More than six decades after Vannevar Bush put forward Memex [3], his vision of a personal information management (PIM) framework, most computer users are still constrained by a rigid hierarchical file organization, where the semantic relationships among data are not emphasized. The semantic desktop leverages the potential of the semantic web to address the challenges of complex PI spaces, which are composed of syntactically and semantically heterogeneous data [11]. In the semantic desktop, ontologies assign meaning to data. In this position paper, we list security issues that arise when the semantic desktop is made available in mobile devices, which may communicate with one another using the peer-to-peer (P2P) paradigm [12, 19]. The need to consider PIM in mobile devices using a semantic web approach has also been recently recognized by others [16]. In addition, we consider collaborative environments, which enable users to share information and to execute common tasks in a variety of applications (e.g., healthcare, emergency response). The idea of context-aware computing, including location-aware computing, also assumes particular relevance, as access to data resources (e.g., web services) or to physical resources (e.g., hospitals) may depend on the geographical location of the users and availability of those resources. We group the security issues as follows:

**Data Integration.** In a P2P network of semantic desktops, instead of access control issues for individual sources [2] one must look at access control for mediated sources [4]. An approach that considers the semantics of data is particularly relevant in our context [14]. Furthermore, security levels may be associated with the ontologies of the different collaborating institutions and integrated in such a way that the confidentiality of the data is not compromised [8]. To achieve data integration, automatic ontology matching is needed [9]. However, when performing ontology matching, specific methods for ontology matching need to be devised when the different parties want to keep their metadata private [10, 17].

**Context-aware Computing.** In mobile environments, the identity of the users may not be known in advance [5, 18]. Therefore, context aware access control systems should have the ability to grant a role to a first time user without permanently registering that user’s data, that is, users’ actions should be dynamically determined based on their own attribute values and on the values of the attributes associated with the resources [1]. A special but important case is the concept of being location-aware [13]. In this case, authorization decisions must be dynamically determined taking into account both organization-based user’s roles and real-time context-based attribute values that can vary over time depending on the user’s location [7].

**Collaborative Environments.** Complex situations arise especially for collaborative environments, where there is a complex interplay among static and dynamic attribute values of users and resources [6, 20]. The collaboration semantics as well as the particular access control models that will enact that semantics need to be determined.

**Semantic Web Languages.** In the above scenarios, it is necessary to model complex situations and to perform reasoning so as to determine at any instant the type of access of each user to each
resource. Several considerations are at play including the expressiveness of the modeling languages and of the reasoning mechanisms, as well as their efficiency, so that such a framework can be used in real time. The expressiveness of semantic web languages has been studied to determine their adequacy to those scenarios [6, 15]. Furthermore, system prototypes provide unique insight into this research [6, 7].

References


