ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# SECUDROID - A Secured Authentication in Android Phones Using 3D Password

Ms. Chandra Prabha K M.E. Ph.D.[1], Mohamed Nowfel[2] E S, Jr., Gowtham V[3], Dhinakaran V[4]

Department of CSE, K.S.Rangasamy College of Technology, Tiruchengode 637215 India, Tamilnadu, India[1, 2, 3, 4]

**ABSTRACT—**The devices used most often for IT services are changing from PCs and laptops to android supported mobile devices and tablets. These devices are in the need of hand held for increased portability. These technologies are more convenient than others, but as the devices start to contain enormous amount of important personal information, a good security mechanism is required. Security systems and authentication techniques such as remote control systems have been rapidly developing since 2006. Although these solutions were proposed to be viable, major problems could still result when the device itself is stolen. In this report, we present our upgraded Lock Screen System, Biometric scheme and Graphical Password scheme which support authentication for the user's convenience and provide a good security measure for smart phones. We also propose an upgraded authentication schemes for Android smart phones to enhance the security. Initially the user enters 3D Virtual Environment and they are free to use that environment and they will select the objects. After that step, the user will enter the Textual Environment and enter the textual password. Then the user has to enter the Graphical environment and they have to enter the pattern in the picture. Finally they will enter in to the Biometric Environment and fingerprint is registered. Then all the inputs are stored in the database. After that all inputs are compared to the stored results. Then the user is authenticated in to the mobile phone. By using this Multifactor Authentication in the Single 3D Virtual Environment, We provide enhanced Security.

**KEYWORDS—**Android, Authentication, Smart phones, Virtual Environment

## I. INTRODUCTION

The number of smartphone users is rapidly increasing worldwide, especially the number of Android OS users. Because of this phenomenon, Home Launcher was developed to support user convenience. Users can download Home Launchers from the Android Market and Google Store; the most commonly used ones are ADW Launcher, Launcher Pro, and GO Launcher. These systems provide convenience but not upright security. The Home Launchers currently on the market do not use secure authentication methods as in Android OS and as developed by smartphone companies. Accordingly, Home Launchers need to have authentication methods to provide better security and convenience.

In this thesis, we will analyze the problems with the current Home Launchers' Lock Screens and suggest an upgraded authentication system and a secured system for Android smartphones.

## II. AUTHENTICATION USING 3D PASSWORD

### *A. Authentication*

Authentication (from Greek: Real or genuine, derived from the word authentes: author) is the act of confirming the truth of an attribute of a datum or entity. This might include authorizing the identity of a person or software program that find the origins of an artifact, or guaranteeing that a product is what it's packaging and labeling claims to be. Authentication often includes proving the validity of at least one form of identification.

Authentication is the process of validating who you are to and whom you requested to be. In common, there are four human authentication techniques:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

1. What you know (knowledge based).
2. What you have (token based).
3. What you are (biometrics).
4. What you recognize (recognition based).

*B. 3D Password*

The 3D password is a multi-factor authentication scheme. The 3D password grants a Three Dimensional virtual environment containing various virtual objects. The user navigates over this environment and cooperates with the objects. The 3D password is the combination and the sequence of user interactions that occur in the 3D virtual environment. The 3D password can syndicate recognition, recall, token, and biometrics based systems into single authentication scheme. The 3D passwords are more customizable and very interesting way of authentication. Now the passwords are established on the fact of Human memory. Generally guileless passwords are established so as to quickly recall them. In our scheme, the human memory has to undergo the facts of Recognition, Recall, Biometrics or Token based authentication scheme. Once implemented and you log in to a secure site, the 3D password GUI Interface opens up. This is an additional textual password which the user can simply give. Once he goes through the first authentication, a 3D virtual environment will show on the screen.

## III. EXISTING SYSTEM

Current authentication system has many loopholes. Current authentication systems suffer from many weaknesses:

- Textual passwords are commonly used. Users tend to select significant words from dictionaries, which make textual passwords easy to crack.
- Textual passwords are in danger to dictionary or brute force attacks.
- Many available graphical passwords have a password space that is less than or equal to the textual password space.
- Smart cards or tokens can be stolen.
- Many biometric authentications have been proposed. However, users tend to attack using biometrics because of their intrusiveness and the effect on their privacy. Moreover, biometrics cannot be canceled. The 3D password is a multi-factor authentication scheme. The design of the 3D environment and the type of objects selected determine the 3D password key space. User have freedom to choose whether the 3D password will be solely recall, recognition, or token based, or mixture of two schemes or more.

## IV. PROPOSED SYSTEM

The proposed system is a multi-factor authentication scheme that combines the benefits of various authentication techniques. Users have the autonomy to select whether the 3D password will be solely recall based, biometrics, recognition based, or token based, or a combination of two or more schemes. This freedom of selection is necessary because users are different and they have different requirements. Therefore, to confirm high user adequacy, the user's freedom of selection is imperative. The following requirements are fulfilled in the proposed scheme

1. The new scheme provide secrets that are easy to remember and very difficult for intruders to guess.
2. The new scheme provides secrets that are not easy to write down on paper. Moreover, the system secrets should be hard to share with others.
3. The new scheme provides secrets that can be easily revoked or changed.
4. It fails all the attacks like brute force attacks, dictionary attacks, etc. Hence the security is enhanced.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## V. BRIEF DESCRIPTION OF THE SYSTEM

The proposed system is a multi-factor authentication scheme. It can syndicate all prevailing authentication schemes into a single 3D virtual environment. This 3D virtual environment comprises some objects or items with which the user can interact. The user is obtainable with this 3D virtual environment where the user navigates and interacts with numerous objects. The categorization of actions and interactions toward the objects inside the 3D environment constructs the user's 3D password. The 3D password can conglomerate most existing authentication techniques such as textual password scheme, graphical password scheme, and various types of biometrics scheme into a 3D virtual environment.

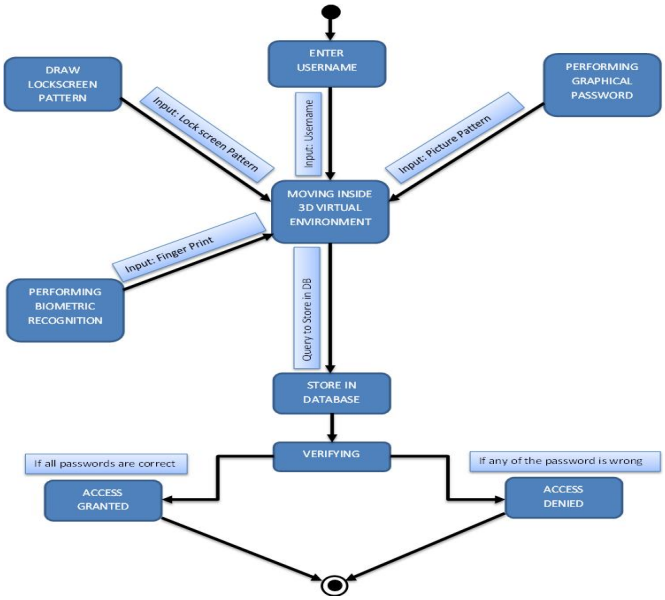


Figure 1: State Diagram For 3D Password

The choice of what authentication schemes will be part of the user's 3D password reflects the user's preferences and requirements. A user who prefers to recollect and remembering a password might choose textual and graphical password as part of their 3D password. Instead users who have more difficulty with memory or recall might prefer to choose smart cards or biometrics as part of their 3D password. Besides user who wishes to keep any kind of biometric data private might not interact with object that requires biometric information. So it is the user's superior and decision to construct the desired and preferred 3D password.

## VI. SECURITY ANALYSIS

To realize and understand how far an authentication scheme is more secure, we have to think through all the possible attack techniques. We have to revise whether the authentication scheme proposed is immune against such attacks or not.

Moreover, if the proposed authentication scheme is not immune, we then have to find the counter methods that prevent such attacks. In this unit, we try to cover most probable attacks and whether the attack is legal or not. Moreover, we try to propose counter methods for those attacks.

*A. Brute force Attack*

The attacker has to try all possible 3D passwords. This kind of attack is precise difficult for the following reasons.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

1. Time required to login the total time needed for a legitimate user to login may vary depending on the number of interfaces and activities, the magnitude of the 3D virtual environment, and the type of movements and interfaces. Therefore, a brute force attack on a 3D password is very difficult and time consuming
2. Cost of attacks in the 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all the probable biometric information and forge all the obligatory tokens. The cost of falsifying such information is very expensive; therefore cracking the 3D password is more stimulating. The more number of possible 3D password spaces leaves the attacker with almost no chance of breaking the 3D password.

*B. Timing Attack*

1. In this attack, the attacker observes how long it takes the legitimate user to perform correct sign in using the 3D password technology. This surveillance gives the attacker an indication of the legitimate user's 3D password length.
2. However, this kind of attack alone cannot be very successful since it gives the attackers the ordinary hints. Therefore, it would be probably being launched as part of a well-studied or the brute force attack. Timing attacks can be very operational if the 3D virtual environment is poorly designed.

*C. Well Studied Attack*

1. The attacker tries to find the highest probable distribution of 3D passwords. In order to takeoff such an attack, the attacker has to procure awareness of the most probable 3D password distributions.
2. This is very difficult because the attacker has to study all the existing authentication schemes that are used in the 3D virtual environment. It requires a revision of the user's selection of objects for the 3D password.
3. Moreover, a well-studied attack is very hard to accomplish since the attacker has to perform a customized attack for every different 3D virtual environment design.
4. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment. Therefore, a wisely personalized study is required to initialize an effective attack.

*D. Shoulder Surfing Attack*

1. An attacker uses a camera to record the user's 3D password or tries to watch the legitimate user while the 3D password is being executed. This attack is the most fruitful type of attack against 3D passwords and some other graphical passwords.
2. However, the user's 3D password may contain biometric data or textual passwords that cannot be hacked using shoulder surfing. Therefore, we undertake that the 3D password should be performed in a secure place where a shoulder surfing attack cannot be performed.

## VII. ADVANTAGES

1. A 3D password gives the user the choice of modeling his 3D password to contain any authentication scheme that the user prefers.
2. Users have the choice to model their 3D password according to their needs and their preferences.
3. Users do not have to provide their fingerprints if they do not wish to.
4. It fails most of the brute force attacks and dictionary attacks.
5. As the authentication system is new and complex the hacker will have to study the new authentication schemes .It requires a study of the user's selection of objects for the 3D password which is quite difficult as the selection of object varies from individual to individual.
6. Provides strong security over critical servers. Now a day as all banking transactions are done on internet.so this module will provide a good security to e-commerce transactions.
7. As this system is based on human quality if recognition and recall, password cracking algorithms fail to crack these passwords.
8. The 3D virtual environment contains biometric recognition objects and token based objects. The attacker has to forge all probable biometric information and forge all the essential tokens. The cost of forging such information is very expensive; therefore cracking the 3D password is more challenging.
9. Easy to use as an end user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

## VIII. DISADVANTAGES

1. Timing attacks can be very effective if the 3D virtual environment is poorly designed.
2. This environment has a number of objects and types of object responses that differ from any other 3D virtual environment to confuse the attacker. So space required store these objects is more.
3. The 3D virtual environment contains biometric recognition objects and token based objects. To fail the attacks made by any hacker, more objects will be required to increase the cost of forging.
4. If there are many users using 3D Passwords then much space will be required to store these in database. So it may affect the speed.
5. Shoulder surfing is more vulnerable. So entering these passwords must be done in secured place.
6. Complexity is more in developing.

## IX. FUTURE WORKS

1. In general, present system uses CAPTCHA (Completely Automated Public Turing test to tell Computers ana Human Apart).But there are some software freely available that can crack CAPTCHA within seconds. So the hacker can create botnets and hence, brute force attacks will be successful.
2. Here the capability of humans to recognize and recall alphabets and objects is used for only authentication schemes when the computer feels that some attacks are being done. In future, this capability of human beings will be used to give passwords.
3. 3D passwords are now currently being used in military armaments like sky-catcher and radars.
4. In future it will be used in banking transactions, accessing your email accounts etc.

## X. APPLICATIONS

The 3D password can have a space that is very large compared to other authentication schemes, so the 3D password's main application domains are protecting critical systems and resources.

1. Many large organizations have critical servers that are usually protected by a textual password. A 3D password technology proposes a sound replacement for a textual password.
2. Nuclear and military facilities such facilities should be protected by the most powerful authentication systems. The 3D password has a very large credible password space, and since it can contains token based, biometrics, recognition and knowledge based authentication schemes in to a distinct authentication scheme, and it is an encyclopedic choice for very high level security locations.
3. Airplanes and jet fighters Because of the possible threat of misusing airplanes and jet fighters for religion, political programs, and usage of such airplanes should be protected by a powerful authentication system.

In addition, 3D passwords can be used in less critical systems because the 3D virtual environment can be designed to fit to any system requirements. A little virtual environment can be used in the following systems like

1. ATM
2. Personal Digital Assistance
3. Desktop Computers & laptop logins
4. Web Authentication
5. Security Analysis

The main application domains of 3D Password are critical systems and resources.

1. Critical systems such as Military Forces, Critical servers and highly confidential areas can be protected by 3D Password technology with large three dimensional virtual environments.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

2. Moreover, a little three dimensional virtual environment can be used to protect less critical systems such as handheld devices, ATM's and operating system's logins.
3. Acquiring the knowledge of the probable distribution of a user's 3D password might show the practical strength of a 3D password.
4. Moreover, finding a solution for shoulder surfing attacks on 3D passwords and other authentication schemes is also a field of study.

## XI. CONCLUSION

The 3D password is a multi-factor authentication scheme that combines the various authentication schemes into a single 3D virtual environment. The 3D virtual environment contains any existing authentication scheme or even any upcoming authentication scheme or even any upcoming authentication schemes by adding it as a response to actions performed on an objects. Therefore the resulting space of password becomes very large compared to any existing schemes. The design of the 3D virtual environment is the selection of objects inside the environment and the object's type reflect the resulted password space. It is the work of the system administrator to plan and design the environment and to select the appropriate object that reflects the protected system necessities. Planning and Designing a simple and easy 3D virtual environment is a factor that leads to a higher user acceptability of a 3D password technology. The choice of which authentication scheme will be the part of user's 3D password reflects the user's preferences and requirements. Textual passwords and token-based passwords are the most commonly used authentication schemes. However, many different schemes have been used in different fields. Other schemes are under research yet they have never been applied in the real world. The motivation of this work is to have a scheme that has a huge password space while also being a combination of many existing single factor authentication schemes into one Multi factor scheme.

## REFERENCES

[1] Daniel Klein.V, (1990), "Foiling the Cracker: A Survey of, and Improvement to Passwords Security", Proceedings of the USENIX Security Workshop.
[2] Darren Davis, Fabian Monrose, and Michael K. Reiter, (2004), "On user choice in Graphical Password Schemes", Proceedings of the 13th USENIX Security Symposium, San Diego.
[3] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, (2008), "Three-Dimensional Pa Password for More Secure Authentication", IEEE Transactions on Instrumentation and Measurement, Vol. 57, pp. 9.
[4] Kwang Il Shin, (2012), "Design and Implementation of Improved Authentication System for Android Smartphone Users", 26th International Conference on Advanced Information Networking and Applications Workshops
[5] G. E. Blonder, (2006), "Graphical password", U.S. Patent 5 559 961.