Energy efficient semantic context model for managing privacy on smartphones

Prajit Kumar Das
University of Maryland
Baltimore County
prajit1@umbc.edu

Dibyajyoti Ghosh
University of Maryland
Baltimore County
dg9@umbc.edu

Anupam Joshi
University of Maryland
Baltimore County
joshi@cs.umbc.edu

Tim Finin
University of Maryland
Baltimore County
finin@cs.umbc.edu

Introduction: Modern smartphones are capable of gathering massive amounts of data about a user and her context. While this data is mostly utilized for providing services that are better suited to the user, user data and context leakage from smart phones can have disastrous results. This is especially true as most enterprises are going to a Bring-Your-Own-Device (BYOD) model for mobile devices such as smartphones. We recognize this change as a potential threat to data privacy, both of the user and also of corporations whose data is on employee owned phones.

Context modeling: Recent advances in context modeling, tracking and collaborative localization has led to the emergence of a new class of smartphone applications that can access and share embedded sensor and context data. Unfortunately, the existing security mechanisms in Android and other mobile OSs are simply not geared to protect such dynamic data. In ongoing work, we have shown application and user context-dependent information sharing policies, which can control data flow among applications dynamically and at a very fine-grained level. Our approach is different from existing literature [2, 4, 5] on context based privacy and security – we create semantically rich policies, and reason over them and the user and application context to either release or obfuscate the sensor/context data being shared with the application [1, 3, 7]. Our context model is realized as a dynamic knowledge base of RDF triples grounded in ontology in the semantic web language OWL. Policies in the form of rules over this knowledge base monitor and control application access to sensitive information and sensor data. The policies filter data flowing from sensor resources to applications to reduce disclosure by generalizing or obfuscating data. Our ontology includes the ability to represent application provenance and other metadata that can be used by the policies. The resulting system provides fine-grained, context-dependent control to sensitive user data [1]. For instance, we can have a policy that says that a location based information service should only get block level data, and not get data at all when the user is attending a confidential meeting.

Energy issues and a possible solution: Unfortunately, the process of gathering context and applying policies has a significant impact on energy consumption, since the system needs to keep the user's context updated at all times. Current work in the literature on the energy consumption study focuses on exact battery utilization of specific applications and also refers to tail energy issues [6], but has not dealt with creating an energy efficient context inference system that can be used for security. Our proposed approach addresses it using the following three methods. First, keep only the sensors required at a particular instant of time, to satisfy the antecedents of policy rules. If multiple policies are to be executed at a given instant of time, and they all require the same sensor data like location information, just detect the location once for all the policies. Second, if certain information can be gathered from multiple sensors, use the sensor with the lowest energy footprint, or one that is being used already (e.g. a wireless location instead of GPS). Third, evaluate the predicates of the rules in increasing order of energy usage. We've created the policy based security mechanism in the Android framework [1, 3], the implementation of energy optimization is ongoing. We're gathering data on energy usage of various sensors. The experiment was done by toggling on/off various sensors of the device and letting the battery drain. Time required to drain the battery is noted for specific sensors. These timings are then compared with the baseline ("airplane" mode). The time difference for the battery drain of each sensor is used as the parameter for deciding which sensor to use in the third method.

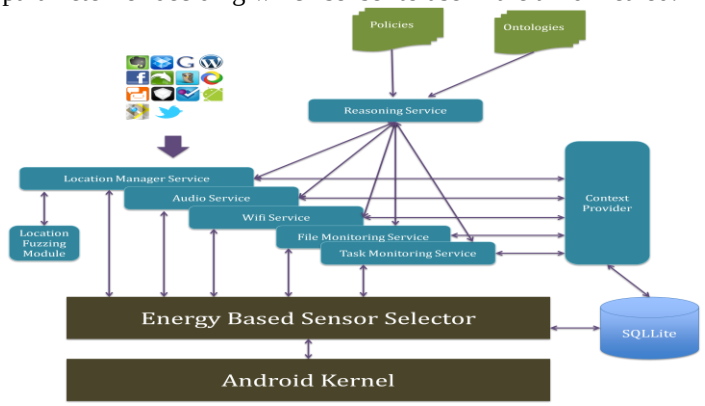

Fig-1: Architecture for the modified Android framework

Conclusion and Future work: As explained before, the security mechanism that has been developed in our recent work [1, 3, 7] which is extremely fine grained and suitable for smart phones. Nevertheless, it creates the overhead of high energy consumption, which is a cause for concern for the phone's battery life. In our on-going work we are building up into the Android framework an energy efficient security mechanism (Fig-1). As a future work we plan to experimentally evaluate the proposed, energy efficient security mechanism.

References

[1] Ghosh, D., "Context based privacy and security in smartphones." Master's thesis, UMBC, 2012.

[2] Sadeh, N. M., "A semantic web environment for context-aware mobile services," in Proc. Wireless World Research Forum, 2001.

[3] Ghosh, D. et al. "Privacy control in smartphones using semantically rich reasoning and context modeling." Security and Privacy Workshops (SPW), 2012 IEEE Symposium.

[4] Enck, W., Gilbert, P., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P. and Sheth, A. N. "Taintdroid: an information-flow tracking system for real-time privacy monitoring on smartphones," in Proc. 9th USENIX conference on Operating systems design and implementation. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–6.

[5] Conti, M., Nguyen, V. T. N. and Crispo, B., "Crepe: Context-related policy 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.

[6] Pathak, A., Hu, Y. C., Zhang, M., Bahl, P., and Wang, Y.-M., "Fine-grained power modeling for smartphones using system call tracing." in Proc. of EuroSys, 2011.

[7] Kodeswaran, P., Nandakumar, V., Kapoor, S., Kamaraju, P., Joshi, A., Mukherjea, S. "Securing Enterprise Data on Smartphones using Run Time Information Flow Control" in Proc. MDM 2012