Gerenciamento de Identidades

Leonardo Pais Cardoso
Marcello Ribeiro Salomão
Victor Torres da Costa

Introdução

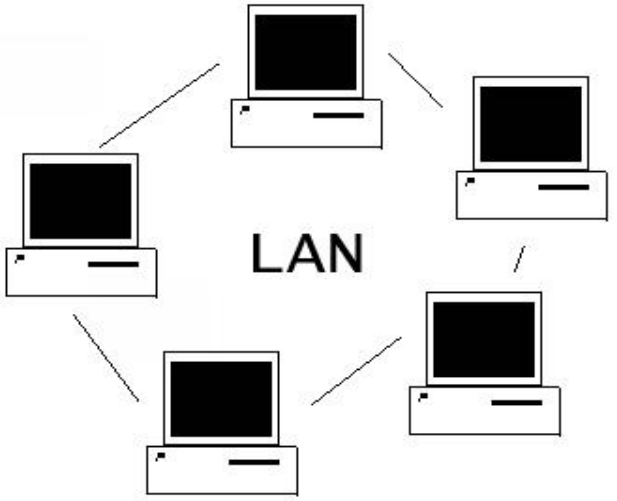
- Desenvolvimento das organizações
  - Empresas puramente virtuais
    - Amazon
  - Organizações em crescimento
    - Tamanho
    - Complexidade
- Gerenciamento de usuários e permissões
  - Privacidade
  - Segurança
  - Eficiência

Histórico

- Era do Mainframe
  - Terminais externos
    - Ligados diretamente ou pela rede telefônica
    - Itermediário até o Mainframe
      - Unidade de Controle (Controle de Acesso - CA)
        - » CA baseado na localização do terminal/usuário

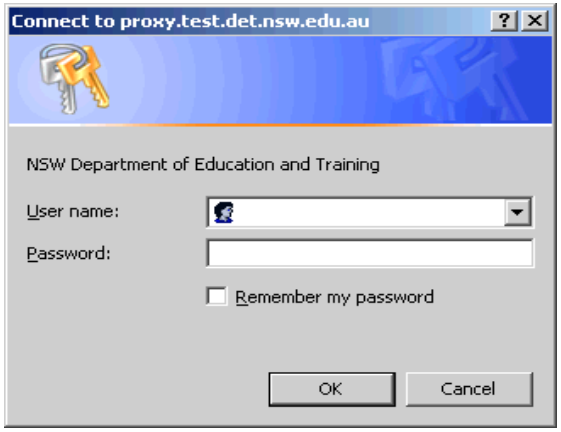
Histórico

- Desenvolvimento da computação
  - Multi-processamento
  - Redes Locais (LAN)
  - Necessidade de um melhor controle de acesso
    - Controle de acesso lógico
      - » Lista de permissões
        - Leitura e Escrita
      - » Sistemas multi-usuário
    - Identificação do usuário
      - » O que você sabe
      - » O que você tem
      - » O que você é



Histórico

- CA – Primeira Geração
  - O que você sabe
    - Utilização de pares Login/Senha
  - Limitações
    - Requer senhas fortes (8 caracteres ou mais)
    - Usuário suscetível a engenharia social
    - Troca de senhas frequêntes necessária
    - Indivíduo com muitos pares Login/Senha



Histórico

- CA – Segunda Geração
  - O que você tem
    - Dispositivo físico para autenticação
  - Limitações
    - Mais trabalho para os usuários
    - Possibilidade de perda do dispositivo
    - Alto custo em caso de problemas comuns
      - Perda do dispositivo
      - Troca de dispositivo
      - Permissões de emergência

Histórico

- CA – Terceira Geração
  - O que você é
    - Autenticação por características físicas (Biometria)
  - Limitações
    - Geralmente fácil de ser forjado
    - Falta de acurácia

- Métodos intrusivos
- Alto custo para sistemas confiáveis
- Aplicável apenas em humanos

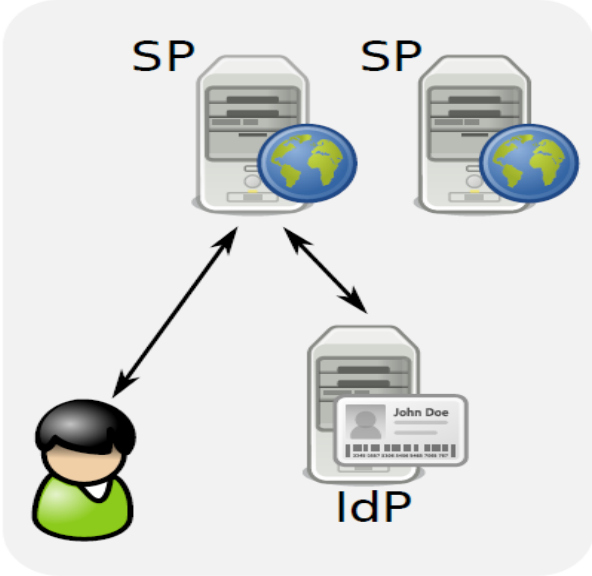
Tempos Atuais

- Generalização de Controle de Acesso
  - Sistemas de Gerenciamento de Identidade (SGI)
    - Verificação da identidade
    - Atribuição de permissões e privilégios
  - Modelos em produção atualmente
    - Sistemas de arquitetura proprietária
    - Usuário gerencia várias identidades
      - Exemplo
        - Usuário se autentica no amazon.com
        - E depois também no facebook.com

Hovav, Anat and Berger Ron "Tutorial: Identity Management Systems and Secured Access Control," Communications of the Association for Information Systems, Vol. 25, article 42, 2009.

Modelos de SGI

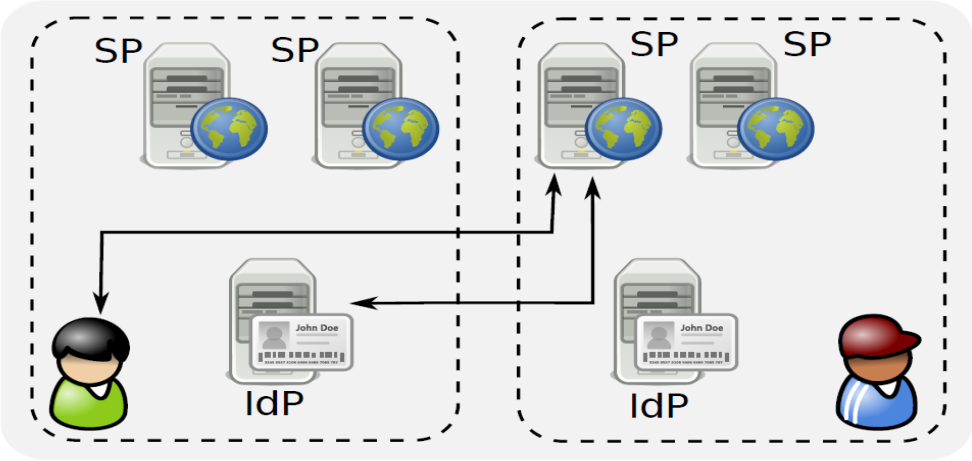
- Centralizado
  - Autenticação única (*Single Sign On* – SSO)
  - Confiança plena no provedor de identidades
    - Ponto único de falha
    - Total poder sobre dados dos usuários
  - Usuário só perde acesso quando credenciais expiram



Centralizado

Modelos de SGI

- Federado
  - Centrado em Provedores de Identidade locais
    - Confiança em todos os provedores
      - Possível disponibilização de dados a terceiros
  - Autenticação única (SSO)
    - Acordo entre diferentes Provedores de Identidade

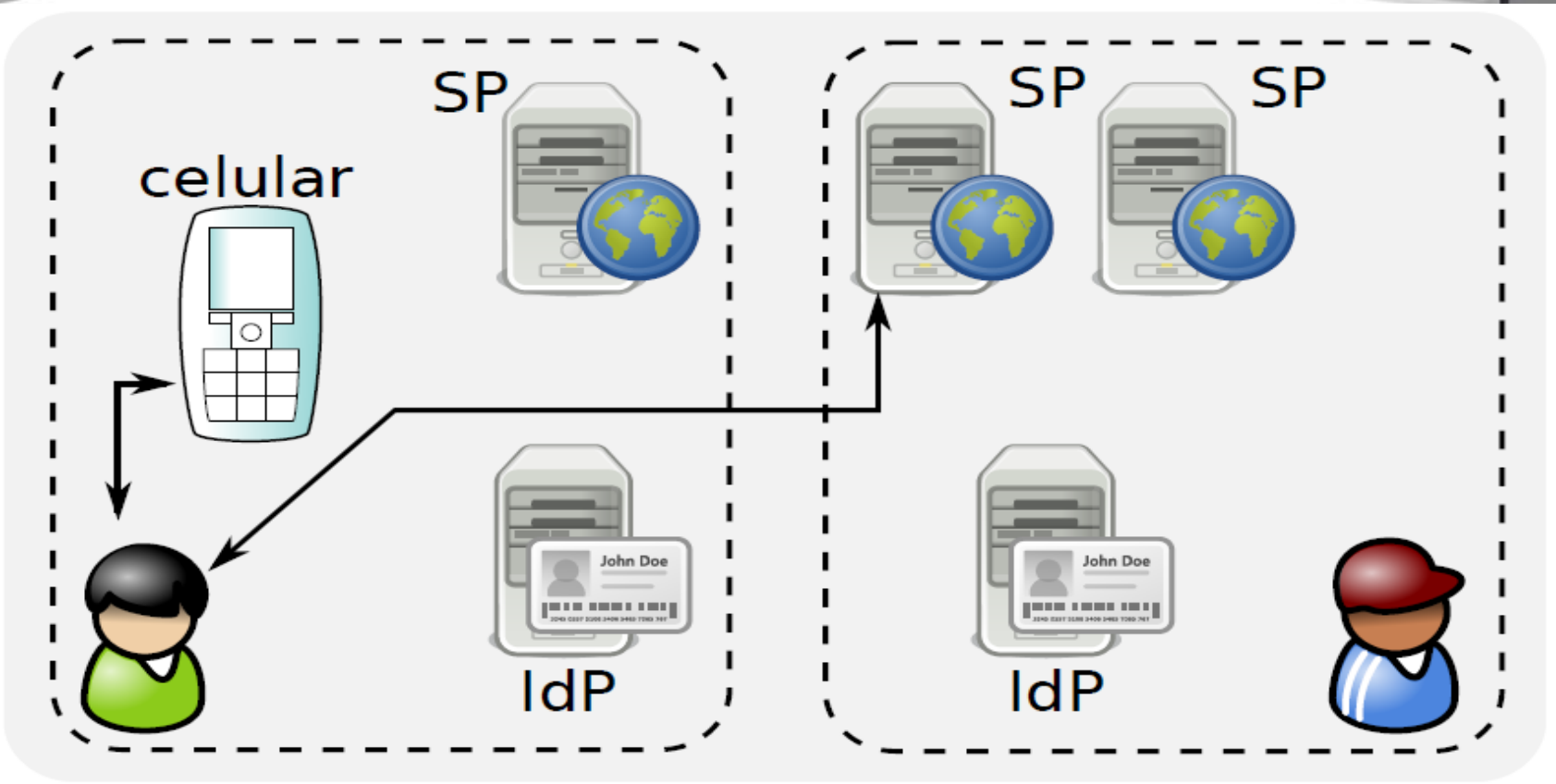


Federado

Modelos de SGI

- Centrado no usuário
  - Identidades armazenados em um dispositivo
    - Smartcard, celular
  - Autenticação no dispositivo
    - Dispositivo se torna um provedor de Identidade
      - Modelo Federado
      - Preferências de privacidade controladas pelo usuário
  - Duas abordagens de identificadores
    - Identidade Baseada no Endereço
    - Identidade Baseada no Cartão

Modelos de SGI



Centrado no usuário

Michelle S. Wangham , Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, Joni da Silva Fraga - "Gerenciamento de Identidades Federadas"in Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais

SGIs Existentes

- Dois principais modelos utilizados
  - Sistema federado
    - Shibboleth
    - Liberty Alliance
    - OpenSSO
  - Sistema centrado no usuário
    - OpenID
    - Windows CardSpace
    - Projeto Higgins

SGIs Existentes

- Principais focos e motivações
  - Área acadêmica
    - No Brasil, CAFe da RNP
  - Setor Privado
  - Geral (sem foco específico)

SGIs Existentes

- Objetivos muito parecidos
  - Permitir uma única autenticação (SSO)
  - Informações pessoais
    - Garantir Privacidade
    - Garantir Segurança
  - Utilização de padrões aceitos
  - Propor novos padrões
  - Pover serviços amigáveis ao usuário

SGIs Existentes

- Uma base utilizada por todos
  - SAML
    - Linguagem de Marcação para Asserções de Segurança
    - Baseada em XML
    - Cuida do envio e recebimento de asserções
      - Mensagens entre provedor de serviço e identidade
    - Usado em protocolos de pedidos e respostas

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    Version="2.0" IssueInstant="2005-01-31T12:00:00Z">
  <saml:Issuer
     Format="urn:oasis:names:SAML:2.0:nameid-format:entity">
    http://idp.example.org
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
      j.doe@example.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions NotBefore="2005-01-31T12:00:00Z"
     NotOnOrAfter="2005-01-31T12:10:00Z" />
  <saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z"
     SessionIndex="67775277772">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

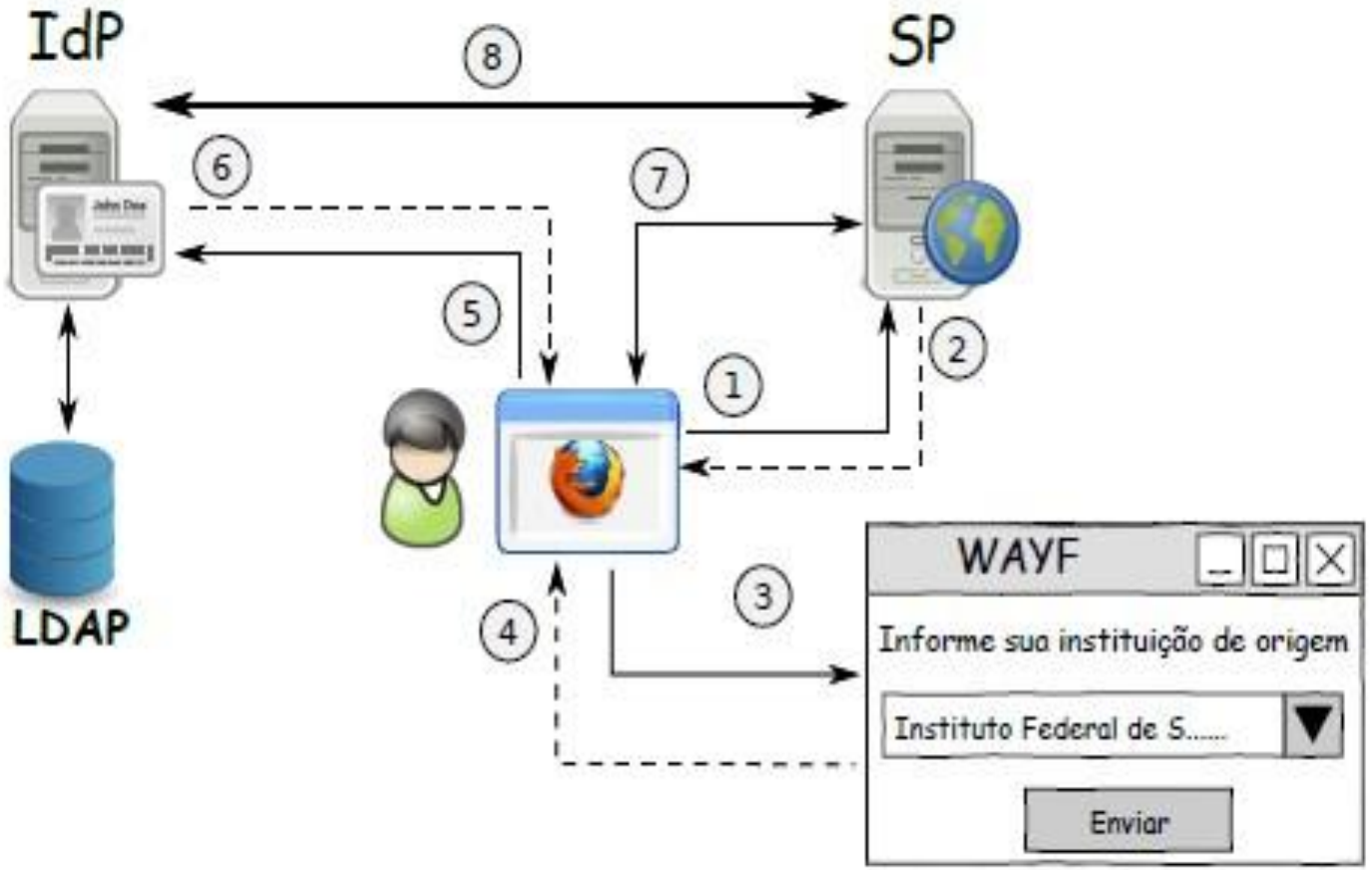
SGIs Existentes

- Shibboleth
  - Iniciativa do consórcio americano internet2
  - Baseado em federações
  - Implementações
    - Código aberto
    - Baseada em padrões abertos
  - Solução genérica para identidades federadas
    - Muito usado em meio acadêmico

SGIs Existentes

- Shibboleth
  - Proposto eduPerson
    - Padrão de atributos de indetidade comuns
    - Aceito pela CAFe
      - Criação do brEduPerson
  - Tem atraído iniciativas privadas
    - Oferecer serviços no meio acadêmico

Shibboleth



Michelle S. Wangham , Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, Joni da Silva Fraga - "Gerenciam
Identidades Federadas"in Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionai

SGIs Existentes

- Liberty Alliance
  - Consórcio formado por empresas de diferentes áreas
    - Mais de 160 atualmente
  - Especificações abertas
  - Identidades federadas
  - Integração com Serviços Web
    - Participou diretamente nas especificações do SAML
    - Baseada em Circuitos de Confiança entre organizações
      - Relações de confiança
      - Acordos de confiança
        - » Voltado para ambiente empresarial

SGIs Existentes

- OpenSSO
  - Sun Microsystems (Oracle)
  - Abandonado como produto estratégico
    - Atualmente desenvolvido pro ForgeRock
    - OpenAM
  - Identidade federada
  - Implementada usando puramente JAVA
    - Grande interoperabilidade
  - Simples de configurar
    - Semelhante ao Shibboleth

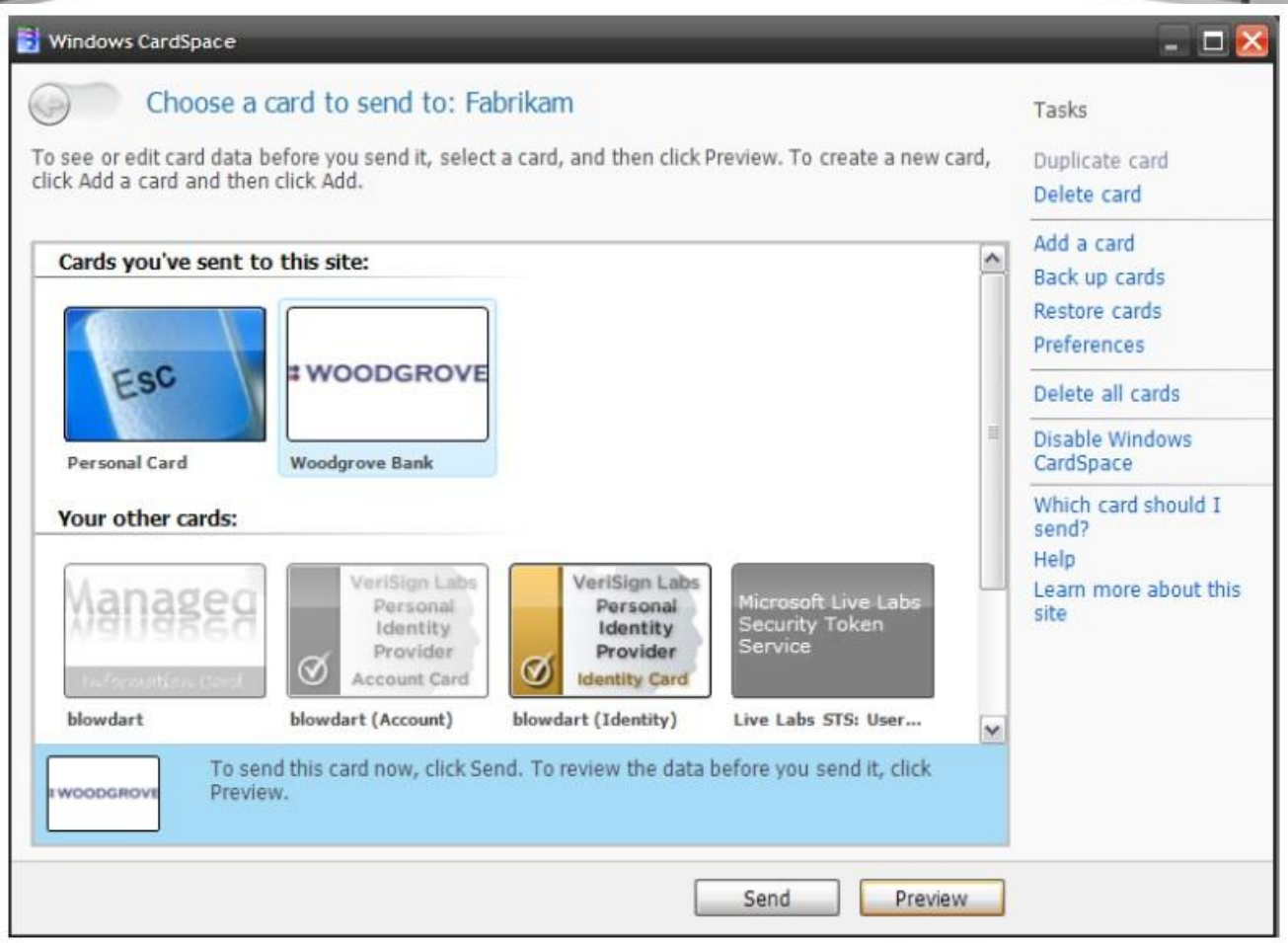
SGIs Existentes

- Windows CardSpace
  - Microsoft
  - Centrado no Usuário
  - Incorporado ao Windows Vista e Seven
  - Compatível com versões 7.0 em diante do Explorer
  - Interface gráfica agradável ao cliente

SGIs Existentes

- Windows CardSpace
  - Gerenciamento inovador de identidade
    - Diversos Cartões
      - Auto-autenticado
      - Administrado
    - Possibilidade de escolher sua identidade
    - Usuário não entra em contato com entidade Autenticadora
      - Menor risco de ataque de phishing
    - Pode trabalhar com qualquer sistema de identidade digital

Windows CardSpace



Michelle S. Wangham , Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, Joni da Silva Fraga - "Gerenciamento de Identidades Federadas"in Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2010

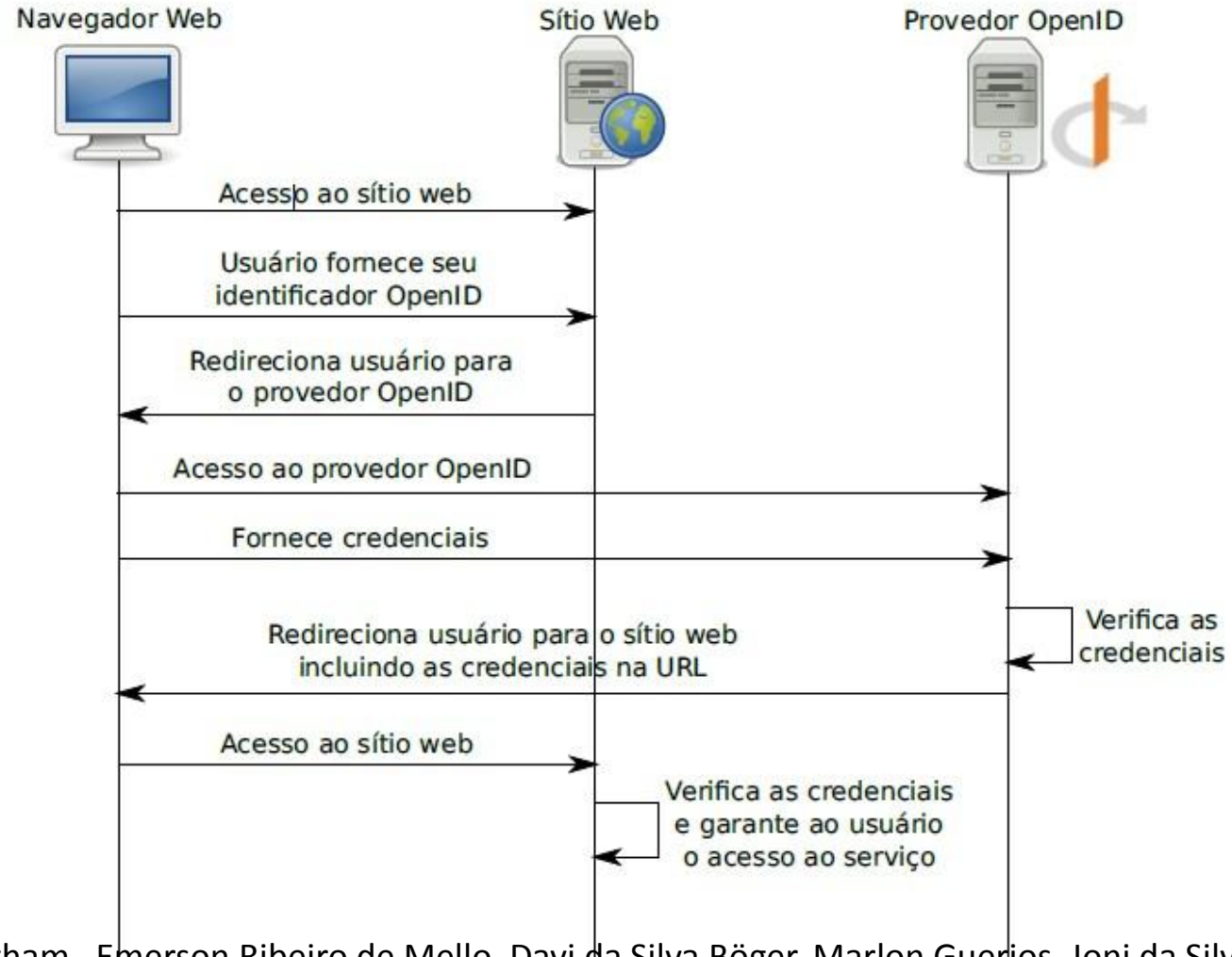
SGIs Existentes

- OpenID
  - Brad Flitzpatrick
    - Arquiteto-chefe da Six Apart
  - Centrado no usuário
  - Inicialmente voltado para um problema local
    - Combater lixo eletrônico
  - Extremamente simples
    - Identidade embutida no endereço
    - Cliente não precisa de software adicional

SGIs Existentes

- Rápido crescimento e popularização
  - Google, Six Apart, Yahoo, Flickr, MySpace, Facebook, Wordpress, Verisign, AOL, Paypal...

OpenID



Michelle S. Wangham , Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, Joni da Silva Fraga - "Gerenciamento de Identidades Federadas"in Minicursos do Simpósio Brasileiro de Segurança da Informação e de

SGIs Existentes

- Higgins
  - Eclipse Foundation
  - Centrado no usuário
  - Semetlhante ao Windows CardSpace
    - Identidade definida através de cartões
  - Multiplataforma
    - Funciona nos principais SOs e navegadores
  - Altamente customizável por meio de plugins
  - Permite extração de dados de identidades
    - Exemplo: Dados de um perfil de rede Social

SGIs Existentes

- Exemplo de como é colocado em funcionamentos um IdP
  - Shibboleth
    - Aplicação web disponível em formato WAR
      - Contêiner java
    - Basta executar e anexar a um servidor Web
      - Ex: Apache HTTP

Desafios Tecnológicos

- Ainda restam complexos desafios técnicos
  - Representação
    - Qual a melhor representação para identidade
    - Qual o melhor formato para troca de atributos
      - Diferentes aplicações
      - Diferentes redes
      - Diferentes sistemas operacionais

Desafios Tecnológicos

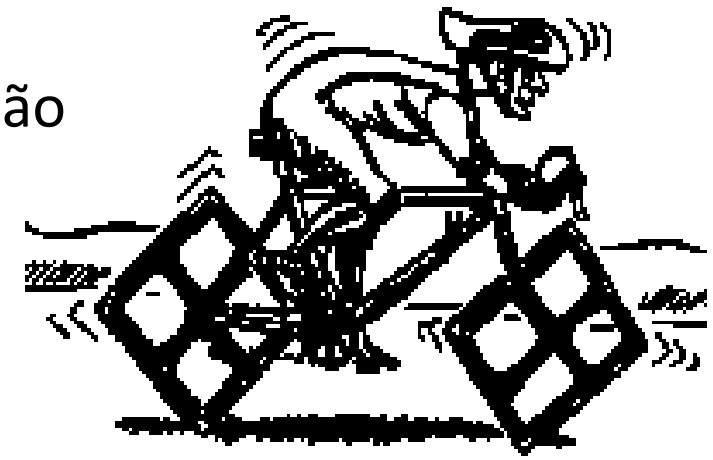
- Ainda restam complexos desafios técnicos
  - Ponto único de falha
    - Serviços vitais no sistema
      - Falha pode comprometer todo o sistema
      - Invasão
      - Queda de energia
      - Problemas de projeto

Desafios Tecnológicos

- Ainda restam desafios técnicos
  - Desempenho
    - Sistema pode ter alta complexidade
      - Forte encriptação
      - Políticas complicadas de acesso
    - Sistemas simplificados para garantir desempenho

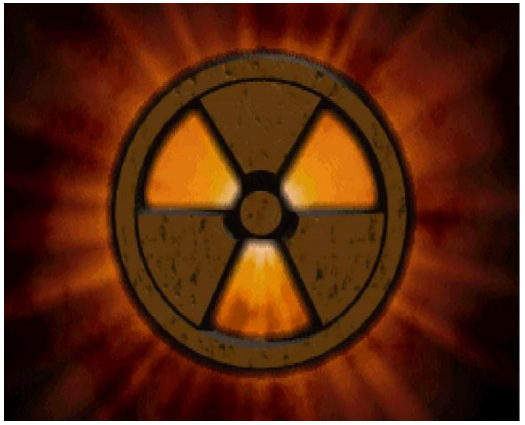
Desafios Sociais

- Desafios sociais igualmente grandes
  - Desconfiança dos usuários na tecnologia
    - Roubos e ataques
  - Dificuldades de padronização
    - Falta de acordo entre instituições
  - Privacidade de informação
    - Diferenças culturais na padronização
      - O que é privado e o que não é



Desafios Sociais

- Desafios sociais igualmente grandes
  - Segurança ou na verdade Falha
    - Bases Centrais de dados importantes
      - Ataques mais perigosos
      - Motivação para ataques
    - Instrumento de dominação de usuários
      - Acesso nas mãos de organizações
      - Governamentais ou não



Conclusão

- SGIs em ativo desenvolvimento atualmente
  - Muitos sistemas em produção
  - E prometem estar por mais alguns anos
- Necessidade de SGI
  - Computação/Internet ubíqua
    - O que pode ser compartilhado
    - Quem pode compartilhar
  - Serviços tendem a aumentar
    - Necessidade de Gerenciamento

Conclusão

- Problemas sérios
  - Integração
  - Interoperabilidade
  - Falta de um padrão utilizado por todos
    - Kantara

Perguntas

- Quais os tipos de modelos de SGI?

Perguntas

- Quais os tipos de modelos de SGI?
  - Centralizado, Federado e Centrado no Usuário

Perguntas

- Por que biometria não é largamente utilizado?

Perguntas

- Por que biometria não é largamente utilizado?
  - Geramente fácil de forjar, e implementações eficientes como scan de Iris são caras e intrusivas.

Perguntas

- Cite um desafio tecnológico relativo à sistemas de gerenciamento de identidade

Perguntas

- Cite um desafio tecnológico relativo à sistemas de gerenciamento de identidade
  - Ponto único de falha, onde a falha em um componente do sistema pode comprometer todo o sistema.

Perguntas

- Cite um desafio social relativo à sistemas de gerenciamento de identidade

Perguntas

- Cite um desafio social relativo à sistemas de gerenciamento de identidade
  - Problemas na unificação de definições devido a choques culturais, de opinião, etc.

Perguntas

- Cite um problema do modelo tradicional largamente utilizado atualmente

Perguntas

- Cite um problema do modelo tradicional largamente utilizado atualmente
  - Usuário necessita gerenciar cada identidade (rede social, sites de compras) separadamente, prejudicando a eficiência do conjunto.

Obrigado!