A. Heil, M. Gaedke, J. Meinecke; Identifying Security Aspects In Web-based Federations IEEE International Conference on Web Services (ICWS 2008), S. 807-808, Beijing, China, 23.-25. September 2008, ISBN 978-0-7695-3313-1

Identifying Security Aspects in Web-based Federations

Andreas Heil[†,*] Martin Gaedke[*] Johannes Meinecke[*]

[†]*Microsoft Research*
Cambridge, UK
v-aheil@microsoft.com

[*]*Chemnitz University of Technology*
Chemnitz, Germany
{firstname.lastname}@cs.tu-chemnitz.de

Abstract

Today's web applications and their respective business processes reside under the control of different organizations. Establishing federations between these organizations, i.e. bringing these business processes together by transcending organizational and security borders, raises a new class of security questions concerning the management of trust relationships between the autonomous bodies that wish to work together. Based on the WebComposition Architecture Model we provide a modeling approach for federated Web applications. In this paper we present a methodology for formalizing these models using the Ambient Calculus for use in further computation. Based on the results we help the users to identify and detect security related aspects in Web-based federations.

1. Introduction

The need to interconnect businesses has affected the Web significantly. The Web has moved consistently from a static source of documents to a dynamic platform for distributed applications. The communication infrastructure of the Web links together applications, e.g. by exposing functionality through Web services. This has led to new classes of applications including 4th generation portals and federated portals. The interconnection of portal backbones within such federations is comprised of accessing functionality as well as sharing resources, data and user accounts. Unlike the centralized approach used by VPN's, federated solutions apply a protocol-based security approach by sharing trust between organizations. Access is granted on a fine-grained level based on individual trust relationships. External users of the federation partners can be granted access to local resources while preserving the autonomy of the federation structure. Standardization efforts such as WS-Federation, SAML and the Liberty Alliance Project establish systems, interoperable especially in terms of security, which provide the basis for federated access and identity management. The proper operation of such systems must be guaranteed even if the systems evolve. Changes in the systems must be reflected in the models and vice versa. The WebComposition Architecture Model (WAM) is a modeling approach for modeling aspects of federated Web applications [1]. To evaluate the operational mode of the system before changes become effective, we use models of federated Web application based on WAM and show how information about federated systems can be formalized and processed in an automated manner.

2. Models for Federated Systems

The approach we propose in this paper is based on the architecture of federated Web-based systems, their involved components such as Web services and the interactions between those services. Therefore, we briefly outline our previous work, the WebComposition Architecture Model (WAM) that allows us to describe the architecture of such systems in a practical way. This includes the involved Web services, applications, their corresponding affiliations (i.e. which organizational restrictions come into effect) and the way they interact. This includes the federated identity management aspect necessary to apply security rules and grant users access to dedicated recourse in partner organizations. The WAM provides a graphical notation, convenient for human users who can quickly sketch WAM diagrams using pen and paper. To support the development and deployment process, sample tool support is provided through a Microsoft Visio add-on and a XML-based notation [2]. Tool support is not limited to a single tool or platform. Models may be stored in and exchanged between multiple different tools. Furthermore, this machine-readable notation can be exported and could be used to monitor or to configure the system of interest.

3. Identifying Security Aspects

The problem that authors and administrators now face is to ensure that changes in the current model do not violate already established processes and policies. The removal of a single trust relationship will immediately affect invocations from the previously trusted partners. Likewise, adding new trust relationships allows establishing interactions between partners, not considered before. For that reason, we provide a methodology to ensure the validity of existing policies. We formalize the model to validate its correctness and to evaluate changes within the model. We identified the Ambient Calculus [3]

A. Heil, M. Gaedke, J. Meinecke; Identifying Security Aspects In Web-based Federations IEEE International Conference on Web Services (ICWS 2008), S. 807-808, Beijing, China, 23.-25. September 2008, ISBN 978-0-7695-3313-1

to be a suitable foundation for formalizing federated Web-based models for further computation.

3.1. Formalized Representation

The most distinctive feature of the WAM approach is that it considers the security aspects of federated systems. It allows designing the system as a whole, considering the most vital aspects of a federated Web-based system. These particular aspects are captured in the formal model using the Ambient Calculus. As the concept of the calculus is based on the idea of the World Wide Web, it lines up well with the idea of services, resources and organizational constructs as provided in WAM. The Ambient Calculus is a process calculus where processes (e.g. programs, processes, threads) reside within a hierarchy of locations. These locations are called ambients whereas an ambient is defined as a bounded place where computation happens. Based on their definition ambients can be used to represent e.g. a XML file, a Web Service or a database. Also virtual constructs such as administrative domains can be identified as ambients. In Figure 1 we identify the various communication mechanisms provided by the calculus, used to encode the interactions between WAM components.

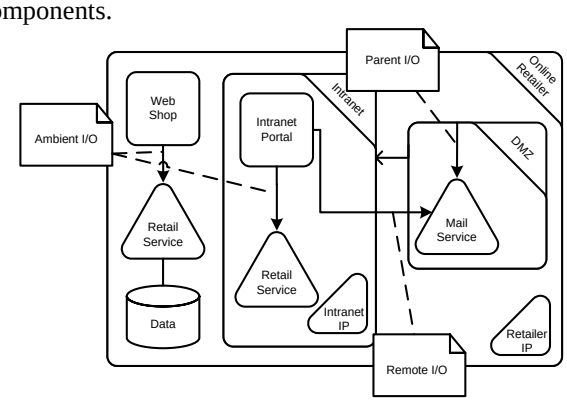

Figure 1. Communication types within a WAM model

The communication mechanisms are used to encode direct inter-process communication between entities within a single security realm but also inter-realm communication where messages traverse the enclosing realm boundaries. These same mechanisms are used to encode invocations among directly nested security realms or realms located within the same enclosing one. Long-range communication allows us to model messages crossing multiple organizational and security boundaries.

3.2. Federation-based Interaction Catalogue

The proposed formalism potentially allows automated reasoning about the future state of a federated system based on its actual state and proposed model changes. We developed a catalogue of encodings for federation-based interactions and their corresponding representation within WAM (cf. Figure 2).

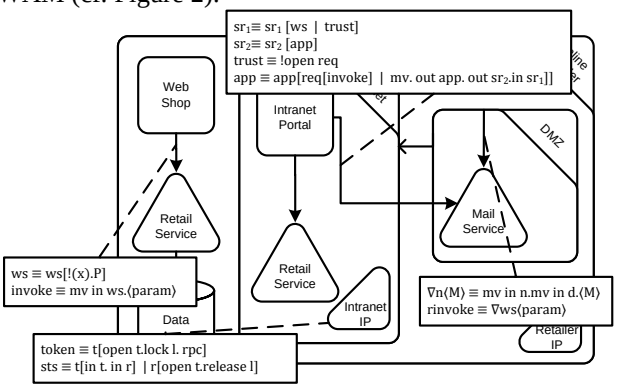

Figure 2. Formal encoding of WAM elements

Intra-realm interactions occur between entities that are located within the same security realm where both parties rely on the same identity provider. A further invocation type is based on an implicit trust relationship, where a user or a resource of the surrounding security realm can access local resources. Based on the calculus primitives, model reductions are applied on the model and we can immediately see the potential effects on the system. Computations on the model can be carried out easily for typical scenarios, including removing, adding, relocating or substituting services and resources. Issues on a federation level, such as missing trust relationships or newly joined or departed federation partners, can be thus identified.

4. Conclusion

The relatively novel concept of federations and the security issues they present are only slowly being recognized. By providing the automated transformation as well as the corresponding tools to model federated Web-based systems and to compute potential effects on the system, we look forward to providing an easy-to-use solution for the user to identify security issues within federated systems and thus to enhance users' understanding of federation concepts in the future.

5. References

[1] J. Meinecke and M. Gaedke, "Modeling Federations of Web Applications with WAM", in *Third Latin American Web Congress (LA-WEB 2005)*, Buenos Aires, Argentina, 2005, pp. 23-31.

[2] J. Meinecke, M. Gaedke, F. Majer, and A. Brändle, "Modeling and Managing Federated Web-based Systems", in *3rd International Conference on Web Information Systems and Technologies (WEBST)*, Barcelona, Spain, 2007, pp. 15-22.

[3] L. Cardelli and A. D. Gordon, "Mobile Ambients", in *First International Conference on Foundations of Software Science and Computation Structures (FoSSaCS '98) at ETAPS'98*, Lissabon, Portugal, 1998, pp. 140-155.