International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Improving Security for Folders in Windows by using Bluetooth and Rijndael Encryption

Dhanraj Poojari†*, Ankita Kesarkar†, Nikita Saple† and Alka Srivastava†

†Department of Computer Engineering, Atharva College of Engineering, Marve Rd, Malad (west), Mumbai-95, Maharashtra, India

Accepted 15 April 2015, Available online 25 April 2015, **Vol.5, No.2 (April 2015)**

Abstract

The security feature of Windows has been the most crucial issue ever since the commencement of the Windows systems. Passwords produced to ensure security for files and folders themselves have disadvantages and drawbacks in them. In this research, the vulnerabilities and disadvantages hosted by passwords shall be studied and minimized. We shall also implement a Two Factor Authentication [T-FA] System in the process by conjugation of Bluetooth and Rijndael Encryption. Selection of Bluetooth as an authentication factor is due to that fact that it's most commonly available and every Bluetooth device has its own unique MAC address. Rijndael Encryption on the other hand is an AES and is widely believed to be most beneficial Cryptographic Encryption Algorithm available. The implemented Two Factor Authentication [T-FA] system should not only take out the disadvantages of passwords but is also aimed at providing a user friendly security system.

Keywords: *Bluetooth, Rijndael, protection, folder, computer, factor, two, authentication, security, windows*

1. Introduction

Protection of data for the computer users who are entrusted with sensitive data has always been a primary concern.

Windows password policies came into effect for the reason to safeguard user sensitive data. Still the need for stronger solutions arises as some of password policies are not enough to safeguard personal and organizational data. Stronger password policies make it difficult for the users to recall the passwords forcing them to note it down, adding to potential risk.

Biometrics may seem as an obvious solution to the vulnerabilities. However, various problems may come about when presenting biometric authentication to T-FA systems. Performance gain with respect to recognition rates is often achieved due to the assumption of unrealistic preconditions. Resulting performance distortions may not be recognized at first sight, yet, these could lead to serious security vulnerabilities. (Christian Rathgeb, *et al,* 2010)

Two-factor authentication has ameliorated security in authentication systems. Using Bluetooth as a token in the Two Factor Authentication System [T-FA] along with the powerful Rijndael Encryption will not only provide a solution to all these disadvantages, but also produce a password decentralized user friendly security system. (Nikita Saple, *et al*, 2015)

2. Existing Systems and its Vulnerabilities

Despite a growing number of graphical and biometric authentication mechanisms, passwords remain the most familiar and commonly-used form of user authentication in organizational settings. (Philip Inglesant, *et al,* 2010)

Let us take into account the various existing folder security systems, including password centralized and decentralized further studying the drawbacks imbibed in them.

2.1 Windows Security feature

In windows, the password feature is connected to user accounts providing the administrator user the right of creation and modification of user accounts. There were no road maps in windows which would ensure that the password entered is secure enough or no, which was a major drawback. Then the password policies came into existence that made sure that the systems were protected by certain guidelines either set into the systems or enforced by the organizations. However, the general adoption of these policies were not extensive. The enforcement of some policies were such that the user had to abide by it, such as, changing of password every day or every week in organizations.

A program known as LC5 is capable of cracking simple passwords with eight characters in a count of seconds. As a matter of fact, most passwords dwell between 5 to 8 characters.

*Corresponding author: **Dhanraj Poojari**

2.2 Implementation of password policies in organizations

The data contained within the organizations are supposed to be so sensitive that there is a need for it to be kept highly secured. In this process, organizations tend to impose stringent password policies. The strictness of these policies may differ from one organization to the other. However, overall these policies are deemed as user unfriendly by those on whom these policies are imposed.

Rightly so, for example, the policy may say, ‘password must contain an alphabet, a capital letter, a number, an alphanumeric symbol, and must be between 8 to 15 characters’. As a user it is very painful to follow this policy and expect to remember the password every time. Moreover the policy may force the user to change the password every day or every week.

Philip Inglesant did a research on password policies imposed by organization on users. His key observation was,

When users cannot cope with the demands of strict password policies, it

a) Reduces their productivity, and
b) Leads them to adopt coping strategies - which usually reduce security. (Philip Inglesant, *et al,* 2010)

2.3 Biometrics

As biometrics was introduced, they were considered as the answer to all the shortcomings of password. However, it was later realized that biometrics themselves had their share of disadvantages.

It is common for the finger print of the person to get affected in Chemical companies. Voice of the person may change with age, throat infection or due to background noise in the environment. The eyes of diabetic patients are affected resulting in differences. Moreover, the biggest drawback is that Biometrics is an exceedingly expensive security solution.

Reetu Awasthi in her research has stated that Biometric systems still need to be amended in the terms of accuracy and speed. Biometric systems with the false rejection rate under 1% (coupled with a reasonably low false acceptance rate) are still rare today. False Acceptance Rate in Biometric Systems is still high. (Reetu Awasthi, *et al*, 2013)

3. Technologies used in the implemented system.

3.1 Bluetooth

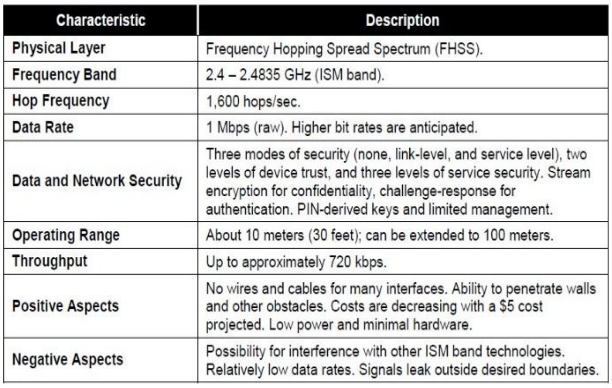
The idea Bluetooth was proposed in 1997 by Jim Kardach who formulated a system that would allow mobile phones to communicate with computers. The Bluetooth logo is a bind rune merging the Younger Futhark runes and Harald's initials.

Bluetooth is of the most efficient system in point-to-point and point-to-multi-point voice and data transfer. Bluetooth network devices exhibit a master-slave relationship.

Bluetooth specifies three basic security services namely

1. Authorization
2. Confidentiality
3. Authentication

Bluetooth device Media Access Control address (MAC address) is absolutely unique. Speed of Bluetooth devices ranges from 1 to 2Mbps. It has a low cost as compared to Wi-Fi and consumes very less power.



Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 – 2.4835 GHz (ISM band).
Hop Frequency	1,600 hops/sec.
Data Rate	1 Mbps (raw). Higher bit rates are anticipated.
Data and Network Security	Three modes of security (none, link-level, and service level), two levels of device trust, and three levels of service security. Stream encryption for confidentiality, challenge-response for authentication. PIN-derived keys and limited management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters.
Throughput	Up to approximately 720 kbps.
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a $5 cost projected. Low power and minimal hardware.
Negative Aspects	Possibility for interference with other ISM band technologies. Relatively low data rates. Signals leak outside desired boundaries.

Fig. 1 Characteristics of Bluetooth (Wankhade S.B., *et al,* 2013)

The contribution of Bluetooth in T-FA System is as follows:

Authentication: Connect to a particular device only if the device is known to the system, otherwise the connection is terminated. MAC Address of the device determines the familiarity of the Bluetooth device.

Authorization: Only registered Bluetooth device can access to the protected data.

Confidentiality: The fact that Bluetooth devices have a range of only 1 meter, there won’t be any spoofing because once the device leaves the Bluetooth vicinity, the protection of personal files and folders get activated.

3.2 Rijndael Encryption

The Advanced Encryption Standard (AES), also cited as Rijndael (its original name), is an encryption of electronic data specification which was established by the U.S. National Institute of Standards and Technology in the year 2001.

AES is grounded on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who presented a subject matter to NIST during the AES selection process. Rijndael is a family of ciphers with varying key and block sizes.

Rijndael algorithm was preferred for this implementation since it is widely considered very difficult to solve. Also performance of Rijndael algorithm is complex which makes it difficult to crack.

Rijndael is one of modern symmetrical cryptography algorithm, which has 4 processes in each round:

1. Sub Bytes Transformation,
2. Shift Rows Transformation,
3. Mix Columns Transformation,
4. Add Round key (DR. Zahir Zainuddin, *et al,* 2013)

Rijndael has various distinguishing strong points due to which it is a part of this security system. The design philosophy of Rijndael adopts three main principles namely:

1. *Simplicity:* Rijndael is described as having a 'rich algebraic structure' which grants the cipher's security to be easily evaluated in a restrained time frame. This is an advantage over more complex designs which has a requirement of extensive thinking, searching and 'bit tracing'.
2. *Performance:* Rijndael is a consistent performer in both hardware and software across broad range of computing environments. Its key setup time coupled with key agility is splendid. Rijndael is perfectly fitted for restricted space environments due to its low memory requirements. The extra security in Rijndael's procedures are amongst the easiest to defend versus power and timing attacks.
3. *Usage of well-understood components:* Rijndael's implementation is very elastic because it can be used with varying key sizes and block sizes. Change of sequence of some steps in Rijndael does not affect the cipher. It is a simple and elegant structure does not involve any complex components. Instead, it profits from the advantages earned by the use of simple components in a well-defined structure.

Joan Daemen in his paper says that “ Design simplicity of Rijndael facilitates understanding the mechanisms that give the algorithm its high resistance against differential cryptanalysis and linear cryptanalysis, to date the most important general methods of cryptanalysis in symmetric cryptography”. (Joan Daemen *et al,* 2010)

4. Proposed System

This research centers at Two Factor Authentication [T-FA] system ushering in the use of mobile phones tokens utilizing Bluetooth and Rijndael Encryption. The research focusses on the following basic thought.

The discovery of Bluetooth devices is done through the Bluetooth enabled computer or laptop. User authorized Bluetooth MAC address, which is unique for every Bluetooth device is then stored in the database.

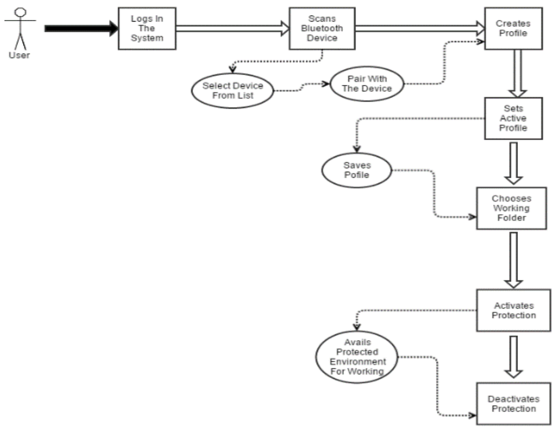


Fig. 2 Proposed System Design. (Nikita Saple, *et al*, 2015)

Protection is enabled for the folder which has been selected by the user. The implementation of handshake protocol then takes place to check whether the authorized Bluetooth device is present in the vicinity. Unavailability of the authorized Bluetooth device in the locality will lead to the encryption of all the files contained in the folder and the software to log off.

The decryption of the files will only take place after a successful log in and the availability of authorized Bluetooth device. In such a case, user will be prompted for a password and all files will be decrypted upon successful password matching. Password will never be asked in case of absence of authorized Bluetooth device.

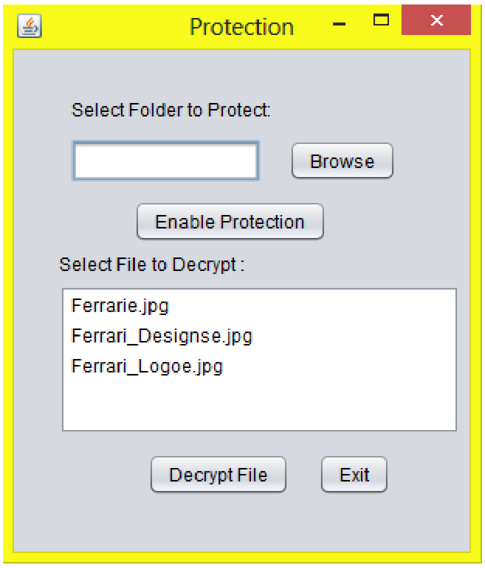
5. Implemented System

This initiates with first time registration where user identification details are to be entered. The system does not accept incorrect details. Only if all the text fields are filled with correct data, the registration gets validated. If anyone field (e.g. date of birth) has been incorrectly entered by user, the registration page does not get validated and an error is shown.

It should be noted that an account gets created based on the user profile when the system's predefined set of rules are followed and all the data fields are correctly filled.

Once the user account is created system initiates pairing with remote Bluetooth device so that to complete creation of user profile. The page scans all the available remote Bluetooth devices in the system's vicinity and pairs with the user's remote bluetooth device. Pairing with more than one Bluetooth device is forbidden by the system. The remote device acts as an authentication pass in two factor authentication.

Successful user profile creation will lead to an encryption page would appear on the computer screen that depicts that, once user's paired remote Bluetooth device is out of system's Bluetooth range, system will encrypt all the files in the folder for which protection has been enabled.



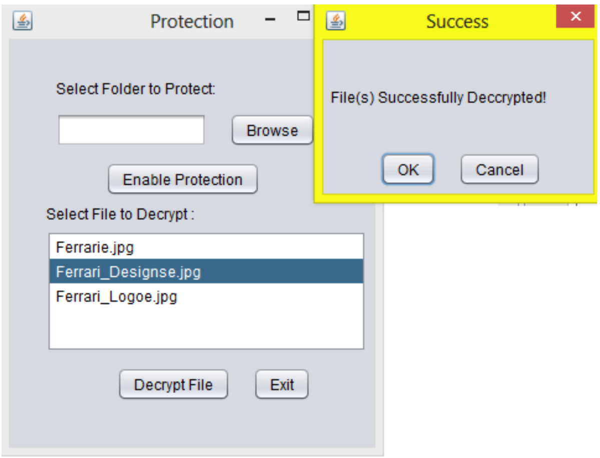
Ferrarie.jpg
Ferrari_Designse.jpg
Ferrari_Logoe.jpg

Fig. 3 Successful Encryption

The system will give an error if any user other than the primary authorized user is trying to register an account in the system. System allows only one authorized registration.

When user exits the system and logins the next time, system will seek the user id and password. If the user's username and password doesn't match then the system does not allow the user/intruder access to the files.

The decryption module in protection page portrays that it is necessary for the remote Bluetooth device to be present at all times in order to decrypt the protected folder. In absence of remote Bluetooth device the folder cannot be decrypted and an error message will be seen.



Ferrarie.jpg
Ferrari_Designse.jpg
Ferrari_Logoe.jpg

File(s) Successfully Deccrypted!

Fig. 4 Successful Decryption

Even in the presence of the remote Bluetooth device, it is mandatory for the user to enter the account password to decrypt a file. If an intruder gets access to the remote Bluetooth device and enters an incorrect password, the protection page in the system will flashes an error message. However, if the user's paired remote bluetooth device is in the system's bluetooth range and the password entered by the user is correct, successful decryption of the protected files will take place.

6. Evaluation and Discussion

The ambivalence and disagreement faced with passwords could be traced back to the ill-considered password policies. A large-scale web study found that users choose weak -mainly lowercase-only - passwords whenever they can (Florêncio, D., *et al,* 2007).

When the idea of the software was first proposed, it was believed to create a total security system which will stress on password decentralization. The whole aim was to build user friendly security system so that users have the freedom not to follow strict password policies. Let us examine how much success has been attained.

When it comes to producing a pocket friendly Two Factor Authentication [T-FA] system, definitely the goal has been achieved. The easy availability of Bluetooth in mobile phones, matched with its unique MAC Address feature, constructs it as a good factor for authentication. Also its short range (<10 meter) serves as an ideal authentication factor. Engagement of Bluetooth as a factor allows the user to set lenient passwords since the system is password decentralized.

The security level of the system is also very high due to the fact that Rijndael algorithm is being used in it. Quoting a line from an article on AES, "Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old." The quote itself justifies that it is impossible to crack Rijndael Algorithm. (go4expert)

There is always a room for improvement in every software. The system in future can allow multiple users and multiple devices of each user just in case the user has more than one Bluetooth devices. A software recovery system can be implanted which will recover the encrypted files if the Bluetooth device is lost or damaged. Time complexity of the software can also be improved.

Conclusions

This Two Factor Authentication [T-FA] system offers dual protection by combining couple of single factor authentication system, namely password and Bluetooth, secured using Rijndael encryption technique.

Thus, the frequency of changing the password & remembering difficult password (set according to the organization's password policies) are overcome. This application continuously assures if the user is working in the protected environment. Also, it furnishes an extra feature that would permit for an automated environment employing the proximity sensor to assert if user's mobile token is in range or not.

The Two Factor Authentication makes this application cost effective, reliable and convenient to use. In future, we plan to allow user with multiple mobile Bluetooth devices, multiple users per software and password changing facility.

Acknowledgements

We wish to express our immense gratitude to the range of people who provided indispensable support in the completion of this research. Their guidance and encouragement has helped in making this research a great success.

We would like to deeply express our sincere gratitude to our respected principal Dr. Shrikant Kallurkar and the management of Atharva College of Engineering for providing such an ideal atmosphere to build up this research with well-equipped library with all the utmost necessary reference materials and up to date Computer Laboratories

We are eager and glad to express our gratitude to the Head of the Computer Engineering Dept. Prof. Mahendra Patil, for his approval of this research. We are also thankful to him for providing us the needed assistance, detailed suggestions and also encouragement to do the same.

We express our gratitude to our project guide Prof Alka Srivastava, who provided us with all the guidance and encouragement and making the laboratory available to us at any time.

We are extremely thankful to all staff and the management of the college for providing us all the facilities and resources required.

References

Christian Rathgeb & Andreas Uhl (2010), Two-Factor Authentication or How to Potentially Counterfeit Experimental Results in Biometric Systems, *ICIAR Springer-Verlag ,Berlin, Heildelberg, Part II,* LNCS 6112, pp. 296–305

Nikita Saple, Dhanraj Poojari, Ankita Kesarkar, & Alka Srivastava (2015). Securing Computer Folders using Bluetooth and Rijndael Encryption. *International Journal of Current Engineering and Technology,* Vol.5, No.1, 397-400

Philip Inglesant & M. Angela Sasse (2010), The True Cost of Unusable Password Policies: Password Use in the Wild, *ACM New York, NY, USA,* 978-1-60558-929-9/10/04

Awasthi, R., & Ingolikar, R. A. (2013). A Study of Biometrics Security System. *International Journal of Innovative Research and Development*, *2*(4), 737-760.

Wankhade, S. B., Damani, A. G., Desai, S. J., & Khanapure, A. V. (2015), An Innovative Approach to File Security Using Bluetooth, *International Journal of Scientific Engineering and Technology*, Volume No.2, Issue No.5, pp : 417-423

Zahir Zainuddin & Evanita V Manullang (2013), E-Learning Concept Design of Rijndael Encryption Process, *IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE),* 978-1-4673-6354-9

Joan Daemen & Vincent Rijmen (2010), The First 10 Years of Advanced Encryption, *The IEEE Computer And Reliability Societies* 1540-7993

Florêncio, D., Herley, C., and Coskun, B. (2007) Do Strong Web Passwords Accomplish Anything? *In Proc. HotSec 07* Understanding AES Advanced Encryption Standard. [Online]. Available: *http:/ /www. go4expert.com /articles/understanding-aes-advanced-encryption-t24712*