

|  |  |  |
| --- | --- | --- |
| MSc Advanced Software Engineering  Research Project | | |
|  | | |
| Assignment Type: | Literature review | |
| Submission Date: | 01/31/2017 | |
|  | | |
| Student Id | | Student Name |
| 2015101 | | K.A.S.C.Kathriarachchi |

|  |
| --- |
|  |
| Literature Review |
| Blocking brute force attacks using binomial ladder filter in .net applications |

Student Id - 2015101

Name - K A S C Kathriarachchi

Supervisor - Mr Cassim Farook

**Table of Contents**

* Abstract 4
* Introduction 4
* Literature Review 5
* Research Method 6
* Findings 7
* Conclusion 7
* Reference 8
* Other Information Sources 8

**Abstract**

Password-based systems and, more generally, authentication systems based on somethingyouknow, are common place on the Internet. Web applications using these systems can be the target of brute force login attacks, in which an attacker tries to compromise a given account or any user account on the system. These applications rarely implement effective protection mechanisms against these attacks. In this paper, we review the other researches relating to this project.

**Introduction**

The internet and mobile communications have been developing and related application or services for managing money and personal information are increasing in number day by day. Thus, now-a-days people rely more on internet to store the confidential and important data. However, there is a risk that private data may be wiretapped. Therefore, it is necessary to authenticate users and in order to keep this web data safe on cloud almost every client and server implement cryptographic techniques to encrypt this sensitive data, as well as verify entities at the other end of the connection. Thus if more confidential data is to be stored online, it is necessary that the network security should stay up to date with modern attacks. However, online users continue to use weak and easily guessable passwords like birth dates, partner names, children names etc. and they are typically only letters. Also, if the user sends the same password every session, an attacker can easily masquerade as a user, because the attacker may succeed in getting the user’s password through internet. So, it is becoming clear that passwords are not sufficient means to protect the online accounts. Various authentication schemes are being in use today to harden the security of online data or information.

It is difficult to blame end users for this, since the number of passwords to remember has ballooned to several dozen for a typical user, making it very impractical to expect people to pick hard-to-guess, yet memorable, passwords for so many accounts. But the main problem lies with password cracking techniques and computer speed. It is very likely that Bishop and Klein would now successfully guess the vast majority of their database, and do so in much less than three CPU years. It is also the case that they would have easy, cheap access to a lot more than three CPU years to run their attack if they wished. It can be argued, and it sometimes is, that the times when it was possible to create a password that a human can remember and that a determined, well equipped attacker cannot crack are behind us.

Even though password-based authentication systems are known not to provide very good security, they are still very popular, and represent the vast majority of authentication systems that are deployed currently. The reasons for this are simple: despite its poor security value, a password-based authentication mechanism is very easy to deploy, does not require any additional hardware, and is well accepted amongst the potential user population. It is arguably the simplest, most cost effective solution to use when you have to authenticate users with some minimal level of security. Because of this, these systems appear to be here to stay.

This bleak situation may not be as bad as it first seems. It is true that password-based authentication mechanisms do not provide adequate protection against well-equipped attackers, but this analysis is based on so-called “offline” attacks, in which the attackers have direct access to some encrypted version of the passwords. In this situation, the only thing that slows down the attack is the generation of encrypted passwords on the one hand, and the comparison of the result with the list on the other hand. Thankfully, this situation is not the most common one. If we assume that the attacker does not have access to the database of passwords directly, then the attack must be performed online, through the system’s legitimate gateway. The situation is very different in that case: for one thing, it is likely much slower, and for another thing designers of the system have an opportunity to act against such attacks.

**LITERATURE REVIEW**

**M.M. Mohammed, M. Elsadig (2013)** provided a multi-layer of multi factors authentication model for Online Banking Services. The security risks of internet banking have always been a matter of concern for the service providers as well as for the users. Various online environments like internet banking, electronic transactions and financial services have been analyzed to identify the characteristics and issues of existing authentication methods in order to present a user authentication level system model that is suitable for different online services. Multi-factor Authentication has been integrated with multi layer authentication techniques in order to produce a standard layered multi factor authentication model suitable for different online banking services suitable based on risk assessment criteria. The proposed model includes 5 levels such that each level contains one or combination of various authentication factors such as knowledge-based, possession based, or biometric based factors. The standard model is compared to multi layering guidelines and it shows improvement and fulfilment of authentication needs. Organizations need to be able to see activity across all products and channels so that they can identify anomalous or potentially fraudulent behavior. Data warehouse for all identity-related information and data mining tools, with which to look at the relationship between entities, can help organizations identify if, for example, a single account try to do transactions using multiple ways and fails. the ability to cross-reference identity-related data is achieving returns on investment for some companies of up to ten fold. According to researcher this is very suitable for high risk organizations and not practical in other normal services because of high cost factor.

**Uymatiao, Mariano Luis T., and William Emmanuel S. Yu (2014)** have worked on Time-based OTP through secure tunnel (TOAST). They have collectively developed a mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke. The main objective of this research is to build upon existing cryptographic standards and web protocols to design an alternative multi-factor authentication cryptosystem for the web. It involves seed exchange to a software-based token through a login-protected Transport Layer Security (TLS/SSL) tunnel, encrypted local storage through a password-protected keystroke (BC UBER) with a strong key derivation function, and offline generation of one-time passwords through the TOTP algorithm. Authentication occurs through the use of a shared secret (the seed) to verify the correctness of the one-time password used to authenticate. To implement this environment, need high tech and knowledge. Because of that this is not practical in every case.

**Nitin Mujal, R. Moona (2009)** described a secure and cost effective transaction model for financial services. As with the advent of the e-commerce, it has become much easier for the intruders or attackers to sit in non-descriptive location and quietly siphon away the money from the service users. Thus also the financial service outlets like Automated Teller Machine (ATM), Point of sale (PoS) terminal have also been an easy target. As the users are forced to trust a service outlet to be authentic but actually they can be spoofed and also a spoofed outlet can collect the account information of the users and can use the same to do financial transactions. These outlets are also very expensive to implement. Thus a secure and cost effective model has been proposed to overcome various securities and cost related issues of financial service models. It is cost effective such that financial services can also reach to the rural population and contribute to rural development. It relies on public key infrastructure (PKI) architecture to provide ensures about both cost and security issues.

**T.V.Raphiri, M.T.dlamini, Hein Venture (2015)** Talked about the best ladder to prevent unauthorized access to authentication systems. First his suggestion is to check actually login credential is valid, he is asking to check that because that’s very basic filtering and can be done by fast. If credentials are valid then they ask to check those login request are continues. If that continuity is abnormal block that request, because some users want to take control of server resources. If that continuity is normal then grant the access. Then they talk about what will happen account credentials are not valid. They suggest to check this request is sending by an actual user or guessing system. If request are coming from guessing system record that and identify the future filtering. According to these peoples research they did not suggest any filtering methodology to follow.

**Research method**

The survey was used to analyze the current characteristics of protection methods in varies systems. Also analyses other factors to use these methodologies in varies systems and pros/cons.

**Findings**

Passwords are still one of the weakest links in information systems because people use weak passwords. Most of the current available methods are high cost and need special knowledge to implement. And also some methodologies are not practical to implement in most of the systems. With the current password-cracking software, these passwords are easy to crack in a matter of seconds. The results of this study also show that people often create passwords based on their personal information such as birthdates, citizen id, telephone number, and family members’ names. These passwords can be easily guessed by friends and colleagues. Sometimes, the hackers do not even need to hack the password. They can set up a website and ask users to register with a username and password. Some people will reuse the same password that they use with other accounts such as email, their company’s systems, and e-banking accounts. According to analysis we need an additional system to prevent attacks to the systems, because most of the peoples using easily hackable passwords.

**Conclusions**

In this article by reviewing the pros and cons of various available login authentication schemes, firstly we reported on already available multi-step authentication mechanisms, how they work, how they are used, where and why. A few popular multistep authentication schemes include: one time pass code or passwords received via SMS, one time codes generated by security token i.e. RSA SecurID, Smartphone applications for generating verification code like Google authenticator and TOAST, using images as verification passwords i.e. Image- based authentication. Almost every kind of authentication system discussed above is widely used today to provide security to the users. One Time Passwords are an efficient technique to generate passwords randomly each time for user. OTP prevent users from replay or eavesdropping attacks. These passwords are valid only for given timeframe thus there is no threat that they can be reused by an intruder to login to user account as they are invalid after one time use. One Time Passwords can be generated either online or offline but offline generation is better as it can also be generated even if there is no network connectivity and it also prevents from the man in the middle attack. Thus it will be better for the services or websites to use offline method of generating one time unique codes like Google Authenticator or TOAST as they provide more confidentiality and authentication to the user on internet. But still these methodologies not having feature of blocking these attacks very simply and cost effectively. That means users not want to see what’s going on inside and how they’re going to protect.

**References**

* Lars R. Knudsen[,](mailto:lars.r.knudsen@mat.dtu.dk) Matthew J. B. Robshaw “Information Security and Cryptography”, series 2016
* Mohammed M.M., Elsadig M., “A multi-layer of multi factors authentication model for online banking services”, International Conference on Computer, Electrical and Electronics Engineering (ICCEEE), August 2013.
* Munjal N., Moona R., “Secure and Cost effective Transaction Model for Financial Services”, International Conference on Ultra Modern Telecommunications and Workshops, 2009, IEEE, ICUMT’09.
* Marc Cameron, “Brute Force (Jericho Quinn Thriller Book 6) “, 2015
* Uymatiao, Mariano Luis T., and William Emmanuel S. Yu. “Time-based OTP Authentication via Secure Tunnel(TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystroke.” 4 thIEEE International Conference on Information Science and Technology(ICIST), 2014,Pp. IEEE,2014.

**Other Information Sources**

* Wikipedia about brute force attacks <https://en.wikipedia.org/wiki/Brute-force_attack>
* Wikibooks Cryptography, Brute\_force\_attack <https://en.wikibooks.org/wiki/Cryptography/Brute_force_attack>