Segurança Informática e nas Organizações

Resumos
2016/2017

João Alegria | 68661

Capítulo 4

Gestão de chaves assimétricas

Problemas a resolver

- **Assegurar uma geração apropriada dos pares de chaves**
  - Geração aleatória de valores secretos
  - Aumentar eficiência sem reduzir a segurança

- **Assegurar um uso apropriado dos pares de chaves assimétricas**
  - Uso / conhecimento exclusivo das chaves privadas
    - para impedir o repúdio das assinaturas digitais
  - Distribuição correta das chaves públicas
    - para assegurar confidencialidade
    - para assegurar uma correta validação de assinaturas digitais

- **Evolução temporal das relações entidade <-> par de chave**
  - Para lidar com situações catastróficas (ex: perda da chave privada)
  - Para lidar que requisitos operacionais normais (ex: refrescamento de pares de chaves para reduzir riscos de personificação)

Cuidados a ter

- **A chave privada deve ser gerada pelo próprio**
  - Para assegurar ao máximo a sua privacidade
  - Este princípio pode ser relaxado se não pretender assinaturas digitais

- **Uso correto**
  - A chave privada representa o próprio
    - o seu comprometimento tem de que ser minimizado
    - cópias de salvaguarda fisicamente seguras
  - O caminho de acesso à chave privada deveria ser controlado
    - proteção com senha ; correção das aplicações que a usam

- **Confinamento**
  - Salvaguarda e uso da chave privada num dispositivo autónomo (ex: smartcard)
    - O dispositivo gera pares de chaves
    - O dispositivo apenas envia para o exterior a chave pública - e nunca a privada
    - O dispositivo cifra / decifra dados com a chave privada

Distribuição de chaves públicas

- **Distribuição aos remetentes de dados confidenciais**
  - Manual
  - Usando um segredo partilhado
  - Distribuição *ad hoc* usando certificados digitais
    - a distribuição *ad hoc* consiste na possibilidade de importação de uma chave pública, a partir de vários repositórios públicos. Para isso é preciso garantir que a cópia importada é correta, ou seja, que é mesmo a chave pública da entidade pretendida. Essa garantia é realizada a partir de certificados digitais.

- **Distribuição aos receptores de assinaturas digitais**
  - Distribuição *ad hoc* usando certificados digitais

Certificados Digitais de Chaves Públicas

A certificação digital consiste na emissão de certificados digitais de chaves públicas. Os certificados são documentos com uma estrutura predefinida que possuem, entre outros elementos, uma chave pública de uma dada entidade e uma assinatura digital do certificado feita pela entidade emissora do mesmo.
Os certificados são documentos com um tempo de validade limitado. Esse tempo pode ser controlado de duas formas: através de um prazo de validade não alterável indicado no próprio certificado e através de certificados de revogação.

- **Documentos emitidos por uma Entidade Certificadora (EC)**
  - Certification Authority (CA)
  - Associam uma chave (pública) a uma entidade
    - pessoa, servidor, serviço
  - São documentos públicos
    - não contêm informação privada, apenas pública
  - São criptograficamente seguros
    - assinados digitalmente pelo emissor

- **Úteis para a distribuição confiável de chaves públicas**
  - O recetor do certificado pode validar o mesmo
    - usando a chave pública da CA
  - Se confiar no assinante (CA) e a assinatura estiver correta, pode confiar na chave pública certificada
    - como a CA confia na K+ certificada, se confiar em KCA+ pode confiar em K+

Padrão X.509v3	PKCS #6	Formatos Binários	Outros formatos
• Campos obrigatórios - versão; sujeito (nome da entidade a quem a chave pertence); chave pública e respetivo algoritmo; datas (de emissão, de validade); emissor (nome da entidade emissora de certificado); assinatura; número de série • Extensões	• Extended-Certificate Syntax Standard	• ASN.1 - DER, CER, BER • PKCS #7 - Cryptografic Message Syntax Standard • PKCS #12 - Personal Information Exchange Syntax Standard	• PEM (Privacy Enhanced Mail) • Codificação de X.509 em base64

Entidades Certificadoras

- **Organizações que gerem certificados**
  - Definem políticas e mecanismos para:
    - Emitir / Revogar / Distribuir certificados
    - Emitir e distribuir as chaves privadas correspondentes
  - Gerem listas de revogação de certificados

- **CAs confiáveis**
  - CAs para as quais se possui uma chave pública confiável
    - Âncora de confiança
      - Normalmente concretizada através de certificados autoassinados (ou autocertificados, sujeito=emissor)
    - Distribuição manual das suas chaves públicas
      - ex: nos navegadores (Internet Explorer, Netscape, etc…)
  - CAs certificados por outras CAs
    - Certificados de chave públicas de CAs ; Hierarquias de certificação

Renovação de Pares de Chaves Assimétricas

- **Os pares de chaves devem ter um período de validade limitado**
  - Porque as chaves privadas podem-se perder / ser descobertas
  - Para lidar com políticas de alteração regular de chaves assimétricas

- **Problema**
  - Os certificados podem ser reproduzidos sem qualquer controlo
  - Não se conhece o universo de detentores de um certificado que pretende eliminar
    - portanto, não se podem contactar para eliminar determinados certificados

- **Soluções**
  - Certificados com prazos de validade
  - Listas de revogação de certificados
    - para certificados revogados antes do termo do seu prazo de validade

Lista de Certificados Revogados (CRL)

- Criado para facilitar a renovação de pares de chaves assimétricas.

É uma lista disponibilizada publicamente por uma PKI X.509v3 com todos os seus certificados que foram revogados e cujo prazo de validade ainda não expirou. Esta lista contém, para cada certificado revogado, uma entrada que possui informação relevante sobre o mesmo, a razão para a sua revogação e a data da mesma.

- **Certificate Revocation Lists**
  - base ou delta

- **São listas assinadas de identificadores de certificados revogados antecipadamente**
  - Devem ser consultadas regularmente pelos detentores de certificados
  - Protocolo OCSP para certificados X.509 individuais (RFC 2560)
  - Podem indicar a justificação da revogação

- **Manutenção e divulgação das CRL**
  - Cada CA mantém e permite a consulta da sua CRL
  - As CAs trocam listas entre si para facilitar o conhecimento das CRL

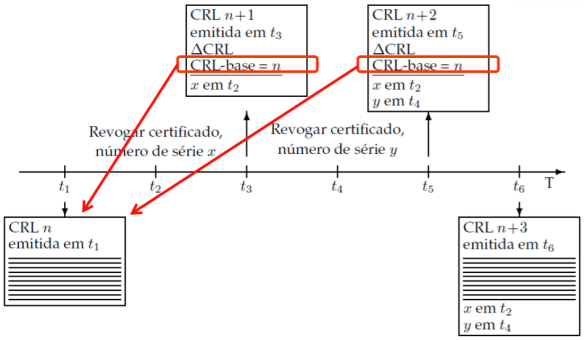
- **Distribuição das CRL**
  - ***Distribuição integral***

  - É fornecida a lista completa de certificados revogados e não expirados relativos a uma PKI numa dada data.
  - Numa distribuição integral, uma CRL mais recente anula completamente uma CRL mais antiga.

  - ***Distribuição parcial***

  - São fornecidas CRL parciais, denominadas delta CRL, criadas com base numa CRL completa de referência.
  - DELTA CRL: possuem apenas entradas relativas a certificados que entraram ou sairam da CRL de referência. Sabendo esta última, é possível ir mantendo atualizada uma lista própria de certificados de revogação atualizando a mesma com as entradas da última delta CRL.

  ➡ As principais diferenças entre os elementos que constituem uma CRL completa e uma delta CRL é que esta última pode referir a remoção de entradas (ou seja, de certificados de revogação) e tem sempre de referir o identificador da CRL completa de referência.



Desvantagem: A principal desvantagem do CRL é que pode criar uma grande sobrecarga enquanto o cliente pesquisa sobre a lista de revogação

OCSP - Online Certificate Status Protocol

Protocolo simples de pergunta-resposta onde é questionado o certificado a consultar através do seu número de série.
A principal vantagem é o cliente poder consultar o estado de um único certificado, em vez de descarregar e analisar uma lista inteira (menos sobrecarga para cliente e rede).
A principal desvantagem é que os pedidos são enviados para cada certificado, devido a isso pode haver uma sobrecarga sobre o OCSP Responder para sites de alto tráfego.

PKI - Public Key Infrastructure

- **Infra-estrutura de apoio ao uso de chaves públicas**
  - Criação segura de pares de chaves assimétricas
  - Criação e distribuição de certificados de chaves públicas
  - Definição e uso de cadeias de certificação
  - Atualização, publicação e consulta de listas de certificados revogados
  - Uso de estruturas de dados e protocolos que permitem a inter-operação entre componentes

PKI - Exemplo: Políticas do Cartão Cidadão

Inscrição
- Em locais próprios, pessoal

Vários pares de chaves por pessoa
- Um para autenticação
- Uma para assinaturas qualificadas
- Ambos gerados dentro do cartão, não exportáveis
- Ambos requerem um PIN em cada operação

Uso autorizado dos certificados
- Autenticação
  - SSL Client Certificate, Email (Netscape cert. type)
  - Signing, Key Agreement (key usage)
- Assinatura
  - Email (Netscape cert. type)
  - Non-repudiation (key usage)

Caminho de certificação
- raiz bem conhecida e amplamente divulgada
  - GTE Cyber Trust Global Root
- CA raiz PT debaixo da GTE
- CA raiz CC debaixo de CA raiz PT
- CAs Autenticação CC e Assinatura CC debaixo CA raiz CC

CRLs
- Certificados de assinatura pré-revogados por omissão
  - A revogação é removida se o dono do CC explicitamente requerer o uso de assinaturas digitais
- Todos os certificados são removidos a pedido do dono
  - Mediante a apresentação de um PIN de revogação
- Os pontos de distribuição das CRL estão explicitamente indicados em cada certificado

PKI - Exemplo: Políticas do Cartão Cidadão

- **Um PKI estabelece relações de confiança de duas formas**
  - Emitindo certificados de chaves públicas de outras CAs
    - abaixo na hierarquia; ou não relacionadas hierarquicamente
  - Requerendo a certificação da sua chave pública a outras CAs
    - acima na hierarquia; ou não relacionadas hierarquicamente

- **Relações de confiança características**

Hierárquicas	Cruzadas	*Ad-Hoc*
	A certificação cruzada é uma forma prática de lidar com o problema de validação de certificados pertencentes a hierarquias de certificação diferentes. A certificação cruzada consiste na emissão recíproca de certificados de chaves públicas entre duas EC, tipicamente duas EC raiz.	A distribuição ad-hoc consiste na possibilidade de importação de uma chave pública, em caso de falta da mesma, a partir de vários repositórios públicos. Para que tal seja possível, é preciso garantir que a cópia importada é correta, ou seja, que é mesmo a chave pública da entidade pretendida. Essa garantia de correção é dada através de um processo de certificação digital.