Ferramentas criptográficas

Sumário:

- PKI(Infra-estrutura de Chave Pública);
- A necessidade de confiança;
- Sistemas de criptografia híbrida; e
- Estenografia.

Ferramentas criptográficas

A concretização da criptografia por IT's consiste na aplicação de ferramentas criptográficas que incorporam as habilidades para esconder mensagens sensíveis, verificar o seu conteúdo e as identidades dos seus remetentes.

Ferramentas criptográficas

Tais ferramentas incluem:

- Assinaturas digitais;
- Certificados digitais;
- Infra-estrutura de Chave Pública;
- Sistemas de criptografia híbrida; e
- Estenografia

PKI

- Objectivo: facilitar o uso da Criptografia assimétrica;
- Definição: é um sistema integrado de software, metodologias de encriptação, protocolos, acordos legais, e serviços de terceiros que permite a comunicação segura de utilizadores;
- É baseado nos criptossistemas de chave pública e inclui **Certificados digitais (CD)** e **Autoridades de certificação (AC).**

PKI

- Fornece as tecnologias necessárias para viabilizar os processos de verificação de identidade e revogação de identidade presentes na certificação cruzada (XC);
- Os certificados digitais permitem aos programas de computador validar a chave e identificar a quem ela pertence;
- O PKI torna os CD's verificáveis por aplicações;

PKI

- Isso permite às aplicações implementarem várias das características chaves de segurança de informação e integrar estas características aos processos de negócio dentro da organização;
- Estes processos incluem: **Autenticação; Integridade, Privacidade, Autorização e não-repúdio.**

Componentes da PKI

Componentes da PKI

- Autoridade de Certificação (AC) – a entidade que emite, gere, autentica, assina e revoga certificados digitais dos usuários, o qual contém o *username*, chave pública, e outra informação de identificação;
- Autoridade de Registo (AR) – entidade que opera, sob colaboração na base de confiança da AC, funções do dia-a-dia tais como verificar a informação de registo, gerar chaves de usuários finais, revogar e validadar certificados destes.

Componentes da PKI

- Directórios de certificado – local central para o armazenamento de CD's que fornece um único ponto de acesso para a admnistração e distribuição;
- Protocolos de gestão – organizam e gerem as comunicações entre AC's, AR's e usuários finais;
- Políticas e procedimentos – assistem a organização na aplicação e gestão de CD's, na formalização dos deveres legais e restrições, e na utilização do negócio actual.

Componentes do PKI

- Proprietário da certificação – a entidade que solicita o cerificado;
- Parte dependente – o sujeito ou usuário que utiliza (e por isso depende) o certificado.

Processos da PKI

- Quando é estabelecida uma PKI, os seguintes processos devem ter lugar, embora não necessariamente, na ordem listada:

1. Os pares de chaves para AC´s devem ser gerados;
2. Os pares de chaves para os usuários devem ser gerados;
3. Os usuários devem solicitar certificados;

Processos da PKI

4. Identidades dos usuários deve ser verificada;
5. Pares de chaves dos usuários deve ser verificada;
6. Os certificados devem ser produzidos;
7. Os certificados devem ser verificados;

Processos da PKI

8. Os certificados devem ser removidos ou actualizados (quando necessário); e
9. Os certificados devem ser revogados quando necessário.

A necessidade de confiança

- Como vimos antes, as chaves são geradas externamente (Porquê?);
- Outra pergunta óbvia é se as chaves devem ser geradas pela AC ou por outra TTP;
- Em 1991, surge a primeira versão de um pacote de software chamado *Pretty Good Privacy* (PGP)

A necessidade de confiança

- O PGP empregava RSA para autenticação de usuários e distribuição de chave simétrica e um algoritmo de criptografia simétrica chamado IDEA para a confidencialidade;
- Qualquer utilizador pode agir como um AC para qualquer outra pessoa - isso ficou conhecido como a Web de abordagem Trust;
- Funciona em redes com poucos usuários.

A necessidade de confiança

- Uma outra possibilidade para a remoção da necessidade de uma AC é permitir que o valor de chave pública de um utilizador seja completamente determinado pela sua identidade;
- Em 1984, Shamir propõe o conceito de chave pública baseada-na-identidade (CP-BI);
- Apenas em 2001 surgem os algoritmos, um por Boneh e Franklin e o outro projectado pelo CESG (Grupo de Segurança Electrónica e de Comunicações do Reino Unido).

A necessidade de confiança

- CP-BI possuem um corpo central universalmente confiável que calcula a chave privada para a chave pública de cada usuário e entrega-lhos;
- CP-BI representa uma alternativa interessante para a abordagem PKI tradicional;
- CP-BI não é prático quando há roubo de identidade;

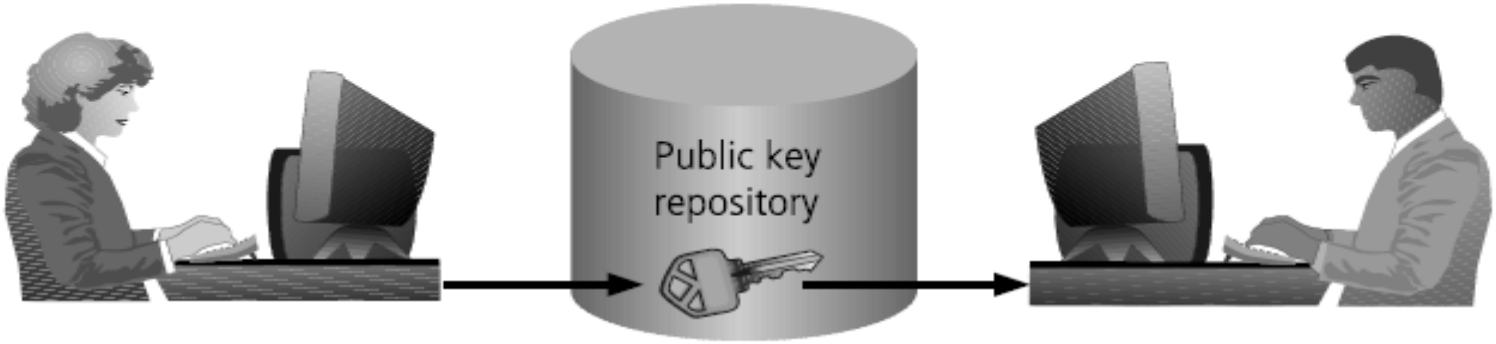
A necessidade de confiança

- Uma solução seria deixar a chave pública do usuário depender de sua identidade e outra variável de conhecimento público, tal como a data;
- Isto assegura que a chave privada do usuário seja trocada a cada dia, mas pode produzir uma carga de trabalho inaceitável para o centro.

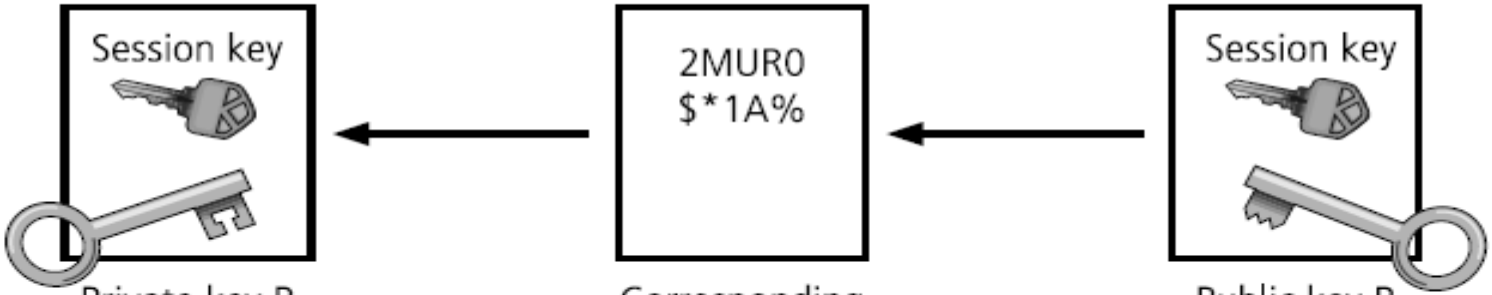
A necessidade de confiança

- Há pessoas que argumentam que a melhor maneira de abordar a segurança é concentrar o maior número de riscos em um único local (AC) e, em seguida, fornecer o máximo de segurança naquele ponto;
- Se você confiar na AC o suficiente para gerar suas chaves, então, assim você pode confiar nele para gerenciá-los em seu nome;
- Isto é conhecido como a **abordagem centrada - no-servidor.**

Sistemas de Criptografia híbrida



Rachel at ABC Corp. stores her public key where it can be accessed. Alex at XYZ Corp. retrieves it and uses it to encrypt his session (symmetric) key. He sends it to Rachel, who decrypts Alex's session key with her private key, and then uses Alex's session key for short-term private communications.



Esteganografia

- **vem do grego**: *steganós* – oculto + *graph(ein)* – escrever;
- **Definição** – é arte ou ciência que permite esconder um dado conteúdo dentro de um outro conteúdo.

Esteganografia

- **Objectivo:** permitir que um dado conteúdo sensível possa ser ocultado dentro de outro conteúdo aparentemente inocente e que aparenta estar correcto.
- Um exemplo mais actual consiste em ocultar conteúdos dentro de figuras digitais ou outras imagens.

Obrigado.