Title: Outsourcing security in service ecosystems with evolving security deployment as a service
Authors: W.F. Ouedraogo and F. Biennier (LIRIS, INSA de Lyon)

Abstract
Enterprises are more and more involved in collaborative business. This leads to open and outsourcing all or part of their information system (IS) to create collaborative processes by composing business services picked in each partner IS and to take advantage of Cloud computing. Business services outsourcing and their dynamic collaboration context can bring lost of control on IS and new security risks can occur. This leads to inconsistent protection allowing competitors to access to unauthorized information. To address this issue, an adaptive security services model deployment is required to provide a business service consistent protection by taking into account the collaboration context (business service data criticity, partners involved in the collaboration, etc.), and the cloud deployment and execution environment. In this paper, we propose an adaptive security model based on MDS@run.time, the marriage of Model Driven Security (MDS) and Models@run.time approaches, allowing to select at runtime the appropriate security components to apply. The MDS approach is used to generate security policies which are interpreted at runtime and load appropriate security mechanisms depending on the context (which takes advantage of the Models@run.time approach) ensuring business process end to end protection. A proof of concept prototype is built on top of the OW2 FraSCAti middleware, validating our proposition efficiency.

Download the presentation