Towards a Secure and Trusted Business Web

Volkmar Lotz

SAP Labs France, Security & Trust Research Practice
805, Avenue du Dr Maurice Donat
06250 Mougins, France
volkmar.lotz@sap.com

Abstract: We currently see a major shift in development, deployment and operation of Enterprise IT systems and business applications. Driven by cost and effectiveness considerations, and facilitated by virtual infrastructures (aka the cloud) and service orientation, application development is distributed over a variety of entities (ISPs - independent service providers), applications are composed of services from different ISPs, and IT operations is run by independent data and computation centers. Using the Internet as fast and ubiquitous communication infrastructure, we see a fabric of resources, platforms, services and applications emerging forming a number of ecosystems that will drive society and business. For this set of ecosystems and facilitating technology and infrastructure, we have coined the term ”Business Web”. Since the Business Web is going to be the critical infrastructure underlying business and private life, concerns related to security and privacy will inevitably be raised. These concerns are grounded in the open and dynamic nature of the Business Web and its coverage of all aspects of business including the most sensitive areas like finance, healthcare, personal information etc. The strength of the Business Web lies in information sharing and spontaneous interaction with entities, even if they are previously unknown, and there is an inherent risk of information being abused and data owners losing control over their data in terms of usage, consistency or availability. To mitigate these risk while being able to exploit the benefits of collaboration, one needs to determine with whom the collaboration takes place, to express which mutual protection needs are to be met, and which controls can be imposed to actually enforce them. In this talk, we focus on the establishment of trust in services and the complementary support of data-centric services.

In addition to traditional means based on observation, recommendation, and reputation which come to their limits upon discovery of new services, rich service descriptions including security and privacy related attributes, attested by trusted parties, provide the needed information and form a service identity where the mere name of the service would not be meaningful. At the same time, such descriptions can serve as a container for policy information expressing the service's protection needs, its abilities to match consumers' policies and its governance. Given that the user can express her policies in a similar, machine-processable way, we are able to match policies and decide if the service can be safely used.

When considering the complexity of Business Web structures, however, we have to ensure that the above approach scales to multiple layers of dynamic collaboration. Data are travelling across domains, services and resources, while still being subject to their owners' policies. This motivates a data-centric security concept, where policies are bound to data and travel with them - ßticky policies”. Each processor of the data, even if it cannot be predicted where they will eventually end up, has access to the policy information and can handle the data accordingly. Sticky policies allow for the

expression of obligations (like a deletion or retention period) to be met by processing entities. While this concept is theoretically pleasing, it faces practical challenges of performance and enforcement asking for further research. We show how a solution meeting some of these challenges can be provided on top of a distributed Java platform.