7:

- Decision rule: {the exact location number of 1, 2, 3, 4, 5 in the first grid of the Sudoku}, password: 59624
- Decision rule: {The exact location number of 1, 2, 3, 4, 5 in the last grid of the Sudoku}, password: 89542
- Decision rule: {The exact location number of 2, 4, 6, 8 in the fifth grid of the Sudoku}, password: 9874
- Decision rule: {The exact location number of 1, 3, 5, 7, 9 in the last grid of the Sudoku}, password: 85267

Date of birth: Date of birth can be used to generate a unique password at each login. All is required is to remember the decision rule given by the security administrator.

Example 8:

- Decision rule: {Step 1: Find the exact location numbers of the user date of birth, from the first grid of the Sudoku. Step 2: in case of zero in the DOB, replace with one and repeat Step 1}:
  - Date of birth: dd/mm/year 11/10/1964 change to 11111964, password 55555832
  - Date of birth: dd/mm/year 05/09/1990 change to 15191991, password 54585885

Selection in a consecutive manner: Numbers in the grids of Sudoku can be chosen in a consecutive way to generate unique passwords.

Example 9: Decision rule: {every second number consecutively in the seventh grid of the Sudoku}, password: 7183.

Example 10: Decision rule: {the last number of the second, fourth, sixth and eight grids of the Sudoku}, password: 3515.

Position or location of numbers in the entire grids of the Sudoku

Example 11:

- Decision rule: {the exact number location of 1 in the entire grid of the Sudoku}, password: 571369428
- Decision rule: {The exact number location of 2 in the entire grid of the Sudoku}, password: 952591149
- Decision rule: {the exact number location of 3 in the entire grid of the Sudoku}, password: 693157815
- Decision rule: {the exact number location of 4 in the entire grid of the Sudoku}, password: 249482934
- Decision rule: {the exact number location of 5 in the entire grid of the Sudoku}, password: 427916592
- Decision rule: {the exact number location of 6 in the entire grid of the Sudoku}, password: 368274753
- Decision rule: {the exact number location of 7 in the entire grid of the Sudoku}, password: 184638276
- Decision rule: {the exact number location of 8 in the entire grid of the Sudoku}, password: 735843681
- Decision rule: {the exact number location of 9 in the entire grid of the Sudoku}, password: 816725367

Reversing of some selected numbers of the sudoku: Reversing of some numbers of the columns or rows of the selected grids of Sudoku can yield unique passwords.

Example 12:

- Decision rule: {the reverse of all the rows of the sixth grid of the Sudoku}, password: 842596173
- Decision rule: {the reverse of all the columns of the eighth grid of the Sudoku}, password: 723861594

Use of some selected Diagonals of the grids of the Sudoku: Diagonals of the grids of the Sudoku can be used to generate unique passwords.

Example 13:

- Decision rule: {the diagonals from left to right of the first 3 grids of the Sudoku}, password: 712923184
- Decision rule: {the diagonals from right to left of the last 3 grids of the Sudoku}, password: 956467639
- Decision rule: {the diagonals from left to right of the first, fifth and ninth grids of the Sudoku}, password: 712532832
- Decision rule: {the diagonals from right to left of the third, fifth and seventh grids of the Sudoku}, password: 385736956

Use of the entire row or column of the sudoku: The entire row or column of some selected grids of Sudoku can be used to generate unique passwords.

Example 14:

- Decision rule: {the entire 9 numbers of the last column of the sudoku}, password: 394851672
- Decision rule: {the entire 9 numbers of the last row of the Sudoku}, password: 634785912

Absolute value of the difference between two selected rows or columns

Example 15:

- Decision rule: {the absolute values of the difference between all the numbers of column 1 and column 2 of the Sudoku}, password: 341321543
- Decision rule: {the absolute values of the difference between all the numbers of the last two rows of the Sudoku}, password: 524524525

Number bases: Number bases can be applied on Sudoku to generate unique passwords.

Example 16:

- Decision rule: {the remainders when all the 9 numbers in the sixth grid of the Sudoku are divided by 4}, password: 200211331
- Decision rule: {the remainders when all the 9 numbers of the second column of the Sudoku are divided by 6}, password: 413022153
- Decision rule: {the remainders when all the 9 numbers of the sixth row of the Sudoku are divided by 4}, password: 101202331

Cryptography: In other to protect the confidentiality, integrity, authenticity and non-repudiation of information systems from unauthorized third parties, Sudoku can be used to generate codes not necessarily ciphertext which can be decrypted by some simple algorithms. The codes may appear meaningless but the authorized receiver can easily decode the message and take the required action encoded in the message. Sudoku can help in transacting business with codes understood within the organization. This is to guide against corporate or commercial espionage.

Example 17:

- Decision database: {update = 1, modify = 2, delete = 3, file = 4, data = 5, folder = 6, none = 7, once = 8, twice = 9}:
  - Code: 248 Action:: modify file once
  - Code: 746 Action:: no action, maintain current operation
  - Code: 513 Action:: no action, maintain status quo
  - Code: 158 Action:: update current data once
  - Code: 437 Action:: don't delete the current file after operation
- Decision database: {transaction = 1, verify = 2, invoice = 3, confirm = 4, access = 5, authorize = 6, refund = 7, payments = 8, sales = 9}:
  - Code: 248 Action:: verify and confirm payments
  - Code: 746 Action:: confirm and authorize refund
  - Code: 513 Action:: no action, maintain status quo
  - Code: 349 Action:: confirm invoice (sales)

DISCUSSION

The results are some of many more mathematical operations that can be applied to Sudoku to generate passwords. Detailed implementation of the results may require algorithms and computer programs. Also the results of this research can inspire software developers to develop application packages for implementation.

CONCLUSION

The various ways Sudoku can be manipulated to generate unique passwords or one time passwords have been shown but the list is not exhaustive because there are several more operations available which are subject to further research. Furthermore, it remains to show whether the knowledge of Sudoku can help in effective secret sharing and a more advanced cryptography.

RECOMMENDATIONS

The merits of using Sudoku in securing information systems, the relevance of this research to information security and detailed recommendations are as follows:

- Sudoku is cheap, readily available and the solutions can easily be obtained by algorithms
- The mode of difficulty is irrelevant as the post-filled is often used
- There are billions of available Sudoku and the probability of obtaining the same Sudoku is almost zero. This is a unique characteristics of passwords generated by using Sudoku because the probability of mimic attack, replay attack, shoulder surfing, dumpster diving is small. This is as a result of a new password at each login
- The user only needs to remember his user name and the decision rules given by the security administrator which is a criterion for successful login. This helps in effective password management and can be helpful to those that have lower cognitive abilities of remembering passwords
- In a touch screen platform, the fingerprints of the user may be authenticated at login
- The uniqueness of the password is an antidote against keystroke logging. This is because the system display different Sudoku and expect the user to simply apply the rule. This can be termed Stochastic Challenge Response Mechanism (SCRM). Each time is different but the user is the same
- To guide against rootkit, the decision rules are changed at each once in a month
- The use of Sudoku in Sign Sign-on systems helps to tackle the incidence of reduced sign-on RSO and can also help to reduce Man-in-the middle attacks, session hijack or piggybacking. This is because the passwords to different applications within the system are known only to the authentic user. This will definitely logged out potential unauthorized third parties
- The results also showed various ways one time passwords can be generated from simple Sudoku puzzle
- An unauthorized user is novice when a Sudoku is displayed at login. This is a defense mechanism against password brute force attack. Consecutive attempt to gain unauthorized access leads to suspension of the account
- The results can be combined with others for strong authentication. This can help to tackle online identity thief, fraud, impersonation
- Organizations can adopt this method for closed-loop authentication where one submits a Sudoku and the other provides a unique solution
- Generation of random numbers using Sudoku as seen the results can be used in security tokens, smart cards, credit and debit cards, security numbers, key generation, digital signatures, launch codes, authorization codes

REFERENCES

Gunther, J. and T. Moon, 2012. Entropy minimization for solving sudoku. Signal Process, IEEE Trans., 60: 508-513.

Khalid, S.K.A., M.M. Deris and K.M. Mohamad, 2013. Anti-cropping digital image watermarking using sudoku. Int. J. Grid Util. Comput., 4: 169-177.

Lewis, R., 2007. Metaheuristics can solve sudoku puzzles. J. Heuristics, 13: 387-401.

Maire, S. and C. Prissette, 2012. A restarted estimation of distribution algorithm for solving sudoku puzzles. Monte Carlo Methods Appl., 18: 147-160.

Santos-Garcia, G. and M. Palomino, 2007. Solving Sudoku puzzles with rewriting rules. Electron. Notes Theor. Comput. Sci., 176: 79-93.