nic.br cgi.br | cert.br

CPBR9 – Campus Party Brasil 9
São Paulo, SP
28 de janeiro de 2016

Criptografia e Privacidade: aprendendo a usar PGP

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

cert.br nic.br cgi.br

Motivação para usar criptografia

- trocar e-mails cifrados
- cifrar arquivos no disco e/ou na nuvem
- cifrar conteúdos de *chats*

- assinar pacotes de software
- assinar código fonte

- conferir autenticidade de programas/códigos
- conferir autenticidade de e-mails
  - de amigos
  - de serviços que assinem mensagens com PGP, como Facebook

O Que é PGP / GnuPG

É um programa de criptografia

- pode ser integrado aos programas leitores de *e-mails*
- pode ser usado separadamente para cifrar outros tipos de informação, como arquivos

O que o PGP não é:

- um programa leitor de e-mail

PGP vs. GPG/GnuPG

- PGP foi a implementação original, que hoje é proprietária
- GPG/GnuPG é a implementação do padrão aberto definido na RFC 4880: "*OpenPGP Message Format*"

No dia-a-dia PGP e GPG são termos intercambiáveis

Antes de Começar: Links para instalar os programas para a parte Prática

Tutoriais online em:

https://ssd.eff.org/pt-br

- **Vá em Tutoriais e escolha o adequado para seu Sistema Operacional:**
  - **Como utilizar PGP para Linux**
  - **Como utilizar PGP para Mac OS X**
  - **Como utilizar o PGP para Windows**
- **Nas demonstrações utilizaremos MacOS X**
  - **GPG (GnuPG)**
  - **Thunderbird com o Complemento (Add-on) Enigmail**

O que é possível fazer com PGP/GPG

Confidencialidade – Cifrar arquivo/mensagem para

- **Protegê-la em trânsito**
- **Protegê-la armazenada no provedor ou no disco**

Autenticação – Assinar arquivo/mensagem para

- **Detectar modificação de seu conteúdo**
- **Permitir ao destinatário checar o autor/remetente e a integridade do arquivo/mensagem**

Chave PGP

É na verdade um par de chaves:

- **Pública**
  - **Distribuída livremente**
  - **Usada por terceiros para cifrar para você**
  - **Usada por você para checar assinaturas de terceiros**
- **Privada**
  - **Deve ser bem protegida**
  - **Não compartilhar com ninguém**
  - **Usada por você para:**
    - Decifrar mensagens
    - Assinar mensagens

Alertas

NÃO ESQUEÇA A PASSPHRASE!!

- Sem ela, perde-se o acesso à chave privada
- Não existe o conceito de “recuperar a senha”
- Emita um Certificado de Revogação enquanto sabe a *passphrase* – e guarde-o em local seguro

Faça *backup* do seu par de chaves

- Por exemplo: em um pendrive usado somente para isto e guardado em uma gaveta com chave
- O certificado de revogação pode ficar nele também

Colocando na Prática

cert.br nic.br cgi.br

Propriedades de Chaves PGP

Chaves são "sequências de *bits*"

- **Cada cópia/instância da chave privada é protegida por uma senha / *passphrase***
  - **Cada cópia/instância tem uma senha própria, que protege somente essa cópia**
  - **Alterar a senha em uma cópia/instância, não altera a senha nas demais instâncias**

***Fingerprint* – identifica unicamente um par de chaves**

Outras Características do Uso de PGP

- **Não há Autoridade Certificadora**
- **A confiança nas chaves é construída pelos próprios usuários**
  - **Através da verificação do *fingerprint***
    - **Via telefone, cartão de visita, *key-signing parties,* etc**
  - **Via cadeia de confiança, através da assinatura de chaves que tenham sido verificadas**
- **Uma mensagem cifrada para vários destinatários, conterá nela a informação de todas as chaves usadas**
  - **Mesmo de quem estiver em `BCc (CCo)` na mensagem**

Obrigado

www.cert.br

cristine@cert.br jessen@cert.br @certbr

28 de janeiro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br