MULTI-FACTOR AUTHENTICATED BY EXCHANGING KEYS IN SERVER SIDE

M.K.Nandhini[1], Karthikeyan[2]
[1](UG Student, Christ the King Engineering College, swasarnan@gmail.com)
[2](Assistant Professor, Christ the King Engineering College, karthikeyan195@gmail.com)

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 where pre-registered information (aka. authentication factor), such as a password or secret authentication, of the user is stored. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE (MFAKE) schemes, e.g. combining both passwords and device simultaneously. However, in some casually designed schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole MFAKE protocol. Furthermore, an inevitable by-product arise that the usability of the protocol often drop greatly. To summarize, the existing multi-factor protocols did not provide enough security and efficiency simultaneously. Here, we make one step ahead by proposing a very efficient MFAKE protocol. We define the security model and give the according security analysis. We also implement our proposed method as textual, graphical and device password to access the user accounts. The theoretic comparisons and the experimental results show that our scheme achieves both security and usability.*

1. INTRODUCTION

The Multifactor Authentication scheme have been proposed, however, users tend to resist using USB device because of their intrusiveness and the effect on their privacy and the hardware also(ex: Usb devices). Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed. We present and evaluate our contribution, Multifactor authentication scheme. To be authenticated, we present a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's graphical password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, device passwords into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the graphical password key space.

2. TEXTUAL AUTHENTICATION

The User Registration has both the sender and receiver registration process. Initially they have to register for their interaction between them. The sender and receiver registered by using the individual textual passwords. The Registration process is common for both the sender and receiver.

During the registration phase the user have to register the graphical password and their finger print. These registered values are stored in database for security verification purposes while the login process.

GRAPHICAL PASSWORD GENERATION

This step is used to login the individual sender and receiver. It creates a graphical password that is used for the login purpose of the 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. These passwords are accessed only in the particular location of the secured image.

These graphical passwords are used to increase the authentication to the data. 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, then only he can login and process this system

3. HARDWARE-BASED AUTHENTICATION

With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. But if it was stolen or lost, which happens in daily life occasionally, the authentication fails completely.

4. RELATED WOKS

Textual passwords are commonly used in systems. However, users do not follow their requirements. Users tend to choose meaningful words from dictionaries, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. The authentication scheme has its disadvantages based on several factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying is its intrusiveness upon a user's personal characteristic. These schemes require the user to willingly subject there to a low-intensity infrared light. In addition, systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users.

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

The feasibility study investigates the problem and the information needs of the stakeholders. It seeks to determine the resources required to provide an information systems solution, the cost and benefits of such a solution, and the feasibility of such a solution.
A Systems Development Life Cycle (SDLC) adheres to important phases that are essential for developers, such as planning, analysis, testing and implementation are explained

in the section below. A number of system development life cycle (SDLC) models have been created: waterfall, fountain, and spiral, build and fix, rapid prototyping, incremental, and synchronize and stabilize. The oldest of these, and the best known, is the waterfall model: a sequence of stages in which the output of each stage becomes the input for the next.

The waterfall model is a popular version of the systems development life cycle model for software engineering. Often considered the classic approach to the systems development life cycle, the waterfall model describes a development method that is linear and sequential. Waterfall development has distinct goals for each phase of development. Imagine a waterfall on the cliff of a steep mountain. Once the water has flowed over the edge of the cliff and has begun its journey down the side of the mountain, it cannot turn back. It is the same with waterfall development. Once a phase of development is completed, the development proceeds to the next phase and there is no turning back.

The advantage of waterfall development is that it allows for departmentalization and managerial control. A schedule can be set with deadlines for each stage of development and a product can proceed through the development process like a car in a carwash, and theoretically, be delivered on time. Development moves from concept, through design, implementation, testing, installation, troubleshooting, and ends up at operation and maintenance. Each phase of development proceeds in strict order, without any overlapping.

5. TEXTUAL AUTHENTICATION

The User Registration has both the sender and receiver registration process. Initially they have to register for their interaction between them. The sender and receiver registered by using the individual textual passwords. The Registration process is common for both the sender and receiver.
During the registration phase the user have to register the graphical password and their finger print. These registered

values are stored in database for security verification purposes while the login process.

6. GRAPHICAL PASSWORD GENERATION

This step is used to login the individual sender and receiver. It creates a graphical password that is used for the login purpose of the 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. These passwords are accessed only in the particular location of the secured image.
These graphical passwords are used to increase the authentication to the data. 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, then only he can login and process this system

7. HARDWARE-BASED AUTHENTICATION

With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. But if it was stolen or lost, which happens in daily life occasionally, the authentication fails completely.

8. DATA SEND

After the multifactor authentication the sender begins to send the data. The sender sends the data to the receiver in the encryption format for the security purpose. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
The encryption process is done by AES algorithm. The data's are encrypted so the unknown person can't access the files which are sent by sender. These encryptions are known only by the authorized sender. AES is considered one of the most efficient algorithms currently available.

9. DATA RECEIVE

After the sender sends the data the receiver access the data using the session password. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.
After finishing multifactor authentication the receiver can decrypt and view the original format of the data which has sent by the sender. Authorized person can only decrypt the file using the key. So the file is prevented from unauthorized access.

10. CONCLUSION

My proposed solution to defend against code-reuse attacks was to increase the entropy by randomizing the function blocks and signature verification. One may apply this randomization technique at various levels of granularity—function level, block level or gadget level. The level of granularity to choose is a trade off between security and performance. In our implementation, we implemented the randomization at the function level which is the most coarse granularity amongst the three mentioned above. However, we show that even this coarse level of granularity provides substantial randomization to make brute force attacks infeasible. DSA algorithm will have will have a great effect on all of our federal agencies because they are required to use this standard when transmitting information that is not declassified. This standard is also available to the private sector and commercial organizations. The DSA is necessary to make sure that our governments' communications are secure. The standard ensures that these federal agencies that may have not had a

secure algorithm to transmit data will now have such a means to make sure communications are secure.

REFERENCES

[1] M. Slain, “Announcing Our Worst Passwords of 2015,” https://www.teamsid.com/worst-passwords-2015/, 2015.
[2] [Online]. Available: https://pages.nist.gov/800- 63-3/sp800-63b. html#out-of-band
[3] S. Bellovin and M. Merritt, “Encrypted Key Exchange: Password- Based Protocols Secure Against Dictionary Attacks,” in IEEE S&P, 1992, pp. 72–44.
[4] O. Goldreich and Y. Lindell, “Session-key generation using human passwords only,” in CRYPTO, 2001, pp. 408–432. [5] S. M. Bellovin and M. Merritt, “Augmented Encrypted Key Exchange: A Password Based Protocol Secure Against Dictionary Attacks and Password File Compromise,” in ACM CCS, 1993, pp