International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Survey Paper on Location Based Device Management Policy Framework for Smart Phone Users

Chinar Bhandari[1], M. D. Ingle[2]

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

[2]Assistant Professor, (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

Abstract: ***Smart Phone Apps have numerous sources to access the sensitive data and vital resources within the user mobile phone. This vital data can be a threat for the user from the malicious apps which use your sensitive data for numerous purpose like privacy leakage or security threat. For Example: A mischievous app recording your private business data or an unwanted app capturing your personal data can lead it to a security threat. So the main cause of this situation starts from that the android phone user has no control over his own device which leads to no control over his own data. Once the mischievous app has been granted with its access privileges, the android user simply loses control over all his sensitive information. However whether the granted access should work at any specific context or region can be handled by the device user by disabling the permissions or simply by revoking them. So in this paper we present you Location based policy management framework for smart phone user which helps you to set your own user policies at a given context/region where the user demands that none of the misleading apps should access his sensitive data. We have performed several test at different regions with different user policies to check if they work accurately.***

Keywords: Location Based Access, Context Based Management, Device policy, Device administration, Framework.

1. Introduction

Nowadays Smart phones have become more powerful in terms of computational power and rich sensor data. But it also comes with a disadvantage that the mobile sensitive data is easily accessible to developers who can make use of this data to threaten the user which makes him exposed to risk and security issues. Thus many malicious app can take advantage of this and capture user's data for numerous reasons risking user's security concerns. This malicious app can capture user personal data For Example: A mischievous app recording your private business data or an unwanted app capturing your personal data can lead it to a security threat.

So the main cause of this situation starts from that the android phone user has no control over his own device which leads to no control over his own data. Once the mischievous app has been granted with its access privileges, the android user simply loses control over all his sensitive information. However whether the granted access should work at any specific context or region can be handled by the device user by disabling the permissions or simply by revoking them. To prevent such problems we introduce Location based Device Management policy for smart phone users which helps smart phone users to administrate their phones which will allow them to set specific policies which they can enable at any given region so that he can handle his phone at certain important places like his business meeting place. Context based policies mainly refers to region and time, and the user has been given every privileges to revoke the app privileges he has given permission while installing. Android phone is missing this feature where the user has the control rights over his smart phone. This policies can be best suited starting from an ordinary employee to a business person. In many private sectors employees are not allowed to carry their cell phones inside the working premises. But time may come that the employees may be needing their cell phones for work purpose. Thus enabling only certain device policy like not been allowing the user to use the camera or cell phone recorder at work place can be done which will help the employees to use their cell phone being used in working hours and making sure for private sector people that no employee is capturing their sensitive data.Device Management Policies can also be use in business meetings where you want to be sure that no app is recording your personal meeting talks so they do not leak any confidential data to outside world. Context based policies make sure that the policies are enable immediately after the user in the marked location and the device management policies are disabled once the user is outside the marked region.

We achieve the marked region using geo fencing concept provided by goggle maps. So in this framework we have provided provisions to track the user location using gps. If the user is found within 10 meter radius of the marked radius the policies which he have set for that location will be immediately enabled. After the user leaves the region the policies will be revoked immediately and the device will be working normal. Provisions are also made in framework that no end user can change some policies right during the region marked. Also no user will be allowed to Uninstall the App during the policy is enabled.With the help of location based policies user can set different policy at different location and can change it dynamically outside the geo fence range. The location based device management policy should satisfy the following conditions:

1) Framework should not allow other applications to fake the user location and try to bypass the device policies for any given location.
2) The device policy should only be enabled when the user is within the geo fence radius, and it should be disabled immediately when the user is out of the context region.
3) The location accuracy plays an important role as the policies depend on the location.
4) The end user cannot make any changes to policies once it has been enabled.
5) The end user cannot uninstall the app once the policies are enabled.
6) The applied device management policy should not hamper the mobile performance.

2. Literature Survey and Related Work

Recently now there has been a lot of solutions provided for mobile securities. Each solution focuses on restricting the third party app from accessing the mobile data. In [1] the author suggest context based device management policies for user which takes care of dynamic policy updating and context switching. The framework takes care of location accuracy with respect to time. It also handles the app permission revoke policies form the end user perspective. But the major disadvantage of this method is that it changes the android OS to apply the policy within the context.

In [2] the author proposed GRBAC, a customized framework which uses the environment data to apply the location based policies. It proved to be very useful and expressive but the major disadvantage of this method was dynamic context switching and policy updating. Also it was difficult to handle the dynamic environmental data changes.

In [3] the author propose dynamic RBAC which dynamically switched the roles and app permission revoke system to end user's. It overcome all the disadvantages of GRBAC, but again it came with a major disadvantage of to handle the dynamic environmental data changes.

In [4] the author suggested a robust authentication user portal framework which incorporated user's data to meet the dynamic environmental data changes. It proved to be a very responsive framework and came with dynamic policy handling system. But again it came with a major disadvantage of not able to handle the context changes.

To prevent such problems we introduce Location based Device Management policy for smart phone users which helps smart phone users to administrate their phones which will allow them to set specific policies which they can enable at any given region so that he can handle his phone at certain important places like his business meeting place. Context based policies mainly refers to region and time, and the user has been given every privileges to revoke the app privileges he has given permission while installing. Android phone is missing this feature where the user has the control rights over his smart phone. This policies can be best suited starting from an ordinary employee to a business person.

So in this framework we have provided provisions to track the user location using gps. If the user is found within 10 meter radius of the marked radius the policies which he have set for that location will be immediately enabled. After the user leaves the region the policies will be revoked immediately and the device will be working normal. Provisions are also made in framework that no end user can change some policies right during the region marked. Also no user will be allowed to Uninstall the App during the policy is enabled. With the help of location based policies user can set different policy at different location and can change it dynamically outside the geo fence range.

3. Proposed Work

The below diagram shows the system overview of location based device management policy: -

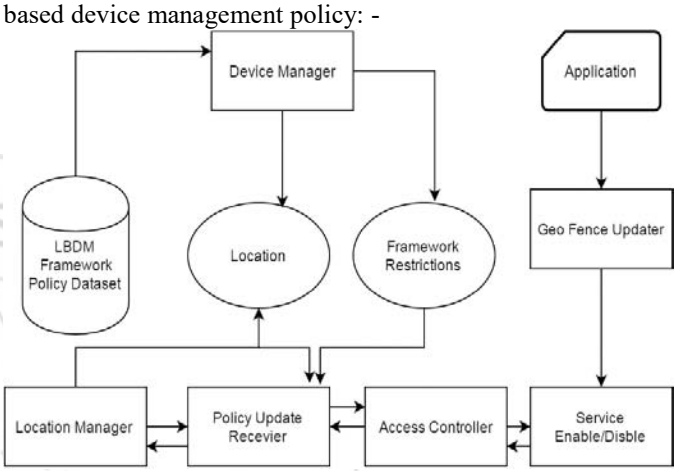

Figure 1: System Architecture for LBDMP Framework

So, the above system architecture can be explained as follows: -

1) First the end user will mark different policies at different location he wishes to.
2) As soon as the policies are set, the framework starts listening to the location provider whether the user is within the geo fence range of the region or not.
3) Once the user is found within the bounds of the location, immediately the policy executor is signaled and the policy for that particular region is located and fetched from the dataset an applied to the device.
4) The policy is enabled and the device management policies work accordingly.
5) If the user tries to change the policy, the framework will not allow to dynamic change the user policy.
6) Also the frameworks keep a watch that no user will uninstall the app.
7) After the user leaves the bound the user policies will be disabled by the policy executor and the device will work normally as before.
8) Care has been taken that the user policies does not hamper the system performance of the device.
9) The end user can anytime disable the policy if he is not found within the bounds.

The main advantage of this framework is that you do not have to modify the android OS. We can add the location based management policies without rooting the device.Also the Framework can work independently or it can be integrated in existing apps easily.

4. Conclusion

In this survey paper we have studied the various methods for context based security provisions provided by 3rd party vendors. But despite of so many solutions each framework fails because it does not consider the important aspect of context based security that is user control and dynamic switching between the policies. Thus we present you Location based policy management framework for smart phone user which helps you to set your own user policies at a given context/region where the user demands that none of the misleading apps should access his sensitive data.

References

[1] Bilal Shebaro, Oyindamola Oluwatimi,Elisa Bertino "Context-Based Access Control Systems For Mobile Devices", pages 150-164, 2015.
[2] M. Moyer and M. Abamad, "Generalized role-based access control," in Proc. 21st Int. Conf. Distrib. Comput. Syst., 2001, pp. 391–398.
[3] M. J. Covington, W. Long, S. Srinivasan, A. K. Dev, M. Ahamad, and G. D. Abowd, "Securing context-aware applications using environment roles," in Proc. 6th ACM Symp. Access Control Models Technol., 2001, pp. 10–20.
[4] R. Sandhu, K. Ranganathan, and X. Zhang, "Secure information sharing enabled by trusted computing and PEI models," in Proc. ACM Symp. Inform., Comput. Commun. Security, 2006, pp. 2–12.
[5] C. Wullems, M. Looi, and A. Clark, "Towards context-aware security: An authorization architecture for intranet environments," in Proc. Pervasive Comput. Commun. Workshops, 2004, pp. 132–137.
[6] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in Proc. 9thUSENIX Conf. Oper. Syst. Des. Implementation, 2010, pp. 1–6.
[7] R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, "Placeraider: Virtual theft in physical spaces with smartphones," in Proc. 20th Annual Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2013.

Author Profile

Mr. Chinar C. Bhandari, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. He received his B.E (Computer) Degree from AISSMS IOIT, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is mobile computing, web mining.

Assistant Prof. M.D Ingle, received his M Tech. (Computer) Degree from Dr. Babasaheb Ambedkar Technological University, Lonere, Dist. Raigad-402 103, Maharashtra, India. He received his B.E (Computer) Degree from Govt college of Engineering, Aurangabad, Maharashtra, India. He is currently working as M.E coordinator and Asst Prof (Computer) at Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is network security and mobile computing.