UGC Approved Journal

IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 7, July 2017

Two way Authentication with Bluetooth and Rijndael Algorithm

Mr. Shreenath Waramballi[1], Sunil B N[2], Mr. Vijay C P[3], Manjunath Raikar[4]

Assistant Professor, Computer Science Engineering, Sahyadri College of Engineering, Mangalore, India[1,2,3,4]

Abstract: 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 present the improvement in windows password policies using a combination of mobile Bluetooth and Rijndael encryption.

Keywords: Rijndael encryption, Access control systems, reliable personal recognition, Mobile Bluetooth tokens

I. INTRODUCTION

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. Key loggers 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.

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

Passwords face several flaws corresponding to book marklet 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. 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 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 focuses on combination of both factors

Rijndael Algorithm

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 AES algorithm consists of ten rounds of encryption. First the 128-bit key is expanded into eleven so-called round keys, each of them 128 bits in size. Each round includes a transformation using the corresponding cipher key to ensure the security of the encryption.

DOI 10.17148/IJIREEICE.2017.5702

UGC Approved Journal

IJIREEICE

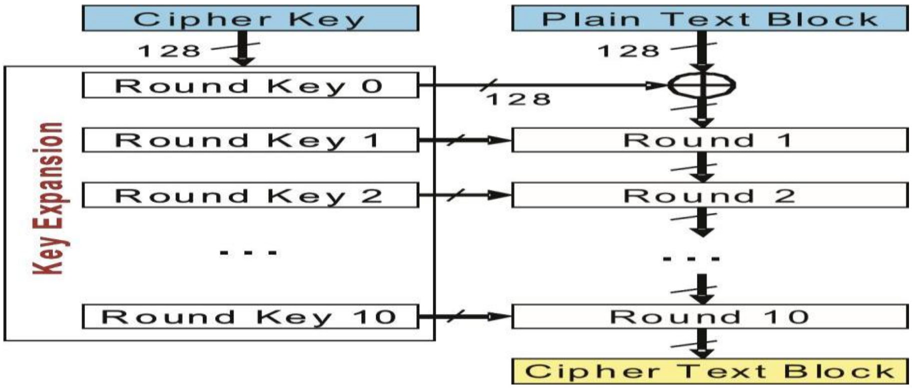
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

International Journal of Innovative Research in
Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified

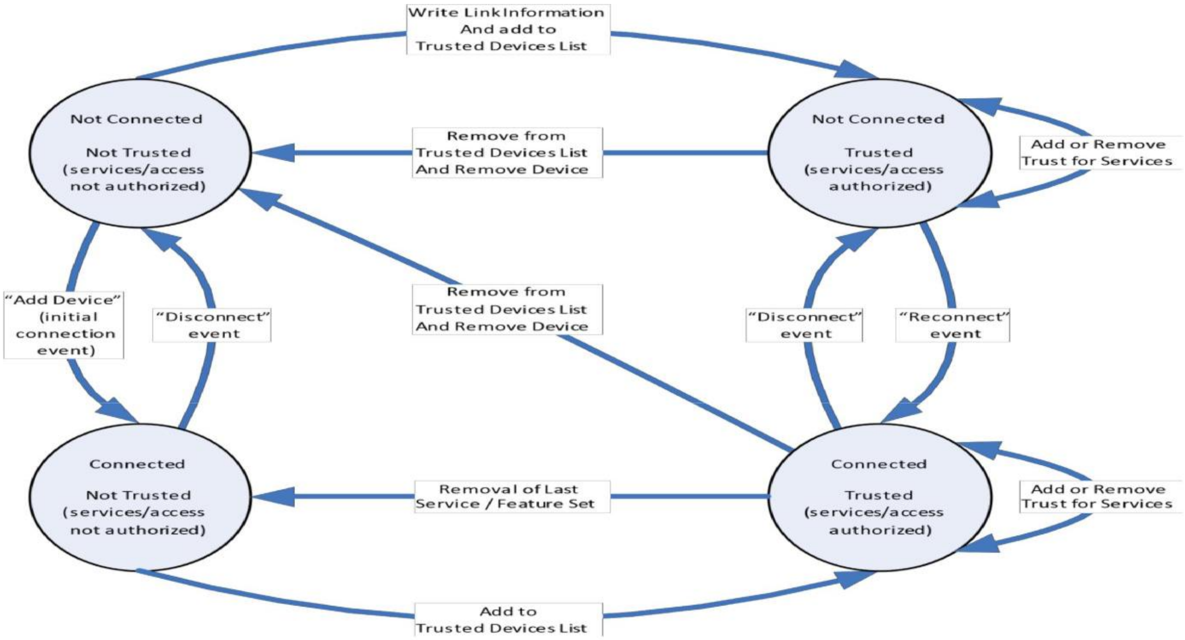
Vol. 5, Issue 7, July 2017

II. BLOCK DIAGRAM



Rijndael Algorithm Block diagram

After an initial round, during which the first round key is XORed to the plain text (Addroundkey operation), nine equally structured rounds follow. Each round consists of the following operations: Substitute bytes, Shift rows, Mix columns, Add round key. The tenth round is similar to rounds one to nine, but the Mix columns step is omitted.



Algorithm for File Encryption

Step1: Login page.
Step2: Login by using Bluetooth MacID if registered and goto step 4 else goto step 3.
Step3: Create profile by filling details and goto step 1.
Step 4: Select file to be encrypted.
Step 5: Give password for authentication as well as encryption (key). Step 6: Logout

Algorithm for File Decryption

Step 1: Login to account.
Step 2: Select file to be decrypted.
Step 3: Give same password provided while encrypting file. Step 4: Logout

Algorithm for Backup

Step 1: Login page.
Step 2: Select 'Forgot' option.
Step 3: Fill the details. Step 4: Select update. Step 5: Logout.

DOI 10.17148/IJIREEICE.2017.5702

Model–view–controller (MVC) is a software architecture pattern which separates the representation of information from the user's interaction with it. The model consists of application data, business rules, logic, and functions. A view can be any output representation of data, such as a chart or a diagram. Multiple views of the same data are possible, such as a bar chart for management and a tabular view for accountants. The controller mediates input, converting it to commands for the model or view. The central ideas behind MVC are code reusability and separation of concerns. In addition to dividing the application into three kinds of components, the MVC design defines the interactions between them: A **controller** can send commands to its associated view to change the view's presentation of the model (e.g., by scrolling through a document). It can also send commands to the model to update the model's state (e.g., editing a document). A **model** notifies its associated views and controllers when there has been a change in its state. This notification allows the views to produce updated output, and the controllers to change the available set of commands. A passive implementation of MVC omits these notifications, because the application does not require them or the software platform does not support them. A **view** requests from the model the information that it needs to generate an output representation to the user.

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.
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

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. 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

Key Expansion (KeyExpansion operation)
Key expansion refers to the process in which the 128 bits of the original key are expanded into eleven 128-bit round key. To compute round key (n+1) from round key (n) these steps are performed: Compute the new first column of the next round key as shown in figure**.** First all the bytes of the old fourth column have to be substituted using the Sub bytes operation. These four bytes are shifted vertically by one byte position and then XORed to the old first column. The result of these operations is the new first column.

Columns 2 to 4 of the new round key are calculated as shown:
[new second column] = [new first column] XOR [old second column]
[new third column] = [new second column] XOR [old third column]
[new fourth column] = [new third column] XOR [old fourth column]

For Connection purpose used in ‘Backup module’ we have used local host network connections. In computer networking, local host means this computer. It is a hostname that the computer's software and users may employ to access the computer's own network services via its loopback network interface. On most computer systems, local host resolves to the address 127.0.0.1, which is the most-commonly used IPv4 loopback address, and to the IPv6 loopback address. The local loopback mechanism is useful for programmers to test software during development independent of any networking configurations. If a computer has been configured to provide a website, directing its web browser to http://localhost may display its home page. Using the loopback interface bypasses local network interface hardware.

DOI 10.17148/IJIREEICE.2017.5702

The name is also a reserved top-level domain name (cf. .localhost); set aside to avoid confusion with the narrower definition as a hostname and the registrars of many second - level domains also prevent registration.

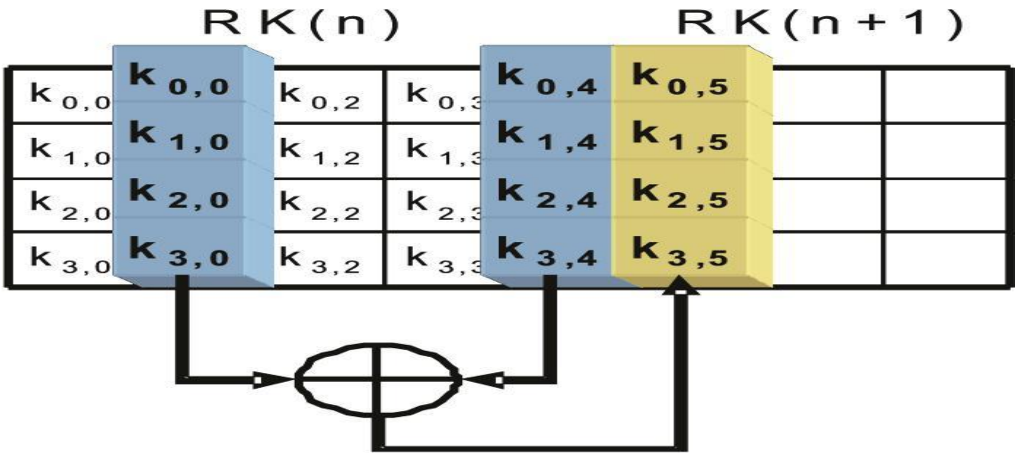


Fig: Expanding Other Columns of Next Round Key

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

III. CONCLUSION

This application program would ensure user authentication by the windows password login and further authentication to most private files employing their Bluetooth enabled mobile phones. This can lead to less frequent password changes 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.

REFERENCES

[1] Kazumaro Aoki and Yu Sasaki. Meet-in-the-middle preimage attacks against reduced SHA-0 and SHA-1. In CRYPTO’09, volume 5677 of Lecture Notes in Computer Science, pages 70–89. Springer, 2009

[2] Alex Biryukov and Ivica Nikoli´c. Automatic Search for Related-Key Differential Characteristics in ByteOriented Block Ciphers: Application to AES, Camellia, Khazad and Others. In EUROCRYPT’10, volume 6110 of Lecture Notes in Computer Science, pages 322–344. Springer, 2010.

[3] T. Jakobsen and L.R. Knudsen, "The interpolation attack on block ciphers," Fast Software Encryption, LNCS 1267, E. Biham, Ed., Springer-Verlag, 1997, pp. 28-40J. Kelsey, B. Schneier and D. Wagner, "Key-schedule cryptanalysis of IDEA,GDES, GOST, SAFER, and Triple-DES," Advances in Cryptology, Proceedings Crypto '96, LNCS 1109, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 237-252.

[4] J. Kelsey, B. Schneier, D. Wagner and Chris Hall, "Cryptanalytic attacks on pseudorandom number generators," Fast Software Encryption, LNCS 1372, S. Vaudenay, Ed., Springer-Verlag, 1998, pp. 168-188.

[5] L.R. Knudsen, "Truncated and higher order differentials," Fast Software Encryption, LNCS 1008, B. Preneel, Ed., Springer-Verlag, 1995, pp. 196-211.

[6] L.R. Knudsen, "A key-schedule weakness in SAFER-K64," Advances in Cryptology, Proceedings Crypto'95, LNCS 963, D. Coppersmith, Ed., Springer-Verlag, 1995, pp. 274-286.

[7] X. Lai, J.L. Massey and S. Murphy, "Markov ciphers and differential cryptanalysis," Advances in Cryptology, Proceedings Eurocrypt'91, LNCS 547, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 17-38.

[8] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1986.

[9] M. Matsui, "Linear cryptanalysis method for DES cipher," Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 386-397.

[10] K.Nyberg, "Differentially uniform mappings for cryptography," Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55-64.