INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume3, Issue3)

Available online at: www.ijarnd.com

Cloak Encryption in Apache

V. Adithya[1], R. Ramya[2], D. Vignesh Kumar[3], M. Madava Krishnan[4]

[1,2,3]Student, Sree Sakthi Engineering College, Coimbatore, Tamil Nadu

[4]Assistant Professor, Sree Sakthi Engineering College, Coimbatore, Tamil Nadu

ABSTRACT

The tremendous growth of mobile devices has pro-generated new form of security flaws. The manifest based permission in android devices is one of the hefty security threats among all .We propose cloak protocol based encryption. We use exterior apache server for generating CSPRN and also we make use of the session id which will be very helpful in tracking user sessions and it will be difficult for the hackers to crack the file. For multiple user registrations we define a new way of two dimensional graphical authentications using one-time password with the session ID to keep track of users. With this, the user can securely transceiver messages.

Keywords: *Mobile Computing, Encryption, Authentication, CSPRN, Graphical Authentication, Transmission.*

1. INTRODUCTION

Mobile Computing is the process of transmitting and receiving the data wirelessly without any physical link, the data may be of any type such as video/voice/image. In wireless networking, the security is always a major concern even though it allows user mobility and device portability. Sending plain text data over the wireless networks makes the intruders a very easy task to crack the file, so there need the proper encryption and decryption of data. The encryption process converts the plain text data to another form known as cipher text and the decrypting of the data takes the cipher text as input and apply an algorithm and key for reverting it back to the plain text. The innovative applications developed by our generation and the cheap prices of high tech mobile devices have increased the count of mobile users. Most of the mobile users store their personal information and secured bank account passwords in a plain text format which can be easily accessed by any third party mobile applications. The mobile now is compiled form of sensitive information which has to be properly secured. Beyond this, the usage of wireless networks has hyped the intrusions of several malware which can easily crack the secured data. The mobile computing mainly focuses on the security of data. Nowadays the files are uploaded and stored in the external server and it is equipped with all the necessary security services which make the intruders very difficult to hack the resources. The information in mobile devices is stored in the local storage which can be easily accessed by third-party applications. The mobile applications with unwanted access to information must be reported and blocked from all devices immediately.

The few guidelines for the mobile computing security are

Encryption-The encryption of sensitive data must be done at its origin and the data must be stored in the encrypted format and key for decryption must be provided only after proper authentication of the user.

External Identification- The mobile devices must be properly labeled with the username and his contact number so that the device can be easily returned to the owner in case if it is lost.

Storing Limited Data- The sensitive information must be stored less in local. The users can make use of the proper cloud storage or external storage servers with high security and authentication.

Lost Device Locator- The mobile device which has secured information has to be tracked from a remote location. There are several third-party applications such as Android Device Manager from google and icloud from apple which can locate the device, lock and erase them with the network connectivity.

Passwords and Timeout- The user has to set a proper password and a timeout if it's left unlocked.

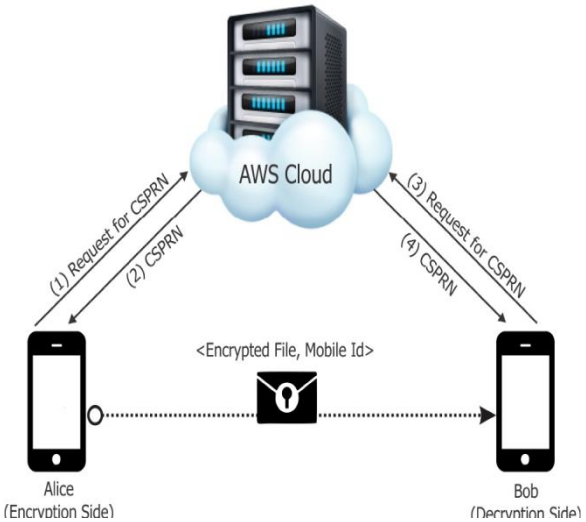
Trusted Sources- There are various sources available for application download but the users have to rely only on trusted sources such as Google Play, Apple iTunes store which can reduce the risk of malware to a significant amount

Updates- Hackers are creating several new methods for getting sensitive user information and defensive software are running battle for superiority, so the frequent updates of all applications will help the users to keep his data secured

Public Networks- Users have to avoid connecting to the public networks where there is a very limited security for the connected devices and it's easier to theft the sensitive user information

Now the availability of high-speed networks has made accessing the cloud resources easier and it also helps the user to connect with their resource from a remote location. The user can also download a huge range of files from the internet and
It increases the security threats as well. More ransom ware which decrypts all the data and requests the user to send bitcoins for the provision of the decryption key in order to avoid such threats the user has to limit the number of download from the internet.

2. EXISTING SYSTEM

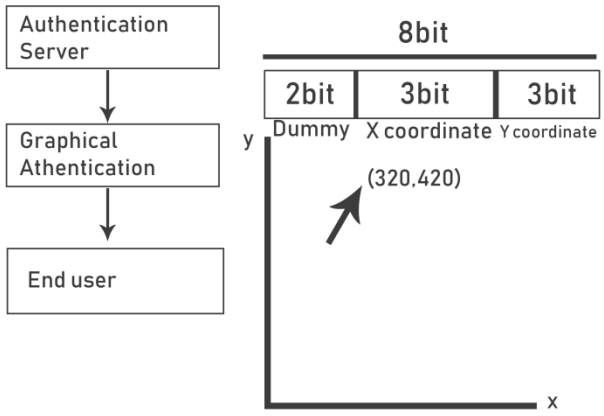


The existing system used Amazon Web Service (AWS) cloud and it generated the RID (Random Identification for Device) locally which is sent as a parameter for getting the CSPRN key from Cloud. Most of the mobile devices now use manifestly based permission method which allows the third party application to access the sensitive data. There was just a kind of registration for users and no proper authentications if the intruders get the RID through any third party application then it is easy to get the CSPRN key. The key used here is symmetrical so the same key will be used for decryption purpose. The CSPRN in the cloud is generated through CLOAK Protocol in which the key is generated based on the number of clockwise and anti-clockwise rotations. The CSPRN further generates the symmetric key for encryption and decryption of data

The major concern is that the cost the AWS servers are very much high even tough it is bought on a rental basis and since the locally generated RID is a major flaw in the security of the system and user data

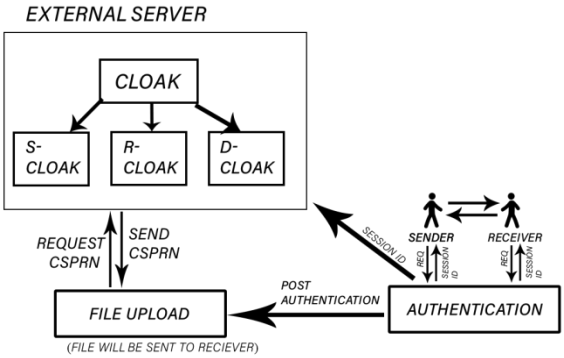
3. PROPOSED SYSTEM

For Proper authentication of the user, we use a new way of Graphical Authentication in which each and every pixel in the monitor is considered as the coordinates. The monitor is 2dimensional and we generate a onetime password of 8 digits first 3digit of the OTP points to the X coordinates and other 3 maps to Y coordinates the remaining 2 digits are considered as the dummy for enhanced security. The graphical authentication is more secured since the awareness of this kind of authentication is very much less among the intruders.



The graphical user authentication is alternate to text-based passwords which makes the user easy to remember the password and visual interaction makes them more convenient to work with. The possibility of intruders guessing the password is very less. The authentication server sends the one time password to the user via mail and the user will interact on the screen based on the OTP provided.

The session id keeps track of the user and provides the security post authentication. Both the sender and receiver are allocated with their own unique session id which monitors them throughout the session in case of any network errors the session id of the user is renewed and all the logs recorded in the previous session is erased. Consider if a hacker is performing an attack and even if he is successful he won't get access to the files since he will be allocated with the separated session id. The session should be monitored, recorded but it has to be deleted once the session gets over.



The entire process occurs in three phases

Authentication Phase

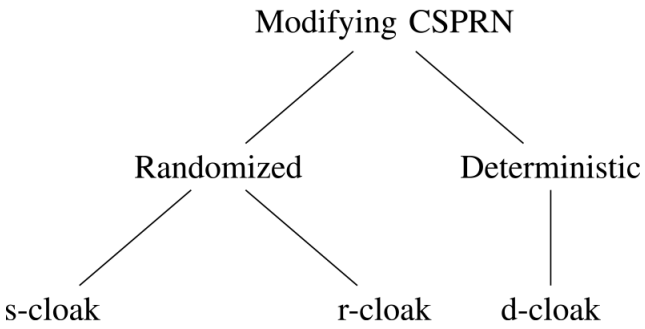
In Authentication, the user will get the one time password and the link to authentication monitor is provided along with the one time password the coordinates are provided as a tooltip when the user clicks in the correct location the authentication will be successful and the unique session id is allocated to the user.

File Upload Phase

As soon as the Graphical authentication is completed the user is prompted with the panel for file upload and the file will be encrypted based on the CSPRN generated by the external server

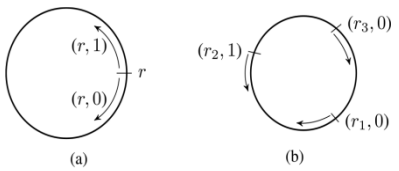
Cloak Protocol

After the file being uploaded to the server, the cloak protocol starts to encrypt the data using the CSPRN and symmetric key the same key will be used for the decryption purpose the cloak protocol may be either randomized or deterministic



s-CLOAK:

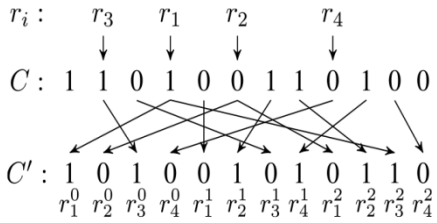
There are two random variables are used. One is used to describing the shifts and another one for directions of the rotation. By using factor, it increases the total size of the key pair.



s-CLOAK with randomized key-pair $k = (r_i, 0/1)$.

r-CLOAK

r-CLOAK is randomized cloak used for modifying CSPRN. Using block/chunk-wise both s-CLOAK and r-CLOAK can be implemented. Which is important for memory efficient mobile devices (MDs).



r-CLOAK with randomized key-pair: $k = \{r_i, 0/1\}$.

d-CLOAK

It is the deterministic approach. Where the preset secret key is used for generating modified CSPRN. The encryption process is inverse of the decryption.

4. CONCLUSION

This is an efficient way for encryption using a cloak Protocol. The CSPRN generation is kept in an eternal server. The session id tracks the user and protects the data transfer from the intruders. The graphical authentication using one-time password is more secured among all the other textual authentication.

5. REFERENCES

[1]Amit Banerjee; Mahamudul Hasan; Md. Auhidur Rahman; Rajesh Chapagain "CLOAK: A Stream Cipher Based Encryption Protocol for Mobile Cloud Computing" IEEE Access Year: 2017, Volume: 5
[2] Martin Mihajlov; Borka Jerman-Blažič Interacting with Computers "On designing usable and secure recognition-based graphical authentication mechanism" Year: 2011, Volume: 23, Issue: 6 Pages: 582 – 593 OUP Journals & Magazines
[3] Nicolas Lopez; Matias Rodriguez; Catalina Fellegi; Darrell Long; Thomas Schwarz"
Even or Odd:Simple Graphical Authentication System
"IEEE Latin America TransactionsYear: 2015, Volume: 13, Issue: 3
[4] Marcos Martinez-Diaz; Julian Fierrez; Javier Galballsy " Graphical Password-Based User Authentication With Free-Form Doodles" IEEE Transactions on Human-Machine Systems Year: 2016, Volume: 46, Issue: 4
[5] Karen Renaud; Elin Skjegstand "OlsenDynaHand: Observation-resistant recognition-based web authentication" IEEE Technology and Society Magazine Year: 2007, Volume: 26, Issue: 2
[6] Marcos Martinez-Diaz; Julian Fierrez; Javier Galbally "The DooDB Graphical Password Database: Data Analysis and Benchmark Results" IEEE Access Year:2013, Volume: 1
[7] Katherine Olstein; Bill Bowhill "New Academic Demo Session Paired with IDS at 2012 ISSCC [Conference Reports]" IEEE Solid-State Circuits Magazine Year: 2012, Volume: 4, Issue: 2
[8] Tarik Taleb; Adlen Ksentini "Follow me cloud: interworking federated clouds and distributed mobile networks" IEEE Network Year: 2013, Volume: 27,
Issue: 5
[9] https://www.rsaconference.com/blogs/guidelines-formobile-computing-security
[10] https://en.wikipedia.org/wiki/Mobile_computing

