Gestão de **senhas**, políticas e o mundo conectado: desafios e soluções

Ivo de Carvalho Peixinho
Perito Criminal Federal

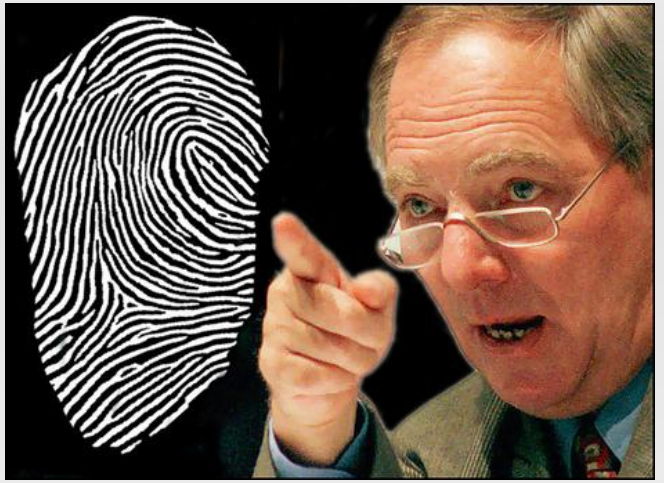
Agenda

1. Introdução
2. Ferramentas
3. Metodologia
4. Conclusões

Introdução

- Autenticação
  - Processo de **identificação** e **confirmação** (identidade digital)
  - Tipos
    - Algo que você sabe
    - Algo que você tem
    - Algo que você é

Introdução



- Autenticação
  - Algo que você é
    - Fatores biométricos
    - Alta segurança / Alto custo
    - Autenticação local (ex: *match-on-card*)
    - **Normalmente implementados em ambientes específicos de alta segurança**

Introdução

- Autenticação
  - Algo que você tem
    - *Tokens, smartcards*, celular, etc.
    - Possui custo de implementação (variado)
    - Certificados digitais (ICP-Brasil)

Introdução

- Autenticação
  - Algo que você sabe
    - **Senhas**, PIN, OTP, *passphrase*
    - Baixo custo
    - **Mais usado em *sites* WWW** (e outros)
    - Pode ser “adivinhado” (recursos x tempo)

Introdução

- Senhas
  - Como tornar mais seguro?
  - Política de senhas
    - Trocar a cada 3 meses
    - 8 caracteres ou mais
    - Símbolos, letras, números
    - Não anotar, bloqueio, etc.
    - *Passphrases?*

Introdução

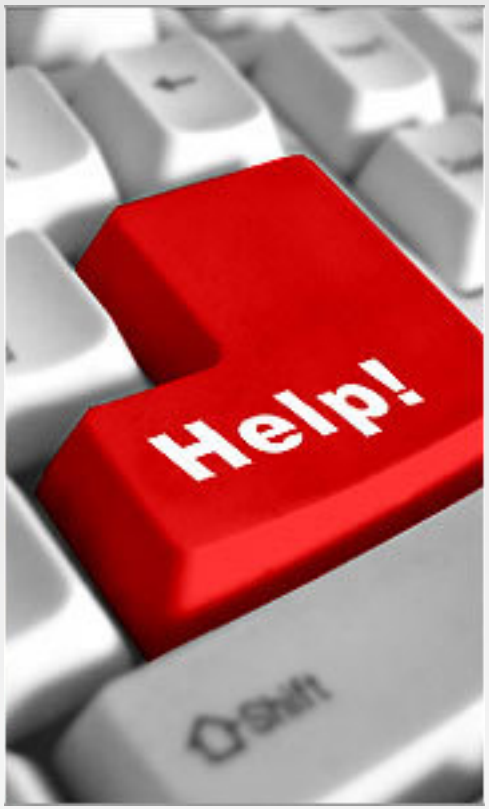
- Senhas
  - Trocar as senhas em caso de pânico?
    - **Microsoft investiga vazamento de senhas do Hotmail na web**
    - **Invasão do Twitter alerta para a segurança das senhas web** (fonte: terra)
  - Iniciar o processo de “decorar” uma nova senha
  - E se esquecer? Tem Backup?

Introdução

- Senhas
  - Quantas senhas um usuário comum normalmente tem que lembrar?
    - Trocar tudo a cada 3 meses?
    - Todas com 8 caracteres ou mais, símbolos e números?
    - Não pode anotar?
  - **Este modelo funciona?????**

Introdução

- "Bíblia das senhas seguras"
  1. Comprimento
  2. Composição (caracteres)
  3. Não palavras de dicionário
  4. Não escrever
  5. Não compartilhar
  6. Mudar com freqüência
  7. Não reutilizar as senhas entre *sites.*



Introdução

- "Bíblia das senhas seguras"
  - Sites diferentes tem políticas diferentes
  - Usuários tem uma média de 25 senhas
    - Média de reuso de 3.9
  - Memorizar senhas complexas é complicado para usuários
  - *Brute-force* de senhas *web* ineficiente
    - Um PIN de 6 dígitos suficiente

Introdução

- "Bíblia das senhas seguras"
  - Anotar senhas em um local seguro = OK (ex: wallet)
  - Mudar a senha só ajuda se for entre o tempo de comprometimento e o tempo de uso.
  - Senhas diferentes para sites diferentes aumentam em 3.9x a complexidade de gerenciamento

Introdução

- Técnicas para lembrar senhas (by Lusers)
  - Usar a mesma senha para tudo
  - Senhas óbvias (11111, qwerty, teste12, dicionário)
  - Fazer padrões para formação de senhas (ex: Ivo@MSN69)
  - Usar hax0r (1v0@I1nk3d1n)
  - Iniciais de frases (Ivaueoo!)

Introdução

- Senhas para NÃO usar

Introdução

- Complexidade de senhas

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Ferramentas

- Wallets
- Recursos de sistema operacional
- Browsers que guardam senhas
- Sites que guardam sua senha
  - https://lastpass.com/
- Chips TPM
- Questões
  - Que houve com o “keep it simple”?
  - Você confia em soluções “automáticas”?
  - Onde ficam as senhas, qual a segurança?

Ferramentas

Dropbox + KeePass

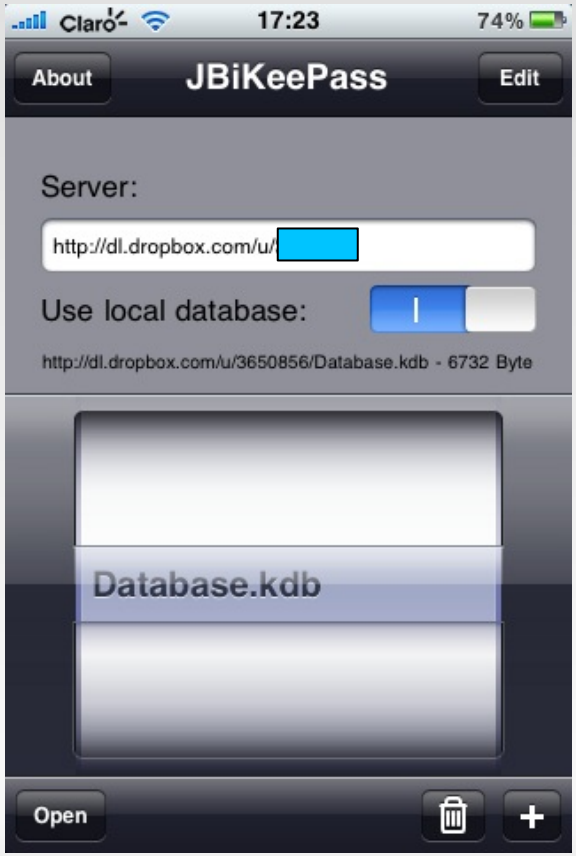
http://www.dropbox.com

http://www.keepass.info

Ou outros da sua preferência...

Ferramentas

- Dropbox
  - Gratuito (até 2GB)
  - Multiplataforma (smartphones)
  - Acessível de qualquer lugar (cloud)
- Keepass
  - Open Source
  - Multiplataforma
  - Integrável ao Dropbox
  - Plugins
  - AES256



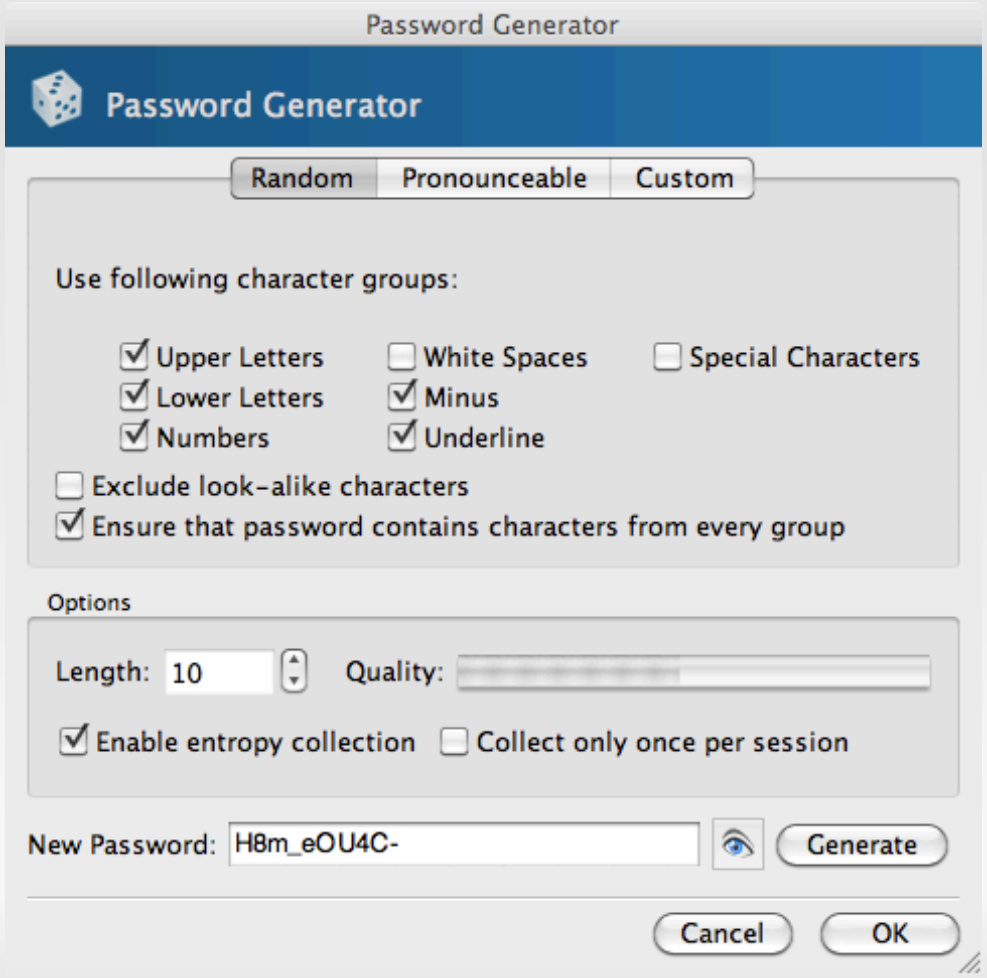
Metodologia

- Classificação em níveis de segurança
  - Máximo: banco, cartão de crédito, paypal, sites de compra com seu cartão.
  - Alto: e-mail corporativo, sistemas, VPN
  - Médio: skype, linkedin, twitter, facebook, etc. (ID theft)
  - Baixo: e-mail de SPAM, foruns, etc.

Metodologia

- Nível máximo: LEMBRE estas ☺ (ou use autenticação mais forte se possível)
- Crie um arquivo do keepass para cada um dos outros.
  - *Paranoia mode*: uma conta dropbox para cada nível.
- Senhas randômicas geradas pelo keepass
  - Nível de complexidade aceitável

Metodologia



Metodologia

- Lembre as senhas do dropbox e do keepass ☺☺
- Complexidade aceitável
  - Você pode precisar teclar a senha!
- Políticas de segurança
  - Hotmail não aceita espaços
  - Skype não aceita “/”
  - Senhas somente numéricas (eg: PIN)

Metodologia

- Problemas
  - Acessos em máquinas de terceiros
    - (Dropbox + keepass + firefox) portable
  - Copiar e colar do smartphone no PC ☺
  - Pacote de dados no smartphone
    - Sincronização dropbox
  - Suas senhas na “nuvem”
  - “todos os ovos num mesmo cesto”

Conclusões

- Senha é barato, mas o gerenciamento é caro
  - Algo mais forte pode ter TCO menor
- Lembrar senhas é inviável (25 em média)
- Necessita de um *breaktrough*
  - Internet smartcard?
  - Reconhecimento facial via webcam?
- É possível melhorar um pouco a situação com ferramentas gratuitas

Ivo de Carvalho Peixinho
Perito Criminal Federal
peixinho.icp @ dpf.gov.br