Jurnal Teknologi

Full Paper

A CASE STUDY OF THE WEAKNESS OF FRESHMEN CHOSEN PASSWORD FOR ACADEMIC INFORMATION SYSTEM

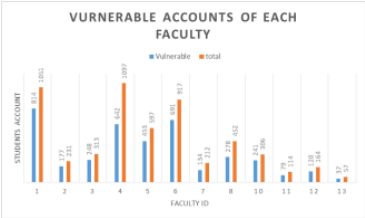
Ahmadiar, Sayed Muchallil*

Jurusan Teknik Elektro, Universitas Syiah Kuala, Aceh, Indonesia

*Corresponding author
sayed.muchallil@unsyiah.ac.id

Article history
Received
27 April 2015
Received in revised form
15 June 2015
Accepted
25 November 2015

Graphical abstract



Abstract

In the last decades, some extensive research explored new algorithms and protocols how to secure data or user information using password and username. There are new methods such as biometrics. The drawback of this method is that it needs other hardware or device. On the other hand, the username and password combination to authenticate user identity has been widely used because cheap and user-friendly. The latter method has some weakness such as dictionary attack, brute force or other method. The purpose of this research to find out the weakness of freshmen chosen password to protect their identity in the Academic Information System. The experiment is done in a public university in Indonesia. This research carried on around 12 faculties and 102 departments. The freshmen at this university is around 6499 students. The sampling method is population, so that all the freshmen student account investigated. The first scenario is to find out how many students use the same password as username. The second scenario is a dictionary attack on some freshmen account that cannot be found on the first scenario. The result of this experiment about 60% to 75% of freshmen's password in each faculty can be guessed because the students used the same username and password. Other method used in this research has been revealed more password from freshmen.

Keywords: Dictionary attack, brute forced, password, academic information system,

1.0 INTRODUCTION

Securing data and hide personal information have been an interested topic for security researchers for years. Some new tools were introduced to upgrade the security level. The drawback of this method sometime these tools are not easy to get or carry. However, even the username and password is less secure, but it still used in many applications. Some applications still use an old method classical one way hash function such as MD5 to authenticate users.

According to SANS institute [1], the word authentication means the confirmation process of someone's identity. This process is looking for the same information or data that has been saved with the information that given by a user. If the information matches, the process confirms that the user is the real person.

O'Gorman in his paper [2] mentioned that machine authentication such as Secure Socket Layer Protocol, is more secure than user authentication like using a password. This happens because users prefer to use the password that easy to remember, as the result, the password is guessable. Morris and Thomson [3] argue that the password mechanism not only to prevent unauthorized user from accessing the system, but also to avoid authorized user to access unauthorized resources.

The weakness of this authentication method has been improved these days, however the password and username authentication system is more acceptable because it can be accessed everywhere

using cell phones or notebook. There are some researches that tried to develop password authentication method. Luo and Paul [4] proposes a new method of password authentication procedure for multiple accounts. They suggest that a user that has more than one username and password combination for multiple account should only remember one password called common password. This can be a good method avoid human memory weakness. However, once the main password has been known, there will be more damage. Yang et al [5] enhanced the password authentication method by using two server authentication. This research tried to overcome the problem that existed with multiple server authentication. Van et al [6] tried a different approach using a framework for protecting the conventional password-based authentication protocols. In their research, it is proven that this framework increased security of conventional password authentication method.

However the weakness of this method mostly is not about the system only, but also comes from the user. Bishop and Klein [7] tried to recommend how to avoid weak password so that it cannot be guessed. The first recommendation is not to use the same password and username or other personal information such as birth date, the second is that the password should not be in a dictionary.

Every organization, including educational institution also implements one or more of many authentication methods [8]. Our research object is A university that adopts its student information system using password authentication. In this system, a student will only be provided with services if his or her identity can be identified. This information system will be explained clearly in the next section.

Our research focuses on guessing chosen password by the freshmen of a selected university (called A university), whether the account can be hacked into or not. This paper has been shown to authorities of the system in A university to be patched before it is published. Our method of guessing password using brute force attack and dictionary attack using common words. There are two types of brute force attack, offline and online brute force attack [5]. In our experiment we used online brute force and dictionary attacks.

This paper is organized as follows. Section 2 gives introduction to online user registration system in A university, security terms, and other literature reviews related to authentication. In Section 3, we discuss about the method we use to data collection and how we do the penetration tested. Section 4, we show the result by department. In this section, we also compare the result of each breakable password using different methods. Finally, we make our conclusion in section 5 with general recommendations of how to upgrade the system so it can be more secure.

2.0 LITERATURE REVIEW

2.1 Academic Information System

A university has implemented online registration system. This system is really powerful and also keep a lot of information about the students such as students' personal detail and their academic records. Accessing the system for the first time, the students use their student number as username and also password. Next, they are required to fulfill their personal detail so the server calculate the tuition fee based on their data. As a result, this information system contains all personal data of every student in A university.

The authentication method used in this system is classical password authentication method. Detail procedure of this authentication method is shown in Figure 1.

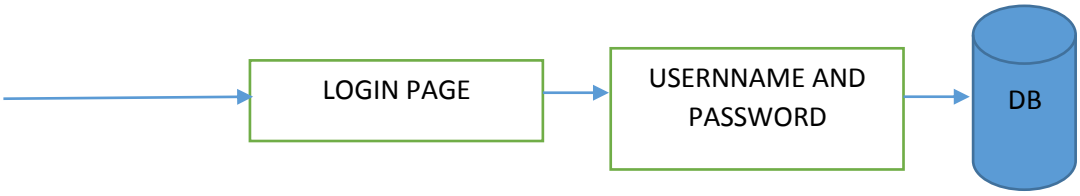


Figure 1 Authentication procedure

A student goes to the login page, enter their user and password. The user name and password sent to a php processing page. This script encrypts the entered password, then query the database for the username and encrypted password. If a record is found, the user will be redirected to a main page. If the login failed, the user will be shown a login page again. The table structure for login usually as shown in table 1.

Table 1 Table structure for login

username	password
Student number	Encrypted passwors
Student number	Encrypted passwors

The problem on the system, there is no limitation on error trial, so the brute force or dictionary can be used against the system. Another drawback of the system is that on the system, users are not forced to change the password when the first time they log in. finally, the

system should help user to choose the more secure password.

2.2 Brute Force Attack

Brute force attack has been known for decades. Moris and Thomson [3] tried to guess password for UNIX system use this brute force method. Brute force method tried to assemble all possible combination of characters. This will work if user chooses a short password. Human as the weakest link in the security threads will use an easy to remember and short password [9]. This method of attack will not work if the user choose a longer password, because this method will need more time if the password is longer than 8 characters. Users usually depend on the system when they create a password. Bank System requires more complicated password than an online chat system [10]. According to Riley [10], most users never change their password.

2.3 Dictionary Attack

Dell'Amico et al [11] mentioned that the most effective wayof guessing a weak password is using dictionary attack. Based on his research using John the Ripper. This recovery tool has been known for a long time in the security field. John the Ripper has multiple dictionary such as different language and password type. This dictionary can be downloaded easily.

Avoiding this kind of attack, some research has been done to password easy to remember, but difficult for an attacker to get it from a dictionary using mnemonic that discuss in Kuo et al [12] research. However, Kuo et al [12] tried to create a dictionary to crack this kind of password. The dictionary attack is based on the word list that will be accessed at a time for a given user name.

2.4 Dictionary Attack Countermeasure

There are some countermeasures that can be taken to avoid the online dictionary attack.

a. Delayed: if the combination of username and password are not correct, the server should reply it with error message longer than if it is correct. Using this method, the attacker will take more time to do online dictionary attack.
b. Locking: this technique is used by the operating system. After several error trials, the system will hold the account for some times. Most online applications also adopted the same method, such as Facebook or Gmail. This method id more effective compare to the first one.
c. Captcha: captcha stands for Completely Automated Public Turing test to tell Computers and Humans Apart. This method asks the user to post answer or response to a challenge, usually an image. Figure 2 shows a captcha challenge.

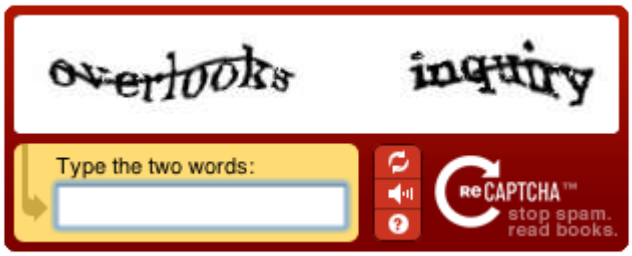


Figure 2 A captcha image

3.0 RELATED WORKS

Ken and Thomson [3] carried on some experiments about user password. In their research, they found that 2,831 passwords from 3,289 passwords (around 86 %) can be classed as 1 to 4 ASCII characters and 5 or 6 letters with all upper case or all lower case.

Klein [13] also conducted an experiment in cracking password from 13,797 accounts. By only using 62,727 words from the list, the password can be cracked about 25% of the time.

Oechslin [14] tried to improve Martin Hellman research [15] using pre calculated data for cryptanalysis that saved in memory. He updated Hellman's table structure to get a better result. In this research, the time used for password cracking has been shortened than the original work of Hellman.

In 1995, Ding and Horster [16] research on undetectable on-line password guessing attack. Their research divided attacks into three classes. (1) On line attack, in this type of attack, the authentication server has to be involved in every attack. After some failed attack, the server logs the attacks. (2) Off-line attack, the attacker will verify the password off-line (3). The attack that still uses the authentication server for verifies the correctness of password guessing. However, if the guess failed, the attack will start a new session with the server. As a result, the attack will not be detected and logged. The result of this research showed that some 3-party protocol authentication that should be protected a weak password are vulnerable to this type of attack. The drawback of this kind of attack, it took a lot of communication with the server comparing to off-line attacks.

Halevi and Krawczyk [17] tried to guest password against public key cryptography. In their experiment, they tried to proof that off-line password guessing will not work if the chosen public key long enough. They also improve the protocol by providing it two way authentication.

Goyal et al. [18] experiment on protecting online password guessing using authentication protocol. The protocol requisite the client to calculate the response based on the challenge sent earlier. Since this calculation will take some time, its guarantee that the attacker cannot launch a lot of attack in small amount of time. They assembled two type of this protocol. The first one using augmenting so that server is not required to store password in plaintext. The latter

is to deal with off-line attack in case of the public key is not in use.

Pinkas and Sander [19] think of human and machine has a different way of seeing things. They provide a challenge that will be easy for human and very difficult for machine. As the dictionary attack is a machine, it should difficult to perform this response-challenge method. They call it reverse Turing tests (RTTs).

4.0 TYPE OF ATTACKS

Attack that are used in this experiment are

1) Try using the user's ID, since the ID is the student identification number, the first trial of the attack will use the same username and password. So that the file consists of the all user id will be used.
2) Using some easy word dictionary that we compiled around 20 wordlist.

This attack is not done manually. The java text based application is built to provide automatic dictionary attack. First, the web based application will be identified what script file processes the username and password input. Next, identify what variable name it login page uses. Finally, investigate what method that use in sending variable, post or get.

The application is designed especially for the A university, so that it is only available for post method. The successful result will be stored in a text file. Figure 3 shows the program algorithm.

5.0 RESULT AND DISCUSSION

Figure 4 shows that the faculty with id 3 has most vulnerable accounts, around 79 %. Faculty with id 11, 12, 13 is new faculty that is why they only have less students than other faculties. From this result, our research should compare male or female students less aware of security. Another question arises that exact sciences faculty or social science faculty students consider more about the security of their data. These two questions can be answer by a survey that will be done later after this experiment. Since we do not have enough data from this application. The faculty 4 students are more concerned about their password compared to 11 other faculties.

Figures 5 shows the department student's accounts in faculty 4 which are vulnerable to the dictionary attack based on the same username and password. Department 4 has the most vulnerable accounts, about 78 %. Departments 2 and 3 have around 76 and 76 respectively. In this faculty, the students that are most aware of security are student of department 6. The vulnerable account is only about 42 %. Since faculty 3 has only one department, the experiment will provide the departmental break down results on faculty 1 and faculty 10.

Figures 6 shows department student accounts in faculty 1 which are vulnerable to the dictionary attack. Department 3 has most vulnerable accounts, about 93 %. Department 10 only has 47 % vulnerable accounts.

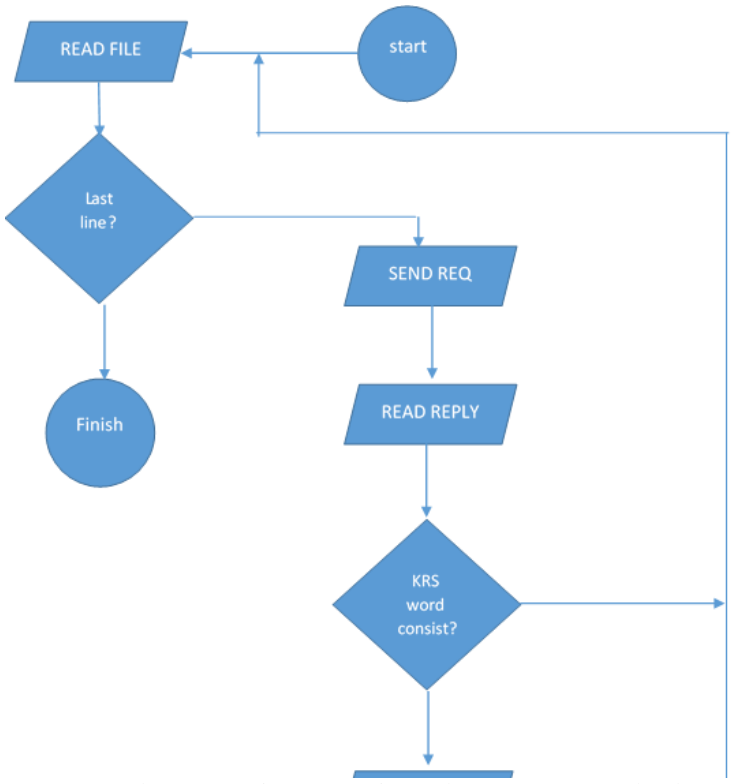


Figure 3 The flowchart of guessing password application

Figures 7 shows department student accounts in faculty 10 which are vulnerable to the dictionary attack. All the department has above 60% vulnerable accounts. The highest vulnerable account rate is in department 1, about 86 %, then followed by departments 2, 3 and 4 about 81%, 79% and 66 % respectively.

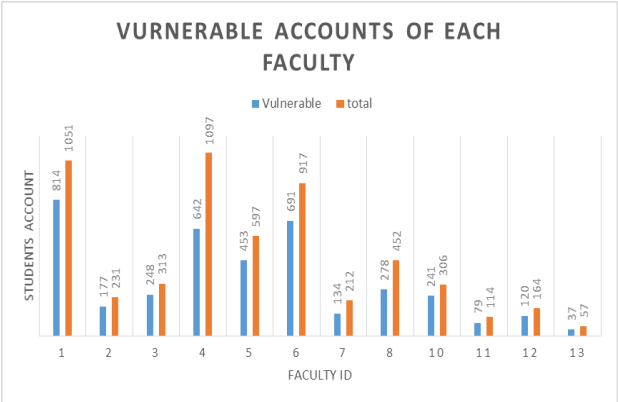


Figure 4 Vulnerable accounts of each faculty in A university

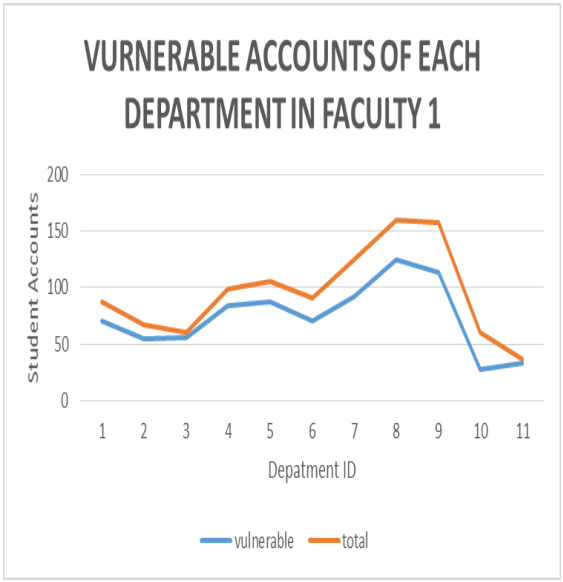


Figure 6 Vulnerable accounts of each department in faculty 1

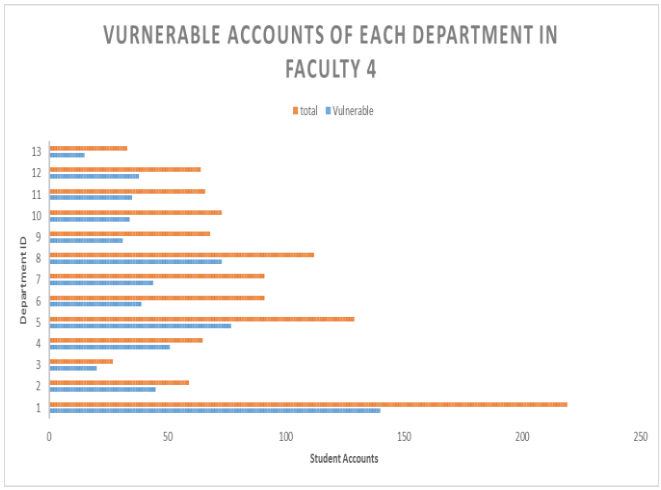


Figure 5 Vulnerable accounts of each department in Faculty 4

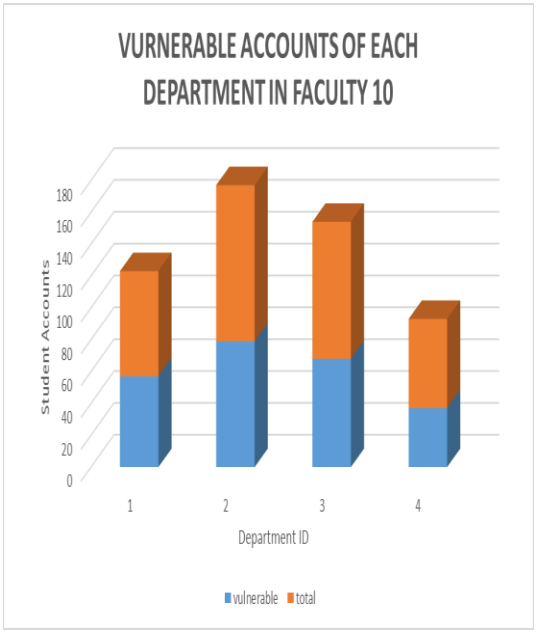


Figure 7 Vulnerable accounts of each department in faculty 10

6.0 CONCLUSION

The most vulnerable accounts are owned by social science faculty students. Faculties 3, 10, and 1 have

more than 75% account vulnerable to the dictionary attack using the same password as username. The system should avoid this by forcing the freshmen to change their passwords during the first time they log into the system. Avoiding weak password the system should require password the combination of alphanumeric character and special characters.

Locking and delayed should also be implemented to make attacker a lot harder to guessing password or it will be time consuming guess password activity. Another help is to apply captcha for every login attempt.

References

[1] G. Stocksdale, "Glossary of Security Terms," SANS Institute Resources, http://www.sans.org/security-resources/glossary-of-terms/

[2] Gorman, L. O. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*. *91*(12): 2021-2040.

[3] Morris, Robert, and Ken Thompson. 1979. Password security: A case history. *Communications of the ACM*. 22(11): 594-597.

[4] Luo, Hui, and Paul Henry. 2003. A common password method for protection of multiple accounts." In *Personal, Indoor and Mobile Radio Communications. PIMRC 2003. 14th IEEE Proceedings. 3: 2749-2754*.

[5] Yang, Yanjiang, Robert H. Deng, and Feng Bao. 2006. A practical password-based two-server authentication and key exchange system. *Dependable and Secure Computing, IEEE Transactions on*. 3(2): 105-114.

[6] Van Der Horst, Timothy W., and Kent E. Seamons. *2008.* pwdArmor: Protecting Conventional Password-Based Authentications. In *Computer Security Applications Conference,. ACSAC 2008. Annual*. 443-452.

[7] M. Bishop, D. V. Klein. 1995. Improving system security via proactive password checking. *Computers and Security*. 143: 233-249.

[8] Khan, Hafiz Zahid Ullah. 2010. Comparative Study Of Authentication Techniques. *International Journal of Video & Image Processing and Network Security IJVIPNS* 10(04).

[9] Narayanan, Arvind, and Vitaly Shmatikov. 2005. Fast dictionary attacks on passwords using time-space tradeoff. In *Proceedings Of The 12th ACM Conference On Computer And Communications Security*. 364-372. ACM.

[10] Riley, Shannon. 2006. Password security: What users know and what they actually do. *Usability News*. 8 (1): 2833-2836.

[11] Dell'Amico, Matteo, Pietro Michiardi, and Yves Roudier. 2010. Password strength: An empirical analysis. In *INFOCOM, 2010 Proceedings IEEE*. 1-9.

[12] Kuo, Cynthia, Sasha Romanosky, and Lorrie Faith Cranor. 2006. Human selection of mnemonic phrase-based passwords. In *Proceedings Of The Second Symposium On Usable Privacy And Security*. 67-78.

[13] Klein, Daniel V. 1990. Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop*. 5-14.

[14] Oechslin, Philippe. 2003. Making a faster cryptanalytic time-memory trade-off. In*Advances in Cryptology-CRYPTO*. 617-630.

[15] Hellman, Martin E. 1980. A cryptanalytic time-memory trade-off. *Information Theory, IEEE Transactions on* 26(4): 401-406.

[16] Ding, Yun, and Patrick Horster. 1995. Undetectable on-line password guessing attacks." *ACM SIGOPS Operating Systems Review*. 29(4): 77-86.

[17] Halevi, Shai, and Hugo Krawczyk. 1999. Public-key cryptography and password protocols. *ACM Transactions on Information and System Security (TISSEC)*. 2(3): 230-268.

[18] Goyal, Vipul, Virendra Kumar, Mayank Singh, Ajith Abraham, and Sugata Sanyal. 2005. CompChall: addressing password guessing attacks. In *Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on* IEEE. 1: 739-744.

[19] Pinkas, Benny and Tomas Sander. 2002. Securing passwords against dictionary attacks. In *Proceedings Of The 9th ACM Conference On Computer And Communications Security*. 161-170.