International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Securing Computer Folders using Bluetooth and Rijndael Encryption

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

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

Accepted 16 Feb 2015, Available online 20 Feb 2015, **Vol.5, No.1 (Feb 2015)**

Abstract

Security of the computer files and folders have been a core issue ever since the advent of the windows. Passwords were then introduced to solve this issue but they themselves lend a host of disadvantages. In this paper, we shall study what disadvantages the passwords bring and how we can tackle them. Also we shall propose a Two Factor Authentication [T-FA] system utilizing Bluetooth as a factor coupled with the powerful Rijndael Encryption Algorithm. Bluetooth is the most commonly used technology for Point to Point short range of communication of devices. Besides from being commonly used, it also offers multi connection. Rijndael algorithm is an Advanced Encryption standard, believed to be the most effective encryption and decryption cryptographic algorithm. Its minimum 10 rounds of encryption and variable key size with a minimum of 128 bits makes it difficult to crack. Coupling the widespread accessibility of Bluetooth and powerful encryption of Rijndael, a Two Factor Authentication System [T-FA] can be created which will not only efface the disadvantages of passwords, but also create a user friendly security system.

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

1. Introduction

In present day, the increasing reliance on computer systems has led to the dependence on confidential security measures. Various methods used to identify a user are Digital signature, Challenge-Response, Biometrics, IPSec (Internet Protocol Security), Single-Sign On and Password.

Password has become one of the most ubiquitous modern day security tool and is very commonly used for authentication. These passwords are string of characters used for authentication or user access. Unfortunately users set passwords that can be easily memorized, in turn increasing threats. Password meters indicating password strength are used to increase effectiveness of passwords and make them less predictable.

Biometrics on the other hand requires the assumption of unrealistic preconditions for performance gain. Access control systems require time-trusted and reliable personal recognition. To overcome the problems faced by these processes individually, we can use a combination of two or more security processes.

Two-factor authentication has ameliorated security in authentication systems. Sensitive files can be provided double protection using Rijndael security extension and Mobile Bluetooth tokens. This paper will mainly compare various authentication methods and present the improvement in windows password policies using a combination of mobile Bluetooth and Rijndael encryption.

2. Existing Systems

Although passwords are usually considered in terms of authentication for a service or a device, today they are encountered in many other ways in the workplace – and existing password policies do not cover these. As a result, users adopt ad-hoc solutions, which are usually insecure. (Philip Inglesant & M. Angela Sasse *et al,* 2010)

2.1 Password security in windows

The password feature is interlinked with windows user accounts. Users possessing administrator privileges can create, modify and delete accounts. In order to judge the strength of passwords, password policies came into existence. This characteristic has been a vital issue in the windows system. Keyloggers or keystroke logging malware can be effectively protected with the help of password managers.

However, these managers cannot fight man-in-the-browser attacks. A major benefit of passwords is that they are portable and stateless. They are very useful in securing web-based and cloud based accounts.

*Corresponding author: **Nikita Saple; Alka Srivastava** is working as Assistant Professor

Passwords face several flaws corresponding to bookmarklet, authorization, web and user interfaces. A bookmarklet is a bookmark stored in a web browser that holds JavaScript commands to stretch the browser's functionality. Although biometrics and security tokens are some of the alternatives to passwords, they increase the overall risk theft, privacy threat and rise in infrastructural costs.

Elizabeth Stobert in her paper explains the password life cycle with the help of following diagram:

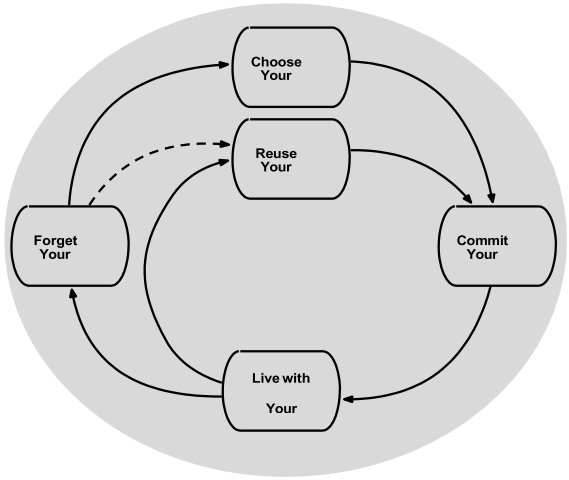

Fig. 1 The password life cycle (Elizabeth Stobert *et al,* 2014)

The length of passwords plays an important role in determining its strength. Success on brute force attack mainly depends on the length of passwords. Generally, brute force attack fails in case of long passwords. Passwords containing alphanumeric characters are another type of strong passwords. Password disclosure should be avoided in order to prevent social engineering attacks.

2.2 Vulnerabilities

There are many reasons due to which password is considered as a weak form of protection. Passwords are user-dependent in network security chain. Users often do not take security procedures for password seriously. This leads to vulnerabilities in passwords.
Major problems faced by passwords are follows:

- Noting down of difficult passwords
- Periodic change of passwords
- Using dictionary words as passwords
- Personal information. Example: Username, initials etc.
- Use of default passwords. Example: password
- Double words
- Reverse words
- Mixed case dictionary

3. Solutions to Password Vulnerabilities

Vulnerability is an imperfection in the system which can be victimized by the intruder to weaken the system. This imperfection may be present in design, implementation or maintenance of the system. We can easily block threats if we establish control over the vulnerability. Various kinds of vulnerabilities exist in the password protection system. Synthesizing a strong password and generating a high extremity on the frequency of guesses to minify cracking. Stronger policies could also be implemented using Single Sign-On. The load on user shrinks with the help stronger passwords. Opportunistic misuse of unattended desktops can be palliated with the help of screen locks and time-out. Password expiry and prevention of recently used passwords also helps reduce the attack on passwords. Different problems faced by passwords have different solutions. To overcome this two factor authentication is used. It provides single solution to all the problems faced by passwords.

4. Two Factor Authentication

The introduction of the Two Factor Authentication has been done in order to heighten the Authentication Systems. The overall access to a System is not defined by a single factor, like password, but the combination of multiple factors. In order to potentiate the security of access control systems, two factor authentication (T-FA) comes in very handy mainly because it focusses on combination of both factors. Christian Rathgeb says in his research, "These factors include, passwords, representing 'something you know', or physical tokens, such as smart-cards, representing 'something you have'. Additionally, biometric traits are applied, representing 'something you are'". (Christian Rathgeb *et a l,* 2010).

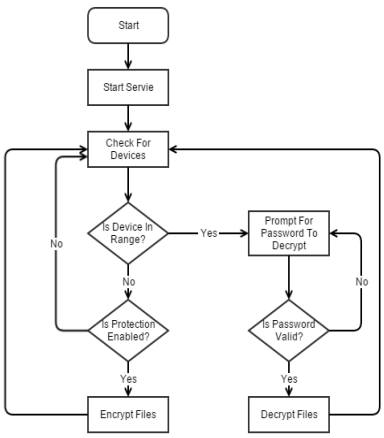

Fig. 2 Windows Service

Popular examples are ATM, Biometrics, etc.

5. Bluetooth in Two Factor Authentication

Bluetooth, a wireless technology for the transmission of data among two devices in close propinquity of each other has veritably changed the world. The connection between two devices are absolutely battened as they

operate on Personal Area Network(PAN).The major advantage that Bluetooth offers for T-FA is its range of network which is just 100 meters and is enough to personify an authenticated user's presence.

Bluetooth is a Radio Frequency (RF) specification for short range voice and data transfer, whether it be point-to-point or point to multiple points. Bluetooth will empower the users to connect to a wide range of computing and telecommunications devices without the need for proprietary cables that often fall short in terms of ease-of-use. The technology constitutes an opportunity for the industry to deliver wireless solutions that are ubiquitous across a broad range of devices. The strength and direction of the underlying Bluetooth standard will ensure that all solutions meet stringent expectations for ease-of-use and interoperability (Smart Handheld Group).

Bluetooth is unremarkably used in Mobile Phone Market. Almost every phone presently contains Bluetooth in it which makes it a very cost effective T-FA Authenticator. The operational terms of Bluetooth in terms of processing power and battery is also very minimalistic.

Bluetooth can conduce in the T-FA System in the following manner:

Authentication: Connect to a particular device only if the device is known to the system, otherwise abort connection. The familiarity of Bluetooth device is ascertained by the MAC Address of the device.
Authorization: Only authorized Bluetooth devices should have the access to the protected data.
Confidentiality: Since Bluetooth devices have a range of only 100 meters, there won't be any spoofing since as soon as the device is out of range, the protected personal files and folder would be encrypted.

6. Rijndael Encryption

Rijndael Cipher is an Advanced Encryption Standard (AES) based on design principle grounded as substitution permutation network and is quick in both software and hardware. Avoidance of the Fiestal network in the AES is its important characteristic. AES, a variant of Rijndael has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. The key size specifies the total number of rounds for conversion of plaintext to ciphertext. They are,

- 10 rounds for 128 bit keys
- 12 rounds for 192 bit keys
- 14 rounds for 256 bit keys

There are 4 processes in each round namely,

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

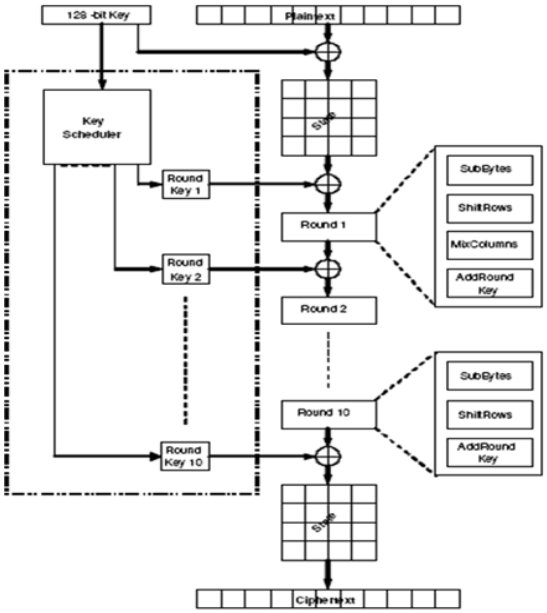

Fig. 3 Steps in Rijndael Encryption (Inno-Logic)

6.1 Advantages

Rijndael Algorithm, A Cryptographic Algorithm, is widely conceived as one of the best algorithms for encryption. Efficient implementation of the algorithm is due to the chasteness of its design which makes the effectuation easy to understand. Joan Daemen in his paper says that " It also 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 & Vincent Rijmen *et al,* 2010)

7. Proposed System

This research focuses on Two Factor Authentication [T-FA] system introducing the use of mobile phones tokens employing Bluetooth and Rijndael Encryption. The following is the basic thought of this research.

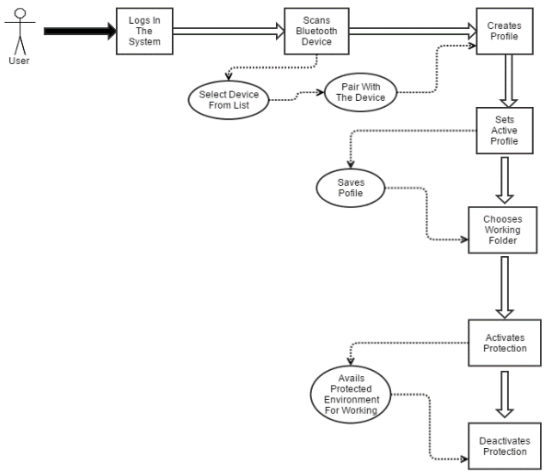

Fig. 4 System Design

Bluetooth is enabled in your laptop or PC. An interface is written to discover the Bluetooth devices by their MAC address and the same is authenticated with the Admin password. Registry of system stores the MAC address. Application is initiated as a background process along with the PC. The folder in which the user is currently working on is selected in the configuration mode. A Handshake protocol is implemented by the program every 5 seconds so that whenever the authenticated Bluetooth device moves away from the PC, all the working files and folders are encrypted and account is logged off. After a successful log in, the program will search for the authenticated Bluetooth device and prompt for the password. Successful password matching then decrypts all the files and folders user was working on. In case of mismatch of Bluetooth devices, the application never demands for the password.

Conclusion

This application program would ensure user authentication by the windows password login further authentication to most private files employing their Bluetooth enabled mobile phones. This can lead to less frequent password changes or have less stringent policies that the users are resistant to and they can and furnish an extra feature that would permit for an automated environment employing the proximity sensor to assert if your mobile token is in range or not.

Acknowledgment

We would like to thank our project guide professor Alka Srivastava for helping and mentoring us throughout this project. We are also grateful to our head of the department, Professor Mahendra Patil for the support. Lastly we would not have been able to conduct this research without the infrastructure and facilities provided to us by Atharva College of Engineering.

References

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

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

Elizabeth Stobert & Robert Biddle (2014), The Password Life Cycle: User Behaviour in Managing Passwords, *Symposium on Usable Privacy and Security (SOUPS) 2014*

Smart Handheld Group, Hewlett-Packard Company, *Bluetooth Technology Overview*

Resources page of Inno-Logic. [Online]. Available: *http://www.inno-logic.com/resources/17.php*

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