UNIDADE 3 – AUTENTICAÇÃO, AUTORIZAÇÃO E CERTIFICAÇÃO DIGITAL
MÓDULO 1 – SISTEMA AAA, CRIPTOGRAFIA SIMÉTRICA

01

1 – INTRODUÇÃO E CONCEITOS BÁSICOS

O processo de identificação de usuários, autenticação, autorização e auditoria é fundamental para garantir a segurança de aplicações e serviços, de modo que somente usuários previamente cadastrados, identificados e autenticados podem ter acesso aos recursos computacionais que lhes foram autorizados pelo responsável.

Para nivelar o conhecimento e permitir o entendimento de alguns assuntos, serão apresentados conceitos básicos sobre criptografia e certificação digital.

Antes de entrar no assunto, tente responder às perguntas abaixo.

- **O que você entende por processo de identificação e autenticação?**

A identificação é sinônimo de autenticação e significa o processo de validação das credenciais de uma pessoa, processo de computador ou dispositivo.

- **O que é autorização?**

A autorização é o processo de conceder acesso a certas informações, serviços ou funcionalidade a uma pessoa, processo de computador ou dispositivo.

- **O que você entende por auditoria?**

A auditoria é o processo de coleta da informação relacionada à utilização de recursos de rede pelos usuários.

02

2 – SISTEMA AAA

O processo de controlar o acesso, garantindo que a origem dos dados é a de quem alega ser, é um dos objetivos da autenticação.

Garantir o uso autorizado de recursos e o registro de todas as atividades dentro de um sistema são tarefas dos sistemas conhecidos por **AAA**:

- Autenticação,
- Autorização e
- Auditoria.

Resumidamente, podemos dizer que o Sistema AAA consiste de:

1) **Autenticação** (*Authentication*) é um mecanismo de identificação do usuário.	2) **Autorização** (*Authorization*) é um mecanismo de validação de privilégios.	3) **Auditoria** (*Account*) é um mecanismo de gerar registros das ações do usuário.

Neste módulo, serão apresentados os protocolos e técnicas para trabalhar com cada um desses três As.

03

2.1- Autenticação

Autenticação é algo que você sabe, por exemplo:

1) Mecanismo de senhas e suas variações. Exemplo: OTP, Passphrases etc.

2) O mais simples de implementar.

3) O menos seguro, por limitação do usuário.

3.1) É algo que você tem, por exemplo: Smartcards, chips, token etc.

3.2) É algo que você é, por exemplo: Biometrias (impressão digital, formato da íris, voz, face etc.).

A **autenticação** é um processo que tem por objetivo garantir que um usuário é realmente quem diz ser.

Esse é um processo básico e fundamental quanto tratamos de segurança de sistemas e serviços, pois basta um usuário usurpar as credenciais de outro usuário que possui maiores privilégios para ser gerado um grave incidente de segurança.

04

O processo de autenticação em geral se baseia em **três princípios básicos** para permitir ao usuário provar a sua autenticidade:

1) Algo que você sabe

Nesse princípio, o sistema solicita ao usuário que informe algo que somente aquele usuário sabe. O exemplo mais comum desse princípio são as senhas e suas variações (OTP e *passphrases*). Saiba+ 1

2) Algo que você tem

Aqui o usuário deve apresentar algo para o sistema que lhe foi dado no momento em que se registrou para obter acesso ao sistema. Dessa forma, ao reapresentar o mesmo objeto, o usuário estaria comprovando que é realmente quem diz ser. Saiba+ 2

3) Algo que você é

Aqui o usuário deve apresentar algo para o sistema que lhe foi dado no momento em que se registrou para obter acesso ao sistema. Dessa forma, ao reapresentar o mesmo objeto, o usuário estaria comprovando que é realmente quem diz ser. Saiba+ 3

Saiba+ 1

Apesar de ser o mais barato de implementar, pois pode ser implementado inteiramente via *software*, em geral é o menos seguro, pois um atacante pode tentar adivinhar a senha de um usuário. Como o cérebro humano é limitado, os usuários tendem a escolher senhas fáceis de lembrar.

Saiba+ 2

Normalmente, são combinados com uma senha (chamada de PIN-Personal Identification Number ou Número de Identificação Pessoal), de modo que não possa ser usado caso seja roubado. Nessa categoria, são muito comuns os smartcards, chips e tokens. São considerados mais seguros que o primeiro, pois para um usuário se passar por outro, deve obter o objeto que o identifica e a senha correspondente.

Saiba+ 3

Essas são consideradas as formas mais seguras de autenticação, pois envolvem uma característica intrínseca ao usuário. Em geral são chamadas de biometrias.

Alguns exemplos: impressões digitais, formato da íris, voz, face etc. Apesar de consideradas seguras, devem ser utilizadas de forma cuidadosa, pois o seu uso indiscriminado pode criar uma falsa sensação de segurança. Um leitor de impressões digitais pode ser enganado com uma impressão digital falsa, caso não tenha um dispositivo que garanta que o dedo em questão é "vivo". Ou o mesmo leitor, caso esteja controlando uma porta, pode ser arrancado do seu lugar e a porta aberta por uma mera junção de dois fios.

05

2.2- Autorização

O usuário obtém acesso somente aos recursos previamente definidos pelo gestor do sistema. A autorização corresponde a um processo seguinte à autenticação, no qual o usuário obtém acesso aos recursos de acordo com o nível de acesso que lhe foi designado por um administrador ou gestor. Dessa forma, uma vez corretamente identificado, o usuário pode ter acesso a determinados recursos.

2.3- Auditoria

A auditoria, por fim, corresponde ao processo de **verificação contínua** se os acessos concedidos estão corretos e se não há acessos indevidos. Normalmente temos um auditor que periodicamente verifica as trilhas de auditoria, que são registros feitos pelos sistemas de autenticação e autorização, contendo todos os acessos realizados pelos usuários do ambiente.

Através de um processo consistente de AAA, podemos ter um ambiente com um nível de segurança adequado, sem comprometer a integridade, a confidencialidade e a disponibilidade dos sistemas.

A seguir, iremos considerar a **autenticação com base em senhas**, visto que é a autenticação mais comum e possível de se implementar via *software*.

Antes, porém, de iniciarmos outro assunto, verifique a seguir o que você aprendeu sobre o que acabamos de estudar.

- **Quais são os princípios básicos em que se baseia o processo de autenticação em geral?**

Algo que você sabe. Algo que você tem. Algo que você é.

- **O que é autorização?**

Processo seguinte à autenticação, onde o usuário obtém acesso aos recursos de acordo com o nível de acesso que lhe foi designado por um administrador ou gestor.

06

3 – CRIPTOGRAFIA

Neste momento veremos a **criptografia simétrica**, também conhecida por criptografia convencional. Em outra etapa do nosso estudo, veremos a criptografia assimétrica, criptografia por chaves pública e privada e, por fim, o Algoritmo de Hash: os cinco fundamentos para um bom algoritmo de Hash.

Esconder seus segredos sempre foi um dos grandes desafios da humanidade. Os antigos generais precisavam transmitir informações para seus exércitos sem o perigo de ter suas mensagens interceptadas e traduzidas pelo inimigo. O uso da criptografia apareceu, possivelmente, nas primeiras guerras da antiguidade e seu primeiro relato de uso na história é atribuído a Cesar, imperador de Roma.

Basicamente, um **processo criptográfico** envolve a aplicação de três conceitos elementares:

1) a mensagem/texto,

2) o algoritmo e

3) a chave.

A **mensagem** consiste, pura e simplesmente, na informação que se deseja transmitir de forma segura.

O **algoritmo** é a forma que será utilizada para cifrar e decifrar uma mensagem.

A **chave**, em alguns modelos computacionais, pode ser entendida como o segredo compartilhado que deve ser conhecido apenas pelas duas partes envolvidas no processo de comunicação.

07

A garantia da confidencialidade está em esconder do atacante o algoritmo ou a chave utilizada.

Um esquema de codificação criptográfica consiste em uma **tupla** (M, C, K, E e D) com as seguintes propriedades:

1) M: é um conjunto conhecido como espaço de texto comum (plaintext).

2) C: é um conjunto conhecido como espaço de texto cifrado (ciphertext).

3) K: é um conjunto conhecido como espaço de chave.

4) E: é uma família de funções de codificação criptográficas tal que E_k:M->C.

5) D: é uma família de funções de decodificação criptográficas tal que D_k:C->M.

O algoritmo criptográfico define a forma como a mensagem será cifrada e decifrada. A definição prévia do algoritmo pelas partes envolvidas (transmissor e receptor) é um dos fatores fundamentais no processo de comunicação seguro.

Os algoritmos criptográficos podem ser divididos em dois grandes grupos:

1) algoritmos simétricos ou de chave secreta e	2) algoritmos assimétricos ou de chave pública.

08

4 – Criptografia Simétrica

A **criptografia simétrica** utiliza a mesma chave para criptografar e descriptografar uma informação.

Essa chave tem de ser compartilhada entre o emissor e o receptor da informação. Entretanto, o uso de criptografia simétrica dificulta o gerenciamento de chaves e não permite a autenticação e o não repúdio do remetente.

Vantagens:	Desvantagens:
•1) Velocidade alta e algoritmos rápidos. •2) Facilidade de implementação em hardware. •3) Chaves pequenas e simples geram cifradores robustos.	•1) Dificuldade do gerenciamento das chaves. •2) Não permite a autenticação. •3) Não permite o não repúdio do remetente.

Imagine a seguinte situação: um usuário A deseja conversar de forma criptografada com um usuário B. Para tal, ele precisa de um algoritmo e de uma chave. Se ele usa criptografia simétrica, a chave para A cifrar a mensagem e B decifrar é a mesma. Agora imagine que A deseja conversar com um usuário C. Para essa nova conversa, haveria a necessidade de uma nova chave, pois se A usar a mesma chave que usa com B, o próprio B poderia decifrar as mensagens. Dessa forma, se estivermos conversando com 100 pessoas, necessitaríamos de 100 chaves diferentes. Rapidamente percebemos que a solução de criptografia simétrica não estende bem, pois quando crescemos o número de usuários envolvidos, a gerência das chaves se torna inviável. Para procurar resolver esse problema de gerenciamento de chaves, foi criada a **criptografia assimétrica**, que veremos no próximo módulo.

Atualmente o algoritmo simétrico recomendado é o AES-256, que utiliza chaves de 256 bits.

09

RESUMO

Foi visto que o processo de identificação de usuários, autenticação, autorização e auditoria é fundamental para garantir a segurança de aplicações e serviços, de modo que somente usuários previamente cadastrados, identificados e autenticados podem ter acesso aos recursos computacionais que lhes foram autorizados pelo responsável.

Resumidamente, podemos dizer que o Sistema AAA consiste de:

1) Autenticação (Authentication) que é um mecanismo de identificação do usuário.

2) Autorização (Authorization) é um mecanismo de validação de privilégios.

3) Auditoria (Account) é um mecanismo de gerar registros das ações do usuário.

O processo de controlar o acesso, garantindo que a origem dos dados é a de quem alega ser, é um dos objetivos da autenticação. Garantir o uso autorizado de recursos e o registro de todas as atividades dentro de um sistema são tarefas dos sistemas conhecidos por: Autenticação, Autorização e Auditoria (AAA).

Neste módulo foram apresentados os protocolos e técnicas para trabalhar com cada um desses três As.

Autenticação é algo que você sabe, por exemplo:

1) Mecanismo de senhas e suas variações. Exemplo: OTP, Passphrases etc.

2) O mais simples de implementar.

3) O menos seguro, por limitação do usuário.

3.1) É algo que você tem, por exemplo: Smartcards, chips, token, etc.

3.2) É algo que você é, por exemplo: Biometrias (impressão digital, formato da íris, voz, face etc.).

Com relação à criptografia, foram vistas a criptografia Simétrica: também conhecida por criptografia convencional e depois a criptografia Assimétrica: criptografia por chaves pública e privada e por fim o Algoritmo de Hash: os cinco fundamentos para um bom algoritmo de Hash.

Basicamente, um processo criptográfico envolve a aplicação de três conceitos elementares:

1) a mensagem/texto,

2) o algoritmo e

3) a chave.

A mensagem consiste, pura e simplesmente, na informação que se deseja transmitir de forma segura; o algoritmo é a forma que será utilizada para cifrar e decifrar uma mensagem; e a chave, em alguns modelos computacionais, pode ser entendida como o segredo compartilhado que deve ser conhecido apenas pelas duas partes envolvidas no processo de comunicação.

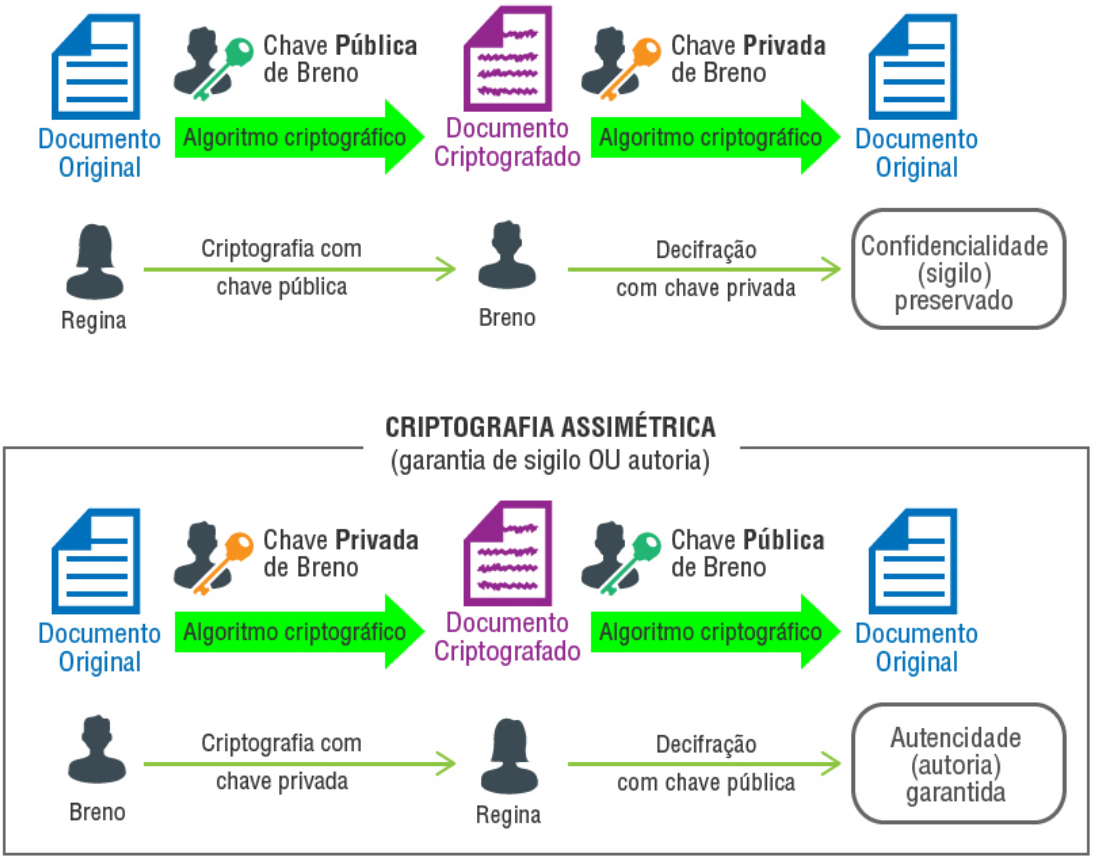
A criptografia simétrica utiliza a mesma chave para criptografar e descriptografar uma informação. Essa chave tem de ser compartilhada entre o emissor e o receptor da informação. Entretanto, o uso de criptografia simétrica dificulta o gerenciamento de chaves e não permite a autenticação e o não repúdio do remetente. Atualmente o algoritmo simétrico recomendado é o AES-256, que utiliza chaves de 256 bits.

UNIDADE 3 – AUTENTICAÇÃO, AUTORIZAÇÃO E CERTIFICAÇÃO DIGITAL
MÓDULO 2 – CRIPTOGRAFIA ASSIMÉTRICA, CERTIFICADOS DIGITAIS
01

1 – CRIPTOGRAFIA ASSIMÉTRICA

Veremos neste momento o gerenciamento de chaves; a implantação de não repúdio do remetente; utilização da criptografia assimétrica para garantir a confidencialidade, a autenticidade ou ambos e a principal desvantagem que é o desempenho, pois é muito mais lenta que a criptografia simétrica.

A **criptografia assimétrica** é uma forma de criptossistema em que a criptografia e a descriptografia são realizadas via diferentes chaves: uma chave pública e uma chave privada. Ela também é conhecida como criptografia de chave pública.



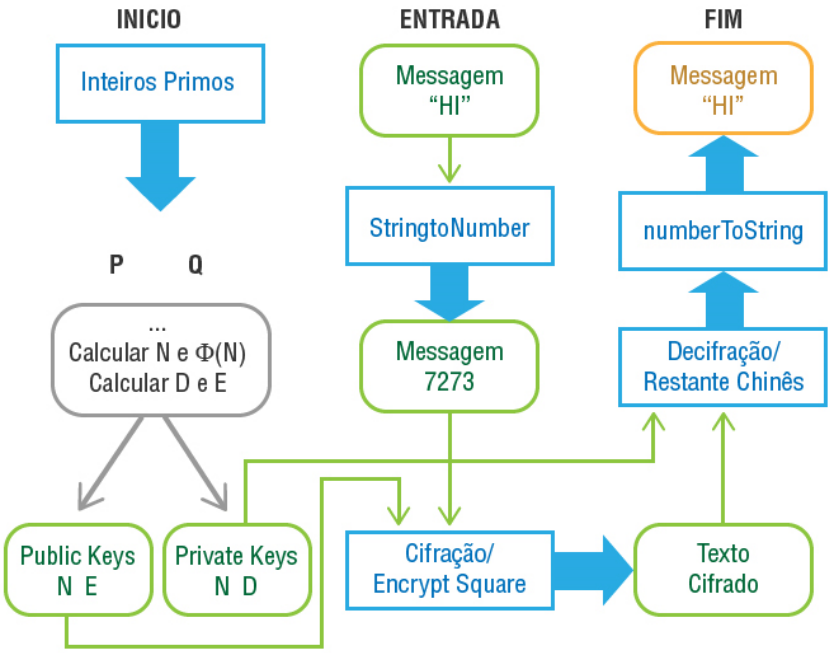
Criptografia assimétrica
Fonte: Internet, 2015

A criptografia assimétrica transforma o texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de descriptografia, o texto claro é recuperado a partir do texto cifrado.

02

Dessa forma, a criptografia assimétrica pode ser utilizada para garantir a confidencialidade, a autenticidade ou ambos. O criptossistema mais utilizado atualmente é o **RSA**, sendo envolvido o conceito de números primos, de modo que é difícil de explorar, pela complexidade de se encontrar números primos de um número composto.

O RSA funciona da seguinte forma:



Fluxograma do algoritmo RSA.
Fonte: http://www.rsasecurity.com, acesso Nov. 2015.

Pré-codificação: converter a mensagem em uma sequência de números.

Exemplo: para este caso, utilizaremos a tabela ASCII (American Standards Code Information Interchange).

Geração da Chave RSA

Cifração RSA

Decifração RSA

Geração da Chave RSA

1. Escolha dois números primos aleatoriamente, "P" e "Q", $P \neq Q$

P=11 e Q=13

2. Calcule N = P * Q

N=11*13=143.

3. Calcule: $\phi(N) = Z = (P-1)(Q-1)$

$\phi(N) = Z = (11-1)*(13-1)=120$

4. Selecione inteiro impar “D”, coprimo de ϕ(N)

D=7.

5. Encontre “E” tal que E*D ≡ 1(mod ϕ (N))

E=103.

6. Publique “N” e “E” como chave pública utilizada para cifrar a mensagem

Chaves públicas: N=143 e E=103.

7. Manter “N” e “D” como chave privada utilizada para decifrar a mensagem

Chaves privadas: N=143 e D=7

Cifração RSA

1. Dada a mensagem “M”, converter ao inteiro < “N”

M= HI em ASCII -> HI = 72 73.

2. Encriptação: $C = M^E \bmod N$

$C1=72^{103} \pmod{143} = 84$

$C2=73^{103} \pmod{143} = 57$

Mensagem encriptada, C = 84 57

Decifração RSA

1. Decifração: $M = C^D \bmod N$

Decifração da mensagem recebida: 84 57

$M1=84^7 \pmod{143}=72$

$M2=57^7 \pmod{143}=73$

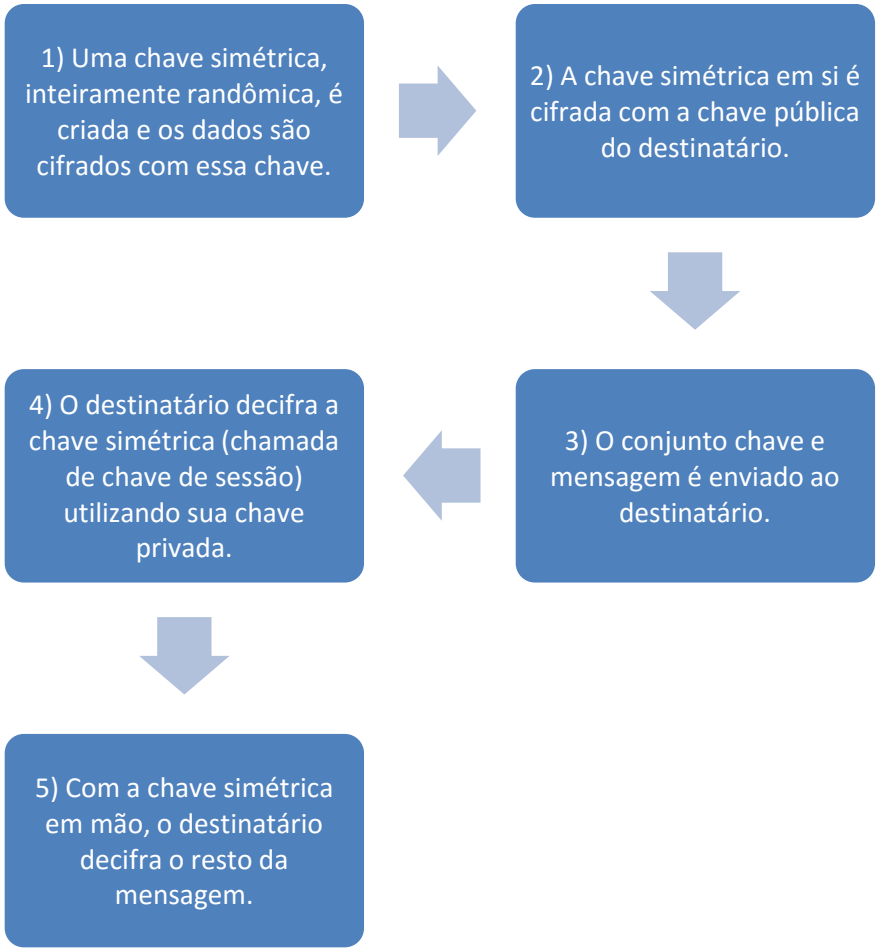
2. Converter de volta a string

M=HI.

03

A criptografia assimétrica tem como **desvantagem** o desempenho, pois é muito mais lenta que a criptografia simétrica. Se usássemos criptografia assimétrica em todas as transações criptográficas, teríamos perda de desempenho bastante significativa.

O mais comum é utilizar de uma forma combinada as duas técnicas:



04

1.1- Tamanho das chaves

Algoritmos **assimétricos** utilizam os tamanhos de chave:

1) 1024 bits.

2) 2048 bits.

3) 4096 bits.

Algoritmos **simétricos** utilizam tamanhos menores:

1) 128 bits.

2) 256 bits.

Em geral, os algoritmos assimétricos utilizam tamanhos de chave (1024, 2048 ou 4096 bits) muito maiores que os algoritmos simétricos (128, 256 bits), pois nestes, o comprometimento de uma chave de sessão invalida apenas uma transação, porém o comprometimento de uma chave assimétrica invalida todas as transações daquele usuário.

Os tamanhos de chave costumam variar, de acordo com a capacidade de processamento da época e do custo médio para se quebrar uma chave.

05

2 - Algoritmos Hash

Algoritmos Hash são funções criptográficas conhecidas como *one-way*. Essas funções possuem como entrada mensagens de tamanho variável e a saída de tamanho fixo. Uma mensagem de entrada, sempre que for submetida à análise da função Hash vai gerar a mesma saída.

Mensagem (tamanho arbitrário) ->Função de hash de uma só via ->Valor do hash (tamanho fixo):

h=H(m)

Fonte: http://www.serafim.eti.br, 2015

O principal propósito da função Hash é criar uma "impressão digital" de um arquivo, mensagem ou bloco de dados.

Um algoritmo Hash pode ser considerado forte quando:

a) One-Way

A partir do resultado da função Hash, não é possível descobrir a mensagem de entrada, de tamanho arbitrário. Também conhecido como algoritmo de uma só via.

b) Fraca resistência à colisão

Quando computacionalmente for impossível encontrar uma segunda entrada diferente de uma primeira entrada conhecida e as duas saídas forem iguais.

c) Forte resistência à colisão

Quando computacionalmente for impossível encontrar um par de entradas diferentes com a mesma saída.

06

2.1 - Algoritmos Hash mais difundidos:

a) MD5

Função de Hash de uma só via, inventada por Ron Rivest, do MIT, que também trabalha para a Indústria RSA de Segurança de Dados.

O algoritmo MD (Message Digest algorithm 5) produz um valor de Hash de 128-bit para um tamanho arbitrário da mensagem inserida.

Foi primeiramente proposto em 1991, depois de alguns ataques de criptoanálise descobertos contra a função de Hash de uma só via, utilizada no MD4 de Rivest. O algoritmo foi projetado para velocidade, simplicidade e segurança. Os detalhes do algoritmo são públicos e foram analisados por diversos criptógrafos.

Uma fraqueza foi descoberta em alguma parte do MD5, mas não afetou a segurança global do algoritmo. Porém, o fato de ele só produzir um valor de Hash de 128-bit é inquietante; é preferível uma função de Hash de uma só via, que produza um valor mais longo.

b) SHA

O SHA (Secure Hash Algorithm) Função de Hash de uma só via, desenvolvida pelo NIST (National Institute of Standards and Technology).

Produz um valor de Hash de 160-bit de um tamanho arbitrário da mensagem. O SHA é uma função Hash baseada na função Hash MD4. Porém, a fraqueza na parte do algoritmo MD5 mencionada ainda não foi possível de aplicar contra o SHA. Acredita-se que o SHA não possui essa vulnerabilidade.

Atualmente, não existe forma conhecida de ataque criptoanalítico contra o SHA, com exceção do ataque de força bruta. Seu valor de 160-bits torna o ataque de força bruta ineficiente. Não há evidências de que alguém não possa quebrar o SHA no futuro próximo ou mesmo quando esse material estiver sendo lido.

07

3 - Modos de operação de algoritmos criptográficos

Outra questão importante acerca de criptografia são os modos de operação. Em especial, temos dois **modos de operação**:

- em bloco e
- em stream.

A **operação em bloco** divide os dados em conjuntos de tamanho fixo (chamados de blocos).

Esses blocos são combinados com repetições da chave para gerar o texto cifrado, muitas vezes utilizando a operação matemática XOR.

Apesar de útil para a cifragem de arquivos, uma cifragem de bloco não é adequada para a transmissão de dados cifrados de forma contínua, como, por exemplo, uma conexão VPN ou uma transmissão de vídeo, pois numa cifra de bloco o algoritmo teria de aguardar um bloco ser completado para fazer a cifragem, o que reduzirá o desempenho.

As cifragens de bloco podem ter vários modos de operação, cada um com suas vantagens e desvantagens, por exemplo: Electronic Codebook (ECB), Cipher-block Chaining (CBC), Propagating Cipher-Block Chaining (PCBC), Cipher Feedback (CFB), Output Feedback (OFB) e Counter (CTR).

Nas aplicações em que temos pressa em enviar os dados, usamos o ***stream cipher***, que realiza a cifragem ao nível de bit, de modo que não há a necessidade de aguardar a formação de um bloco.

Alguns exemplos de cifragem stream são RC4 e A5/1 (usado em redes GSM de telefonia celular).

08

Antes de iniciarmos um novo tópico de estudo, verifique se você aprendeu os conceitos abaixo.

- Explique a criptografia assimétrica.

A criptografia assimétrica é uma forma de sistema criptográfico em que a criptografia e a descriptografia são realizadas via diferentes chaves: uma chave pública e uma chave privada, conhecida como criptografia de chave pública.

- O que são e para que servem os algoritmos hash?

Algoritmos Hash são funções criptográficas conhecidas como one-way. Essas funções possuem como entrada mensagens de tamanho variável e a saída de tamanho fixo e servem para criar uma "impressão digital" de um arquivo, mensagem ou bloco de dados.

09

4 – Certificado Digital

O ponto crucial da especificação do esquema X.509 é a associação de certificados de chaves públicas a cada usuário do diretório. Esses certificados digitais devem ser gerados por uma Autoridade Certificadora (AC) confiável e armazenados no servidor de diretório.

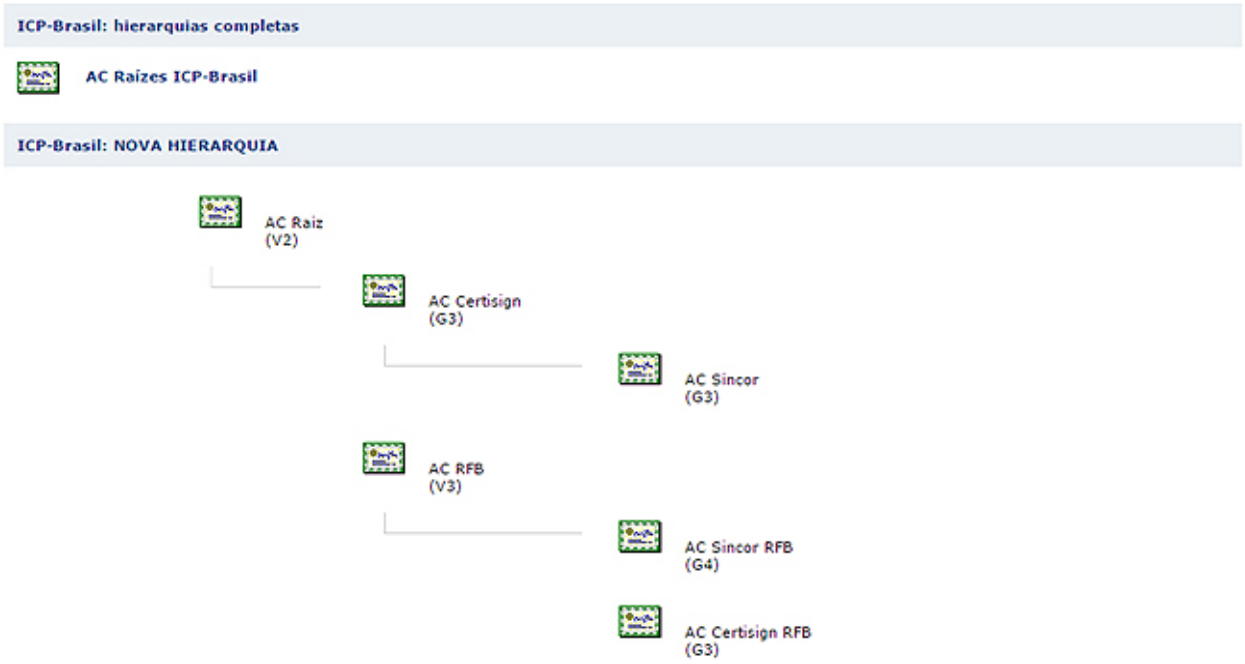
Esse armazenamento pode ser feito pelo AC e pelo usuário. Dessa forma, o servidor de diretório não é responsável pela criação desses certificados de chave pública, mas apenas provê fácil acesso aos certificados de usuários.

10

5 - Obtendo certificado de usuário

A ICP (Infraestrutura de Chave Pública) é construída de forma hierárquica, onde a AC certificadora Raiz concede permissão para uma AC e permissão de emissão de certificados.

A figura a seguir ilustra a nova hierarquia de certificados digitais da ICP-Brasil.



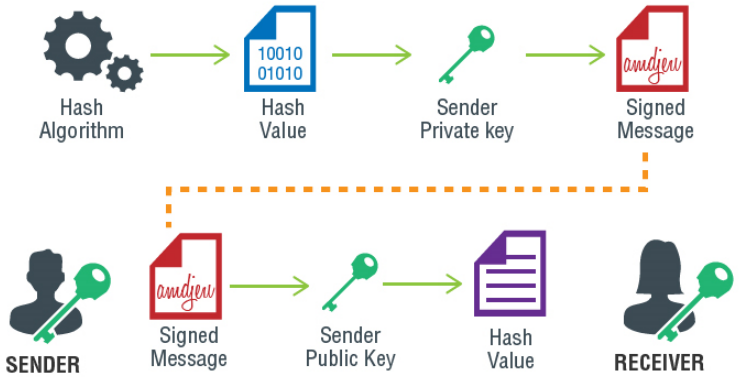
Hierarquia de AC
Fonte: http://www.acsincor.com.br/conteudo.aspx?IdConteudo=5, 2015.

ICP-Brasil

Para mais informações sobre a ICP-Brasil acesse a URL: http://www.iti.gov.br.

11

O certificado de usuário é gerado por sistema de Autoridade Certificadora, que emite a chave pública e privada do certificado. A chave pública pode ser armazenada em um repositório de diretórios e a chave privada fica sob a guarda do usuário.



Certificado do usuário
Fonte: Internet, 2015.

Existem várias implementações de PKI (Public Key Infrastructure), ou Infraestrutura de Chaves Públicas, comerciais e de *software* livre:

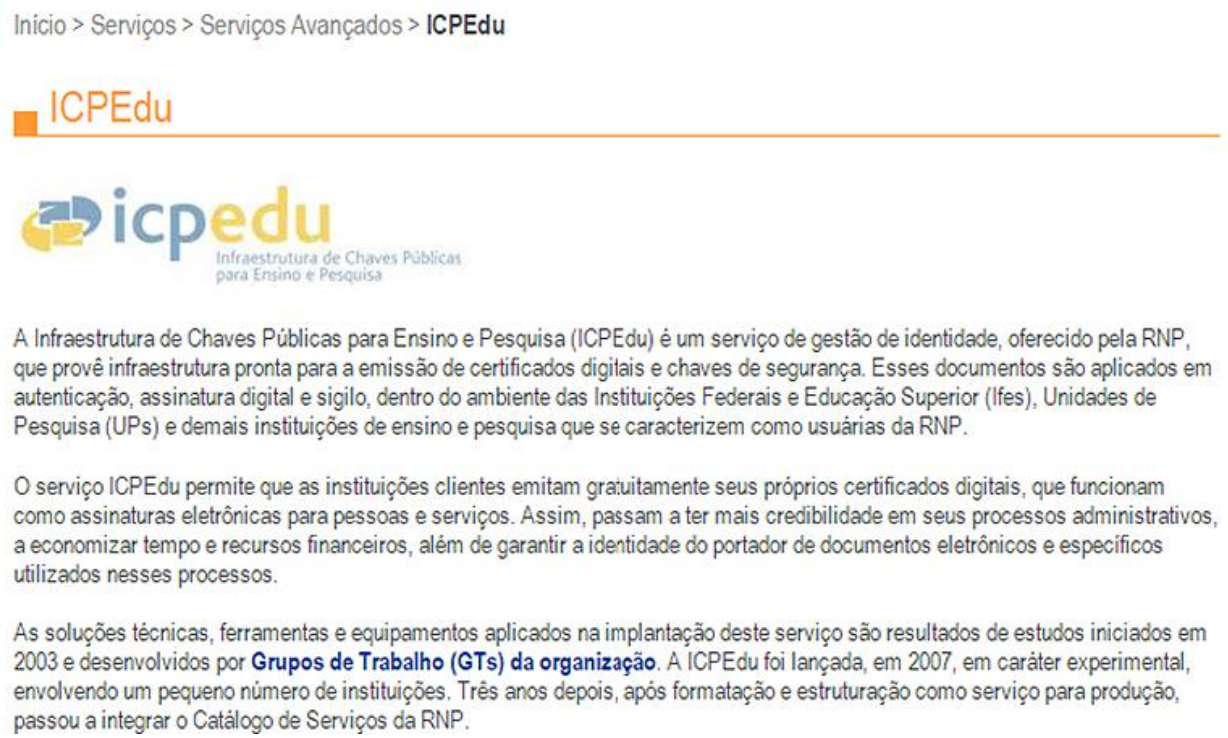
a) Microsoft Windows 2008 Server – Certificate Autority.

b) Microsoft Public Key Infrastructure (PKI) for Windows Server 2003.

c) Projeto de *software* livre OpenCA PKI.

12

Existe ainda um projeto educacional de infraestrutura de chaves públicas, com o objetivo de prover uma ICP para as universidades brasileiras. Informações sobre esse projeto podem ser encontradas em: http://www.rnp.br/servicos/servicos-avancados/icpedu, conforme mostra a figura abaixo.

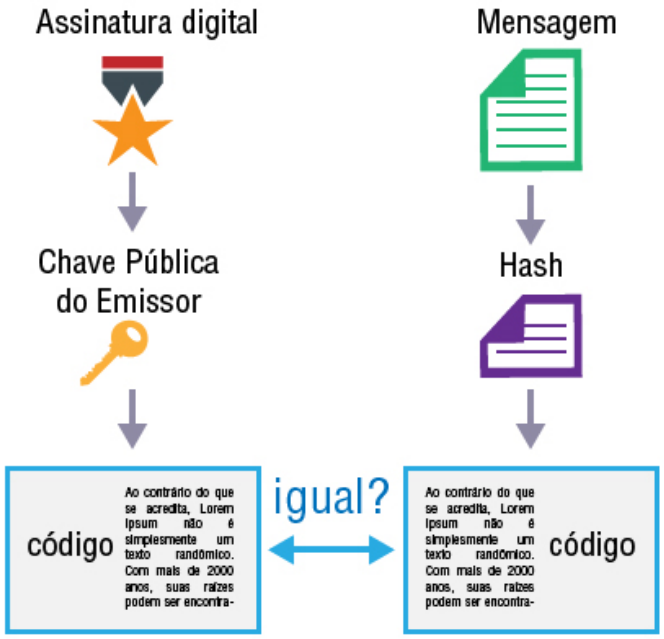


ICPEdu

Fonte: http://www.rnp.br/servicos/servicos-avancados/icpedu, 2015.

13

A figura a seguir ilustra o processo de geração de um certificado.



ICPEdu

Fonte: Internet, 2015.

Nessa figura:

1) O certificado não assinado contém o ID e a chave pública do usuário.

2) É gerado o código hash do certificado não assinado.

3) O código hash criptografado com a chave privada da AC irá formar a assinatura.

4) O certificado assinado é gerado que poderá ser verificar a assinatura por meio da chave publica da AC.

14

6 - Revogando o certificado do usuário

No momento da geração do certificado digital, é necessário indicar o período de sua validade. Dessa forma, se por algum motivo um certificado necessite de ser cancelado antes da data final de validade, esse certificado será incluído em uma base de certificados revogados.

A Infraestrutura de Chaves Públicas disponibiliza essa base para que, no processo de validação de um certificado, esse serviço de validação consulte a base antes de permitir ou negar determinado acesso.

Manter essa base atualizada e garantir que as aplicações acessem o certificado é mais um dos desafios do administrador de segurança da rede.

Para fixar, responda:

- O que são certificados digitais?

É uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web.

15

RESUMO

A criptografia assimétrica é uma forma de criptossistema em que a criptografia e a descriptografia são realizadas via diferentes chaves: uma chave pública e uma chave privada. Ela também é conhecida como criptografia de chave pública. A criptografia assimétrica transforma o texto claro em texto cifrado usando uma de duas chaves e um algoritmo de criptografia. Usando a outra chave associada e um algoritmo de descriptografia, o texto claro é recuperado a partir do texto cifrado.

O criptossistema mais utilizado atualmente é o RSA, sendo envolvido o conceito de números primos, de modo que é difícil de explorar, pela complexidade de se encontrar números primos de um número composto.

A criptografia assimétrica tem como desvantagem o desempenho, pois é muito mais lenta que a criptografia simétrica. Se usássemos criptografia assimétrica em todas as transações criptográficas, teríamos perda de desempenho bastante significativa.

Quanto aos algoritmos Hash, são funções criptográficas conhecidas como one-way. Essas funções possuem como entrada mensagens de tamanho variável e a saída de tamanho fixo. Uma mensagem de entrada, sempre que for submetida à análise da função Hash vai gerar a mesma saída.

O principal propósito da função Hash é criar uma “impressão digital” de um arquivo, mensagem ou bloco de dados.

Outra questão importante acerca de criptografia são os modos de operação. Em especial, temos os modos de operação em bloco e os modos de operação em stream. A operação em bloco divide os dados em conjuntos de tamanho fixo (chamados de blocos). Nas aplicações em que temos pressa em enviar os dados, usamos o stream cipher, que realiza a cifragem a nível de bit, de modo que não há a necessidade de aguardar a formação de um bloco.

Com relação aos certificados digitais, foi visto que o ponto crucial da especificação do esquema X.509 é a associação de certificados de chaves públicas a cada usuário do diretório. Esses certificados digitais devem ser gerados por uma Autoridade Certificadora (AC) confiável e armazenados no servidor de diretório.

A ICP (Infraestrutura de Chave Pública) é construída de forma hierárquica, onde a AC certificadora Raiz concede permissão para uma AC e permissão de emissão de certificados.

O certificado de usuário é gerado por sistema de Autoridade Certificadora, que emite a chave pública e privada do certificado. A chave pública pode ser armazenada em um repositório de diretórios e a chave privada fica sob a guarda do usuário.

No momento da geração do certificado digital, é necessário indicar o período de sua validade. Dessa forma, se por algum motivo um certificado necessite de ser cancelado antes da data final de validade, esse certificado será incluído em uma base de certificados revogados. A Infraestrutura de Chaves Públicas disponibiliza essa base para que, no processo de validação de um certificado, esse serviço de validação consulte a base, antes de permitir ou negar determinado acesso.

Manter essa base atualizada e garantir que as aplicações acessem o certificado é mais um dos desafios do administrador de segurança da rede.

UNIDADE 3 – AUTENTICAÇÃO, AUTORIZAÇÃO E CERTIFICAÇÃO DIGITAL
MÓDULO 3 – GERÊNCIA DE SENHAS E SISTEMAS DE AUTENTICAÇÃO ÚNICA
01

1 – GERENCIAMENTO DE SENHAS

A primeira fronteira de proteção contra intrusos é o **sistema de senhas**.

Praticamente todos os sistemas multiusuários utilizam um mecanismo de autenticação em que o usuário é induzido a entrar com o **identificador** (**ID**) e uma senha secreta. A senha serve para autenticar o ID do usuário, liberando ou não o acesso ao sistema.

O ID é utilizado para:

a) Determinar se o usuário está autorizado a obter acesso ao sistema (autenticação). Em alguns sistemas específicos, apenas usuários previamente cadastrados terão permissão de acesso.

b) Determinar o nível de acesso concedido a um usuário específico (autorização). Alguns usuários, por exemplo, podem ter acesso de administração do sistema, enquanto outros terão acesso apenas de operação.

Os itens mais importantes que trataremos aqui acerca do gerenciamento de senhas são:

a) Sistemas de senhas Linux.

b) Sistemas de senhas Windows.

1) Hash LM – Lan Manager.

2) 2 Hash NTLM.

c) Administrando as senhas.

Veremos cada um desses itens a seguir.

02

1.1- Sistema de senhas Linux

No sistema Linux devemos saber que:

a) Ao criar um usuário no sistema Linux, uma senha é associada ao ID do usuário.

b) A senha é manipulada pela função crypt().

c) A conta do usuário é armazenada no arquivo /etc/passwd.

d) A senha é armazenada no arquivo /etc/shadow.

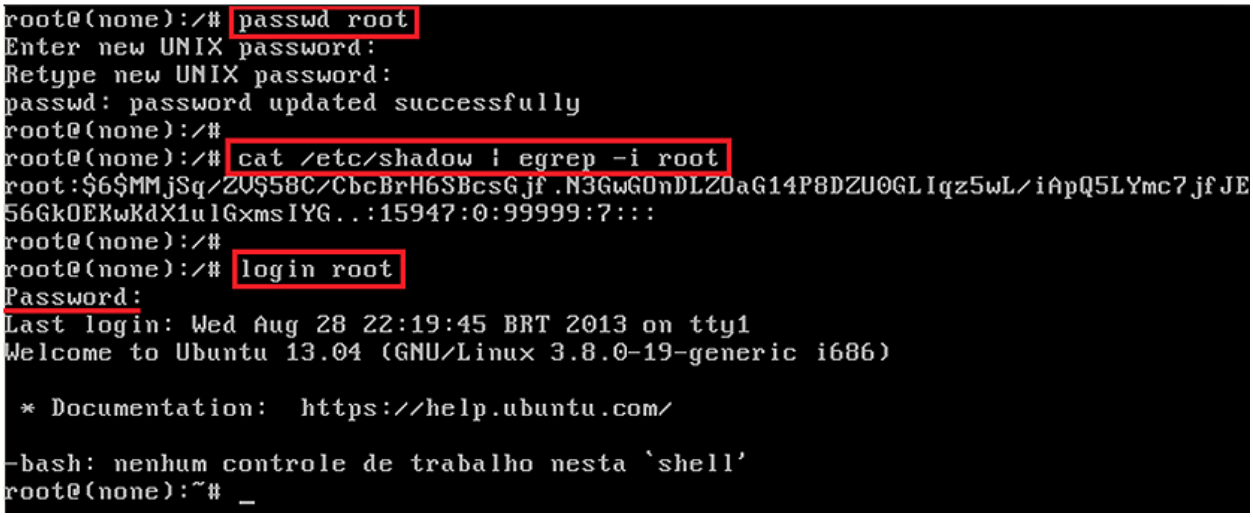
Garantir o uso de senhas fortes por parte do usuário é uma difícil tarefa do administrador do sistema, em qualquer ambiente operacional.

03

1.1.1- Como o sistema de senhas funciona em um ambiente Unix?

Quando um usuário é criado no sistema, uma senha é associada ao seu ID. Essa senha é manipulada pela função **crypt**(), que pode trabalhar com criptografia baseada em DES, MD5 ou SHA, para geração do Hash da senha e do SALT (é um número para evitar a pré-computação de um invasor que deseja criar um dicionário de senhas comuns e chaves KEK-Key Encription Key-associadas) que será armazenado no arquivo de senhas do sistema, normalmente armazenado em /etc/shadow.

A cifragem das senhas permite um nível adicional de proteção, visto que mesmo que um atacante tenha acesso ao arquivo de senhas, terá de realizar um ataque de força bruta no arquivo de senhas para tentar descobrir as senhas dos usuários do sistema.



Verificação da Senha
Fonte: Internet, 2015

04

1.1.2 - Valor do SALT

O SALT é gerado no momento em que a senha é criada. É guardado em texto claro no arquivo de senhas.

Objetivos do SALT:

a) Evitar que senhas duplicadas sejam visualizadas no arquivo de senhas. Mesmo que mais de um usuário tenha escolhido a mesma senha, o valor de SALT será diferente, resultando em valores de Hash diferentes.

b) Aumentar o tamanho da senha, sem a necessidade de o usuário lembrar de todo o comprimento adicional da senha, assim dificultando a tarefa de sistemas adivinhadores de senha.

c) Impedir o uso de uma implementação que utilize o DES em *hardware*, minimizando a possibilidade de ataques de descoberta da senha por força bruta.

Quando um usuário Unix vai realizar o processo de login no sistema, fornece o ID do usuário e a senha. O sistema utiliza o ID do usuário para varrer o arquivo de usuários /etc/passwd para encontrar o UID (número identificador do usuário no sistema) e em seguida consultar o arquivo de senhas para encontrar o SALT do usuário e o Hash.

Com essas informações disponíveis, a função crypt() é chamada, a senha é digitada pelo usuário e passada junto com seu respectivo SALT. Se o Hash gerado pela função for igual ao Hash do arquivo de senhas, o acesso ao sistema é concedido.

O arquivo /etc/shadow possui permissão de leitura apenas pelo administrador do sistema, formando uma barreira adicional de proteção, visto que os usuários comuns do sistema não possuem acesso de leitura a esse arquivo, e consequentemente não possuem acesso às senhas cifradas dos usuários.

05

Agora vamos verificar se você aprendeu o conteúdo que acabamos de estudar. Tente responder às perguntas a seguir, depois clique para ver a resposta.

- **Para que é utilizado o ID?**

É utilizado para determinar se o usuário está autorizado a obter acesso ao sistema (autenticação) e determinar o nível de acesso concedido a um usuário específico (autorização).

- **Quais os objetivos do SALT?**

Evitar que senhas duplicadas sejam visualizadas no arquivo de senhas, aumentar o tamanho da senha, sem a necessidade de o usuário lembrar de todo o comprimento adicional da senha, assim dificultando a tarefa de sistemas adivinhadores de senha e impedir o uso de uma implementação que utilize o DES em *hardware*, minimizando a possibilidade de ataques de descoberta da senha por força bruta.

06

1.2 - Sistema de senhas Windows

Registros de usuário Windows (NT4, 2000, XP e 2003 Server) são armazenados no banco de dados do Security Account Manager (SAM), do gerenciador de contas de segurança ou no banco de dados do Active Directory.

Cada conta de usuário está associada a duas senhas:

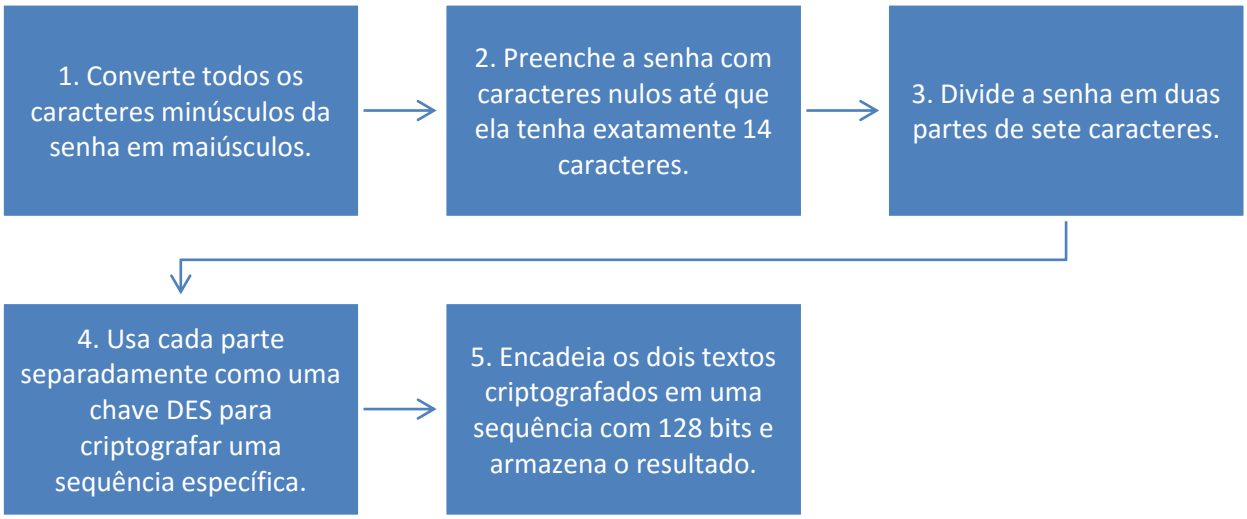
- a senha compatível com o LAN Manager e
- a senha do Windows.

Cada senha é criptografada e armazenada no banco de dados SAM ou no banco de dados do Active Directory.

07

1.2.1 - Hash LM

O Hash LM (Lan Manager) não é exatamente um Hash, sendo gerado como resultado de um processo de manipulação de strings, e obtido com os seguintes passos:



Como resultado do algoritmo usado para gerar o Hash LM, o Hash é muito fácil de ser quebrado. Em primeiro lugar, mesmo uma senha com mais de oito caracteres pode ser atacada em duas partes distintas. Em segundo lugar, todo o conjunto de caracteres minúsculos pode ser ignorado. Isso significa que a maioria das ferramentas para quebrar senhas começa quebrando os Hashes LM e depois simplesmente varia os caracteres alfabéticos na senha quebrada para gerar senhas que fazem distinção entre maiúsculas e minúsculas.

08

1.2.2 - Hash NTLM

É a solução proprietária da Microsoft que abriu a especificação para parceiros implementarem soluções integradas.

Características:

- É também conhecido como Hash Unicode por dar suporte a todo o conjunto de caracteres Unicode.
- Hash MD4: o hash NTLM é calculado por meio da senha no formato de texto claro e é gerado um Hash Message Digest 4 (MD4) a partir dele.

- Apresenta mais resistência a ataques de força bruta do que o Hash LM, pois dá suporte a todo o conjunto de caracteres.

O Hash MD4 é armazenado no banco de dados do Active Directory, ou no banco de dados do Security Accounts Manager (SAM) ou no Gerenciador de Contas de Segurança.

09

1.3 - Administrando as senhas

A administração de senhas requer os requisitos a seguir:

1) Treinamento do usuário.
2) Requisitos de complexidade.
3) Tempo de duração da senha.

Se um usuário mal-intencionado conseguir algum tipo de acesso ao sistema, como, por exemplo, pelo uso de uma conta de convidado ou de sistema desprotegida de senha ou com senha padrão, ele poderá conseguir uma listagem dos usuários válidos do sistema e dessa forma tentar um ataque de dicionário.

Como a maioria dos usuários utilizam senhas com palavras existentes em dicionários, será fácil conseguir quebrar essa primeira barreira de segurança do sistema.

Use senhas longas, combinando letras maiúsculas e minúsculas, números e caracteres especiais, dificultando os ataques.

Esse usuário mal-intencionado poderá descobrir as senhas do sistema se conseguir enviar a base de dados das senhas para uma máquina remota e nessa máquina remota utilizar um programa de quebra de senhas, com um dicionário. Dependendo da quantidade de senhas presentes no arquivo e do poder computacional disponível para o usuário mal-intencionado, este pode conseguir quebrar um número grande de senhas em um pequeno intervalo de tempo.

Para proteger as contas dos usuários do sistema, o administrador pode minimizar os efeitos dessas ferramentas utilizando práticas recomendadas para o gerenciamento de senhas.

10

1.3.1 - Treinamento do usuário

É imprescindível reforçar aos usuários a importância de manter suas senhas protegidas de amigos e familiares (especialmente crianças), que poderiam divulgá-las a outras pessoas menos confiáveis. As senhas que você precisa compartilhar, como a senha de uma conta conjunta *on-line*, são as únicas exceções.

Jamais anote senhas em agendas, no monitor do computador, embaixo do teclado etc.

1.3.2 - Requisitos de complexidade

Uma boa senha possui as seguintes características:

- Deve possuir um número mínimo de caracteres,
- Deve utilizar caracteres de diversos conjuntos (maiúsculas, minúsculas, números e símbolos),
- Não deve constar em dicionários e
- Deve ser fácil de lembrar.

É importante que o administrador seja sensível à dificuldade dos usuários de lembrar senhas, de modo que ele não aplique regras muito restritivas, que possam forçar os usuários a anotar as senhas. A troca de senhas a cada mês ou requisitos de complexidade muito severos são alguns exemplos de regras que podem complicar a vida do usuário.

11

Antes de avançarmos para o próximo item, vamos verificar o que você aprendeu sobre o gerenciamento de senhas no Windows. Tente responder à questão a seguir, depois clique para ver a resposta.

- **Explique onde são armazenadas as senhas no Windows.**

São armazenados no banco de dados do Security Account Manager (SAM), do gerenciador de contas de segurança ou no banco de dados do Active Directory.

12

1.3.3 – Tempo de duração da senha

A respeito do tempo de duração da senha, é importante configurar algumas diretivas, tais como:

- Configure a diretiva *"**Aplicar histórico de senhas**"* para que todas as senhas anteriores sejam memorizadas.

Com essa diretiva, os usuários serão impedidos de utilizar a mesma senha depois que a atual expira.

- Aplique a configuração de diretiva *"**Tempo de vida máximo da senha**"* para que todas as senhas expirem com a frequência necessária ao ambiente, o que, em geral, ocorre no período de 30 a 90 dias.

Após aplicada essa configuração de diretiva, se uma senha for decifrada, o intruso terá acesso à rede somente até a senha expirar.

- Configure a diretiva "***Tempo de vida mínimo***" da senha, de modo que as senhas não possam ser alteradas até atingirem um número mínimo de dias.

Essa configuração funciona junto com a diretiva *"Aplicar histórico de senhas"*. Caso um tempo de vida mínimo seja definido para a senha, os usuários não poderão alterá-la repetidamente para burlarem a opção "*Aplicar histórico de senhas"* e usarem a senha original. Portanto, os usuários deverão aguardar o número de dias especificado para alterarem suas senhas.

13

2 – Sistemas de Autenticação Única

Com o uso cada vez mais intenso de sistemas informatizados para soluções comerciais, novos sistemas vão surgindo em implementações que automatizam os processos do negócio.

A implementação de um mecanismo único de autenticação é desejável para simplificar a gerência de usuários e senhas dos clientes dos sistemas, assim como para simplificar e aumentar a eficiência do gerenciamento das contas e suas respectivas senhas pelo administrador.

É importante que as soluções informatizadas possam integrar uma solução de autenticação única para todos os sistemas. Um usuário, uma vez autenticado, deverá ter acesso a todos os sistemas que tiver autorização para acessar.

Existem várias soluções de implementação de SSO (single sign-on), como a já mencionada NTLM. Outros sistemas baseados em Kerberos são:

- Smart Card e
- OTP Token.

Abordaremos esses sistemas a seguir.

14

3– OTP (One Time Password)

One Time Password (OTP) é um mecanismo que utiliza senhas descartáveis, isto é, uma senha é gerada para cada acesso e esta perde o valor após o processo de autenticação.

Dessa forma, caso a senha de um usuário seja capturada, não poderá comprometer o sistema, uma vez que, para novo acesso, uma nova senha deverá ser gerada e informada.

Há várias maneiras de gerar as senhas, como, por exemplo, o uso de calculadoras Java, que podem estar em sistemas embarcados como um PDA ou um celular.

No entanto, há um problema nessas implementações, pois o usuário tem a necessidade de estar perto da calculadora para acessar o sistema.

PDA

PDA - Personal digital assistants (assistente pessoal digital) é um computador de pequeno porte (até 10 polegadas), geralmente usado com função de agenda, é dotado de alta capacidade computacional e possibilidade de interconexão com um computador pessoal e uma rede sem fio — Wi-Fi — para acesso a e-mail e internet.

15

4 - S/Key e Smart Card

4.1 - S/Key

É um sistema de autenticação OTP desenvolvido para sistemas operacionais Unix e derivados, como o caso do Linux.

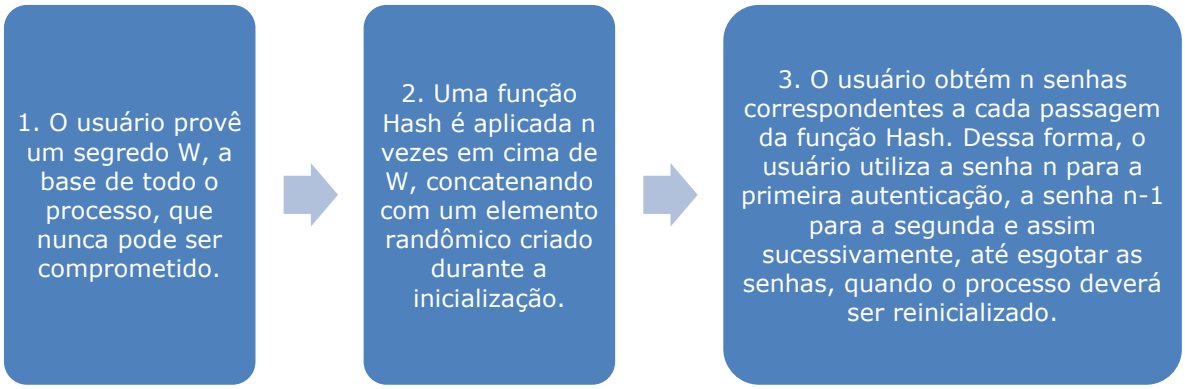
No sistema S/Key:

a) O usuário provê um segredo W.

b) Uma função Hash é aplicada n vezes em cima de W.

c) O usuário obtém n senhas correspondentes a cada passagem da função Hash.

A proposta do S/Key é obter um conjunto de senhas em que cada uma só pode ser utilizada uma vez. O processo de inicialização do S/Key funciona da seguinte forma:



Considerando que a partir de *n* é inviável deduzir *n-1* (envolve reverter uma função Hash), caso n seja comprometida, ela já não mais poderá ser usada, pois cada senha só é usada uma vez. Para facilitar a digitação por parte do usuário, os bytes de cada Hash são convertidos para palavras, utilizando uma tabela de conversão padronizada.

16

4.2 - Smart Card

O Smart Card, ou Cartão Inteligente, é um cartão de plástico, semelhante a um cartão de crédito, com um microchip (microprocessador) embutido para fins de segurança.

O conceito de Smart Card foi patenteado pelo Dr. Kunitaka Arimura no Japão, em 1970. Hoje nosso Smart Card se parece com o da figura abaixo.

Exemplo de Smart Card.
Fonte: Internet, 2015.

Embora existam muitos tipos, qualquer Smart Card pode ser classificado quanto à forma de conexão com a leitora:

a) **Por contato físico**,

b) **Sem contato físico**.

Por contato físico

Entende-se a inserção do cartão na leitora, na qual os contatos dos terminais do cartão com os da leitura permitem a troca de dados entre ambos. É importante salientar que a maioria dos Smart Cards possuem terminais para esse tipo de conexão.

Sem contato físico

Refere-se aos cartões que não necessitam de contato físico com a leitora, o que indica que a conexão é feita através de ondas eletromagnéticas. A ausência do ato de inserção traz benefícios, como economia de tempo e preservação dos terminais do cartão. Um exemplo interessante deste tipo de cartão são os passaportes eletrônicos.

17

Por serem muito mais baratos, os **cartões por contato** ainda são os mais utilizados, oferecendo um nível razoável de segurança e abrangendo uma ampla gama de aplicações.

Os Smart Cards que não fazem uso de contato físico são tipicamente **Cartões Microprocessados**.

Embora não seja do escopo dos cartões de identificação, a modalidade de transmissão sem contato permite que o cartão propriamente dito seja apenas um portador do **chip**, ou seja, a presença do chip em anéis, relógios, braceletes e tornozeleiras ainda não quebra o conceito de Smart Card.

Os cartões por contato são também chamados de **Cartões de Memória** (Memory Cards).

Os cartões inteligentes por contato físico podem ser utilizados com leitores conectados em um computador pessoal, a fim de autenticar um usuário.

Softwares de navegação na internet também podem utilizar a tecnologia do Smart Card para complementar SSL (*Secure Sockets Layer*), com o objetivo de melhorar a segurança em transações na internet. Como o cartão inteligente possui arquitetura de *hardware* e *software*, ele interage com o sistema, permitindo ou negando acesso quando necessário. Saiba+

Hoje em dia é muito comum Smart Cards nos nossos cartões de crédito, em chips de celulares GSM ou em cartões emitidos pelo governo, como o e-CPF e o e-CNPJ, além do recém-anunciado Registro de Identificação Civil (RIC). Nesses casos, o cartão contém um certificado digital padrão ICP-Brasil. Os certificados digitais serão vistos em mais detalhes à frente.

Em alguns desses cartões, existe um sistema complexo de proteção do material criptográfico contido dentro do cartão, que se apaga caso o cartão seja aberto ou haja erro na senha de acesso em um determinado número de vezes.

Normalmente, as chaves privadas nunca saem de dentro do cartão, que possui um chip capaz de realizar operações criptográficas dentro do próprio cartão.

Saiba+

O Smart Card pode ser programado, por exemplo, para que após cinco tentativas de autenticação sem sucesso, o conteúdo da memória seja destruído, inutilizando-o.

18

RESUMO

Foi visto que a primeira fronteira de proteção contra intrusos é o sistema de senhas. Praticamente todos os sistemas multiusuários utilizam um mecanismo de autenticação no qual o usuário é induzido a entrar com o identificador (ID) e uma senha secreta. A senha serve para autenticar o ID do usuário, liberando ou não o acesso ao sistema. O ID é utilizado para:

a) Determinar se o usuário está autorizado a obter acesso ao sistema (autenticação). Em alguns sistemas específicos, apenas usuários previamente cadastrados terão permissão de acesso.

b) O ID determina o nível de acesso concedido a um usuário específico (autorização). Alguns usuários, por exemplo, podem ter acesso de administração do sistema, enquanto outros terão acesso apenas de operação.

Em relação ao gerenciamento de senhas no sistema Linux, devemos saber que:

a) Ao criar um usuário no sistema Linux, uma senha é associada ao ID do usuário.

b) A senha é manipulada pela função crypt().

c) A conta do usuário é armazenada no arquivo /etc/passwd.

d) A senha é armazenada no arquivo /etc/shadow.

Em um ambiente Unix, quando um usuário é criado no sistema, uma senha é associada ao seu ID. Essa senha é manipulada pela função crypt(), que pode trabalhar com criptografia baseada em DES, MD5 ou SHA, para geração do Hash da senha e do SALT (é um número para evitar a pré-computação de um invasor que deseja criar um dicionário de senhas comuns e chaves KEK-Key Encription Key-associadas) que será armazenado no arquivo de senhas do sistema, normalmente armazenado em /etc/shadow.

O SALT é gerado no momento em que a senha é criada. É guardado em texto claro no arquivo de senhas. Objetivos do SALT:

a) Evitar que senhas duplicadas sejam visualizadas no arquivo de senhas.

b) Aumentar o tamanho da senha, sem a necessidade de o usuário lembrar de todo o comprimento adicional da senha.

c) Impedir o uso de uma implementação que utilize o DES em *hardware*.

19

No Windows, os registros de usuário Windows são armazenados no banco de dados do Security Account Manager (SAM), no gerenciador de contas de segurança ou no banco de dados do Active Directory. Cada conta de usuário está associada a duas senhas: a senha compatível com o LAN Manager e a senha do Windows. Cada senha é criptografada e armazenada no banco de dados SAM ou no banco de dados do Active Directory.

O Hash NTLM foi a solução proprietária da Microsoft que abriu a especificação para parceiros implementarem soluções integradas. O Hash NTLM é calculado por meio da senha no formato de texto claro e é gerado um Hash Message Digest 4 (MD4) a partir dele. O Hash NTLM é muito mais resistente a ataques de força bruta do que o Hash LM.

Com relação à administração de senhas foram vistos os requisitos:

1) Treinamento do usuário.

2) Requisitos de complexidade.

3) Tempo de duração da senha.

Com o aumento e a disseminação do uso de sistemas em rede, a implementação de um mecanismo único de autenticação foi criado para simplificar a gerência de usuários e senhas dos clientes dos sistemas, assim como para simplificar e aumentar a eficiência do gerenciamento das contas e suas respectivas senhas pelo administrador.

A implementação de SSO (single sign-on), como NTLM, uma solução proprietária da Microsoft abriu a especificação para parceiros implementarem soluções integradas. Outros sistemas baseados em Kerberos são Smart Card e OTP Token.

One Time Passwords (OTP) é um mecanismo que utiliza senhas descartáveis. O S/Key é um sistema de autenticação OTP desenvolvido para sistemas operacionais Unix e derivados, como o caso do Linux.

A proposta do S/Key é obter um conjunto de senhas em que cada uma só pode ser utilizada uma vez. O Smart Card, ou Cartão Inteligente, é um cartão de plástico, semelhante a um cartão de crédito, com um microchip embutido.

UNIDADE 3 – AUTENTICAÇÃO, AUTORIZAÇÃO E CERTIFICAÇÃO DIGITAL
MÓDULO 4 - SERVIDORES DE DIRETÓRIO: LDAP

01

1 – SERVIDORES LDAP (LIGHWEIGHT DIRECTORY ACCESS PROTOCOL)

O LDAP foi criado para prover acesso aos serviços de diretórios do X.500 (série de recomendações do ITU-T que definem o serviço de diretório) pelos protocolos da pilha TCP/IP. O LDAP tem a implementação facilitada, exige menos recursos da rede e de memória. Ele foi desenvolvido para aplicações TCP/IP com bom desempenho. Por esses motivos recebeu o nome Lightweight Directory Access Protocol (**Protocolo leve de acesso a diretórios**).

O servidor LDAP é um banco de dados com informações descritivas, baseado em atributos e organizado em forma hierárquica (árvore) e não relacional (tabelas), otimizado para leitura e com certificação digital e baseado em **entradas**.

Uma **entrada** é um conjunto de atributos referenciado por Nome Distinto (DN) de forma não ambígua. Cada atributo de entrada tem um tipo de valor, como, por exemplo, CN e ON.

Em suma, LDAP é um protocolo (TCP/IP) cliente-servidor, utilizado para acessar um serviço de diretório. Pode ser utilizado também com autonomia e com outros tipos de servidores de diretório. Atualmente tornou-se padrão e diversos programas já têm suporte a LDAP. Livros de endereços, autenticação, armazenamento de certificados digitais (S/MIME) e de chaves públicas (PGP-Pretty Good Privacy) são alguns dos exemplos de onde o LDAP já é amplamente utilizado.

X500

O X.500 é um padrão de protocolos de serviços de diretórios, utilizados em redes de computadores, e foi elaborado para trabalhar sobre modelo OSI e incorporado ao pacote de protocolos ISO/IEC 9594. Designado para dar suporte ao padrão X.400, que define a troca de mensagens eletrônicas entre os usuários da rede local, a função do X.500 é prover serviços de diretórios para rede, centralizando a base de dados dos usuários da rede em um servidor X.500. Fonte: http://www.teleco.com.br

ITU-T

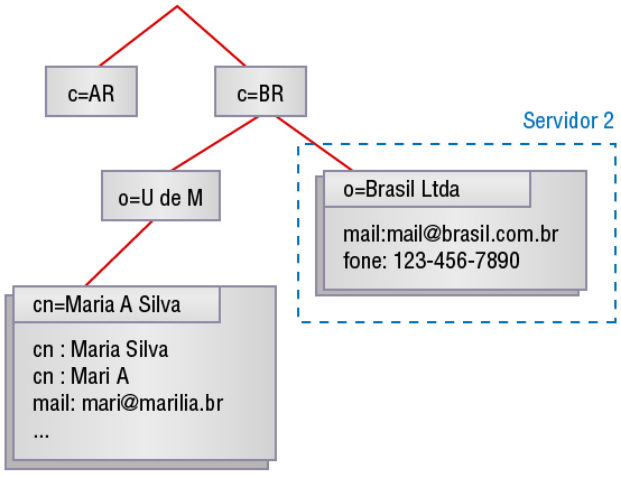
ITU-T - Telecommunication Standardization Sector ou Setor de Normatização das Telecomunicações é uma área da União Internacional de Telecomunicações (ITU) responsável por coordenar padronizações relacionadas a telecomunicações. (Fonte: Wikipedia).

02

1.2 - Serviço de diretório

Um diretório é como um banco de dados, que tende a conter informações descritivas, baseadas em atributo, sendo organizado em forma hierárquica (árvore) e não relacional (tabelas).

A informação em um diretório é geralmente mais lida do que escrita, de modo que normalmente os diretórios são otimizados para leitura. Em consequência, diretórios em geral não são usados para programar transações complexas ou esquemas de consultas regulares em bancos de dados.



Árvore de Diretório LDAP

Fonte: Internet, 2015

A figura acima ilustra outra vantagem de um serviço de Diretórios. Os ramos da árvore podem estar em máquinas diferentes. No caso, a entrada o=Brasil Ltda está em outro computador. Esta característica também é típica do DNS.

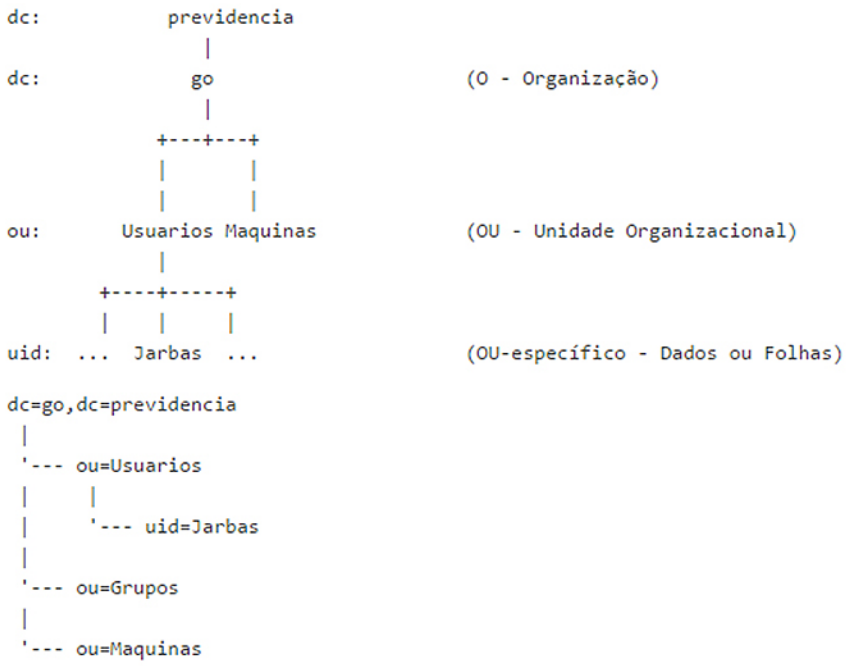
03

Diretórios são preparados para dar resposta rápida a um grande volume de consultas ou operações de busca. Eles também podem ter a habilidade de replicar informações extensamente; isso é usado para acrescentar disponibilidade e confiabilidade, enquanto reduzem o tempo de resposta.

As recomendações do ITU-T X.509 são parte da série de recomendações X.500, que definem serviços de diretório. A ITU-T (Setor de normatização de telecomunicações, responsável por coordenar padronizações relacionadas a telecomunicações da União Internacional de Telecomunicações) define que o diretório é um servidor ou um conjunto de servidores distribuídos que mantêm a base de informações de usuários. Nessa base de informações estão contidos endereços de rede e outros atributos e informações de usuários.

Vejamos um exemplo:

Por exemplo, sabendo-se que Jarbas é uma das pessoas do estado de Goiás que trabalha na previdência, podemos apresentar a figura abaixo para permitir uma melhor visualização deste conhecimento.



Visualização da estrutura do LDAP
Fonte: http://wiki.ubuntu-br.org, 2015.

Na figura acima, o nó mais alto (raiz) é tipicamente o componente nome de domínio “dc” de uma companhia, estado ou organização. Abaixo ficam as entradas representando estados ou organizações nacionais. Abaixo, elas podem ser entradas representando pessoas, unidades organizacionais, impressoras, documentos, ou qualquer outra coisa em que você possa pensar.

04

Antes de iniciarmos o estudo de um novo tópico, verifique se você aprendeu o que acabamos de ver. Responda às perguntas abaixo e, em seguida, clique para verificar a resposta.

- **O que é o LDAP?**

LDAP é um protocolo (TCP/IP) cliente-servidor, utilizado para acessar um serviço de diretório.

- **O que é um serviço de diretório?**

São serviços baseados em diretórios que são preparados para dar resposta rápida a um grande volume de consultas ou operações de busca.

05

1.3 - Tipos de informação

O modelo de serviço do diretório LDAP é baseado em entradas. Como já vimos, uma entrada é um conjunto de atributos e é referenciada através de um nome distinto (DN).

O DN é usado para referenciar uma entrada de forma não ambígua. Cada um dos atributos de entrada tem um tipo e um ou mais valores. Esses tipos geralmente são palavras mnemônicas, como CN para nome comum, ou mail para endereço de correio eletrônico; existem RFCs que determinam essas palavras, com os valores dependendo do tipo de atributo.

Por exemplo, um atributo mail pode conter o valor <usuario@dominio.com.br>. Um atributo fotoJpeg conterá uma fotografia.

06

1.4 - Protocolo Kerberos

É um protocolo de autenticação de rede desenvolvido em 1983 pelo MIT (Massachusetts Institute of Technology), como parte de um projeto de segurança que visava produzir um ambiente de TI seguro e amplamente distribuído pelo campus da universidade.

O Kerberos faz uso de criptografia de chave privada, provê autenticação em redes abertas mediante uso de **algoritmo de autenticação de três vias** (TTP – Trusted Third Party), proposto por Needham e Schroeder.

Todos os equipamentos envolvidos devem confiar mutuamente no sistema de autenticação central provido pelo Kerberos. Esse conceito é semelhante a um cartório no mundo real, ou seja, a sociedade confiará na assinatura de um tabelião para afirmar que os envolvidos realmente se identificaram (autenticaram) durante a assinatura de um determinado contrato.

07

O Kerberos funciona, basicamente, como três componentes principais, um para cada função específica:

a) Ticket	b) Autenticador	c) Centro de distribuição de chaves
• tipo de certificado/token que informa com segurança, para todos os equipamentos conectados ao sistema de autenticação, a identidade do usuário para quem o ticket foi concedido.	• uma credencial gerada pelo cliente com informações que são comparadas com as informações do ticket, para garantir que o cliente que está apresentando o ticket é o mesmo para o qual o ticket foi concedido.	• para acessar uma aplicação, o usuário obtém temporariamente tickets válidos através do centro de distribuição de chaves que ratificam os tickets com o autenticador. A aplicação examina o ticket e o autenticador quanto à validade e concede acesso caso sejam válidos.

Simplificadamente, imagine um sistema de vendas de ingressos para um filme de cinema com classificação para maiores de 18 anos. Para comprar o ingresso, você deve ir então à bilheteria (centro de distribuição) para realizar o pagamento e provar que você possui mais de 18 anos. Ao realizar essas atividades com sucesso, a bilheteria vai lhe fornecer um ingresso (ticket) que você apresentará ao bilheteiro (autenticador), assim que tentar entrar na sala do filme. O bilheteiro vai verificar se o ticket é verdadeiro antes de lhe permitir entrar na sala de cinema.

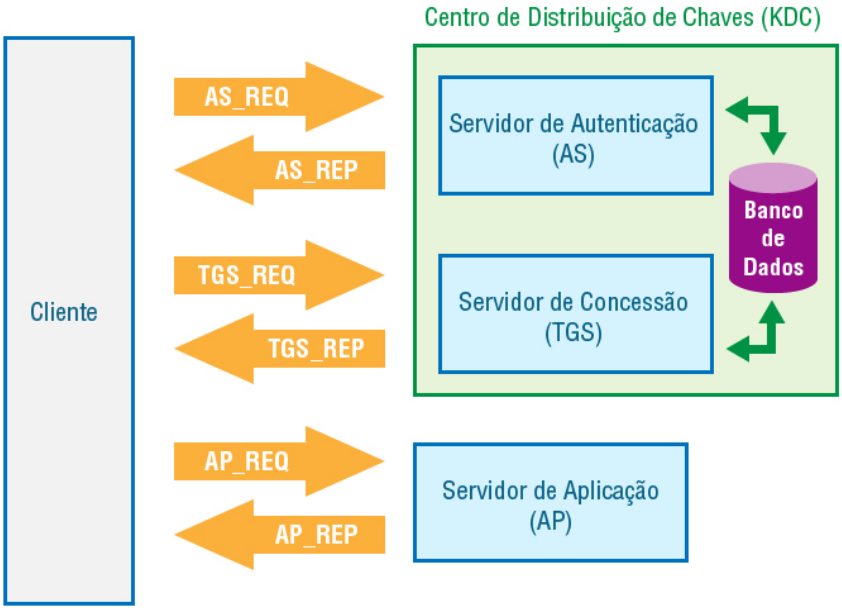
08

Para o processo de autenticação são utilizados três servidores:

a) Servidor de Autenticação (Authentication Server – AS);

b) Servidor de Concessão de Tickets (Ticket Granting Server – TGS);

c) Servidor de Administração (KADM).



Processo de autenticação do Kerberos
Fonte: Internet, 2015.

Servidor de Autenticação (Authentication Server – AS)

Responsável por receber um pedido de autenticação de um usuário e verificar se a identidade desse usuário é autêntica. Sendo válida essa identidade, o AS fornece um ticket e uma chave de sessão, que vai permitir o contato com outro servidor, o TGS.

Servidor de Concessão de Tickets (Ticket Granting Server – TGS)

Responsável por fornecer tickets para serviços específicos requeridos pelo usuário. O contato com o TGS é feito após a autenticação pelo AS. O usuário tem seu ticket avaliado e, uma vez validado pelo TGS, recebe um novo ticket, agora para obter algum serviço disponível.

Servidor de Administração (KADM)

Servidor responsável por controlar as chaves secretas (informações criptografadas). Antes de realizar o processo de autenticação, é preciso que o usuário cadastre seus dados através do KADM, para que possua um login e uma senha.

Resumidamente, os seguintes **passos** são executados quando um usuário tentar acessar um determinado serviço em um Application Server.

1) O usuário realiza uma autenticação em sua estação (utilizando usuário e senha, por exemplo).
2) O Cliente Kerberos então executa uma função hash sobre a senha digitada e isso se torna a Chave Secreta do Cliente/Usuário (aqui chamada de K1).
3) O Cliente Kerberos envia uma mensagem em texto claro para o Authentication Server (AS) contendo o Identificador do Usuário (nessa fase, não é enviada a chave K1 e/ou a senha do usuário para o AS).
4) O AS gera a chave secreta (K1) aplicando a mesma função hash utilizada pelo usuário a partir da senha do usuário encontrada no servidor de banco de dados (por exemplo, o Active Directory no Windows Server).
5) O AS envia de volta ao cliente duas mensagens:
    a. Mensagem A contendo a Chave de Sessão do TGS (K2) cifrada utilizando a chave K1 gerada no passo anterior.
    b. Mensagem B contendo o TGT (Ticket-Granting-Ticket), que inclui a identificação do cliente, endereço de rede do cliente, prazo de validade do ticket e a Chave de Sessão do cliente TGS (K2). Todo o conteúdo do ticket TGT é criptografado usando a Chave Secreta TGS, gerada pelo Servidor TGS e enviada de forma cifrada na Mensagem A.
6) O cliente recebe mensagens A e B e tenta decifrá-las utilizando a chave K1 e, após, tenta recuperar a Chave TGS da Sessão (k2), que está cifrada na mensagem A. Caso não consiga, fica claro que o usuário não possui a chave secreta (k1) e, portanto, não deve ser autenticado.

10

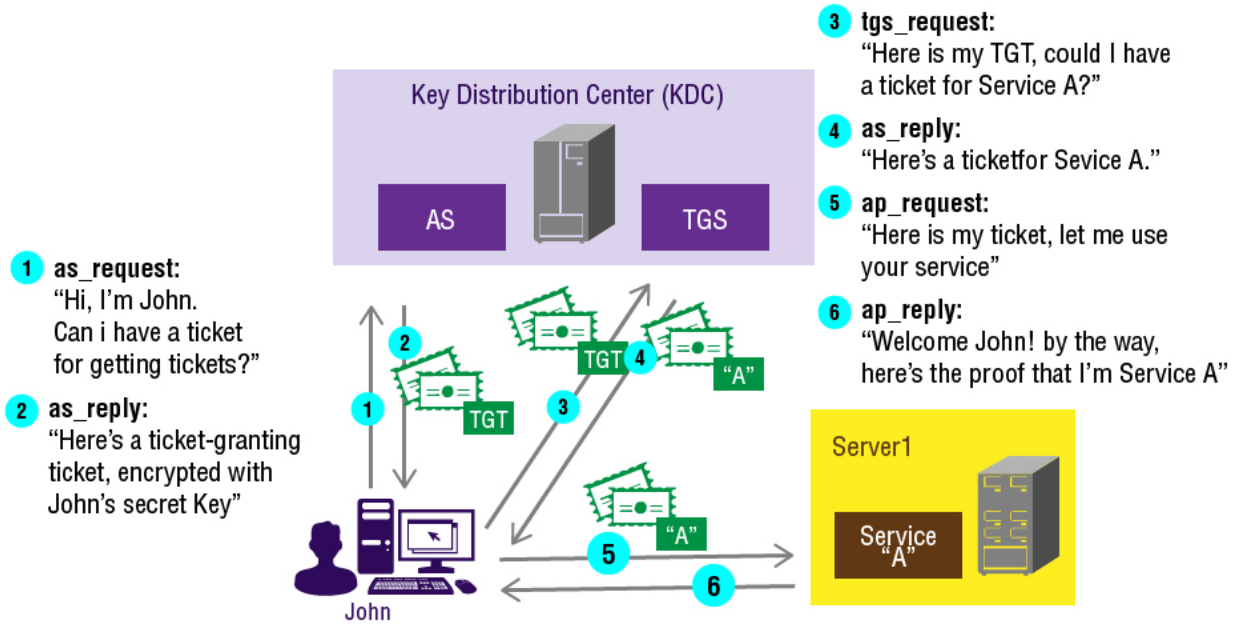
1.5 - Kerberos no Windows

A implementação Kerberos do Windows ocorreu a partir do Windows 2000 Server, o qual passou a ser padrão no Active Directory, o serviço de diretórios da Microsoft.

O Active Directory consiste em um diretório X.500 (LDAP), combinado com autenticação Kerberos. No Active Directory, o Kerberos substitui a autenticação NTLM, facilitando o uso de single sign-on (SSO) e tornando a solução mais segura.

Apesar de o Kerberos ser um protocolo mais robusto, as senhas ainda são armazenadas em formato de Hash no diretório e podem ser obtidas através de utilitários encontrados na internet, como o Cain & Abel, Pwdump e Ophcrack.

A figura a seguir mostra o funcionamento geral do Kerberos.



Funcionamento do Kerberos no Windows.
Fonte: Internet, 2015.

11

1.6 - Acesso a serviços em uma rede

Sempre que um usuário tentar acessar um serviço na rede, o cliente Kerberos enviará para o TGS o TGT que foi gerado pelo serviço de autenticação (KDS). O TGS vai gerar um ticket para o serviço em particular que será utilizado pelo cliente.

Esse funcionamento é detalhado nos passos abaixo, que explicam o funcionamento do protocolo nessa situação:

a) Ao tentar acessar um serviço em um servidor, o cliente Kerberos envia duas mensagens ao TGS.

1) Mensagem C

2) Mensagem D

b) De posse das mensagens C e D, o servidor TGS tentará recuperar o TGT da Mensagem B a partir da mensagem C. Ele vai decifrar a mensagem B utilizando a Chave de Sessão TGS (K2) que ele gerou nos passos anteriores. Isso vai produzir uma Chave de Sessão TGS (k2), que foi informada pelo cliente, a qual ele vai comparar com sua Chave de Sessão TG (K2) que ele possui associada ao cliente. Após isso, ele decifrará a mensagem D e, se tudo tiver acontecido de forma correta, ele enviará ao cliente:

1) Mensagem E

2) Mensagem F

c) De posse das mensagens E e F geradas pelo TGS, o cliente encaminha essas informações para o servidor responsável pelo serviço em que o usuário está tentando acesso, enviando as mensagens:

1) Mensagem E

2) Mensagem G

d) O servidor do serviço decifra o ticket utilizando sua própria chave secreta e recupera a Chave de Sessão Cliente/Servidor (K3). Usando a chave de sessão K3, ele decifra a mensagem G e confirma a veracidade do processo de autenticação. Se tudo tiver acontecido corretamente, o servidor do serviço enviará uma mensagem para o cliente, confirmando sua identidade e o período de validade informado pelo cliente na mensagem G, acrescido de 1.

e) O cliente, ao receber essa mensagem do servidor, verifica a autenticidade da mensagem decifrando-a com a Chave de Sessão Cliente/Servidor (K3) e, também, se a hora está atualizada corretamente. Após esse processo, é iniciado então o acesso ao serviço solicitado.

a.1) Mensagem C

Composta pelo TGT informado na Mensagem B do item anterior e o identificador do serviço que está sendo requisitado.

a.2) Mensagem D

Autenticador, composto pelo identificador do cliente e de um período de validade cifrado com a Chave de Sessão TGS do cliente (K2).

b.1) Mensagem E

Ticket Client-to-Server, que inclui o Identificador do Cliente, o endereço de rede do cliente, um período de validade para a Session Key entre o cliente e o servidor (K3), tudo cifrado, utilizando a chave secreta gerada para o serviço (k2).

b.2) Mensagem F

Chave Secreta entre cliente e servidor (k3) cifrada utilizando a chave TGS gerada para o cliente.

c.1) Mensagem E

Gerada no passo anterior, contendo o Ticket Client-to-Server cifrado utilizando a chave Secreta do Serviço (K3).

c.2) Mensagem G

Uma nova mensagem de autenticação, incluindo o identificador do cliente e um período de validade. Todas essas informações cifradas, utilizando a chave de sessão K3.

12

1.7 - Benefícios do Kerberos

Dentre os principais benefícios de se utilizar o Kerberos em redes de computadores, podemos destacar:

a) Padrões baseados em autenticação robusta.

b) Amplo suporte ao sistema operacional.

c) Provê capacidade de Single Sign-On (SSO).

d) Senhas nunca percorrem a rede.

e) Senhas de difícil previsão.

f) Tickets de autenticação roubados não podem ser reutilizados.

13

1.8 - Organização do Kerberos

O Kerberos oferece um mecanismo para autenticação mútua entre partes, antes de se estabelecer efetivamente uma comunicação segura. O Kerberos usa o que é conhecido como KDC (Key Distribution Center), para facilitar a distribuição segura de permissões e de chaves simétricas dentro de uma rede. O KDC é executado como um serviço em um servidor e mantém uma base de dados para todas as entidades de segurança dentro do chamado Domínio Kerberos.

O Kerberos divide a rede nos chamados reinos (realms). Cada reino possui seu servidor de autenticação e uma política de segurança própria, permitindo diferentes níveis de segurança por reino. Essa divisão

de reinos pode ser hierarquizada, de forma que cada área da organização possua um reino local vinculado a um reino central.

Administrativo Empresa 1 ← → Internet ← → Financeiro Empresa 1

Por exemplo, para que o domínio “Administrativo Empresa1” consiga acessar serviços de “Financeiro Empresa1” em um meio inseguro como a internet, basta que os servidores Kerberos troquem chaves de segurança e se autentiquem mutuamente.

O usuário autenticado em “Administrativo Empresa1” não necessita de outra autenticação para acessar serviços em “Financeiro Empresa1”. Em uma rede Windows, o Kerberos funciona no controlador de domínio e utiliza o Active directory para autenticar, efetivamente, todas as entidades constantes nesse diretório.

Clique aqui para mais informações sobre o funcionamento do protocolo Kerberos.

Clique aqui

Para mais informações sobre o funcionamento do protocolo Kerberos, consulte:

a) RFC 4120 – Related Requests For Comments - The Kerberos Network Authentication Service (V5).

b) RFC 4537 – Kerberos Cryptosystem Negotiation Extension.

c) RFC 4752 – The Kerberos V5 (GSSAPI) Simple Authentication and Security Layer (SASL) Mechanism.

d) RFC 6111 – Additional Kerberos Naming Constraints.

e) RFC 6112 – Anonymity Support for Kerberos.

f) RFC 6113 – A Generalized Framework for Kerberos Pre-Authentication.

g) RFC 6251 – Using Kerberos Version 5 over the Transport Layer Security (TLS) Protocol.

14

Vamos verificar o que você aprendeu sobre o protocolo Kerberos? Responda à questão abaixo e, em seguida, clique para ver a resposta.

- O que é Kerberos e como é utilizado?

Protocolo para autenticar usuários e criptografar informações, criando uma rede na qual em nenhum momento a senha possa ser furtada ou que um computador estranho possa invadi-la durante a

comunicação sem a necessidade de ficar recolhendo dados constantemente durante o processo. É utilizado por meio de três servidores: O AS (servidor de autenticação), o TGS (Ticket Granting Server) e o servidor do serviço desejado.

A primeira fase, autenticação, se baseia em o cliente enviar um pedido para o AS com suas credenciais registradas e o pedido relacionado ao servidor desejado, que serão verificadas com base nos dados armazenados já no servidor AS.

Em caso positivo, o AS irá enviar um TGT (Ticket Granting Ticket) e uma chave criptográfica Cliente/TGS. O TGT contém informações especiais, que carrega as informações tanto do cliente como da própria rede que estavam contidos no servidor AS. Elas serão necessárias posteriormente pelo TGS, o servidor de tickets. Dentro deste ticket existirá um timestamp (marcação do tempo atual do servidor) para cortar a comunicação se ela ficar inativa por muito tempo, por exemplo, cinco minutos. Isto também é importante, pelo fato de o Kerberos contar os segundos entre um envio de uma mensagem para a outra, com o intuito de verificar se houve invasão ou se um dos parceiros na rede foi clonado ou derrubado.

A chave de sessão é criada e em 8 horas ela perderá o seu valor. O cliente envia o TGT recebido para o servidor TGS juntamente com o pacote das suas credenciais. Este é o intermediador entre o servidor de autenticação e os servidores que ofereceram serviços. O ticket estará chaveado de modo que somente o servidor de serviços poderá abri-lo. Depois, o cliente irá receber o ticket junto da chave de sessão Cliente/TGS. Ele irá descriptografar a chave recebida e, após, avisar o servidor TGS que acabou de fazê-lo. Envia o ticket de serviço para o serviço desejado, que irá descriptografá-lo e verificar se o timestamp ainda será válido. Se estas informações estiverem corretas, o serviço enviará uma mensagem para o KDC (Key Data Center) para receber uma chave sessão. Ela será direcionada ao cliente, que irá descriptografá-la e se tudo estiver correto, a comunicação será iniciada e continuará até o cliente interrompê-la ou a validade da sessão se esgotar.

15

1.9 - Certificação digital

A certificação digital é a tecnologia de segurança que provê mecanismos de autenticidade, confidencialidade e integridade às informações eletrônicas que transitam pela Internet e redes de computadores.

No centro da certificação digital está o **certificado digital**, um documento eletrônico que contém o nome, um número público exclusivo denominado "**chave pública"** e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos.

A recomendação X.509 define um framework para provimento de serviços de autenticação de usuário do diretório X.500.

O diretório também pode servir como um repositório de certificados públicos de usuários do repositório. O X.509 define também alternativas de protocolos de autenticação com base no uso de certificados digitais.

A recomendação X.509 é baseada no uso de algoritmos criptográficos de chave pública e assinatura digital. Ela não explicita o uso de um algoritmo especificamente, mas recomenda o uso do RSA.

assinatura digital

É um método de autenticação dos algoritmos de criptografia de chave pública operando em conjunto com uma função Hash, também conhecida como função resumo.

16

1.10 - Autoridades certificadoras

Existem várias implementações de Infraestrutura de Chave Pública (PKI), comerciais e de *software* livre:

a) Microsoft Windows 2008 Server – CertificateAutority.

b) Microsoft Public Key Infrastructure (PKI) for Windows Server 2003.

c) Projeto de *software* livre OpenCA PKI – PublicKeyInfrastructure.

17

2- TRILHAS DE AUDITORIA

A análise dos eventos é uma atividade vital para identificar o que ou quem causou algo ao sistema. O processo de auditoria pode ser dividido em fases definidas na elaboração da política de segurança.

A auditoria em segurança da informação tem o papel de assegurar a qualidade da informação e participar do processo de garantia quanto a possíveis e indesejáveis problemas de falha humana.

Trilha de auditoria é termo genérico para registro de uma sequência de atividades em um sistema ou conjunto deles. A ideia básica da análise de trilhas de auditoria é, em primeiro lugar, registrar e armazenar as atividades do sistema em uma sequência selecionada por projetistas ou administradores com base nas políticas previamente definidas.

Uma auditoria é indispensável para o monitoramento relacionado à segurança de qualquer aplicativo baseado em servidor, de servidores de e-mail a bancos de dados e servidores web. Nos ambientes atuais que valorizam a segurança, uma trilha de auditoria confiável é uma ferramenta valiosa e normalmente um requisito legal para determinadas indústrias.

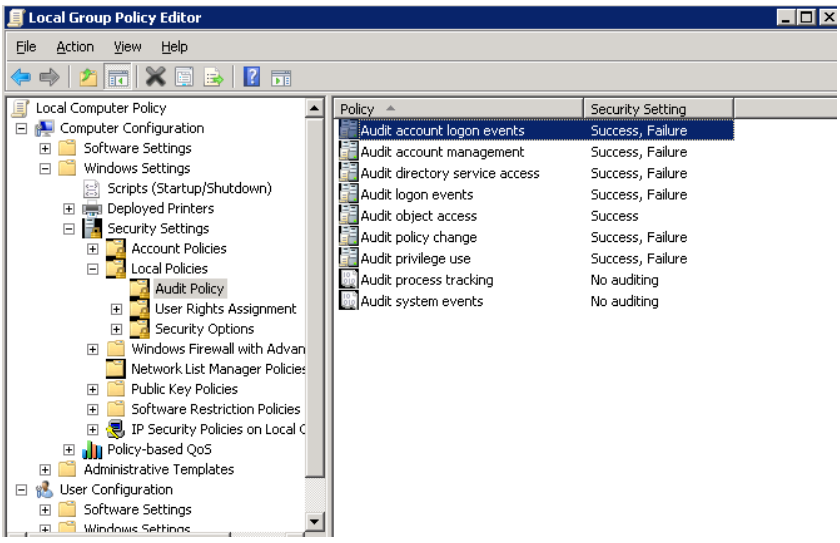
Por exemplo, normas norte-americanas como a Sarbanes-Oxley e a HIPAA (Health Insurance Portability Accountability Act) requerem trilhas de auditoria para determinados sistemas, aplicativos e dados.

18

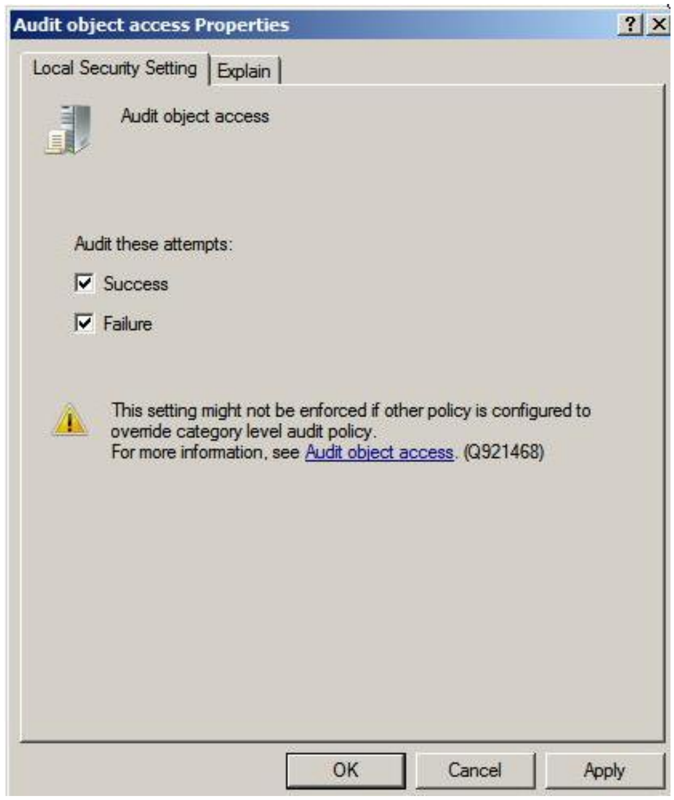
3 - Geração dos dados

Os sistemas operacionais Windows Server 2003 e 2008 fornecem recursos que permitem que um grande número de aplicativos use a funcionalidade de auditoria. Podem ser registrados eventos das atividades realizadas pelo e no sistema.

Um exemplo é a **configuração das diretivas de segurança local do Windows**, ferramenta que permite configurar o registro de eventos, como o acesso a objetos locais, conforme as figuras a seguir.

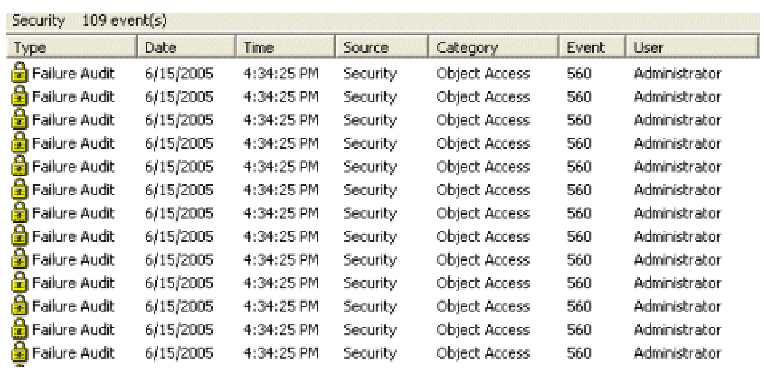


Acesso às funcionalidades de Audit Policy do Windows.
Fonte: Internet, 2015.



Configurando as propriedades de Audit Object Access do Windows.

Fonte: Internet, 2015.



Security 109 event(s)

Type	Date	Time	Source	Category	Event	User
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator
Failure Audit	6/15/2005	4:34:25 PM	Security	Object Access	560	Administrator

Visualizador de Eventos (Audit Failure).

Fonte: Internet, 2015.

19

RESUMO

O LDAP foi criado para prover acesso aos serviços de diretórios do X.500 pelos protocolos da pilha TCP/IP. O LDAP tem a implementação facilitada, exige menos recursos da rede e de memória. Ele foi desenvolvido para aplicações TCP/IP com bom desempenho. Por esses motivos recebeu o nome Lightweight Directory Access Protocol (protocolo leve de acesso a diretórios).

Servidor LDAP é um banco de dados com informações descritivas, baseado em atributos e organizado em forma hierárquica (árvore) e não relacional (tabelas), otimizado para leitura e com certificação digital e baseado em entradas.

Uma entrada é um conjunto de atributos referenciado por Nome Distinto (DN) de forma não ambígua. Cada atributo de entrada tem um tipo de valor, como, por exemplo, CN e ON.

LDAP é um protocolo (TCP/IP) cliente-servidor, utilizado para acessar um serviço de diretório. Foi inicialmente usado como uma interface para o X.500 (Série de recomendações do ITU-T que definem o serviço de diretório). Pode ser utilizado também com autonomia e com outros tipos de servidores de diretório. Atualmente tornou-se padrão e diversos programas já têm suporte a LDAP. Livros de endereços, autenticação, armazenamento de certificados digitais (S/MIME) e de chaves públicas (PGP-Pretty Good Privacy) são alguns dos exemplos de onde o LDAP já é amplamente utilizado.

O modelo de serviço do diretório LDAP é baseado em entradas. Uma entrada é um conjunto de atributos e é referenciada através de um nome distinto (DN). O DN é usado para referenciar uma entrada de forma não ambígua.

Com relação ao Protocolo Kerberos, foi visto que ele é um protocolo de autenticação de rede desenvolvido em 1983 pelo MIT (Massachusetts Institute of Technology), como parte de um projeto de segurança que visava produzir um ambiente de TI seguro e amplamente distribuído pelo campus da universidade. Faz uso de criptografia de chave privada, provê autenticação em redes abertas mediante uso de algoritmo de autenticação de três vias (TTP – Trusted Third Party), proposto por Needham e Schroeder.Todos os equipamentos envolvidos devem confiar mutualmente no sistema de autenticação central provido pelo Kerberos. Esse conceito é semelhante a um cartório no mundo real, ou seja, a sociedade confiará na assinatura de um tabelião para afirmar que os envolvidos realmente se identificaram (autenticaram) durante a assinatura de um determinado contrato.

20

A implementação Kerberos do Windows ocorreu a partir do Windows 2000 Server, onde passou a ser padrão no Active Directory, o serviço de diretórios da Microsoft. O Active Directory consiste em um diretório X.500 (LDAP), combinado com autenticação Kerberos. No Active Directory, o Kerberos substitui a autenticação NTLM, facilitando o uso de single sign-on (SSO) e tornando a solução mais segura. Apesar de o Kerberos ser um protocolo mais robusto, as senhas ainda são armazenadas em formato de Hash no diretório e podem ser obtidas através de utilitários encontrados na internet, como o Cain & Abel, Pwdump e Ophcrack.

Dentre os principais benefícios de se utilizar o Kerberos em redes de computadores, podemos destacar:

a) Padrões baseados em autenticação robusta.

b) Amplo suporte ao sistema operacional.

c) Provê capacidade de Single Sign-On (SSO).

d) Senhas nunca percorrem a rede.

e) Senhas de difícil previsão.

f) Tickets de autenticação roubados não podem ser reutilizados.

Com relação à certificação digital, vimos que é a tecnologia de segurança que provê mecanismos de autenticidade, confidencialidade e integridade às informações eletrônicas que transitam pela Internet e redes de computadores. No centro da certificação digital está o certificado digital, um documento eletrônico que contém o nome, um número público exclusivo denominado chave pública e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos.

Finalmente a Trilha de auditoria que é termo genérico para o registro de uma sequência de atividades em um sistema ou conjunto deles. A ideia básica da análise de trilhas de auditoria é, em primeiro lugar, registrar e armazenar as atividades do sistema em uma sequência selecionada por projetistas ou administradores com base nas políticas previamente definidas. Uma auditoria é indispensável para o monitoramento relacionado à segurança de qualquer aplicativo baseado em servidor, de servidores de e-mail a bancos de dados e servidores web.