Implantação de uma Comunidade Acadêmica Federada para Experimentação usando Framework Shibboleth

Maykon Chagas de Souza[1], **Michelle S. Wangham**[2], **Emerson Ribeiro de Mello**[1]

[1]Instituto Federal de Santa Catarina (IFSC)
São José – SC – Brasil

[2]Universidade do Vale do Itajaí (UNIVALI)

maykon.c@aluno.ifsc.edu.br, wangham@univali, mello@ifsc.edu.br

Abstract. *The availability of accessible services and applications on the Internet has complicated the management of identities, both for users and system administrators. To go around this, the federated identity model aims to improve the access to services. However the implementation of a federation is not trivial, and, for many researchers who are developing studies on this ?eld, deploying a federation to conduct practical experiments is a long and costly task. This paper aims to implement and provide a virtual environment for researchers to conduct experiments in a framework-based Shibboleth federation.*

1. Introdução

A disponibilidade de serviços e aplicações acessíveis remotamente hoje na Internet se tornou um processo relativamente simples de implementação. O avanço das tecnologias de redes de computadores foi responsável pela construção dessas aplicações e o acesso remoto (e em tempo real) às mesmas. No entanto, além de manter a própria aplicação, administradores de sistemas necessitam ainda manter uma base de usuários própria com informações e níveis de privilégio para permitir acesso aos serviços, tornando o trabalho custoso [MOREIRA et al. 2011].

Do lado do usuário, com tantos serviços disponíveis, o sistema permite ao usuário a criação de múltiplas identidades para acesso a esses serviços. Cada novo serviço que o usuário deseja acessar, este deve repassar algumas informações pessoais e um nome de usuário e senha para acessar o serviço. Criar um nome de usuário e senha para cada serviço seria uma boa prática de segurança, porém, administrar essas informações é uma tarefa difícil para os usuários, diante da grande gama de serviços que são oferecidos hoje [WANGHAM et al. 2010b].

2. Modelo federado

No modelo de gestão de identidade federada [WANGHAM et al. 2010a], objetiva-se remover essa complexidade do usuário em ter que administrar um nome de usuário e senha para cada serviço que deseja acessar. O conceito de federação visa minimizar as demandas dos provedores de serviço e de usuários de uma instituição, delegando serviços bem específicos para cada elemento da estrutura da federação. Uma federação é composta por dois componentes principais, (1) provedores de identidades (*Identity Provider - IdP*), que são responsáveis pela autenticação e gerenciamento das identidades dos usuários de

um domínio, além de definir o método de autenticação o IdP deve garantir que cada usuário do seu domínio tenha um identificador único, (2) provedores de serviços (*Service Provider - SP*), que disponibilizam serviços para acesso dos usuários, podem requisitar informações adicionais para garantir acesso a um determinado serviço, independente do domínio [MOREIRA et al. 2011].

Neste modelo, informações dos usuários são compartilhadas entre provedores de identidade e provedores de serviços, que possuem relações de confiança entre si e pertencem ao círculo de confiança da federação. Neste modelo, é introduzida a facilidade de autenticação única (*Single Sign-On*), que garante ao usuário passar uma única vez pelo processo de autenticação e acessar qualquer provedor de serviços da federação, cabendo a esses provedores realizarem somente o controle de acesso dos usuários. Este modelo se mostra vantajoso para o usuário, que necessitará de uma única identidade para acessar os diversos serviços da federação, e para o administrador do sistema, que ao prover um serviço para a federação não precisa se preocupar com a autenticação e com o cadastro de usuários.

No Brasil, a Rede Nacional de Ensino e Pesquisa (RNP), em conjunto com as instituições de ensino UFC, UFMG, UFF, UFRGS e Cefet-MG, iniciaram o projeto da Comunidade Acadêmica Federada (CAFe) com o intuito de reunir as universidades e instituições de pesquisa do País [MOREIRA et al. 2011]. Desde 2009, a RNP disponibiliza o serviço da CAFe às suas organizações usuárias. Através da CAFe[1], um usuário mantém todas as suas informações na sua instituição de origem e pode acessar serviços oferecidos pelas instituições que participam da federação acadêmica.

3. Problema de pesquisa

Desenvolver pesquisa aplicada na area de gestã de identidades federadas exige que os experimentos sejam conduzidos em um ambiente que implemente uma federação em sua totalidade, sendo que a complexidade de montar tal ambiente depende do framework escolhido [WANGHAM et al. 2013]

A federação CAFe é um ambiente de produção, ou seja, nesta federação não deve ser permitida a realização de experimentos e assim pesquisadores que fazem prospecções tecnológicas e pesquisas científicas em gestão de identidade necessitam montar sua própria federação de testes para que possam conduzir seus projetos e experimentos.

Ciente desta necessidade, a RNP criou em 2013 o Projeto GId Lab[2] - Laboratório de Experimentação em Gestão de Identidade que tem por objetivo geral disponibilizar para a comunidade acadêmica um ambiente virtual no qual os pesquisadores poderão realizar testes com Infraestruturas de Autenticação e Autorização (IAA) e também Infraestruturas de Chaves Públicas (ICPs).

4. Objetivo

O objetivo deste trabalho é implantar a parte de IAA do GId Lab que inicialmente disponibilizará uma federação Shibboleth[3], chamada CAFe Expresso (Comunidade Acadêmica

[1] http://portal.rnp.br/web/servicos/cafe
[2] http://wiki.rnp.br/display/gidlab/
[3] http://shibboleth.net

para Experimentação). A CAFe Expresso consistirá de Provedores de Identidade (IdP), Provedores de Serviço (SP) e o serviço *Where Are You From* (WAYF)[4] também denominado *Discovery Service* (DS) que realiza o redirecionamento do usuário para o seu IdP de origem para que este se autentique. Ainda no contexto deste trabalho, máquinas virtuais com IdPs e SPs serão configuradas e disponibilizadas para download de forma a facilitar a implantação destes provedores nas instituições que estão realizando seus experimentos no GId Lab.

Referências

MOREIRA, E. Q., FOSCARINI, É. D., JUNIOR, G. C. S., ALIXANDRINA, L. A. O., NETO, L. P. V., and ROSSETTO, S. (2011). Federação CAFe: Implantação do Provedor de Identidade.

WANGHAM, M. S., MELLO, E. R., BÖGER, D. S., GUERIOS, M., and FRAGA, J. S. (2010a). Gerenciamento de Identidades Federadas. *Minicursos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 3–52.

WANGHAM, M. S., MELLO, E. R., FRAGA, J. S., and GUERIOS, M. (2010b). Uma Infraestrutura para Tradução de Credenciais de Autenticação para Federações Shibboleth. *X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 447–360.

WANGHAM, M. S., MELLO, E. R., SOUZA, M. C., and COELHO, H. (2013). GId Lab: Laboratório de Experimentação em Gestão de Identidades. *Anais XIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 481–486.

[4]https://wayf.switch.ch/