

10 de novembro de 2011

Motivação

- Migração de serviços para as nuvens;
- Necessidade de autenticação;
- Preocupação crescente com privacidade;

Problema e Objetivo

Problema

Falta de mecanismos de proteção à privacidade em sistemas de gerenciamento de identidades.

Objetivo

Inserir o gerenciamento de identidades com proteção à privacidade em ambientes de computação em nuvem.

Agenda

- 1 Introdução
- 2 Identidade Digital
- 3 Privacidade
- 4 Computação em Nuvem
- 5 Desenvolvimento
- 6 Conclusões

O que é

Identidades digitais são coleções de dados que representam atributos ou características de uma entidade [Windley 2005].

Funcionam como um meio de autenticação e autorização e são utilizadas em diversos cenários, entre os quais podemos destacar: comércio eletrônico, governo eletrônico, redes sociais, *e-mail*, finanças e saúde online.

Sistemas de Gerenciamento de Identidades

Um serviço de gerenciamento de identidades pode ser definido como "o processo de criação, gerenciamento e utilização de identidades de usuários e a infraestrutura que suporta esse processo." [Lee et al. 2009]

Muitas vezes as informações associadas a uma identidade são sensíveis, como no caso de dados médicos e financeiros. Por causa da natureza privada e sensível dessas informações associadas os sistemas de gerenciamento de identidades devem ser seguros e confiáveis.

Papéis

Os seguintes papéis são desempenhados num sistema de gerenciamento de identidades [Bertino e Takahashi 2011]:

Usuário Possui uma identidade e utiliza os serviços do IdP e do SP;

Provedor de Identidades (IdP) Fornece os serviços de gerenciamento de identidades;

Provedor de Serviços (SP) Fornece os serviços que o usuário efetivamente deseja utilizar, como *e-mail*, *e-commerce* e outros. Delega a autenticação e autorização dos usuários a um IdP.

Agenda

- 1 Introdução
- 2 Identidade Digital
- 3 Privacidade**
- 4 Computação em Nuvem
- 5 Desenvolvimento
- 6 Conclusões

Conceitos Básicos

Privacidade relaciona-se com a capacidade de um indivíduo proteger informações sobre si [Mather et al. 2009].

O Fair Information Practice Principles (FIPS) é um conjunto de regras para manipulação de informações com proteção à privacidade que regula o uso de informações privadas nos Estados Unidos e serve de base para regras de outros países [Federal Trade Commission 2011]. Os FIPs definem cinco princípios básicos.

Princípios

- Advertência/Consciência** Os usuários devem ser avisados das práticas de uma entidade que irá manipular informações sensíveis antes que qualquer informação seja coletada;
- Escolha/Consentimento** Dar aos usuários opções sobre como quaisquer dados coletados serão utilizados;
- Acesso/Participação** Possibilidade de um usuário acessar as informações coletadas sobre si e poder alterar esses valores;
- Integridade/Segurança** Coleta de dados a partir de fontes confiáveis e armazenamento seguro;
- Cumprimento/Reparação** Garantias de que os princípios serão respeitados.

Agenda

- 1 Introdução
- 2 Identidade Digital
- 3 Privacidade
- 4 Computação em Nuvem**
- 5 Desenvolvimento
- 6 Conclusões

Definição

O trabalho de [Marston et al. 2011] define computação em nuvem da seguinte forma: “É um modelo de serviço de tecnologia da informação onde os serviços computacionais (ambos hardware e software) são entregues sob demanda para os usuários através de uma rede na forma de **auto-atendimento**, independente de dispositivo e de localização. Os recursos necessários para fornecer os diferentes níveis de qualidade de serviço são **compartilhados**, dinamicamente **escaláveis**, alocados rapidamente, **virtualizados** e liberados com **interação mínima com o provedor de serviço**”.

SAAS

- GOOGLE DOCS
- NETSUITE
- FRESHBOOKS
- GMAIL
- SALESFORCE
- BASECAMP

PAAS

- FORCE.COM
- APP ENGINE
- AZURE

IAAS

- RACKSPACE.COM
- GO GRID
- AWS

end customers

developers

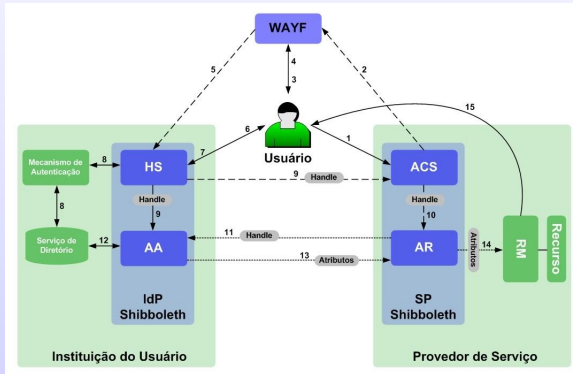
sysadmins

Agenda

- 1 Introdução
- 2 Identidade Digital
- 3 Privacidade
- 4 Computação em Nuvem
- 5 Desenvolvimento**
- 6 Conclusões

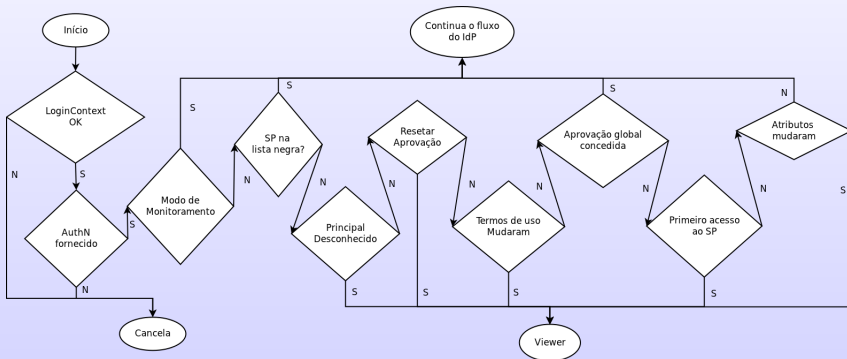
```
graph LR
    U[Usuário] <--> SP((Provedor de Serviços SP))
    SP <--> IdP
    subgraph Cloud [Provedor de Serviços de Nuvem]
        direction TB
        IdP((Provedor de Identidades IdP))
        IdP --- A[Autenticação]
        A --- GI[Gerenciamento de Identidades]
        GI <--> PP[Plugin de Privacidade]
        A --> BD[(Base de Dados)]
        GI --> BD
        PP --> BD
    end
```


- Amazon EC2 Provedor de serviços de nuvem (IaaS);
- Shibboleth Sistema de gerenciamento de identidades;
- uApprove *Plugin* de privacidade.



- *Plugin* de privacidade para o Shibboleth desenvolvido pela rede de universidades suíças SWITCH.
- Objetivo de garantir que o usuário saiba quais dados seus são liberados e para quem são liberados, além disso o usuário deve concordar com os termos de uso do provedor de serviços.
- Dividido em três componentes principais: *IdP plugin*, *Viewer* e *Reset approvals*.

uApprove



Desenvolvimento - Infra-estrutura básica

- Instanciação da máquina virtual;
 - High-CPU;
 - Windows Server 2008;
 - Armazenamento EBS 30GB.
- Configuração de IP estático e regras de *firewall*;
 - IP: 50.19.108.64
 - Firewall: liberação das portas 80 (HTTP), 443 (HTTPS), 3389 (RDP), 8080 (Tomcat)
- Instalação do servidor web Apache e servidor de aplicações Tomcat;
- Configurações de SSL e proxy;

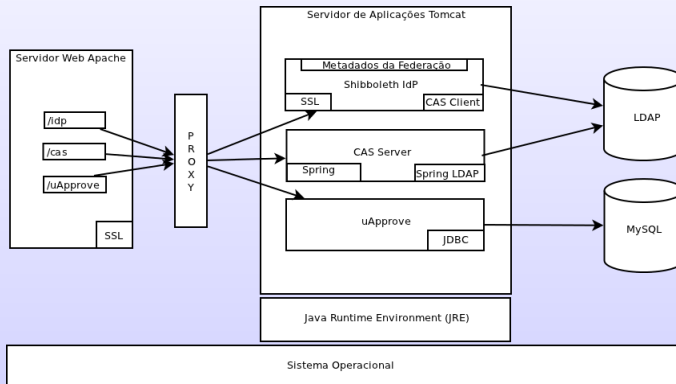
Desenvolvimento - Shibboleth

- Instalação do serviço de autenticação CAS;
 - Configuração de pesquisa dos usuários em diretório LDAP;
- Cadastro na federação TestShib;
- Instalação do Shibboleth;
 - Configuração de utilização da TestShib;
 - Configuração de autenticação através do CAS;
 - Configuração dos atributos;
 - Configuração da liberação de atributos;

Desenvolvimento - uApprove

- Instalação do MySQL;
 - Criação do banco de dados e das tabelas usadas pelo uApprove;
- Instalação do uApprove;
 - Criação dos termos de uso;
 - Configuração do filtro no Shibboleth;

Desenvolvimento



Resultados



The screenshot shows a web browser window with the address bar containing 'g/'. The browser's toolbar includes a star icon, a refresh icon, and a Google search icon. The main content area of the browser displays the TestShib website. At the top left of the page is a logo featuring a griffin. To the right of the logo, the text 'TESTSHIB' is displayed in a large, bold, green font. Below the logo and title, there is a welcome message: 'Welcome to the [TestShib](#) Service Provider! Hopefully, you won't be here too long. Make sure you've already [joined TestShib](#) and [configured your IdP](#). You can also test against other TestShib members later.'

Below the welcome message, there is a paragraph of instructions: 'If you don't make it back successfully, **first check the Shibboleth Wiki (1.3)**. If that doesn't solve it, send a detailed description of the error, your configuration, and log information to shibboleth-users@internet2.edu'.

Another paragraph follows: 'To start, you'll need to enter the entityID of your IdP in the box below. You'll be redirected to your IdP, where you'll use credentials such as `myself/myself` or others you've added to authenticate. Afterwards, you'll bounce back and see some results. If you enter your entityID incorrectly, you'll see a Session Creation Failure.'

Below this text is a text input field containing the URL: `https://ec2-50-19-108-64.compute-1.amazonaws.com/idp/shibboleth`. Below the input field is a button labeled 'Go!'. At the bottom of the page, there is a copyright notice: '© Copyright 2006-2009 Internet2.'

Resultados

Firefox CAS – Central Authentication Service +

← → amazonaws.com https://ec2-50-19-108-64.compute-1.amazonaws.com/cas/login?service=https%3A%2F%2Fec2-50-19-108-64.compute-1.amazonaws.com

JASIG

Central Authentication Service (CAS)

Enter your NetID and Password

NetID:

Password:

☐ Warn me before logging me into other sites.

For security reasons, please Log Out and Exit your web browser when you are done.

Languages:
[English](#) | [Spanish](#) | [French](#) | [Russian](#) | [Nederlands](#) | [Svenskt](#) | [Italiano](#) | [Urdu](#) | [Chinese \(Simplified\)](#) | [Deutsch](#) | [Japanese](#) | [Croatian](#) | [Czech](#) | [Slovenian](#) | [Polish](#) | [Turkish](#)

Copyright © 2005-2007 JA-SIG. All rights reserved.
Powered by [JA-SIG Central Authentication Service 3.3.2](#)

Resultados

LDAP - uid=jose,ou=people,dc=compute-1,dc=amazonaws,dc=com - ec2-50-16-87-125.compute-1.amazonaws.com - Apache Directory Studio

File Edit Navigate LDAP Window Help

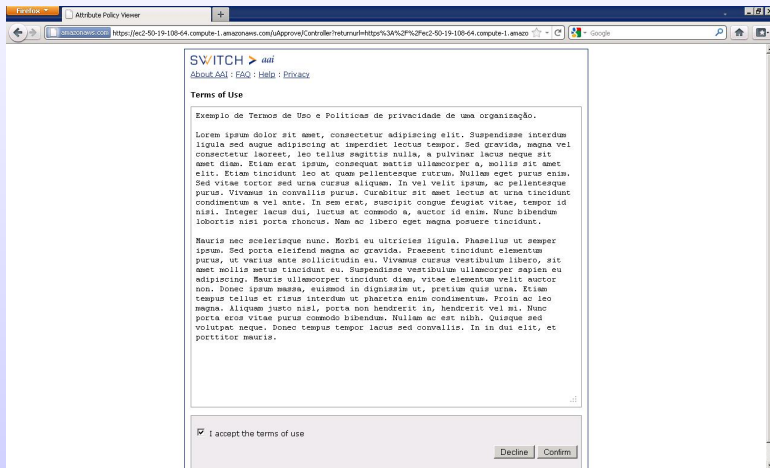
LDAP Browser

uid=jose,ou=people,dc=compute-1,dc=amazonaws,dc=com

DN: uid=jose,ou=people,dc=compute-1,dc=amazonaws,dc=com

Attribute Description	Value
objectClass	brPerson (auxiliary)
objectClass	inetOrgPerson (structural)
objectClass	person (structural)
objectClass	schacPersonAttributes (auxiliary)
cn	Jose
sn	Silva
brPersonCPF	01234567890
mail	jose@ufsc.br
schacCountryOfCitizenship	Brazil
schacDateOfBirth	19900215
uid	jose
userPassword	Plain text password

Resultados



Resultados

+

0-19-108-64.compute-1.amazonaws.com/u/Approve/Controller?terms-agree=on&terms-confirm=Confirm

☆ ◁ ▷ Google

SWITCH > *aai*
[About AAI](#) : [FAQ](#) : [Help](#) : [Privacy](#)

To use '**sp.testshib.org**', their system needs to receive some information about you in the form of a Digital ID Card. You will need to agree to send the following information to access their services. All this information is needed or access to the service will not be granted.

Digital ID Card	
eduPersonAffiliation	member
sn	Silva
brPersonCPF	01234567890
cn	Jose
eduPersonPrincipalName	jose@compute-1.amazonaws.com

☐ Don't show me this page again. I agree that my Digital ID Card (possibly including more data than shown above) will be sent automatically in the future to this site as well as to other services I will access.

Cancel

Confirm

Resultados

+

ib.org/testing/sample.jsp

☆ ↻ Google



TESTSHIB

Shibboleth-protected TestShib Content

This page is protected by the TestShib Service Provider. If you're reading this, your IdP successfully provided authentication information. If you have data about you and an assertion below, then your IdP also released attribute and authorization information. Cool!

If something's missing, you should check your IdP's `shib_error.log` or `idp-process.log`.

TestShib also allows you to check out the last lines of `shibd.log` or `native.log` on the SP side.

Generally, for WARN level information(or worse) for indications as to the problem. Check the [Shibboleth Wiki](#) to see if you can find a match. If that doesn't help, please check our [mailing list archives](#), then ask on the [mailing list](#).

Here are some pieces of information I can tell about you using the information Shibboleth gives me:

- Keep-Alive is: 115
- Shib-Session-ID is: `_8e350028b69bbf4ef85bcb22565c1e5f`
- Shib-Authentication-Method is: `urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified`
- Shib-Authentication-Instant is: `2011-05-04T18:57:38.717Z`
- Shib-AuthnContext-Class is: `urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified`
- Shib-Assertion-Count is: 01
- transient-id is: `_1a534256c86f99414c458fe1ef49a985`
- eppn is: `jose@compute-1.amazonaws.com`
- unscoped-affiliation is: `member;Silva;01234567890;Jose`
- persistent-id is: `https://ec2-50-19-108-64.compute-1.amazonaws.com/idp/shibboleth!https://sp.testshib.org/shibboleth-sp!a8VE0enZ5tYAe9Y2ENwjLJE2MII=`
- Shib-Application-ID is: `default`
- Shib-Assertion-01 is: `http://localhost/Shibboleth.sso`

Resultados



Conclusões

- Tratados dois problemas importantes: a falta de consciência dos usuários quanto à liberação de seus atributos para provedores de serviço e a falta de preocupação dos provedores de identidades quanto à apresentação de seus termos de uso.
- A proposta de solução, com o uso dos softwares Shibboleth e uApprove, mostrou que é possível resolver os dois problemas de maneira eficiente e sem comprometer a usabilidade da aplicação.
- A proposta se mostrou viável e pôde ser implantada em uma nuvem pública, com a possibilidade de utilização em federações consolidadas.

- Automação da verificação de compatibilidade entre políticas de privacidade de provedores e de usuários pode ser considerado um trabalho futuro.

Obrigado

Obrigado!

Daniel Ricardo dos Santos

danielricardo.santos@gmail.com