Segurança e Auditoria de Sistemas

Criptografia

Criptografia

- Criptografia:
  - resumo criptográfico;
  - assinatura digital;
  - certificado de chave pública;
  - infraestrutura de chaves públicas.

Resumo criptográfico

- Um resumo criptográfico (cryptographic hash)
  - Sequência de bytes de tamanho pequeno e **fixo**
    - (algumas dezenas ou centenas de bytes)
  - Gerado a partir de um conjunto de dados de tamanho variável.
    - usados para identificar um arquivo ou outra informação digital,
    - ou para atestar sua integridade:
  - Caso o conteúdo de um documento digital seja modificado, seu resumo também será alterado.

Resumo criptográfico

- Colisão = entradas diferentes geram saídas iguais.
- Propiedades esperadas:
  - Minimizar colisão.
  - Espalhamento
    - Modificação em partes especificas da entrada gera modificação em diversas partes na saída.
  - Sensibilidade
    - Pequena alteração na entrada gera grande alteração na saída
- Algoritmos mais conhecidos: MD5 e o SHA1
  - Comandos no Linux md5sum e sha1sum

Assinatura digital.

- Assinatura digital
  - Mecanismo para verificar a autoria e integridade.
  - Usa criptografia assimétrica e resumos criptográficos.
  - Assinatura digital s(d,u) é documento d assinado por u
    - $S(d,u) = \{hash(d)\}_{kv(u)}$
    - Se $hash(d) = \{S\}_{kp(u)}^{-1}$ documento esta correto e foi assinado por U

Certificado de chave pública

- A identificação confiável do proprietário de uma chave pública é fundamental.
- chave pública é uma mera sequência de bytes
  - não permite a identificação direta de seu proprietário
- Certificados digitais = associação chaves públicas e proprietários.
  - Ex: certificados PGP e X.509

Certificado de chave pública

- Certificados digitais:
  - A chave pública do proprietário do certificado;
  - Identidade do proprietário do certificado
    - (nome, endereço, e-mail, URL, número IP e/ou outras informações que permitam identifica-lo unicamente);
    - Pode ser: usuário, sistemas que precisem ser identificados.
  - Outras informações:
    - período de validade do certificado, algoritmos de criptografia e resumos preferidos ou suportados, etc.;
  - Uma ou mais assinaturas digitais do conteúdo
    - emitidas por entidades confiáveis pelos usuários.

Infraestrutura de chaves públicas.

- Todo certificado deve ser assinado por alguma entidade confiável do usuário.
- Essas entidades são as Autoridades Certificadoras (AC ou CA – Certification Authorities).
- **Problema**:
  - como garantir que uma chave pública realmente pertence a uma dada autoridade certificadora?

Infraestrutura de chaves públicas.

- Solução:
  - basta criar um certificado para essa AC, assinado por outra AC ainda mais confiável.
  - Formar uma estrutura hierárquica de certificação,
    - AC de ordem mais elevada (denominada **AC raiz**) assina os certificados de outras ACs
  - Esta estrutura de certificação se chama Infra-estrutura de Chaves Públicas (ICP ou PKI - Public-Key Infrastructure)
    - A chave pública da AC raiz **deve** ser conhecida de todos e
    - é considerada **íntegra**