Segurança do Serviço de Registro no .br

João Ricardo Petreli Jorge
joao@registro.br

Alguns fatos

- Abril de 2011 - PlayStation Network
  - 77 milhões de contas roubadas
- Junho de 2012 - LinkedIn
  - 6,5 milhões de contas roubadas
- Outubro de 2012
  - google.ie e yahoo.ie - DNS Hijacked
  - NIC.pe - 96 mil contas roubadas

Alguns fatos

- Novembro de 2012 - DNS Hijacked
  - .PK e .RO domínios: Google, Yahoo, Microsoft, PayPal e outros.
- Novembro de 2012 - NIC.gp
  - 12.721 contas roubadas

Dados do Registro.br

- 4 milhões de usuários
- 3,1 milhões de domínios
- 1,9 mil ASNs
- 100 mil blocos IP

- 500 mil domínios administrados via EPP
- 2,7 milhões de domínios administrados via ID

Tática Arquitetural de Segurança

Ataque → **Controlando a Segurança**

- **Resistência**
- **Detecção**
- **Recuperação**

Tática Arquitetural de Segurança

Controlando a Segurança

Resistir

- Autenticar usuários
- Autorizar usuários
- Confidencialidade dos dados
- Integridade dos dados
- Limitar exposição
- Limitar acesso

Detectar

- Mecanismos de detecção:
  - Padrões de acesso
  - Histórico de tráfego
  - Filtros
  - Registros / log
  - Endereços e portas

Recuperar

- Recuperando o estado:
  - Cópias de dados
  - Restauração dos dados
- Identificação do ataque:
  - Trilhas de auditoria

Armazenamento de Credenciais

- Texto simples (plaintext)
  - abcd1234
- Hash Criptográfico
  - x := h(p)
  - a770c42661e573d30f7ac40854a7979b4530cbd2
- Salted Hash
  - x := h(p || s)
  - xyzh-2acf93b5327f02e162995dbab9352e77558e0461

Armazenamento de Credenciais

- **Salted Adaptive Hash (Stretching)**
  - $x_i := h(x_{i-1} \| p \| s)$
  - **010d9f3283ff3dff-86cbd8fced5f199d2afc0d4aba165041c0fa98b5**
  - **Bcrypt, Scrypt, etc**
- **Encrypted Salted Adaptive Hash**
  - **Chave simétrica**
  - **OFB Mode**

Precauções

- Adaptive Hash Function
  - Negação de serviço (DOS)

- Promover o uso de senhas fortes
  - http://cartilha.cert.br/senhas

Rate Limit

- Todas as operações de autenticação passam por um Rate Limit
  - Endereço de origem
  - ID
- Algoritmo Token Bucket
- Estado armazenado no Redis

Autenticação de Dois Fatores

- Algo que você conhece
  - Senha ou frase
- Algo que você possui
  - Token via One-Time Password (OTP)
- Time-Based OTP (TOTP) - número sequencial temporal
  - RFC-6238
- HMAC-Based OTP (HOTP) - número sequencial
  - RFC-4226

Sistema de Autenticação

- **Servidor:**
  - **Autenticação desacoplada do frontend**
  - **API RESTful escrita em GO**
  - **Escuta em 3 portas diferentes**
  - **Ativação via Shamir's Secret Sharing**
  - **Persistência em BD Relacional**
  - **Credencias criptografadas**

Sistema de Autenticação

- Cliente do sistema de autenticação:
  - Escrito em C++
  - Chamadas REST efetuadas via libcurl
- Cliente de Ativação e Monitoração do servidor escrito em GO
- Todas as requisições são assinadas e criptografadas

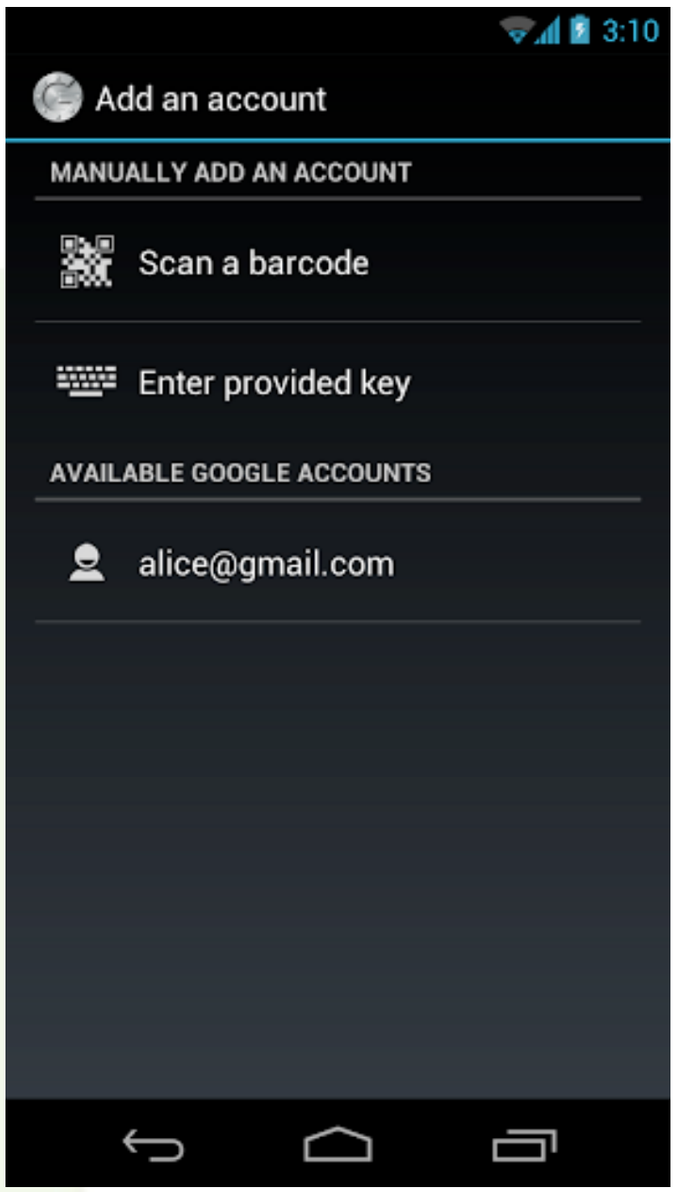
Interface RESTful

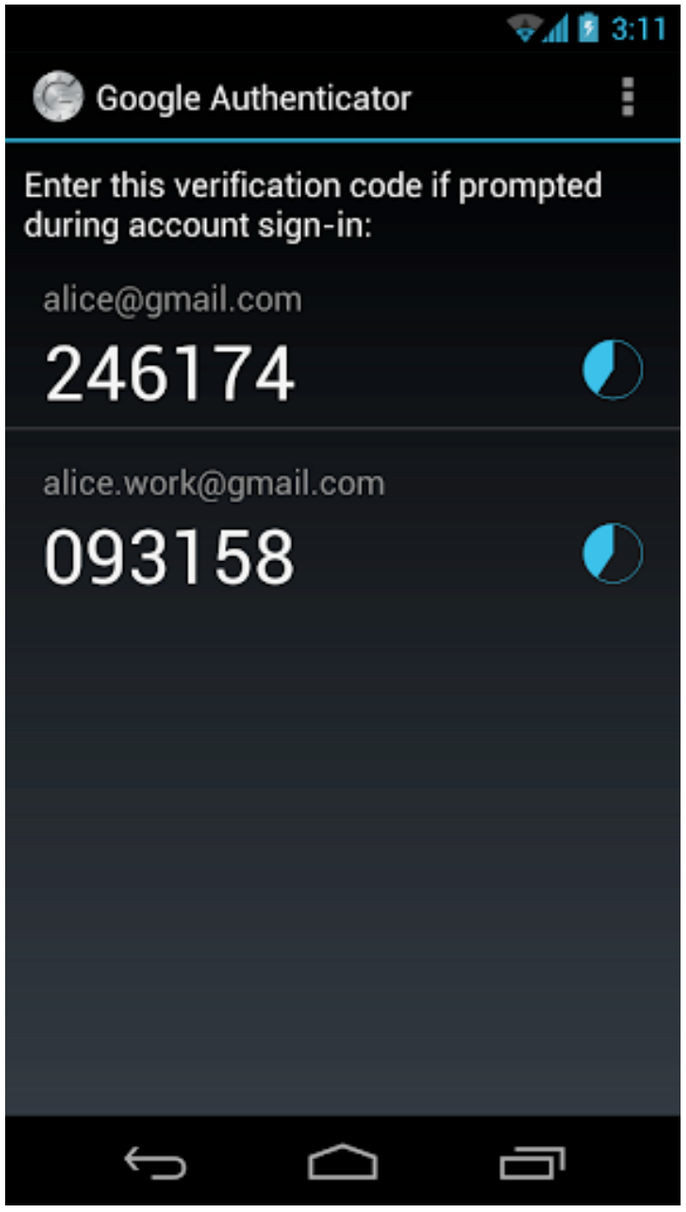
Autenticação de 2 Fatores	Senhas
PUT /otp/	PUT /pwd/<auth>
GET /secret/<id>	GET /pwd/<id>/<auth>
GET /otp/<id>/<auth>	DELETE /pwd/<id>
GET /hotp/<id>	
DELETE /otp/<id>	

Google Authenticator

- Disponível para:
  - Android
  - iOS
  - Windows Phone

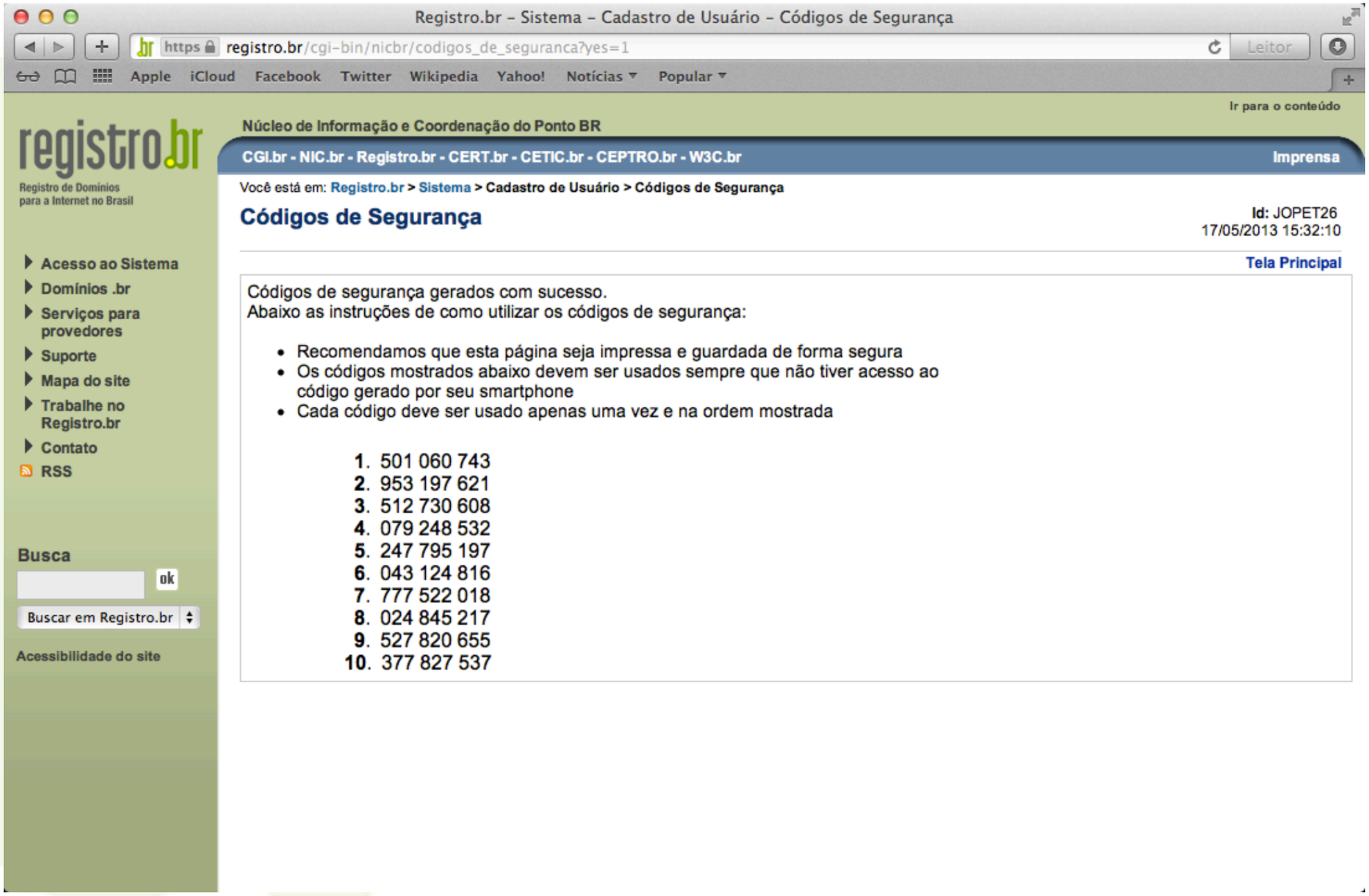
Google Authenticator





Ativando o Token

Ativando o Token



Obrigado!

Referências

- http://cartilha.cert.br/senhas/
- https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- http://en.wikipedia.org/wiki/PlayStation_Network_outage
- http://en.wikipedia.org/wiki/2012_LinkedIn_hack
- http://www.lucidity.ie/blog/166-google-ie-hijacked-not-hacked
- http://www.cyberwarnews.info/2012/10/20/peru-pe-domain-service-hacked-96000-credentials-leaked/
- http://www.computerworld.com/s/article/9234089/Attackers_hijack_the_.ro_domains_of_Google_Microsoft_Yahoo_others
- http://www.theverge.com/2012/11/24/3685334/pakistani-domains-hacked
- http://thehackernews.com/2012/11/guadeloupe-national-domain-registrar.html
- http://en.wikipedia.org/wiki/Token_bucket