Privacy Control in Smartphones Using Semantics

A.R Apoorva
CSE Department
Saveetha School of Engineering
Chennai

Abstract—we are going to tell about how client data and confidentiality maintained in mobile devices through semantic analysis. Recent advance in context modeling, tracking and mutual localization has led to the materialization of a new class of smart phone applications that can access and share implanted sensor data. Mobile devices which have OS frameworks like Android mechanisms for vibrant privacy control. We tell how data flow among applications can be achieved through using semantic web driven technology. In this paper we deal with user data isolation control.

Keywords: - context awareness, mobile, android, semantic web.

I. INTRODUCTION

Smart phone devices cause huge amount of data on user choice, on device intercommunication on user context. Smart phone which are having sensors in the devices have become attracted to human sensing devices. Applications like Instagram allow us to take pictures and share with social networks. The devices which are having raised area like android, windows and so on will have seclusion control over the user data and relative data. Now a day's most of the mobile applications has moved beyond geo-location understanding and has given a new meaning to the client data. spot privacy consists of k-anonymity and l-diversity .As per the basic knowledge semantic word describes about the things of words and sentences. High logic of semantic is used to control time alone like location semantic for shielding location and also in smart phones through context modeling. Compared to the usual security, security of mobile devices makes more challenges then compared to other devices as they possess unique features. Unique features include mobility, pay-for-services and limited resources. The existing controls in context-aware systems are based on the static information and are predetermined. In most of the cases user is asked to make decision to share sensor information or not. We can't have privacy control over the context aware system because the content is dynamic it means we can change the content whenever it is needed. This is implemented by using semantic web language OWL and reasoning was done on the mobile devices using subset of the Jena software framework. In this paper we discuss only about the privacy control through semantic. A context aware systems service gives so many multi features like camera, image uploading and so on.

II. RELATED WORK

We all know about perspective aware system from long time onwards it essentially gives value more in the position and activity assumption. In research of the Norman Sadeh has discussed about the semantic web driven from the circumstance aware system. In his research most of the applications use intranet and internet services during the process. Privacy control has got highlighted in the field of the software history five years. Anony sense is a architect for a privacy aware of common limited applications that uses mobile sensing devices. Roll based access control is similar to the distinctive roll base access control database application in some features. Context privacy services describes about the plan and the implementation of the privacy control in any software devices. way of action language named as Rei is used for constant computing applications. It is used for the security framework for many other applications. It has been used to build a safety outline that addresses the issues of security for web assets, agents and services in the Semantic Web. Rein (Rei and N3) is a distributed support for describing and reasoning over policies in the Semantic Web.

III. SEMANTIC WEB AND POLICY DESCRIPTION

We agree to sketch logic , in particular OWL (WebOntology Language), and related presumption mechanisms
[Share GPS Rule: (? asker ex: ask for Time ?local Time)
(?user ex: system User ?true)
(?local Time time:dayOfWeek ?day)
ge(?day, 1) le(?day, 6)
->
(? requester ex: can Access GPS Coordinates "True")] Fig . 1 This simple policy rule permits sharing GPS coordinates on weekdays.

To develop a model of circumstance and policies. In our ontology model [27], the actions are in wide-ranging lower level tasks and have no connected role. The performance is introduced as means to elusive multiple actions and further, to correlate roles to the sets of proceedings. Places can be defined in terms of the behavior that occurs there. Environment includes concepts describing the environment of the principal (e.g., noise level, setting light, and warmth). Using this ontology, each device contains a declarative knowledge base with semantically rich information about user's information, activities, inferences, and further appropriate information. The knowledge base aligns with the context ontology which defines the key context concepts used for making access control decisions. The ontology supports simplification of context information by having hierarchical models for different aspects of context viz. activity and location. The following section describes location overview and action generality in detail. Consider another situation where requester is currently inside Building XYZ and the user does not want any purpose to know that she is present at Building XYZ.

IV. PROTOTYPE IMPLEMENTATION

The model implementations have two works one is privacy control and another one is device operating system. As we all know that prototype means a working model usually

whatever we develop either product or new apps we need some privacy that no one should use. so for this purpose we use privacy control in so many ways either through semantically or having security in normal way. Privacy control module main job is to protect the user privacy by using reasoning over the context .It deals with the privacy of the context of the user and which the user want to access when it is necessary. It have a rule that only the specified person or owner should have the privacy control over the context as it may be static or dynamic information depending upon the user information. It mainly consists of 1.set of ontologies. Ontology is a word that describes about the properties/activities related to the context.2.the knowledge about the owner whether he is maintaining his own data for a privacy or not.3.related privacy are to be chosen .4.and reasoning over the context.

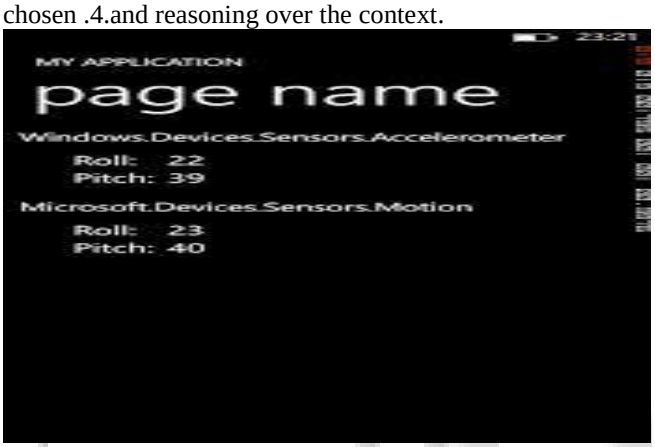

Fig. 1:

In the above diagram it shows about apps which is having the platform of the android. We can also have privacy control over the content in the apps so that no one can misuse or delete the content through having calculation .The reasoning service was provided with two different facts which represent of two different applications working on the device: one with privileges to right to use present location and the other one without the privileges. The word privilege describes about a special activity or advantage of the related thing. We can see one thing that present location doesn't have link when subsequent randomized are part of the information. For example if the device location is shown as Hong Kong and Chicago in two different readings taken few minutes apart then the recipient will clearly figure out that device location is masked. Two figures listed below shows the results rendered on the mobile screen. The policy used by the reasoner in this case is a fairly simple one which uses only the requester identity for resource sharing decision making. The reasoned maps user identity to a predefined group and infers from the group´s allocated privileges. But the current implementation can be amplified to handle other more composite policies such as "share a false location to the requester if the device is in Building ABC".

V. CONCLUSION

Whatever we discuss in the paper it doesn't reduces the android security. Our completion only says how to protect the data through semantic reasoning and data modeling. However, every way in is not controlled by the user so android check authorization is not partial by the present work or implementation. As productivity our implementation decreases the no. of access allowed but not the safety in the devices. We tell again that our implementation is basically an extension of Android and it runs with the privileges of the Android Middleware. The rival cannot authority the context activation since the principles considered for all context collection operation (e.g. current time) are taken directly from the underlying Android system. In order to avoid the opponent modifying the operating system of the phone (drivers and the prototype included) Trusted Computing mechanisms leveraging Trusted Platform Module can be used. However, the talk of these mechanisms is outside the scope of this paper. Thus in this paper we show how by embedding semantically rich policies based on device context in the smart phone' construction, user privacy can be protected at runtime as opposed to the current generation of smart phones where application's runtime privileges are decided on the basis of install time user input. We intend to test and improve the prototype to handle complex policies similar to the one we touched upon in the prototype architecture discussion and we plan to make other underlying services on smart phone context aware to facilitate finer degree of privacy preservation.

ACKNOWLEDGMENT

This research was incompletely support by the National Science Foundation (award 0910838) and the Air Force Office of Scientific Research (grant FA550-08-0265).

REFERENCES

[1] E. M. Airoldi, D. M. Blei, S. E. Fienberg, and E. P. Xing, "Mixed membership stochastic blockmodels," J. Mach. Learn.Res., vol. 9, pp.1981–2014, Jun. 2008.
[2] D. Ashbrook and T. Starner, "Using GPS to learn significant locations and predict movement across multiple users," Personal Ubiquitous Computing, vol. 7, no. 5, pp. 275–286, Oct. 2003.
[3] "Jawbone with MotionX technology,http://content.jawbone.com/static/www/pdf/press-releases/up-press-release-110311.pdf.
[4] C. R. Mulliner, "Security of smart phones - masters thesis," Master's thesis, Department of Computer Science, University of California, Santa Barbara, 2006.
[5] Google, "Android reference. developers guide." http://developer.android.com/guide/index.html.
[6] Google.com, "Android security reference," http://source.android.com/tech/security.
[7] B. Jesse, "Android security reference," http://www.blackhaAndroidSurgery-PAPER.pdf.
[8] G. R. Hayes, S. N. Patel, K. N. Truong, G. Iachello, J. A. Kientz, R. Farmer, and G. D. Abowd, "The personal audio loop: Designing a ubiquitous audio-based memory aid," in Proc. Sixth International Symposium on Mobile Human-Computer Interaction. Springer Verlag, 2004, pp. 168–179.
[9] G. Iachello, K. N. Truong, G. D. Abowd, G. R. Hayes, and M. Stevens,"Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world," in Proc. SIGCHI conference on Human Factors in computing systems. New York, NY, USA: ACM, 2006,pp. 1009–1018.
[10] H. Chen, F. Perich, T. Finin, and A. Joshi, "SOUPA: Standard Ontology for Ubiquitous and Pervasive

Applications," in First International Conference on Mobile and Ubiquitous Systems: Networking and Services, Boston, MA, August 2004.
[11] P. Jagtap, A. Joshi, T. Finin, and L. Zavala, "Preserving privacy in context-aware systems," in Proc. 2011 IEEE Fifth International Conference on Semantic Computing. Washington, DC, USA: IEEE Computer Society, 2011, pp. 149–153.
[12] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, "Mockdroid: trading privacy for application functionality on smartphones," in Proc. 12th Workshop on Mobile Computing Systems and Applications. New York, NY, USA: ACM, 2011, pp. 49–54.
[13] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel, "Semantically rich application-centric security in android," in 2009 Annual Computer Security Applications Conference. IEEE, 2009.
[14] N. M. Sadeh, "A semantic web environment for context aware mobile services," in Proc. Wireless World Research Forum, 2001.
[15] N. M. Sadeh, T.-C. Chan, L. Van, O. Kwon, and K. Takizawa, "A semantic web environment for context-aware m-commerce," in Proc. Fourth ACM Conference on Electronic commerce. New York, NY, USA: ACM, 2003, pp. 268–269.
[16] F. Gandon, "Semantic web technologies to reconcile privacy and context awareness," Web Semantics Science Services and Agents on the World Wide Web, vol. 1, pp. 241–260, 2004.
[17] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, "AnonySense: A system for anonymous opportunistic sensing," Journal of Pervasive and Mobile Computing, vol. 7, no. 1, pp. 16–30, February 2011.
[18] A. D. Kidd, R. Orr, G. D. Abowd, C. G. Atkeson, I. A. Essa, B. Mac- Intyre, E. Mynatt, T. E. Starner, and W. Newstetter, The Aware Home: A Living Laboratory for Ubiquitous Computing Research. Springer, 1999, pp. 191–198.
[19] V. Sacramento, M. Endler, and F. Nascimento, "A privacy service forcontext-aware mobile computing," in First International Conference on Security and Privacy for Emerging Areas in Communications Networks. New York, NY, USA: ACM, 2005, pp. 182–193.
[20] L. Kagal, T. Finin, and A. Joshi, "A policy language for a pervasive computing environment," in Proc. 4th IEEE International Workshop on Policies for Distributed Systems and Networks. Washington, DC,USA: IEEE Computer Society, 2003, pp. 63–.
[21] "A Policy Based Approach to Security for the Semantic Web," in Second International Semantic Web Conference, September 2003.
[22] L. Kagal and T. Berners-Lee, "Rein : Where policies meet rules in the semantic web," Massachusetts Institute of Technology, Tech. Rep., 2005.
[23] T. Berners-Lee and D. Connolly, "Notation3 (N3): A readable RDF syntax," W3C, Tech. Rep., 2008.
[24] A. Khalil and K. Connelly, "Context-aware telephony: privacy preferences and sharing patterns," in Proc. 2006 20th anniversary conference on Computer supported cooperative work. New York, NY, USA: ACM,2006, pp. 469–478.
[25] 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. 9th USENIX conference on Operating systems design and implementation. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–6.
[26] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: Context-relatedpolicy enforcement for android," in ISC, ser. Lecture Notes in Computer Science, M. Burmester, G. Tsudik, S. S. Magliveras, and I. Ilic, Eds., vol. 6531. Springer, 2010, pp. 331–345.
[27] L. Zavala, R. Dharurkar, P. Jagtap, T. Finin, and A. Joshi, "Mobile,Collaborative, Context-Aware Systems," in Proc. AAAI Workshop on Activity Context Representation: Techniques and Languages, AAAI.AAAI Press, August 2011.
[28] A. D. Team, "Androjena - Jena Android port," http://code.google.com/p/androjena/.
[29] Apache.org, "Java framework for building semantic web applications,"http://incubator.apache.org/jena/.
[30] cyanogenmod.com, "Nexus one: Full update guide," http://wiki.cyanogenmod.com/wiki/Nexus One: Full Update Guide.
[31] android.com, "Android 2.3 platform," http://developer.android.com/sdk/android-2.3.html.

