International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 2, February- 2013

3 Factor Authentication for Remote Accessing Using Android Device

Dhananjay .A.Sherigar
Student

Aniket M.Patwardhan
Student

Anjali .More
Professor

Abstract

The Goal of this paper is how remote access to a server/system can be done using Android device phone with the help of 3 Factor authentications. In today's world there is a need to security, whatever we do on the internet it needs to be secured. And today's world is all about the Smartphone's. So now people want everything on their mobile phone for example Newspaper, Payment and etc. So if a user wants to access a data on the server he need to login to a system first and then only he can access it. Which is time consuming and less secure. So to provide more security and save users time we will use the 3 Factor authentication for remote accessing process.
The 3 factors are 1.password 2.USIM (Universal Subscriber Identity Module) 3.Biometric Authentication. These three factors play a very important role in accessing our remote desktop and make the accessing more secure and less vulnerable attacks.
So in this paper we will see the other authentication method available and the proposed 3 Factor authentication system for remote accessing.

Keyword: 3Factor Authentication, Remote Accessing, Android Device.

1. Introduction

The remote accessing using android phone must be secure and data confidentiality should be maintained. But the current authentication systems are not secure and may be attacked by the attacker if not provided proper security. So there is need of 3 factor authentication.

For remote desktop accessing we would be using 3 factors of Authentication.

- Password (What user has): This is the most simplest and the common method used for authentication. The user or the one trying to access the remote desktop inserts the password. It's basically a secret key combined of character, special symbols and number.

- USIM (What user knows): USIM stands for Universal Subscriber Identity Module. The USIM number is 20 or 24 digit code depending on the size of the SIM card. This USIM number is directly send to server where the authentication is performed.

- Biometric Authentication (What user is): It's the third and the most important part for authentication. We would be using **Face Recognition** as the third factor for authentication. In this the Android Device would capture the image for authentication purpose. The image would be the transferred to local server for authentication.

Fig 1: Topology for 3 Factor Authentication

2. Literature Survey

2.1 One Factor Authentication:

One factor authentication is commonly used where security is not a high concern or where any misuse of data cannot be happened. One factor basically involve one factor for authentication i.e. PASSWORD which is of length 8-16 character and composed of combination of letters, number and special character. One factor authentication can also contain factor as one time password. But it can also be guessed if the algorithm is guessed.

Factor of one factor authentication is

- **What user has.**

Basically one factor authentication is used for social networking site, Bank website and etc.

2.1.1 Advantages:

1. It is more User Friendly and less time is required for accessing the account.
2. Password are easy to remember as they are which user know.

2.1.2 Disadvantages:

1. It is easy to guess by the attacker as it may be user name, birth day and etc.
2. Vulnerable to the attacks.

2.2 Two factor authentication:

Two factors provide more security than 1 factor authentication as it has two factors which user must have. The one factor is password and the second factor depends on the organization or website. The second factor may be pass code, PIN Number, one time password, Token and etc. Here the second factor can also be the biometric identification.

Pass code are nothing but a code which is provided by the service provided to user through mobile. PIN can be 16 digit numbers which user has.

Basically Two factor authentication factor are:

- **What user knows.**
- **What user has.**

The two factor authentication is provided by Google while accessing the account, first we enter the password then it sends a pass code to user mobile if user has provided it and after entering it user gets access to the account. So this is one example of two factor authentication.

2.2.1 Advantages:

1. Security level is increased.
2. Here user don't have to remember the password as password is what he known and 2 factor is sent to him or his Credit card number which he has.

2.2.2 Disadvantages:

1. It is not user Friendly as it requires more time for accessing the account.
2. The password and pass code can be identified by the attacker.
3. Security level is not high though the security is increased.

3. Biometric Authentication

The main question is that why to use face identification technique only? The reasons are that, there are other types of Bio metric authentication like Face recognition retina scan, finger print scan and voice recognition, but there is there are a lot of anomalies in retina scan and finger print scan(thumb print scan).Moreover it increases the cost of the system and mounting the high end devices on android phone is not worth acceptance. The anomaly in voice recognition is that we cannot assume that the user is in place where there is no noise. Noise factor plays a very important role in voice recognition; a slight noise in background may affect authentication. Thus even if microphone jacks are present in every android device it cannot be used as the third factor of authentication

4. Proposed Methodology

In prototype phase we would be considering how the 3 factors actually come into play, while they are authenticating the user.

- In the first phase the users is requested to enter the User ID and Password. This is then send to the server for verification.

Fig:3.1 Login

- If the above step is performed successfully then the USIM number is transferred to the server for authentication. It states that the user is using the same SIM for accessing the server.

In the third and last step face recognition takes place. Here the camera captures the image runtime and sends it to the server for authentication.

Fig: 3.2Biometric authentication

4.1 Advantages

1. The security provided is high.
2. It is not easy for attacker to attack the system.
3. As the second factor is based on USIM number so the user with his own SIM can only login to the system.

4.2 Disadvantage:

1. It is not user friendly as it requires more time for authentication.
2. A Little bit complex process.

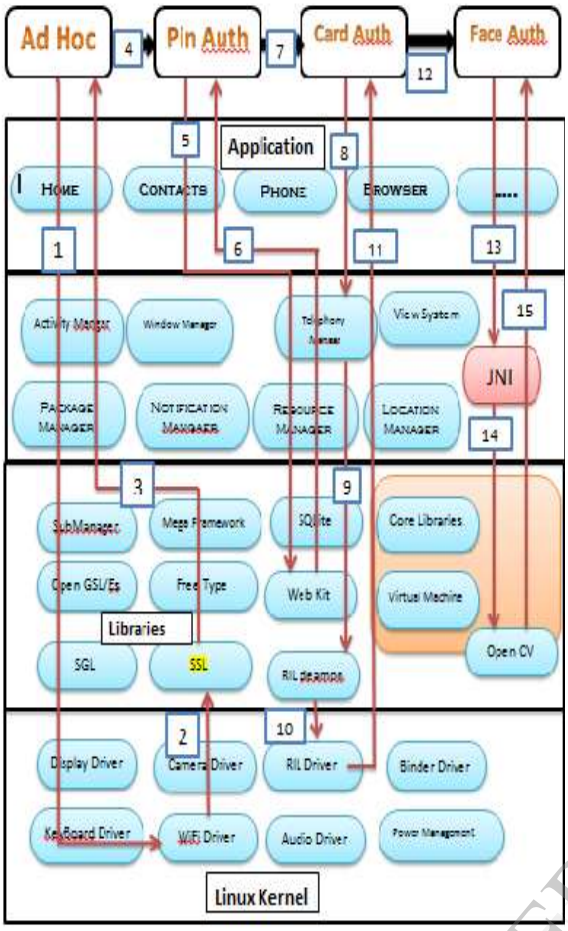

Fig:4.1 Android phone kernel.

5. Conclusion

As the technology develops people demands also increases so people want everything at their finger tip. So remote accessing through the phone using 3 Factor authentications will provide the data required for the user at his finger tips. So by looking at the loopholes of other authentication method we can say that the 3 factor authentication is better and provide more security.

6. Refrences

[1] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6154013&contentType=Conference+Publications&queryText%3D3+factor+authentication

[2] http://en.wikipedia.org/wiki/Two-factor_authentication

[3] http://en.wikipedia.org/wiki/Two-factor_authentication

[4] http://ecommerce.about.com/od/eCommerce-Design-and-Dev/f/What-Ecommerce-Players-Need-To-Know-About-Two-Factor-Authentication.htm

[5] http://www.checkpoint.com/securitycafe/readingroom/general/truth_authentication.html

[6] https://isc.sans.edu/diary/When+factors+collapse+and+two+factor+authentication+becomes+one.+/13276