A Secure Infrastructure for Dynamic Collaborative Working Environments

Matthias Assel
High Performance Computing Center
University Stuttgart
Stuttgart, Germany

Alexander Kipp
High Performance Computing Center
University Stuttgart
Stuttgart, Germany

Abstract *With more distributed and at the same time more complex interdisciplinary business workflows, security issues are of the utmost priority and importance while developing collaborative working environments for business partners and / or academic institutions. Several levels of security implying trustworthiness among participants have to be considered in order to meet appropriate (business) goals without violating legal issues as well as keeping the privacy of single users.*

The following paper shall give a brief overview of security requirements to be considered within the EU Research Project CoSpaces[1]. Technological concepts, focusing on user authentication, user authorization, and secure data exchange, shall be explained in more detail, and how these are exploited in a concrete usage scenario.

Keywords: Dynamic Collaborative Working Environments, Business Collaborations, Security Infrastructure, Authentication and Authorization Infrastructure, Data Exchange Security

1 Introduction

Current B2B[2] collaborations take place in a very limited and even reserved way. Most cross-organizational data transfer is carried out via a simple e-mail exchange between corresponding business partners. These messages typically contain confidential information that is usually neither encrypted nor digitally signed. Instead of directly accessing data at the appropriate location or sharing data across different partners within a secure environment, for example a Virtual Organization (VO) [1], many companies are afraid of having their data abused not only by a third party, but in the same way even by the trusted organization(s).

CoSpaces [2], an Integration Project (IP) under the 6th Framework Programme of the European Commission, aims to develop a reference architecture and implementation framework to support the setup and execution of dynamic sessions for designers and engineers in the aerospace, automotive, and construction sectors. The project's main challenge is to meet the requirements of workers within these fields, supporting the dynamic nature of collaborative work, whilst considering associated issues of trust and security. The system shall provide information support to users, supporting knowledge of availability of users and applications, and must also consider current user contexts. Specifically, the framework will support users in the on-demand selection of participants, documents, and data required in a collaborative session. Participants will be easily integrated into collaborative sessions with regards to their access to and from both their co-collaborators and applications, requiring partner machines that can be automatically configured for ad-hoc collaborations.

Similar approaches with a focus on dynamic composition of services regarding business aspects have been considered in other projects, like Akogrimo[3] [3] and TrustCoM[4] [4]. The currently running IP BREIN[5] extends this eBusiness approach by merging semantics, agents, and Grid technologies to provide an intelligent, self-manageable infrastructure [5]. However, these approaches do not consider the needs of collaborative user sessions.

To face real user's needs and requirements, concrete user scenarios (compare to figure 1) have been developed in co-operation with industrial partners,

[1] Innovative Collaborative Work Environments for Design and Engineering

[2] Business-To-Business

[3] Access to Knowledge through the Grid in a mobile World

[4] A framework for trust, security and contract management within dynamic virtual organizations

[5] Business objective driven Reliable and Intelligent grids for real busiNess

and these will be evaluated against the defined concepts. Sharing data and documents between partners stresses security issues to be of the utmost significance while developing collaborative working environments for business partners. These include several levels of security implying trustworthiness among participants to meet appropriate collaboration goals without encountering legal issues as well as maintaining the user's privacy.

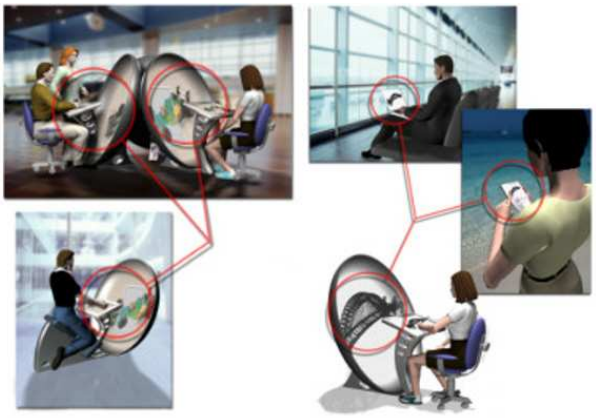

Figure 1: Innovative collaboration environment within CoSpaces

In the following, we will present general security issues to be regarded while developing environments for dynamic business collaborations, corresponding technologies that meet those requirements, as well as an example demonstrating such a secure infrastructure to be realized within the CoSpaces project.

2 Security Requirements

Focusing on distributed collaboration environments between organizations across different countries, the specific and even dynamic requirements for services and applications regarding security issues differ from normal local collaboration federations.
In order to determine appropriate technologies for different usage scenarios, we have analyzed and roughly summarized important prerequisites.

- The easy usage of the collaboration platform should be provided through a decentralized authentication and authorization model based on a Single-Sign On (SSO) procedure across and within organizational boundaries

- The dynamic setup of collaboration partners including also the dynamic setup of firewalls in order to guarantee that only trusted partners are allowed to execute corresponding operations

- Hierarchical user roles and unified user attributes to perform role-based access control

- Dynamic management and control of attribute-based access policies necessary to authorize users before accessing services, applications, and resources

- The data being shared between partners is only available for those being foreseen for the collaboration

- The control about who is allowed to access data, services, and applications remains at the corresponding resource or service provider site

- Recording of user interactions (what you did or tried to do) for auditing, accounting, and prizing

- Secure data transmission based on data encryption on different levels (e.g. encrypted messages as well as secure protocols) guaranteeing trustworthiness and integrity of exchanged information

- Additional security for data storage due to high sensitivity of exchanged information

- Keeping the user's privacy and protecting his confidentiality by anonymizing personal data and / or excluding irrelevant information before messages are transferred

- Satisfying requirements under the Data Protection Act as well as explicit consent from all parties concerned

3 Technological Concepts

Several technologies and solutions that meet presented requirements have been considered. Shibboleth[6] [6] could be used for authentication and authorization of users concentrating on the decentralized approach. Security of communication between machines could be ensured by using for instance the Grid Security Infrastructure (GSI) [7]. While dealing with simple Web Services or even invoking applications directly, other standards such as WS-Security [8] or SSL[7] should be utilized. As provided

[6] http://shibboleth.internet2.edu

[7] Secure Sockets Layer

solutions are complex and contain many separate components, different setup patterns can be used in various ways. The approach taken to provide authentication, authorization, and data encryption within the CoSpaces project will be described in detail in the following sections.

3.1 Authentication and Authorization using Shibboleth

Since the CoSpaces project involves intensive collaboration between several institutions across different countries around Europe, a scalable, decentralized, and flexible authentication and authorization system is essential. In our approach, the service / application providers make authorization decisions basing on the attributes assigned to the user by his / her organization. This protects the resources without harming the flexibility and maintainability of the working environment. The architecture of Shibboleth perfectly meets the above-mentioned requirements.

The basic Shibboleth components need to be connected to different elements of the CoSpaces infrastructure, generally named as the Home Organization (HO) and the Application Controller (AC). In figure 2, these components are shown together with corresponding CoSpaces elements.

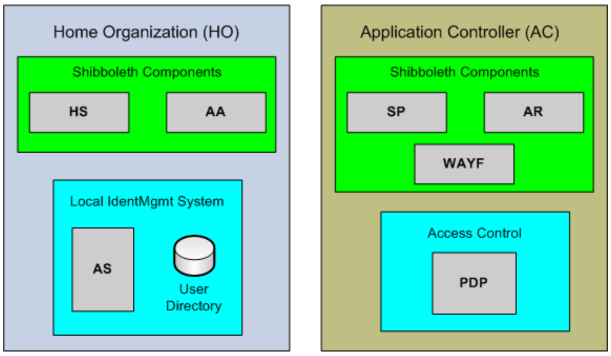

Figure 2: Location of Shibboleth modules together with other components

There are two security-related tasks that Home Organizations in CoSpaces should handle. Firstly, the HO is responsible for the authentication of people who belong to this institution. This is usually performed by their own system - for example using a LDAP-Server. After successful authentication, a handle including a proper Security Assertion Markup Language (SAML) entry will be created and passed to the AC using a cookie session mechanism.

The second task of the HO is to manage attributes of users. Resource providers ask the HO for authorization attributes associated with a given handle by sending a request to the HO's Attribute Authority (AA). Once more, SAML information encapsulating those attributes is created and sent back to the provider (compare with step 7 and 8 explained in figure 3).

The Application Controller to be developed within CoSpaces also binds different security functionalities. It is responsible for checking a user's authentication, which is mainly done by the Service Provider (SP) module provided by Shibbolehth. In the case of an unknown user, the WAYF[8] service redirects the unknown person to his / her corresponding HO in order to authenticate the user against the "shibbolized" infrastructure. If someone wants to access a resource behind the AC, the SP also demands authorization. Then, the Attribute Requester (AR) sends a message to the user's HO using his current security token and requests the attributes which can be passed to a local Policy Decision Point (PDP) [9], which grants or denies access to a specific service or resource.

3.2 Secure Data Transfer

At the lowest level of communication we must ensure that data is transferred via a secure conversation between different parties. Firstly, we have to ensure a secure communication as well as message integrity in communication between users and components over an un-trusted network, like the Internet. A solution is the "Transport Layer Security"/"Secure Sockets Layer" (TLS/SSL) paradigm. The second concern is to make nodes communicate only with trusted machines and services that are part of the federation. To ensure that, the Grid Security Infrastructure (GSI) or WS-Security can be applied depending on the provided services and technologies.

Apart from internal collaborations within the corresponding company intranet, CoSpaces assumes that parties also connect with each other over the Internet where encrypted data exchange is a prerequisite for security reasons. Specifically all information being sent between user site, Home Organization, and provider site has to be secured. The most popular solution, based on a public key cryptography, is the TLS/SSL protocol.

The Secure Sockets Layer, which can be placed between the network connection layer (e.g. TCP/IP) and the application protocol layer (e.g. HTTP),

[8] Where Are You From

establishes secure communication based on mutual authentication, integrity based on digital signatures, and privacy based on encryption.
One of the problems in providing security within Virtual Organizations is to make sure that grid nodes know and recognize each other. This means nodes in a collaborative working environment can contact each other and be sure that security is sufficiently assured. To provide this, Grid Security Infrastructure is applied. When resources get requests from some user(s), they have to perform a verification on two levels: check if the user is allowed to access a specific resource (user authorization) and if communication with target service is done in secure way (encrypted information).
GSI is also based on a public key cryptography. The central element in GSI is a certificate. All parties in the Grid are typically identified by certificates which contain the following information: subject name - object for which certificate is issued, public key of an object, the identity of the Certificate Authority (CA) and signature of the CA. Certificates are encoded in X.509 format [10]. Users can generate proxy certificates with short life-spans that are passed from one component to another and form the basis of authentication, access control, and logging.
GSI provides low-level authentication meaning that nodes know and trust each other. It allows access to nodes directly from other machines but it does not provide access to resources for particular users. This is done for example using the Shibboleth approach.

4 CoSpaces Usage Scenario

In the following figure and usage scenario, we assume to have an Application Controller as the basic communication and controlling element installed at each partner site which coordinates every outgoing as well as incoming request by consecutively enforcing different activities such as authentication, authorization, or message encryption on request according to the current circumstance.

Specifying a typical use case, we consider the following situation where a user wants to access and execute an application provided by a specific business partner. Basically, access to this application is restricted and only permitted to users participating within the CoSpaces collaboration working environment. To run and use the application, the following steps are needed and principally performed in an more or less automated way.

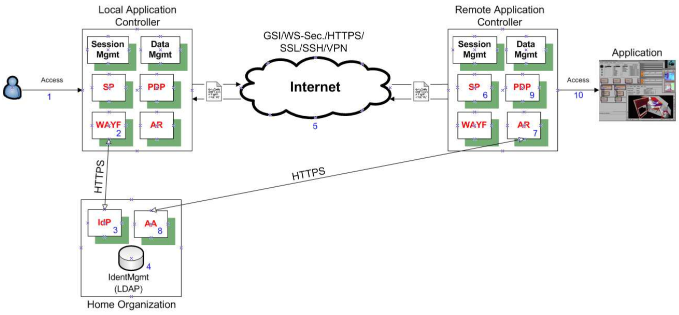

Figure 3: Typical usage scenario depicting the core security operations

1. A user wants to invoke the application directly but his request is interrupted by his own local Application Controller (AC)

2. If the current user is unknown meaning he has not a valid session id (session cookie set by Shibboleth) he is redirected by the WAYF service to his home organization via a secure channel (e.g. HTTPS)

3. His Home Organization (HO) acting as a Shibboleth Identity Provider (IdP) forces him to provide his credentials (usually username and password or optionally X.509 certificates) in order to authenticate himself

4. The login information provided is verified by the local identity management system (e.g. LDAP repository) and authentication information is sent back to the IdP which accepts or rejects the inputs

5. If the user is successfully identified, his call is either encrypted before delivering for example using GSI in the case of dealing with grid services or WS-Security for simple Web Services, or his data is transferred via a secure channel like HTTPS, SSL, SSH, or even VPN to the appropriate endpoint

6. Arriving at the remote AC of the corresponding partner, the request is now interrupted by the Service Provider (SP) component, which indicates that the partner is also "shibbolized"

7. In order to grant access to the local application, the Attribute Requester (AR) at the partner site requests user attributes from the Attribute Authority (AA) of the user's HO

8. The AA responds with a set of specified attributes based on the user's security information (SAML token)

9. To manage access control, a Policy Decision Point (PDP) which contains a set of access policies is called and the current user attributes are compared to the existing policies

10. If access is permitted, the user's request is decrypted before he can finally run the application, and if access is denied, his request is rejected and sent back to his local AC which then does some kind of exception handling

5 Conclusions

Dynamic collaboration based on distributed business workflows, is an exciting and promising field of interdisciplinary cooperation and will provide new and interesting working environments that facilitate cross-organizational data exchange and communication. It has attracted worldwide attention and several international research projects have already designed and implemented first prototypes for appropriate infrastructures. Currently, there is one big lack, which all these developments comprise. Security is seen as important and critical but instead of looking for a flexible solution, almost every project is favoring a static security infrastructure, which does not allow dynamic changes and / or adjustments, particularly during runtime.

In this paper, we have presented the vision of the European Research Project CoSpaces, which aims to create ad-hoc collaborative work environments that guarantee the utmost dynamic configuration for providers and customers without neglecting important security issues. We have identified some key features and requirements, which make the mission of CoSpaces different to current collaboration infrastructures. A short overview of technologies involved was given and how those could be applied within CoSpaces to meet the overall objectives and to overcome the difficulties of current approaches. We hope that CoSpaces will have a great impact on almost every aspect of future business collaborations and will also play an important role in future research projects.

6 Acknowledgements

The results presented in this paper are partially funded by the European Commission under contract IST-5-034245 through the project CoSpaces. The authors want to thank all who contributed to this paper, especially all members of the consortium.

References

[1] L. Schubert, S. Wesner, T. Dimitrakos. Secure and Dynamic Virtual Organizations for Business. *Paul Cunningham & Miriam Cunningham, ed., Innovation and the Knowledge Economy: Issues, Applications, Case Studies, IOS Press Amsterdam*, 2005, pp. 1201 - 1208.

[2] CoSpaces - EU IST Project (IST-5-034245). *http://www.cospaces.org.*

[3] AkoGrimo - EU IST Project (IST-004293). *http://www.mobilegrids.org.*

[4] TrustCoM - EU IST Project (IST-2003-01945). *http://www.eu-trustcom.com.*

[5] BREIN - EU IST Project (IST- 034556). *http://www.gridsforbusiness.eu.*

[6] T. Barton, J. Basney, T. Freeman, T. Scavo, F. Siebenlist, V. Welch, R. Ananthakrishnan, B. Baker, M. Goode, K. Keahey. Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy. *Proceedings of 5th Annual PKI R&D Workshop*, March 2006.

[7] The Globus Toolkit Homepage. *http://www.globus.org/toolkit.*

[8] D. Golby, M.D. Wilson, L. Schubert, C. Geuer-Pollmann. An assured environment for collaborativeengineering using web services. *CE2006.*

[9] S. Wesner, L. Schubert, T. Dimitrakos. Dynamic Virtual Organisations in Engineering. *2nd Russian-German Advanced Research Workshop on Computational Science and High Performance Computing*, March 14 - 16, 2005.

[10] A. Arenas, I. Djordjevic, T. Dimitrakos, L. Titkov, J. Claessens, C. Geuer-Pollmann, E. Lupu, N. Tuptuk, S. Wesner, L. Schubert. Toward Web Services Profiles for Trust and Security in Virtual Organisations. *Proc. 6th IFIP Working Conference on Virtual Enterprises (PRO-VE 2005)*, Valencia, Spain, 26-28 Sep 2005.