Replacement for Passwords

Systematic Literature Review

Kaavya Rekanar
940521P120
kare15@student.bth.se

Biswajeet Mohanty
9303167754
bimo15@student.bth.se

I. Group Members Participation

The group members participated in idea creation and in report writing with the following amount of involvement:

Group Member	*Idea Creation*	*Report Writing*
Kaavya Rekanar	50%	50%
Biswajeet Mohanty	50%	50%

***Abstract*— With Information and technology advancing at a rapid pace, the need to secure and protect classified data from cyber criminals has become an imminent threat and challenge. Hence, an increasing amount of research in this direction has become prevalent. Conflicts in securing the data have been a serious impediment in recent years. A login protocol could be proposed which automatically logs into the system without the use of a password. This paper endeavors to provide a basic knowledge in the related literature pertaining to the gradual replacements for passwords with improvements in technology by conducting a systematic literature review (SLR). The SLR has been carried out keeping in mind the guidelines given in Kitchenham and Charters.**

Keywords— *password; replacement; security.*

II. Introduction

A. Context:

The changing era of technology and advancement has failed in updating the concept of passwords. No matter how much pride the world takes on advancing itself in technology and new inventions, the concept of protecting data has always dwelled in the usage of passwords as the only medium. At a later stage, the protection of data has grown to the level of biometrics where only the authorized person can access the data which is secured very well due to the usage of facial, voice, signature, DNA, retinal, iris, fingerprint recognition and hand geometry, but it has its' own set of disadvantages as well. Apart from being expensive and using a large setup, the technique of biometrics has failed to garner acceptance in the society because of its inherent, tedious and complicated process. The 'Smart-card and digital signature' systems seem to be an improvement over the traditional password based security system, but they still retain the same roots of user authentication process. Password based security system has been able to exist over the decades mainly due to its simplicity and its frugal requirement of elementary software/hardware resources. 'One Time Password (OTP)' based security system combined with traditional password techniques have proven to be superior but are not flexible and robust as they are largely dependent on telecommunication services.

B. Background

Authentication is a key requirement for securing today's user specific sensitive data. With IT increasing at a rapid pace, password based authentication has had its fair share of issues keeping up. Nowadays every user has multiple personal and professional accounts over several websites requiring username and passwords, which makes it extremely difficult for a user to remember those many passwords to gain access over those sites. This phenomenon has resulted in a rather disturbing turn of events wherein users resort to using a single password over all the websites. Also, users commit to easier ways of creating passwords such as '123456','changepwd', use of personal info such as DOB, favorite color etc., as shown in Figure 1. At the same time, hackers are getting better tools to infiltrate into sensitive and protected information. Anyone can today get a sophisticated password cracking tool from the Internet to crack passwords. Also, deducing/decrypting the passwords which aren't changed frequently and are created solely to facilitate ease of operation rather than securing the authentication, have become much more easier. For this very reason, passwords have always been plagued by security problems [1] and openly hated by users [2].

To counter these user's traits of complacency in creating genuine cryptic passwords, IT has come up with stringent rules and regulations for creation and maintenance of password protected accounts. Enormous efforts are being taken to systematize the knowledge in a better manner regarding both passwords and its alternatives [3]. Advanced biometric and One-time-password (OTP) systems are now being adopted to add an extra layer of security. Also, the emphasis on extensive research in cryptography related fields and advanced encryption systems, has grown manifold.

1. What is your favourite colour?
2. What is your mother's maiden name?
3. What is your favourite sport?
4. Where were you born?
5. What was the name of your first pet?

Figure 1: Questions requesting non-sensitive information [4]

C. Objectives

The prime objective behind conducting this systematic literature review is to understand and track the attempts made by various researchers in improvising the process of securing data over the years. Users prefer passwords over other methods of securing their data despite its disadvantages. It is relevant only when it's a secret based approach (that is, something only the user knows), used in preference to methods based on something the user is (user-authentication, biometrics) or something the user has (authentication using tokens) [4]. Although biometrics can be a solution to some of the problems faced by passwords, the system requires special equipment that adds up to additional expenses for the setup and implementation.

Authentication based on tokens introduces a completely different set of complications. Although they do not share the problems of biometrics considering errors, they suffer from problems relating to theft, loss or sharing of tokens [4], which can prove to be more risky than the negativity of biometrics. These constraints have led to the research and development in this field where the method developed retains the approach of secret knowledge but nonetheless overcomes the failures, which are observed in the above approaches. This literature review seeks to explore the proposed methods of securing data, which may offer buoyancy against the imposters in the future.

D. Methods

Scientific databases were searched to gather relevant information related to passwords, for conducting the Systematic Literature Review.

E. Results

As the software security is old concept, from our initial search string we found large number of articles. We limited the articles to 2005- present and also considered some relevant papers and considered the articles, which are only written in English language. By refining search string, the articles found are thoroughly analyzed and summarized.

Reference [1] discusses about the design of a password scheme. Reference [2] discusses about the relation between users and their passwords. Reference [3] discusses about the way the passwords are been used and its persistence since a long time. Reference [4] discusses about the need to replace the techniques being used currently in order to secure data in a much better manner. Reference [5] gave an insight into the different techniques in which the secret code method can be used. Reference [6] depicted the need to replace the existing methods of security management.

F. Conclusion

The purpose of securing data is well served by passwords to a certain extent. Biometrics, though useful in some aspects, prove to be very expensive when it comes to extensive usage. The concept of One Time Passwords has by far proved to be successful but it has its' own set of drawbacks. The need for a full proof technique to secure data has to be searched and implemented.

III. Review Questions

1. **Why is every improvement in technology rooting to the ancient concept of secret code when it comes to securing data?**

There has been a tremendous change in technology over the past years. No stone has been left unturned when it comes to decreasing the work involved and optimizing it to a better level. There are concepts like Steganography (the science of concealing information within different types of media, such that only the sender and the receiver are aware of its exact location) [5] and Cryptography (the practice and study of techniques for secure communication performed over unsecured channels) [5] in existence. The fact that methods of securing data have been improved over the years can be considered, though the argument is that all these methods also use text as the secret key to protect data, and that secret key is an ancient concept where there has been no advancement. The research done in this field has helped in improvising the technique of wrapping text into an efficient key but has not really left the root of the concept and developed into something else.

2. **"Biometrics is the most feasible solution when it comes to securing data". How far is the statement true?**

Researchers confidently accept to the fact that "Biometrics is the most feasible solution when it comes to securing data". But in reality this is not the truth. It is not quite a success when compared to the secret key technique. For the concept that a biometric passkey cannot be duplicated by any means, it can be definitely applauded. But there lies a huge drawback in the very existence of this so-called perfect solution. The Biometrics method of securing data is not reachable to the public far-and-wide as the secret key method. Its' setup takes a large amount of time and investment. It is not merely a-software, which can just be installed and the data can be secured. Looking at this we need to find a better way of securing the data.

3. **Is One Time Password the best solution to maintain secrecy and secure data better than any other method ever proposed?**

One Time Password is a key that is used to authorize a single transaction, on devices supporting this facility. This method of securing information and avoiding any kind of mistakes as far as possible is a huge leap taken from the usual static passwords, which have been in use since long. But this password generated could not be of any use and also prove to be a major setback if the device, which is synced to receive the dynamic code is lost. Also, there is a chance of cracking down the algorithm used to generate the OTP's. Hence, research has to be done further in this field in order to overcome this difficulty as well.

IV. REVIEW METHODOLOGY

A. PILOT STUDY

There are many methods proposed to secure data, which is the most valuable source of information. But there are loopholes in these methods as well. Hackers may break-in through these loopholes and may cause malicious activities. So we need to search for a better technique in order to protect data. "**Replacement For Passwords**" rose as a suitable topic to discuss on, so as to find a better way in securing the data.

Secret code was the initial concept of securing data, which kept on evolving according to the need of technology. Then biometrics was introduced, which was much more stable than secret code and made use of a different technique from secret code. This technique worked very well in securing data, but it showed up some flaws and also it was very expensive. So the need of better techniques has roused, replacing previous ones, which is much simpler, cost effective and data is much more secured.

B. REFINING SEARCH STRATEGY

The scientific database, "Engineering Village" is chosen, where articles from both Inspec and Compendex are considered for conducting the Systematic Literature Review.

The initial keywords used are: replacement and password.

A search in the database initially showed 299 results.

S.NO	DATABASE	RESULTS
1	Inspec	175
2	Compendex	124

Table 1: Initial Search Results

48 relevant papers were obtained after applying exclusion criteria. This is shown in Table 2

S.NO	DATABASE	RESULTS
1	Inspec	42
2	Compendex	6

Table 2: Results after applying Exclusion criteria

The search has been repeated. The keywords used were: (replacement*) AND ((password) AND (security*)). This search resulted in 22 papers. Even other important papers (Reference [1] was taken from Inspec database and reference [2], reference [5] was taken from compendex database) were selected depending on relevance.

C. SEARCH STRATEGY

Initially a data extraction form has been created consisting of the different questions that is to be addressed. This form is then used for preparing the literature review using the relevant information. A database search with keywords is then done. Then, the selection of good and relevant papers is done, by reviewing the abstracts. This is shown in figure 2.

D. INCLUDE / EXCLUDE CRITERIA

Inspec and Compendex database has been searched. Depending on the searched results the inclusion and exclusion criteria are:

INCLUSION CRITERIA:

- Papers related to security of password.
- Papers published in English.
- Papers from the past 10 years.
- As an exception, papers relevant to our topic, have also been considered.

EXCLUSION CRITERIA:

- Unrelated papers are excluded.
- Papers not containing password terms are excluded.

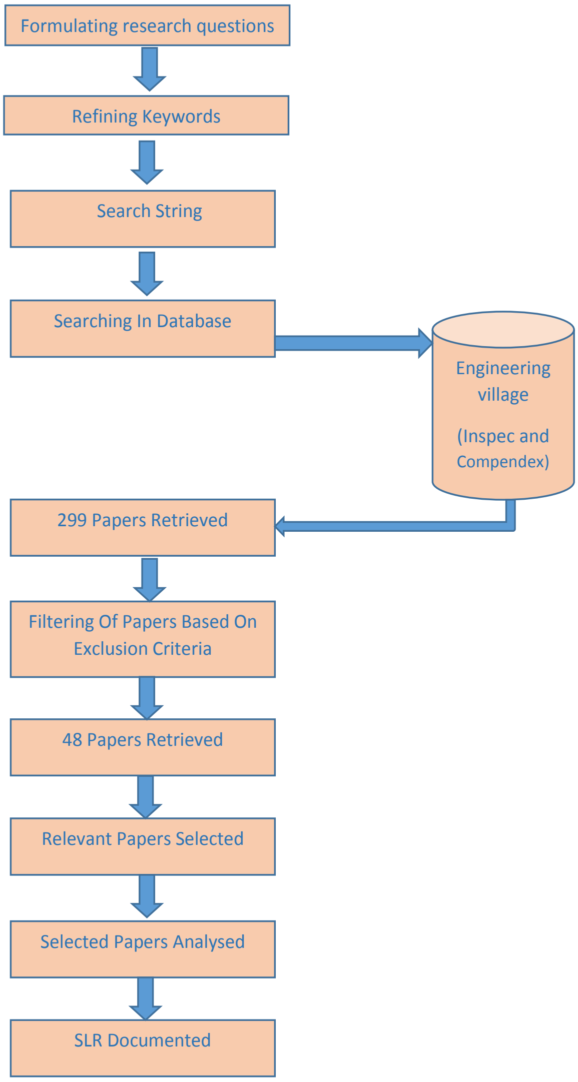

Figure 2: Flowchart showing how SLR is conducted

E. QUALITY ASSESSMENT CRITERIA

The selected papers for the systemic literature review have been graded as (low, medium, average, high) based on the quality criteria. The various quality criteria that have been considered are

QC 1: Is the security method clearly described?

QC 2:What is the quality of literature used in the research paper?

QC 3: Was the author successful in implementing the security methods described?

Papers	QC 1	QC 2	QC 3
Ref [1]	High	Average	High
Ref [2]	Medium	High	Average
Ref [3]	Average	Average	Average
Ref [4]	Average	Average	Medium
Ref [5]	Average	Medium	Average
Ref [6]	High	Low	Average

Table3: Assessing quality criteria of the selected study

F. DATA EXTRACTION PROCESS

All the selected papers have been read; rephrased and answer to the questions are given in the data extraction form. Systematic literature review is then done after retrieving the important matter from the selected papers. This is shown in Table 4.

G. VALIDATION OF THE PROTOCOL

A companion was asked to retest the search results for verifying the protocols. Companion got the same search results as was retrieved earlier.

V. INCLUDED AND EXCLUDED STUDIES

Inspec and compendex were chosen as the databases, which retrieved relevant papers by using the initial keywords retrieving 299 papers. Then, 48 papers were retrieved, by using exclusion principle. These 48 papers were relevant to the topic. From these, the most relevant papers were chosen, by defining new keywords. The initial search of the database using the keywords returned various studies that spoke about the security measures being used now a days in order to secure data. However, some papers have been excluded as they fail in describing about the security measures. Figure 3 shows the included and excluded studies.

Papers containing the concepts of secret key technique, biometrics and one-time-passwords were also involved in the study.

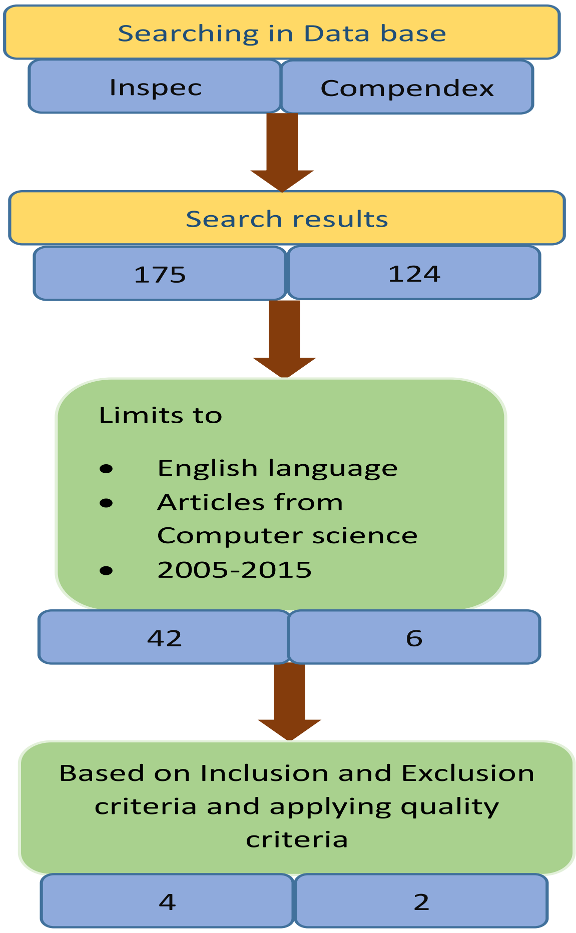
Searching in Data base
Inspec
Compendex
Search results
175
124
Limits to
English language
Articles from Computer science
2005-2015
42
6
Based on Inclusion and Exclusion criteria and applying quality criteria
4
2

Figure 3:Included and excluded studies

VI. DISCUSSION

All the findings discovered while conducting the Systematic Literature Review are presented as follows:

- Security plays a very important role in protecting the data from threats. Security is mainly provided using two techniques: the secret-code technique and the Biometrics.
- Technology has advanced a lot over the years and so have the ways to breach into the security of any system. This has created a need for technological advancement in securing the information.
- Secret code has undergone many changes since the most basic version. Reference [2] gives a brief idea of usage of cryptography and how it has helped in securing the data. But this method is found to have some loopholes, which needs to be looked into and invention of new theories are required to rectify the loopholes.
- Biometrics has come out as an alternative to the secret code technique. It overcomes some of the disadvantages of secret code, but also brings a new package of worries with it. In spite of being expensive, accuracy is not maintained every time, which lets it down. This makes the use of biometrics,

Questions	Ref [1]	Ref [2]	Ref [3]	Ref [4]	Ref [5]	Ref [6]
What kind of security is paper focusing on?	Password security as a case history	Secure code method	Secure code method	Replacement of currently existing security method	Data encryption and biometrics	Comparison of existing web authentication schemes
What kind of problems are discussed in the paper?	Case study of problems due to improper security	Difficulties with passwords to users	Lack of proper security measures	Lack of security	Static passwords lead to the risk of being hacked	Pros and cons of secure-code, secure-token and biometrics
What are the approaches proposed to solve the problems?	Secure code technique- usage of encryption and decryption	Difficulties due to poor security could be noted	Agenda has been acknowledged on the need of new technology	Enhancements of the existing methods	Randomized error correcting DNA codes	Need for a full proof security mechanism is proposed
How successful was the technique in resolving the problem?	Being an outdated paper, not considered successful in present time.	Successful in explaining the plight of the user	Drawback could be distinctly understood	OTPs' have been proposed	Costly but proves to be effective	Gave an insight into the requirements of security
What can you infer from this paper?	Case studies about the need of security	Difficulties of the user	Reason behind need for replacement of passwords	Reasons for security of data	Biometrics have a large scope	Need to enhance the security measures

Table 4: Data Extraction Form

limited to all fields of life. This is discussed in Reference [5].

- Research has to be done in the field of security such that it overcomes both the faults of secure code technique and the biometrics. Reference [6] clearly portrays the need of future work in this prospective.

VII. LIMITATIONS

- The main reason for the limited ways of securing information cannot be blamed at the loss of creativity. All the creativity existing has been put into transforming the secret code technique of securing data in unimaginable ways. The security of data has to follow simplicity and cost effectiveness. Hence, there are limited ways in securing the data.
- Many papers were left unread due to the time restriction.
- There were limited papers available which were relevant.
- Some papers were left out due to the constraint of full text availability.

VIII. CONCLUSIONS

The fact that the field of security is still in its adolescence can be deduced from this SLR. Further research in this field would greatly improve the face of securing data. The basic aspect to be considered is that the concept of securing data has to move on from mere secure code and biometric approaches to something much more simple, cost effective and resistant to hackers.

IX. REFERENCES

[1] R. Morris and K. Thompson, "Password security: a case history," *Communications of the ACM*, v 22, n 11, p 594-7, Nov. 1979

[2] A. Adams and M. Sasse,"Users Are Not The Enemy," Source of the Document, Communications of the ACM, 42 (12), pp. 41-46, 1999.

[3] C.Herley and P.C.van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Security & Privacy*, v 10, n 1, p 28-36, Jan.-Feb. 2012.

[4]Steven Furnell and Leith Zekri, "Replacing passwords: in search of the secret remedy", *Network Security*, v 2006, n 1, p 4-8, Jan. 2006.

[5] Tulpan D., Regoui C., Durand G., Belliveau L., Léger S., "HyDEn: A Hybrid Steganocryptographic Approach for Data Encryption Using Randomized Error-Correcting DNA Codes", BioMed Research International, 2013.

[6] Joseph Bonneau, Cormac Herley, P.C. van Oorschot, Frank Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”, *2012 IEEE Symposium on Security and Privacy*, p 553-67, 2012.

[7] B. A. Kitchenham, "Guidelines for performing Systematic Literature Reviews in Software Engineering," Version 2.3, EBSE Technical Report, EBSE-2007-01, Software Engineering Group, School of Computer Science and Mathematics, Keele University, Keele, Staffs, ST5 5BG, UK and Department of Computer Science, University of Durham, UK, 2007.