Detection of Intrusion and Recovery for Smartphones using Cloud Services

I.B.Rajeswari[#1], Prof.Dipti Patil[*2]

[#]*Computer Department, Pillai Institute of Technology,*
University of Mumbai
New Panvel, Maharashtra, India
[1]rajeswari_ib@yahoo.co.in
[2]ibrajeswari@mes.ac.in

[*] *Computer Department, Pillai Institute of Technology,*
University of Mumbai
New Panvel, Maharashtra, India
[1]dpatil@mes.ac.in
[2]dypatil75@gmail.com

***Abstract*—Smart phones are popular and most used. Since smart phones use the same software architecture as in PCs, they are vulnerable to similar classes of security risks such as intrusion and hacking. This project proposes an intrusion detection and prevention for smart phone using cloud services which continuously performs an in-depth forensics analysis on the smart phone to detect any misbehaviour such as wrong passwords and intrusion. It protects the smart phone, from the data steeling and other security issues. In case misbehaviour is detected, the proposed engine decides upon and takes optimal response actions to prevent the occurrence of ongoing attacks. Despite the computational and storage resource limitations in smart phone devices, the engine can perform a complete and in-depth analysis on the smart phone and data storage, since all the investigations are carried out on an emulated device in a cloud environment. To address the critical challenge of keeping smart phone secure, cloud services has been proposed to prevent the intrusion and block the attack immediately.**

***Keywords*— Cloud environment, Intrusion Detection System, OTP (One Time Password), Recovery system**

I. INTRODUCTION

Cloud based intrusion detection was developed to address the critical challenge of keeping the smart phone secure. A cloud based intrusion detection and response framework for the purpose of transparent operation for the users. An accurate intrusion detection and response has been proposed in this system. A smart phone to be protected by the framework should be registered by its owner to the framework's online registration system. To register, the client should first specify his or her device, so that the framework can work on the smart phone in cloud and the key is provided to download the documents for the client. The light-weight agent on the smart phone performs three main tasks. It gathers all user information and sensor inputs to the device, then it sends them to the cloud environment, data from the cloud in made visible to the client. The client can store his valuable data into the cloud environment using his login. Once the client attempts to download the data from his account, he has to type the key which is provided to him when he registered his smart phone. Once he successfully logins to the download page, an OTP (One Time Password) is generated and sent to the client smart phone. The client has to enter the OTP in his account to download the data. If the client attempts three wrong OTPs, the intrusion detection system will forensic and respond to the client. The light weight agent which is running on the smart phone will wait for potential response and recovery commands. In case intrusion is detected, the agent in the smart phone will receive the response from the cloud environment and then the agent can take the required actions to recover the smart phone back to its normal mode.

II. CLIENT REGISTRATION

A smart phone to be protected by the framework should be registered by its owner to the framework's online registration system. To register, the client should first specify his or her device name and mobile number, so that the frameworks can instantiate a communication between the smart phone and the cloud. The intrusion detection is performed in the cloud.

A. Client Registration Module

The client registration module has the following steps involved in it.

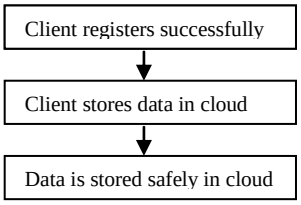
- Create client registration form
  - client should specify his/her device
  - Mobile number, address of the client
- Once the details get registered successfully. It will be automatically store in the cloud server.
- Once the details get registered successfully. It will be automatically store in the cloud server.

- Client is asked to install very lightweight software agent in his smart phone that will automatically configure the proxy settings.

- Once the client registers the smart phone, he can login to his account to store his/her data into the cloud. The storage page contains the files and folders of the client.

III. CLIENT STORAGE

The client logs into the cloud framework and the authentication is verified by the IDS (Intrusion Detection System). The client stores the data from the cloud.



3.1 BLOCK DIAGRAM FOR DATA STORAGE

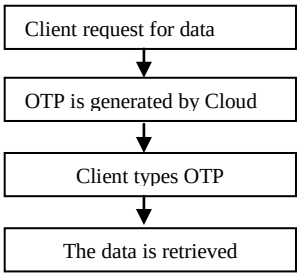
To store the data, the client first login to his mobile registration page. Once the verification is done, he can upload the data into the cloud.

IV. LIGHT WEIGHT AGENT

The client is asked to install a very light-weight software agent on the smart phone that will automatically configure the proxy settings. The light-weight agent on the smart phone performs three main tasks. It senses the input given to the device, it works in the downloading of the data and it waits for potential response and recovery commands from IDS, e.g., killing the malicious application such as blocking the account.

V. CLIENT DATA RETRIVAL

The client can retrieve his data stored in cloud through smart phone. The IDS continually monitors the smart phone through the password entered by the client in his smart phone. The data can be retrieved by clicking the particular file. Once the file is clicked, an OTP is generated and sent to smart phone. The OTP should be entered, and then the data is retrieved for the client.



4.1 Block Diagram for Data Retrieval

V. INTRUSION DECETION SYSTEM

The client gets connected to the cloud and request for the data. Then the IDS will send OTP to the smart phone which is registered with the framework. The client has to type the OTP and can download the data. In case misbehaviour is detected, the wrong OTP is typed for three consecutive times. Then intrusion response engine in the cloud environment will send the response action to the agent running on the smart phone device [7]. The agent can take the required action. It will block the account and recover the smart phone back to its normal secure operational mode.

1) Intrusion detection system monitors the smart phone.

2) Perform online and in-depth analysis to identify any intrusion activity.

3) Any misbehaviour is detected; the intrusion response engine sends the response action.

4) Response is sent to the agent running on the smart phone device.

5) Agent in turn takes required actions and recovers the smart phone.

VI. PROPOSED SYSTEM PERFORMANCE

The performance result set of IDS that are deployed and monitoring various aspects of the system. Data stored in the cloud by the client is secure and the IDS provide OTP to the smart phone. If the OTP is mismatching, the cloud environment blocks the account for the further and sends message to the light weight agent to stop the action and recover the smart phone. Two level securities are provided to secure the data from intrusion. First, the login key and the second is the OTP.

VII. CONCLUSION AND FUTURE WORK

The proposed system provides cloud-based intrusion detection and the response framework for the smart phone devices. The proposed system currently makes use of the framework on the android equipped smart phones. The proposed system provides two level securities for the smart phones. The future work is to later leveraged by generating attack-graph and IDS can decide upon response actions automatically by the graph in an emulated smart phone environment as it works in computer systems.

REFERENCES

[1] Amir Houmansadr, Saman A.Zonouz, andRobin Berthier. A cloud-based Intrusion Detection and Response System for Mobile Phones. 978-1-4577-0375-1/11 /2011 Dependable Systems and Networks Workshops (DSN-W), 2011 pages 31-32 IEEE/IFIP 41st International Conference on 2011/6/27 .

[2] Xiaoming Kou ; Qiaoyan Wen. Intrusion detection model based on Android Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on Digital Object Identifier: 10.1109/ICBNMT.2011.6156010 Publication Year: 2011.

[3] A cloud-based intrusion detection system for Android smart phones : Khune, R.S. ; Thangakumar, J. Radar, Communication and Computing (ICRCC), 2012 International Conference on 10.1109/ICRCC.2012.6450572 Publication Year: 2012.

[4] A. Boukerche and M. S. M. A. Notare. Behavior-based intrusion detection in mobile phone systems. Jour. Paral. & Dist. Comp., 62(9):1476 – 1490, 2008.

[5] J. Cheng, S. H. Wong, H. Yang, and S. Lu. Smartsiren: Intrusion detection and alert for smartphones. In MobiSys, pages 258– 271, New York, NY, USA, ACM 2007.

[6] J. Jamaluddin, N. Zotou, and P. Coulton. Mobile phone vulnerabilities: a new generation of intrusion. In Consumer Electronics, 2004 IEEE International Symposium on, pages 199 – 202, 2004.

[7] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. Virtualized in-cloud security services for mobile devices. In Proceedings of the First Workshop on Virtualizationin Mobile Computing, pages 31–35. Citeseer, 2008.

[8] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos. Paranoid Android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, pages 347–356. ACM, 2010. Fig. 1 A sample line graph using colors which contrast well both on screen and on a black-and-white hardcopy