A necessidade de autenticação multi-fator

Emerson Ribeiro de Mello

Instituto Federal de Santa Catarina
campus São José
mello@ifsc.edu.br

GTER 45 | GTS 31
Florianópolis

23 de maio de 2018

Década de 80

Computadores pessoais, sejam bem vindos!

- Voltados para usuários residenciais
- Sistemas operacionais mais populares eram **monousuário**

Década de 90

Aplicações e interação na web

- Popularização da Internet comercial
- Serviços de e-mail gratuitos
- Interação entre usuários nas páginas web

Presente

Software como Serviço

- Aplicações, tradicionalmente dentro das redes locais, passam agora para a nuvem

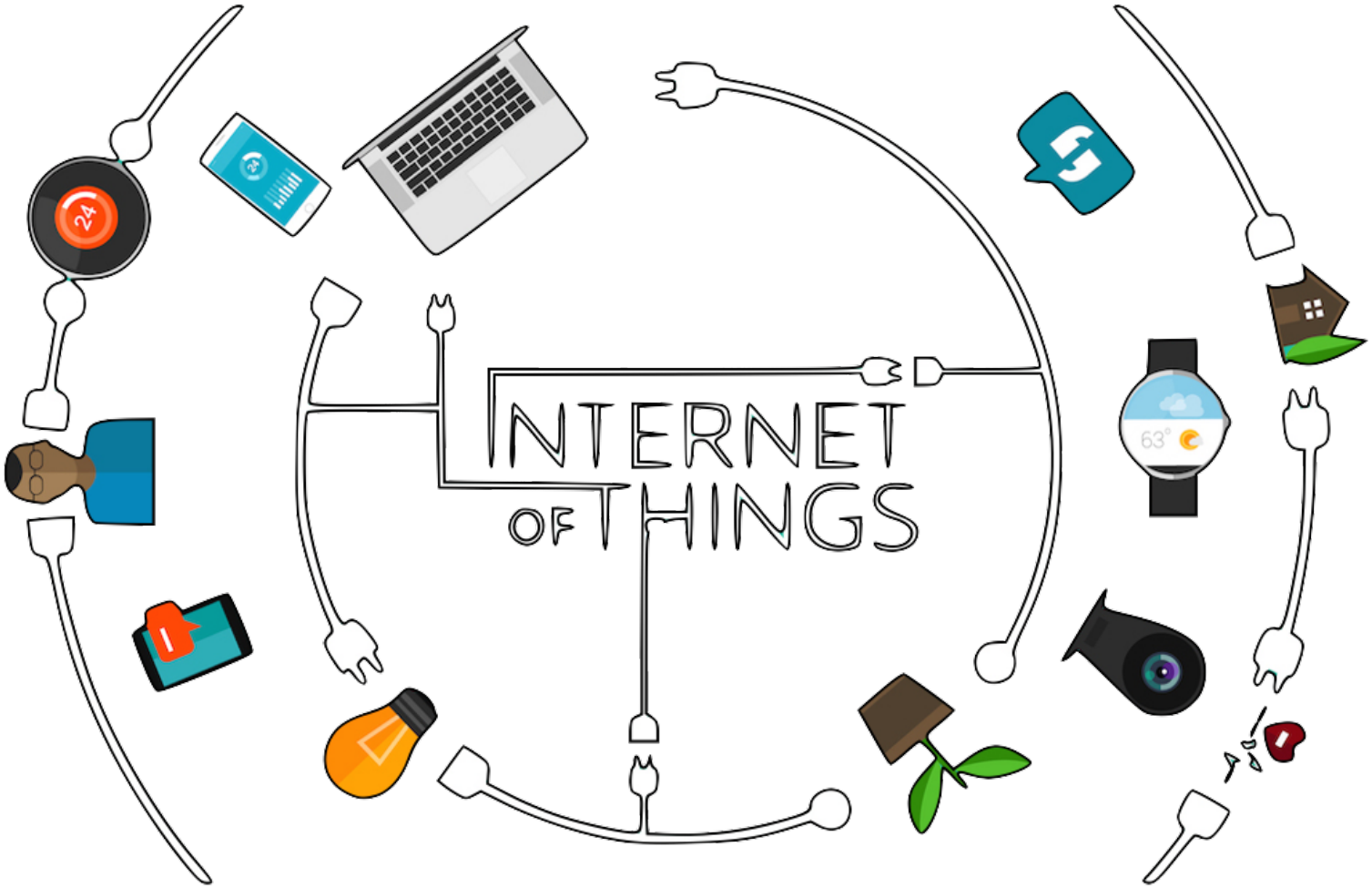
Presente

Dispositivos móveis

"Computação do século 21 será móvel e onipresente" – Mark Weiser, 1991

- Telefones inteligentes levaram a computação para o dia-a-dia dos usuários
- Atingiu pessoas que sequer usaram um computador

Internet das Coisas



Análise sobre o cenário atual

Dentro do contexto de gestão de identidade

- Grande parte das aplicações são acessadas remotamente
- Pessoas que nunca usaram um computador, agora interagem diariamente com sistemas de informação
- Dispositivos domésticos conectados à nuvem
- O par *username/password* ainda é a principal forma de autenticar usuários

Análise sobre o cenário atual

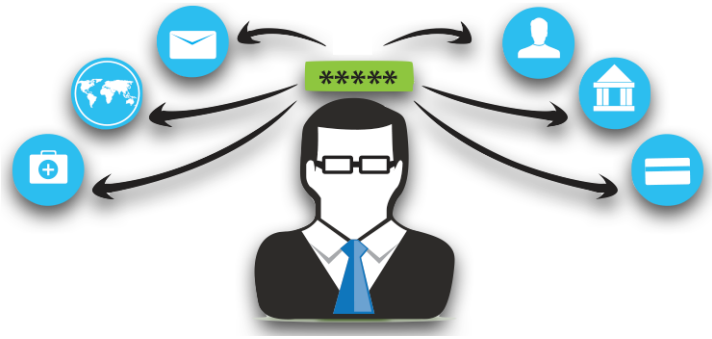
Dentro do contexto de gestão de identidade

- Grande parte das aplicações são acessadas remotamente
- Pessoas que nunca usaram um computador, agora interagem diariamente com sistemas de informação
- Dispositivos domésticos conectados à nuvem
- O par *username/password* ainda é a principal forma de autenticar usuários

Cenário perfeito para ataques de personificação e contra privacidade dos usuários

Como o usuário pode se identificar para usar um sistema?

Senha, aquilo que você sabe!

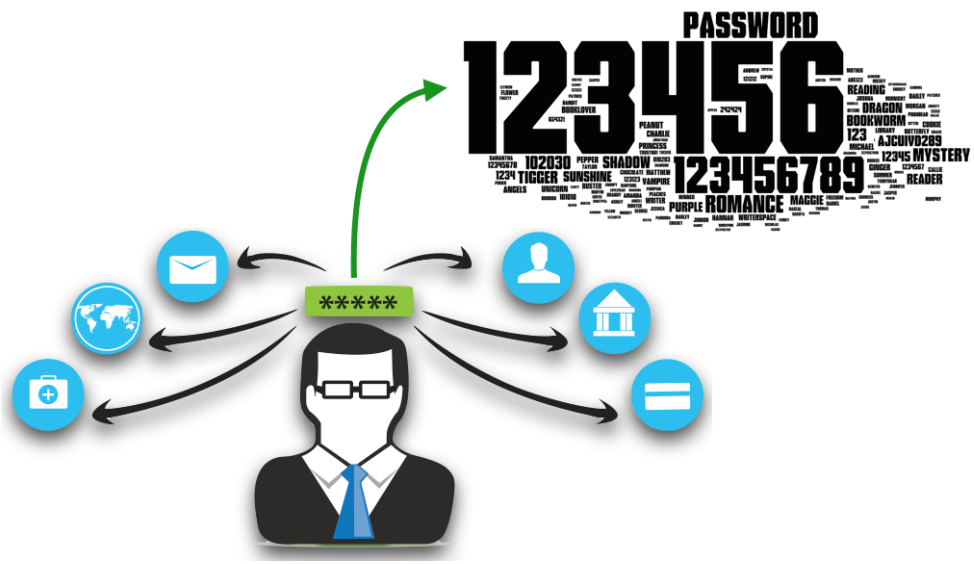


Qual abordagem seria mais interessante?

1. Usar a mesma senha em diferentes serviços
2. Usar um gerenciador de senhas
3. Usufruir do **modelo federado**
   - CAFe, Google, Facebook

Como o usuário pode se identificar para usar um sistema?

Senha, aquilo que você sabe!



Qual abordagem seria mais interessante?

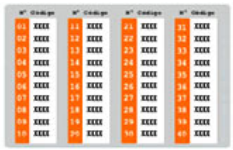
1. Usar a mesma senha em diferentes serviços
2. Usar um gerenciador de senhas
3. Usufruir do **modelo federado**
   - CAFe, Google, Facebook

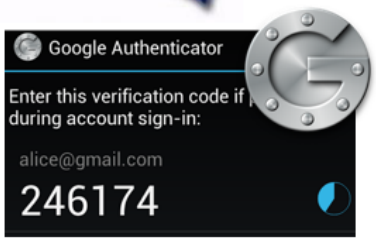
Como se proteger de senhas fracas ou interceptação?

"Senhas acabaram se tornando um pesadelo" – Fernando Corbató, 2014

Outras formas de autenticação

Fatores de autenticação





- **O que você sabe**
  - username/password, PIN
- **O que você possui**
  - chave privada, dispositivo móvel, token criptográfico
- **O que você é**
  - Impressão digital, íris, face e voz

Aumentando a robustez do processo de autenticação

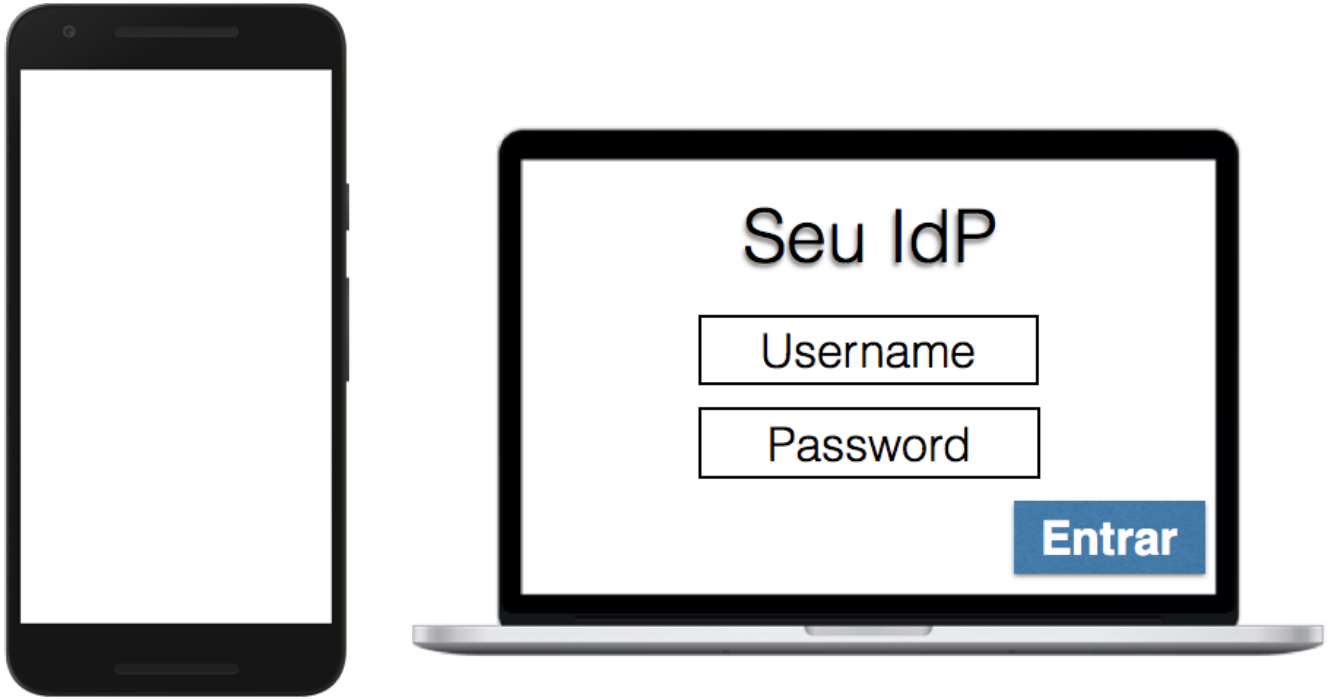
Autenticação multi-fator

Combinar dois ou mais fatores de diferentes categorias (sabe, possui ou é)

- Parte-se do pressuposto que o grau de dificuldade aumenta muito para comprometer mais de um fator
- **Aquilo que você sabe** poderia ser obtido por meio de um ataque de *phishing* – O atacante poderia estar em qualquer lugar no mundo
- Para comprometer **aquilo que você possui** o atacante precisaria ter acesso físico ao seu cartão, etc.

Senhas descartáveis (*One-Time Password* – OTP)

Usuário precisa abrir aplicativo no celular, olhar o número e digitar



Senhas descartáveis (*One-Time Password* – OTP)

Usuário precisa abrir aplicativo no celular, olhar o número e digitar

Senhas descartáveis (*One-Time Password* – OTP)

Usuário precisa abrir aplicativo no celular, olhar o número e digitar

O que seria um bom segundo fator?

Usabilidade x robustez

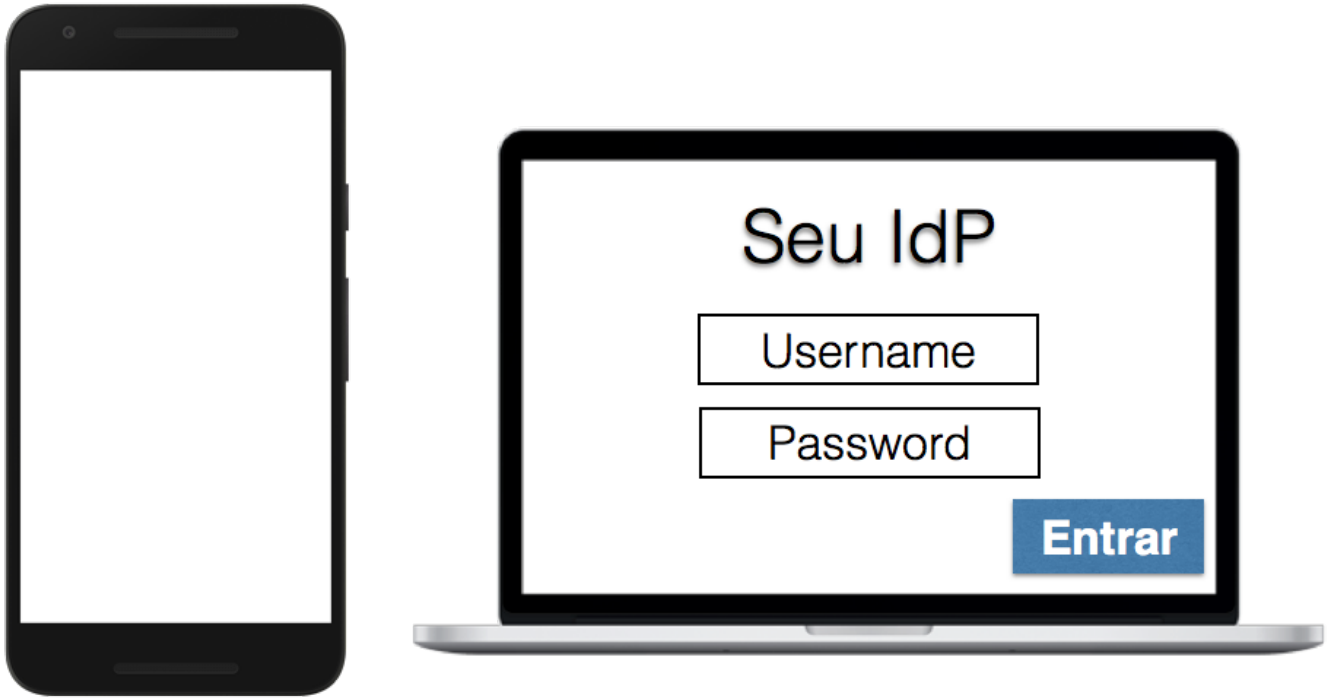
- **Senhas descartáveis com App ou token com display**
  - Usabilidade ruim
- **Senhas descartáveis por SMS**
  - Usabilidade ruim
  - Em 2016 *National Institute of Standards and Technology* (NIST) considerou como inseguro
- **Certificados digitais / cripto de chave pública**
  - Usabilidade ruim – leitor, instalação de driver, plugin no navegador
  - Meio de armazenamento da chave privada (i.e. arquivo no computador do usuário) pode enfraquecer sua robustez

Questões de pesquisa

1. Como **aumentar a robustez do processo de autenticação** sem que isso tenha um grande impacto na usabilidade?
2. Como as **soluções de autenticação** de usuário poderiam ser moldadas para **oferecer uma melhor experiência de uso em dispositivos móveis**, como os telefones inteligentes?

Diálogo de confirmação

Usuário não precisa abrir aplicativo, só precisar clicar em um botão para confirmar



Diálogo de confirmação

Usuário não precisa abrir aplicativo, só precisar clicar em um botão para confirmar

Diálogo de confirmação

Usuário não precisa abrir aplicativo, só precisar clicar em um botão para confirmar

FIDO Alliance – Fevereiro 2013

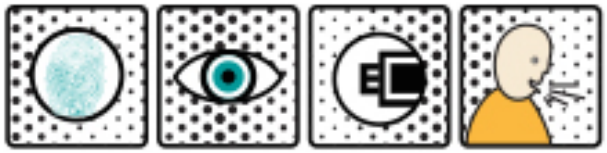
Mudar a forma de autenticação online

Lidar com a falta de **interoperabilidade entre dispositivos** de autenticação robustos, bem como o problema dos usuários de criarem e manterem **múltiplos nomes de usuários e senhas**

FIDO Alliance, qual a novidade?

Autenticação além de senhas ou mesmo OTP

- **Padrões abertos (sem royalties) para a indústria**
  - Protocolo criptográfico online
  - Interface modular nos clientes para métodos de autenticação



- **Facilidade de uso**
  - Dispositivos com leitores biométricos ou pendrive
  - Transposição da autenticação local para serviços online
- **Segurança e privacidade**
  - Criptografia de chave pública – par de chaves por serviço
  - Requer interação do usuário para destravar chave privada
  - Informações trocadas não permitem rastrear usuário, mesmo que serviços colaborem

Universal Authentication Framework – UAF

Experiência sem senha

Universal Second Factor - U2F

Experiência com segundo fator

Universal Second Factor - U2F

Experiência com segundo fator

Universal Second Factor - U2F

Experiência com segundo fator

Web Authentication (WebAuthn) - padrão W3C

Também conhecido como FIDO2

- Define uma API web para ser usada pelos navegadores
  - Em março de 2018 está como W3C Candidate Recommendation
  - Firefox já implementou e está em vias de aparecer no Chrome e Edge
- A autenticação do usuário poderá ser feita por pendrive ou telefone móvel e a comunicação com seu dispositivo (computador ou telefone) poderá se dar por USB, Bluetooth ou NFC

Consolidando conceitos

1. O aumento do número de serviços e uso de senhas faz com que usuários adotem estratégias ruins
   - Ex: *Poor man SSO*, 123456, data nascimento, ...

Consolidando conceitos

1. O aumento do número de serviços e uso de senhas faz com que usuários adotem estratégias ruins
   - Ex: *Poor man SSO*, 123456, data nascimento, ...
2. Autenticação com múltiplos fatores (senha, OTP, biometria) não é novidade e é bem usada em aplicações móveis
   - Usabilidade e soluções proprietárias são pontos negativos

Consolidando conceitos

1. O aumento do número de serviços e uso de senhas faz com que usuários adotem estratégias ruins
   - Ex: *Poor man SSO*, 123456, data nascimento, ...
2. Autenticação com múltiplos fatores (senha, OTP, biometria) não é novidade e é bem usada em aplicações móveis
   - Usabilidade e soluções proprietárias são pontos negativos
3. A adoção da WebAuthn pelos navegadores abrirão caminho para adoção de uma solução robusta, interoperável e amigável para o usuário

Obrigado!

Emerson Ribeiro de Mello
mello@ifsc.edu.br