Segurança do Serviço de Registro no .br

Diretoria de Serviços e de Tecnologia

Frederico A. C. Neves

CGI.br – Curitiba – 19/03/2013

Sistema de Registro

- Registro e administração dos domínios .br

- Alocação e administração de ASNs, blocos de endereços IPv4 e IPv6

- Base para o sistema de publicação DNS – direto/reverso
  - 6 cluster globais [a-f].dns.br
  - 19 copias anycast nos principais PTTs

Tamanho do problema
- 3.1M domínios
- 1.9K ASNs
- 100K blocos de endereços

500K domínios são administrados por contas em 60 provedores via protocolo EPP

Diretamente temos 2.7M objetos (domínios, ASNs e blocos) administrados por 1.4M contas

Comprometimentos em Sistemas de Credenciais no passado recente

Abril/2007 – PlayStation Network
http://en.wikipedia.org/wiki/PlayStation_Network_outage

Junho/2012 – LinkedIn
http://en.wikipedia.org/wiki/2012_LinkedIn_hack

Outubro/2012 – google.ie Sequestrado / nic.pe comprometido
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/

Novembro/2012 – [google|yahoo|apple|microsoft].[ro|pk] Sequestrados
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

Novembro/2012 – nic.gp comprometido
http://thehackernews.com/2012/11/guadeloupe-national-domain-registrar.html

Armazenamento de Credenciais

Texto simples
abcd1234
Assinatura Criptográfica (hash)
61ee8b5601a84d5154387578466c8998848ba089
Trivial de explorar com dicionários pré-computados, em poucas horas nas CPUs atuais (2M hashs/s)
Salted Hash
xyzh-7be44f960a49c4f7f4ad862be96904dbb91b20b7
Passível de se explorar com as GPUs atuais (350G hashs/s)
90% dos hashs do Linkedin foram quebrados com um equipamento destes
Salted Adaptative Hash
010d9f3283ff3dff-86cbd8fced5f199d2afc0d4aba165041c0fa98b5
Maior dificuldade de se adaptar GPUs devido ao algoritmo de seleção do tipo de hash, escolha, tamanho, e uso do sal e o número de iteraçõs. (PBKDF2, Bcrypt, Scrypt)
Salted Adaptative Hash Cifrado
Resultado do modo anterior cifrado com algoritmo simétrico em modo OFB com IV de boa qualidade.

Muito cuidado na escolha para não aplicar um auto DOS no sistema de verificação de credenciais.

Promoção das dicas sobre o uso de credenciais
http://cartilha.cert.br/senhas/
Frases senha, mesmo com tamanhos moderados – duas palavras 15 caracteres, tem ataque de força bruta reduzido em oito ordens de grandeza.

Autenticação com dois Fatores – 2FA

Algo que você sabe

- Usuario e Senha

Algo que você tem

- Token com credenciais de uso único

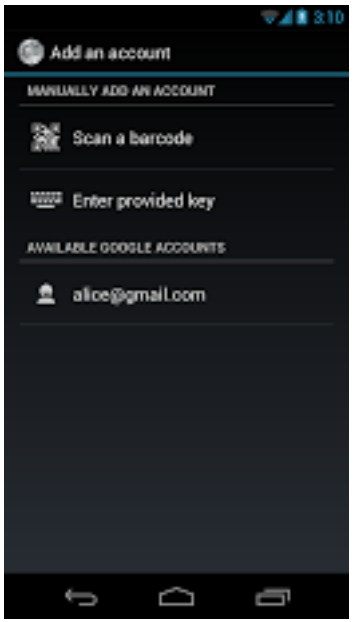
Tecnologia aberta desenvolvida no IETF

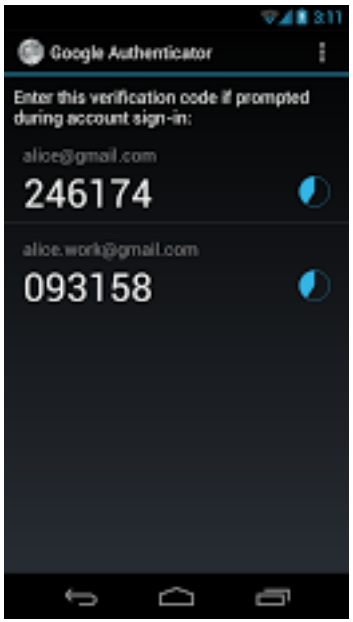
- HOTP/TOTP (RFCs 4226 e 6238)
- HMAC – Hash Based Message Authentication Code
- Chave Compatilhada
- HOTP número sequencial
- TOTP número sequencial baseado em intervalos de tempo
  - Origem (epoch 1/1/1970), intervalo de 30 segundos
- Estado com o último número de sequencia usado

- Servidor de autenticação com interface Restful – desacoplamento total (ASM)

Token App – Google Authenticator

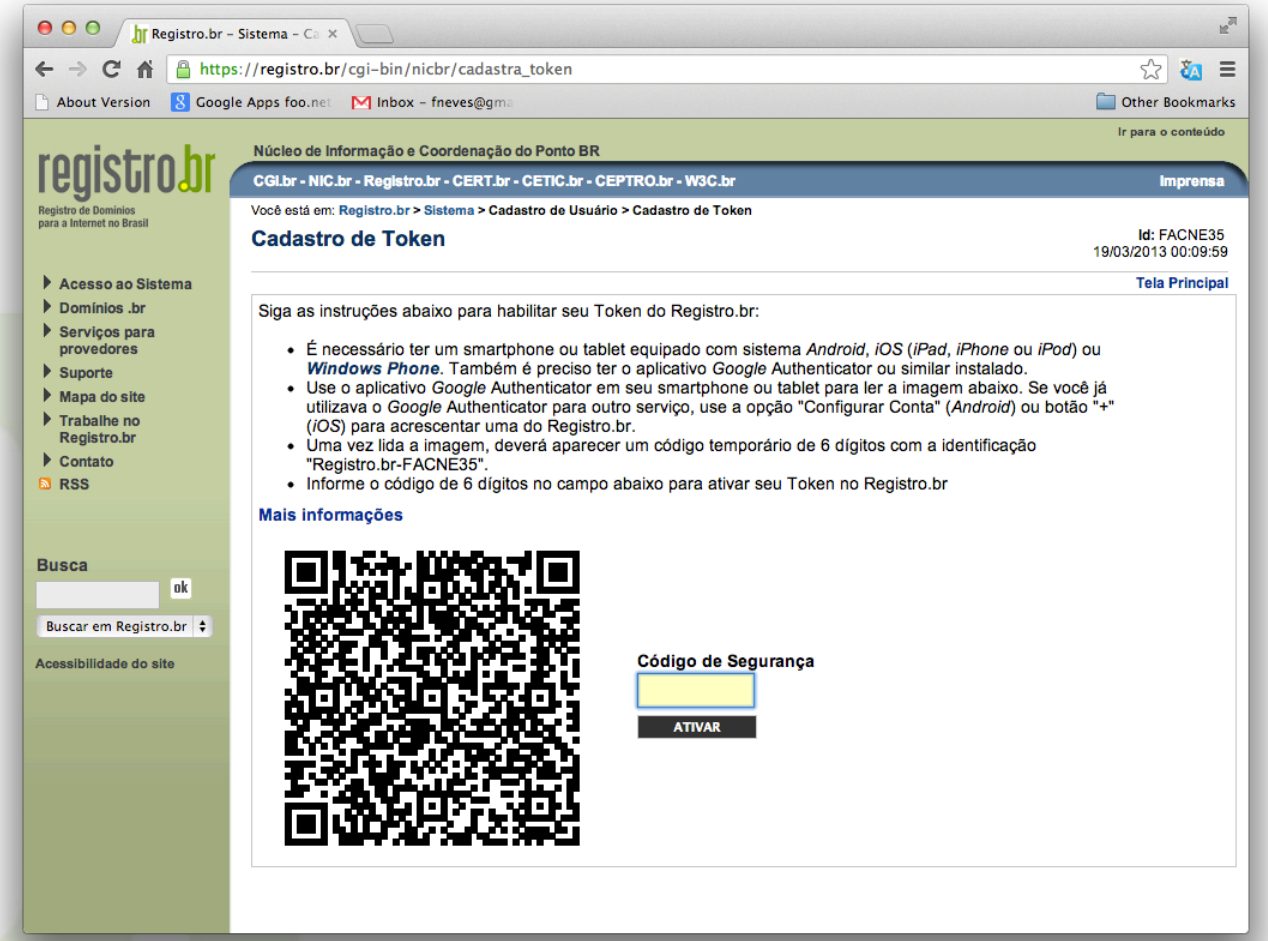
Implementações de boa qualidade
Android
iOS
Windows Phone (Authenticator)



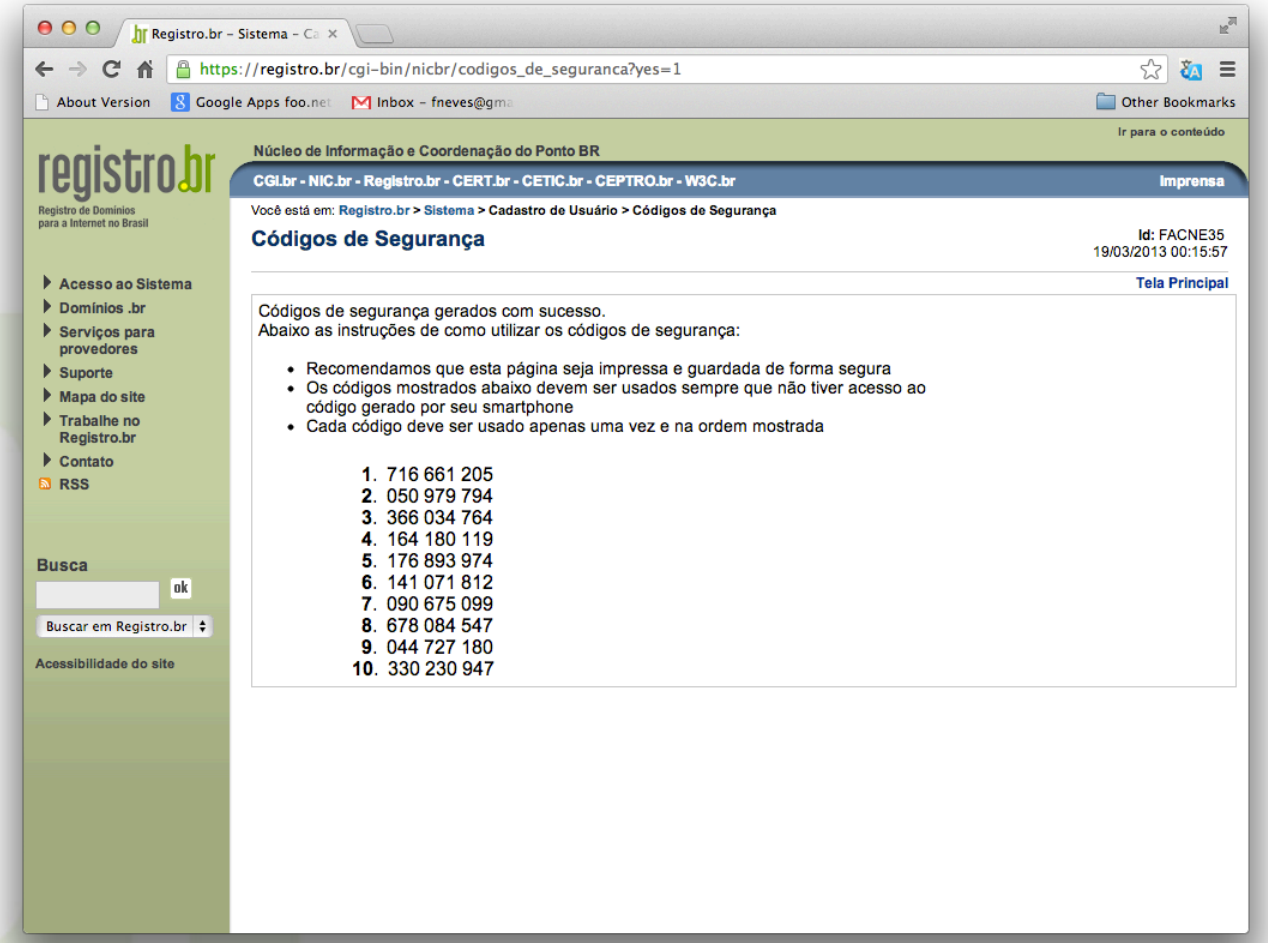


Provisionamento do Segredo Compartilhado

QR Code



Ativação seguida de HOTPs



Documentação

http://registro.br/suporte/token.html

http://registro.br/suporte/faq/faq10.html

Obrigado

Comentários/Perguntas?