AUTHENTICATION AND KEY MANAGEMENT WITH SESSION BASED AUTOMATED KEY UPDATION

Bavani S[1], Markco M[2]

Department of CSE, E.G.S. Pillay Engineering College, Nagapattinam , Tamil Nadu

ABSTRACT

Authenticated key exchange (AKE) is one of the most important applications in applied cryptography, where a user interacts with a server to set up a session key using pre-registered information about the user. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE schemes, e.g. combining both passwords and biometrics and device simultaneously. However, in some schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole authentication process. Furthermore, an inevitable by-product arises that the usability of the protocol often drops greatly. To summarize, the existing multi-factor protocols using 3DES algorithm is did not provide enough security and efficiency simultaneously. Here, one step ahead by proposing a very efficient authentication method to overcome the security issues, proposed method use Four factor authentication, it is a newer security paradigm in multi factor authentication implement by combining textual, graphical, and biometric and device password to access the user accounts and an efficient AES algorithm for data transaction from user to server which is more secured algorithm. The result from the security testing shows that image based passwords is more secure because the possibility of the key bits placed on the image to be guessed is very low.

Keywords: Authenticated key exchange, advanced encryption standard, four factor authentication

1. INTRODUCTION:

At the time of systems are connected through the network, attacks are possible during transmission time. Network security is a process that is designed to detect, prevent and recover from a security attacks. User authentication is a very important part for many information systems. The authentication service is concerned with assuring that a communication is

authentic. It helps to prove that the source entity only has involved the transaction. Key exchange protocols allow two or more parties communication over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have suggested over the years for a variety settings. In order to avoid mistakes and impersonations during the process we can use various authentication means. It is often done via the following methods:

- **Password-authenticated** can make server-to-client authentication easier and resistant to offline dictionary attacks, and additionally provides a secure key for encryption. Textual Authentication is the most popular way, while quite insecure in some cases. The statistics show that most passwords in use are not so hard to guess.
- **Secret Hardware Key Based Authentication** provides higher security than password with storage space for long secret keys and computation power for authentication. But if it is stolen or lost, the authentication fails completely.
- **Biometric verification systems** may require a significant outlay for enterprise deployment. Depending on the degree of security required, it may be preferable to implement multifactor authentication (MFA).
- **Graphical password** is more difficult to defend against. If a user's computer is compromised by passive spyware that records keystrokes and occasionally transmits this information to an attacker's server, then the use of one-time passwords may be effective, since a previously used one-time password cannot be used again.

AUTHENTICATED KEY EXCHANGE

Authenticated Key Exchange (AKE) (or Authenticated Key Agreement) is the exchange of session key in a key exchange protocol which also authenticate the identities of parties involved in the key exchange.

Single Factor Authentication

Single-factor authentication (SFA) is a process for securing access to a given system, such as a network or website that identifies the party requesting access through only one category of credentials. The most common example of SFA is password-based authentication. Password security relies on the diligence of the system administrator or user who sets up the account. Best practices include creating a strong password and ensuring that no one can access it.

PROPOSED SYSTEM

Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is).

Levels of multifactor authentication

A 2FA system strengthens security by requiring the user to provide dual means of identification from separate categories. Typically, one proof of identity is a physical token, such as an ID card, and the other is something memorized, such as a security code or password. The second factor helps to ensure that, even if an intruder steals a user password, they would also have to access the physical device to get into the user account.

3FA adds another factor for further difficulty in falsifying authentication. Typically a biometric trait measurement is added for the inherence factor. Such a system verifies that the person logging in knows the password, has their ID card and that their fingerprint matches the stored record.

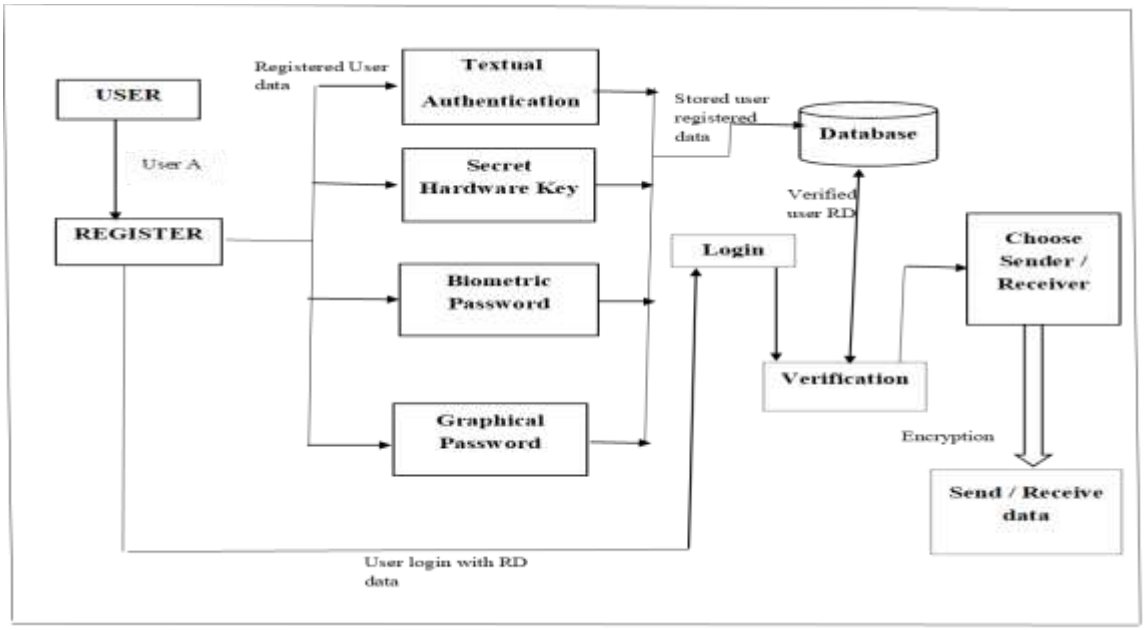
4FA ups the authentication ante again taking four unique factors of authentication. It starts to seem like mission impossible in order to break the security. Like a spy using a portable compute device to hack a password, while plugging in cloned USB token, and finally the matching employee's eye for a retina scan.

5FA system would use the three commonly-used factors (knowledge, possession and inherence) plus location and time. In such a system, a user has to reproduce something he knows or remembers, provide proof that he has some item with him, provide a biometric sample for matching and have his location verified -- all within allowed times before he is granted access.

GRAPHICAL AUTHENTICATION

This step is used to login the individual sender and receiver. This graphical password is created by using the information about the sender and receiver and with the help of sessions using in it and is sent to the user registered phone number. These passwords are accessed only in the particular location of the secured 3D image. The graphical password is generated based on the users clicking point which is based on the corresponding **x** axis and **y** axis value. If the values of the clicking point match with the registered value, only then the user can login and process

this system. After finding the coordinates a text box will be displayed and the graphical password should be entered.



METHODOLOGY

Four-factor authentication is a newer security paradigm than two-factor or three-factor authentication. Four factor systems are sometimes used in businesses and government agencies that require extremely high security. Higher levels of multifactor authentication categories make it increasingly unlikely that an attacker can fake or steal all elements involved.

- Knowledge factors include all things a user must know in order to log in, such as a user name and password or personal identification number (PIN).
- Possession factors include anything a user must have in their possession to log in, such as a one- time password token (OTP token) or a smart phone with an OTP app.
- Inherence factors include biometric user data that are confirmed for login, such as iris scans, fingerprint scans and voice recognition.

Advanced Encryption Standard

The (**AES**), also known by its original name Rijndael (Dutch pronunciation is a specification for the encryption of electronic data. The more popular and widely adopted

symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael, with a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael *per se* is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.

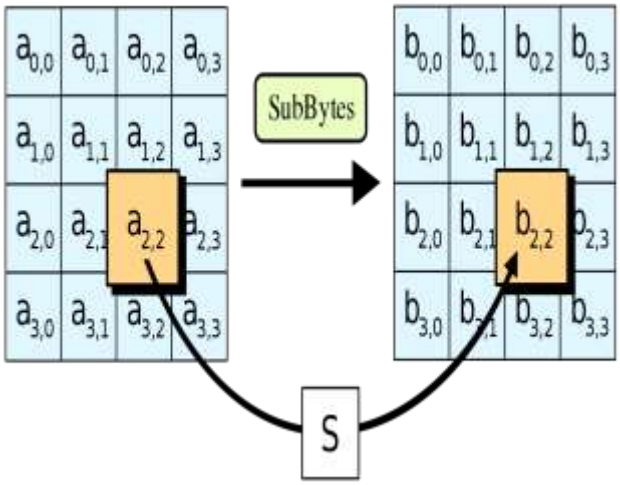
AES operates on a 4 × 4 column-major order array of bytes, termed the *state*. Most AES calculations are done in a particular finite field. For instance, if there are 16 bytes, b0, b1… b15 these bytes are represented as this two-dimensional array:

b0 b4 b8 b12
b1 b5 b9 b13
b2b6 b10 b14
b3b7b11b15

The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the cipher text. The number of rounds are as follows:

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

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.



Conclusion

The Multi-dimensional password is a multifactor authentication scheme that combines these various authentication schemes into a single 3-D virtual environment. Therefore, the resulted password space becomes very large compared to any existing authentication schemes. The design of the 3-D virtual environment, the selections of objects inside the environment, and the object's type reflect the resulted password space. Additionally, designing a simple and easy to use 3-D virtual environment is a factor that leads to a higher user acceptability of a multi factor authenticated system. A user who prefers to remember and recall a password might choose textual and graphical passwords. For more security bio-metric is also used for secure transaction. A main focus for future work will be extending authentication factor 5FA to provide secure transaction.

REFERENCES

1. **Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards** AUTHORS: Xiao-Min Wang, Wen-Fang Zhang, Jia-Shu Zhang, Muhammad Khurram Khan, Computer Standards & Interfaces, 2007.
2. **Efficient Multi-Factor Authenticated Key Exchange Scheme**

AUTHORS: Rue Zhang, Yuting Xiao, Zhuzhou Sun and Hui Ma, IEEE Transactions on Dependable and Secure Computing 2017 (Volume: PP, Issue: 99).

3. **System Analysis and Design** AUTHORS: Elias M. Award Galatia Publications, Second Edition.
4. **Enhancing security and privacy in biometrics-based authentication systems** AUTHORS: N. K. Rather, J. H. Connell and R. M. Bole, IBM SYSTEMS JOURNAL, VOL 40, NO 3, 2001.
5. **Two-factor mutual authentication based on smart cards and passwords** AUTHORS: Tianjin CAO, Shi HUANG, 2013.
6. Richard Blum, "C# Network Programming", John Wiley & Sons Publishers, 2006.
7. Robin Dawson, "**Pro SQL Server 2005",** Press Publisher.
8. Roger S. Pressman, "Software Engineering", Fourth Edition, 2005.