*Publishing privacy logs to facilitate transparency and accountability*

Honya Elfayoumy

*INTERNET PROGRAMMING CIS4813*

*Littleton | November 11, 2018*

As the number of companies grows every day, it is vital that privacy policy requirements are being met. As technology advances, it becomes more difficult to protect individuals’ privacy. In order to ensure compliance, it is vital that there are maintainable audit privacy logs and reports. However, since these logs and reports are built on an application by application basis, it may not be the safest option. This paper deals with creating a Linked Data model and ontologies to ensure that the sharing of logs supports the privacy accountability for the applications and the participants. L2TAP is an ontology module that helps accommodate different privacy scenarios and policies. SCIP is a key module which facilitates privacy auditing. This model is a solution for obligation derivation and compliance checking logs that deal with privacy auditing processes to analyze L2TAP logs.

The L2TAP ontology model creates specifications that are able to capture the relevant privacy events and produce solutions for the participants in the workflow. This ontology is intended for individuals, data collectors, and privacy auditors who would like to express their privacy preferences. This model contains four L2TAP modules: L2TAP-Core, L2TAP-Initialize, L2TAP-Participant, and L2TAP-SCIP.

The L2TAP-Core is the module that provides the “core” infrastructure for logging the privacy events. URIs are used to identify the statements in the body of a log which in return will create a “named graph.” These “named graphs” are given an abstract syntax, a formal semantics, an XML syntax, and a syntax based on N3 [1]. By using these graphs, the model verifies that the assertions are applicable to all privacy logs. The second module, L2TAP-Initialize, supports the assertions about the log itself. This module essentially “initializes” by identifying the logger, the time expressed in the log, and when the log was initialized. After initializing, it points the logger to the L2TAP-Participant module. The L2TAP-Participant is very important since it supports the assertions about the participants. Since the logger publishes the log events and owns the domain, only participants who are known to the logger are able to contribute log events into the log. Also, this module identifies the log participant’s hierarchical structure, the authentication method, and more domain-dependent related characteristics. Lastly, the L2TAP-SCIP module allows for assertions about the privacy semantics of the event being expressed. Essentially this module identifies who accessed the information, when the information was accessed, who performed an obligation, and when the obligation was performed, etc.

In order to apply this L2TAP ontology, the first step is log initialization which defines the instance of an L2TAP log to capture the characteristics. The second event is registering the participant. Eventually all of the privacy events are captured and attempt to access the personal information. Next, the SCIP ontology is used to encode the setting of privacy preferences and obligations. SCIP provides properties that allow the requestor to assert the requested data item and determine the purpose of access, requested privacy privilege, and the requestor’s role. For each of these access request, there should be an access response that determines the access decision and the obligations; these accesses are then recorded in the access activity data. The next step is PROV-O which allows for mapping of the PROV data model to Resource Description Framework (RDF). This deals with real-time processes since it determines whether a subject has accessed a resource in the given circumstances. The last step is essentially logging XACML (access control policy language) policies and events.

In conclusion, this privacy model uses Linked Data to facilitate transparency among all participants. The L2TAP ontology discussed has the potential to change industry-standard privacy audit logs. Since compliance checking and deriving obligations are challenges in privacy today, the conflict could be resolved using this ontology!

References

[1] J.J. Carroll, C. Bizer, P. Hayes, P. Stickler, Named graphs, Web Semant.: Sci. Serv. Agents World Wide Web 3 (4) (2005) 247–267. http://dx.doi.org/10. 1016/j.websem.2005.09.001

[2] R. Samavi and M.P. Consens. 2018. Publishing privacy logs to facilitate transparency and accountability. Retrieved November 9, 2018 from <https://www.sciencedirect.com/science/article/pii/S1570826818300088?via%3Dihub>