Curso de Extensão em Tecnologias Microsoft

INF0998 Programação segura (segurança de software)

Atividades práticas de criptografia aplicada

As seguintes ferramentas são usadas ao longo das tarefas destes playbooks:

- Cryptool Online https://www.cryptool.org/en/cto
- Cryptool para Windows https://www.cryptool.org/en/ct1
- JCryptool https://www.cryptool.org/en/jct/
- OpenPGP, GPG4win e Kleopatra https://www.openpgp.org/software
- OpenSSL (Usar o openssl da sua distribuição Linux preferida)

Atividades com o OpenPGP/Kleopatra

Usar Kleopatra para encriptar/decriptar arquivos

Esta atividade deve ser preferencialmente realizada com o Kleopatra na máquina hospedeira.

1. Abrir o Kleopatra e ativar o menu *File → Sign/Encrypt*.
2. Na janela de seleção de arquivos, escolher o arquivo Lenna.png (usado anteriormente). Pode escolher outro arquivo de sua preferência.
3. Na janela de encriptação/assinatura, escolher a opção *Encrypt with password*. Desativar a opção *Sign* e a opção *Encrypt to others*. Observar onde será gravado o arquivo de saída (extensão .pgp). Clicar no botão *Encrypt*.
4. Escolher uma senha fácil de lembrar para este exemplo. Ela será necessária na decriptação. Digitar a senha na janela de senha. Digitar a senha novamente. A encriptação prosseguirá.
5. Verificar a janela de saída do resultado da operação. Clicar no botão *Finish*.
6. Realizar o processo de decriptação pela opção de menu *File → Decrypt/Verify*.

Opcionalmente, o aluno pode repetir a tarefa com outras opções. Por exemplo, com assinaturas digitais, com chaves públicas para vários destinatários ou ainda a encriptação de pastas.

Criação de um par de chaves para encriptação

Na janela do Kleopatra, selecionar a opção de menu *File → New Key Pair* para criar um par de chaves RSA para encriptação.

Na janela *Create key pair wizard*, clicar na opção *Create a personal OpenPGP key pair*. Na janela, dar um nome para o par de chaves. Por exemplo, Bob RSA ou outro nome de sua preferência.

Clicar em *Advanced Settings*. Selecionar RSA (+RSA) de 3072 para encriptação e assinatura. Clicar em OK. Clicar em Next.

Na janela, selecionar *show details*. Visualizar os detalhes do par de chaves. Clicar no botão *Create*. Digitar e repetir uma senha para proteção da chave privada. Por exemplo, nesse exercício, a senha pode ser 1234. O par de chave é criado. Clicar em *Finish*.

Criar mais dois pares de chaves: Ana com DSA e Carlo com ECDSA e a curva ed25519.

Encriptando com o padrão do PGP

Esta atividade usa o Kleopatra para visualizar o formato de encapsulamento de mensagens usado pelo OpenPGP.

1. Na área de bloco de notas (notepad) do Kleopatra, escrever um texto de teste qualquer, por exemplo, o conteúdo do arquivo textoclaro.txt da tarefa anterior (ou outro arquivo txt de sua preferência). (Dica: os atalhos de teclado CTRL-C e CTRL-V funcionam no bloco de noras do Kleopatra).
2. No Kleopatra, clicar no botão “Bloco de notas Assinar/Encriptar” se já houver um destinatário.

3. A aba/guia “Destinatários”, escolher um destinatário (e a chave pública do destinatário). Criar um par de chaves se necessário chamado Beto (senha: 1234). Escolher Beto e opção OpenPGP. Clicar em Next. A encriptação foi bem-sucedida.
4. No Kleopatra, clicar no botão “Bloco de notas” e selecionar a opção *Decrypt/Verify*. O Kleopatra vai pedir a senha do Beto para acessar a chave privada (senha: 1234). A decriptação é bem-sucedida. Clicar em *Finish*.

Inspeção de certificados digitais no Kleopatra

Acessar o aplicativo Kleopatra e clicar no botão Certificados. A lista de certificados é mostrada na região central da janela da aplicação. Certificados digitais são estruturas de dados em que uma identidade é associada ou vinculada a uma chave pública por meio de uma assinatura digital de um terceiro confiável. Quem confia no terceiro, também confia que a a chave pública contida no certificado pertence a entidade cuja identidade está indicada no certificado.

Escolher um certificado da lista e clicar com o botão direito do mouse e selecionar a opção *Details* para abrir os detalhes do certificado e seu par de chaves. Observar as informações do par de chaves, tais como expiração, validade, tipo e fingerprint.

Clicar no botão *More Details*. No caso de certificados para assinatura digital, observar que as chaves ECDSA de 512 bits podem ser usada para confecção e verificação de assinaturas digitais. Elas também podem ser usadas no acordo de chaves ECDH. Fechar as janelas de detalhes.

Voltar a lista de certificados. Escolher um certificado com chaves RSA, clicar com o botão direito do mouse e selecionar a opção *Details* e depois em *More Details* para exibir os detalhes do par de chaves. Observar as informações do par de chaves e explicar em que ela é diferente do anterior. Fechar as janelas de detalhes.

Assinatura digital ECDSA no Kleopatra

Para iniciar o processo de confecção da assinatura digital, clicar no botão Sign/Encrypt e seguir os passos:

1. Na janela de seleção de arquivo, escolher o arquivo CancaoDoExilio.txt. Clicar em *Open*.
2. Na janela de *Sign/Encrypt*, desmarcar a opção *Encrypt*, marcar a opção *Sign as* e escolher a chave privada de “Ana Alice” na caixa de seleção.
3. Clicar no botão *Sign/Encrypt* e digitar a senha 1234 na janela de digitação de senha.
4. A assinatura foi bem-sucedida e está no arquivo CancaoDoExilio.txt.gpg, que está localizado na mesma pasta do arquivo CancaoDoExilio.txt.

Para iniciar o processo de verificação da assinatura digital, clicar no botão *Decrypt/Verify*. Na janela de seleção de arquivos, escolher o arquivo CancaoDoExilio.txt.gpg. Clicar em *Open*. A verificação acontecerá automaticamente e será bem-sucedida. Analisar as informações apresentadas sobre a verificação. Fechar a janela sem salvar.

Opcionalmente, criar um par de chaves para o RSA e repetir o processo de assinatura e verificação com esse par de chaves.

Encriptação da chave de sessão

Esta atividade usa o software Kleopatra para ilustrar o funcionamento dos sistemas criptográficos híbridos com a encriptação assimétrica da chave de sessão simétrica.

A encriptação com chave de sessão serve para encriptar o mesmo texto claro uma única vez para múltiplos usuários. Para iniciar o processo de encriptação com chave de sessão, clicar no botão Sign/Encrypt e seguir os passos:

1. Na janela de seleção de arquivo, escolher o arquivo CancaoDoExilio.txt. Clicar em *Open*.
2. Na janela de *Sign/Encrypt*, marcar a opção *Encrypt for others*, e escolher a chave pública de todos os usuários (Por exemplo, Ana, Beto, Bob, Carlo, etc.).
3. Clicar no botão *Sign/Encrypt*.
4. A encriptação com chave de sessão está no arquivo CancaoDoExilio.txt.gpg, que está localizado na mesma pasta do arquivo CancaoDoExilio.txt. Clicar no botão *Finish*.
5. Renomear o arquivo para não sobrescrever o original: CancaoDoExilio2.txt.gpg.

Para iniciar o processo de decriptação, clicar no botão Decrypt/Verify. Na janela de seleção de arquivos, escolher o arquivo CancaoDoExilio2.txt.gpg. Clicar em *Open*.

A decriptação acontecerá automaticamente para as chaves privadas já instaladas. Digitar a senha se for solicitado. Clicar em *Save All* para decriptar e salvar uma cópia do arquivo.

Sistema criptográfico com autenticação e sigilo

Esta atividade usa o software Kleopatra para ilustrar o funcionamento dos sistemas criptográficos com a encriptação e assinaturas digitais.

Para iniciar o processo de encriptação e assinatura digital, clicar no botão *Sign/Encrypt* e seguir os passos:

6. Na janela de seleção de arquivo, escolher o arquivo CancaoDoExilio.txt. Clicar em *Open*.
7. Na janela de *Sign/Encrypt*, marcar a opção *Encrypt for me*, e escolher a chave pública Encriptação de Bob (criada no exercício anterior).
8. Ainda na janela de *Sign/Encrypt,* marcar a opção *Sign as* e escolher a chave privada de “Ana Alice” na caixa de seleção.
9. Clicar no botão *Sign/Encrypt* e digitar a senha 1234 (senha fraca, apenas para o exemplo de aula) na janela de digitação de senha.
10. A encriptação com assinatura foi bem-sucedida e está no arquivo CancaoDoExilio.txt.gpg, que está localizado na mesma pasta do arquivo CancaoDoExilio.txt. Clicar no botão *Finish*.

Para iniciar o processo de decriptação com verificação da assinatura digital, clicar no botão *Decrypt/Verify*. Na janela de seleção de arquivos, escolher o arquivo CancaoDoExilio.txt.gpg. Clicar em *Open*.

A verificação da assinatura acontecerá automaticamente e será bem-sucedida. Clicar em *Save All* para decriptar com a chave privada de Bob.