Unidade II

2 SISTEMAS DE AUTENTICAÇÃO

Segundo Moraes (2010), para ser mais eficiente, o processo de autenticação deve confirmar o acesso do usuário através de três esferas ou instâncias, o que é chamado de **triple A** ou simplesmente **AAA**. Por meio desse procedimento, verifica-se se o acesso é autêntico, autorizado e auditado.

As soluções AAA são amplamente utilizadas nas redes locais, para acesso remoto, nas intranets, nas extranets e na própria internet.

2.1 Autenticação

A autenticação é o processo de determinar se alguém (ou algo) é realmente quem (ou o que) diz ser (MORAES, 2010).

Os métodos de autenticação são variados. Todos, porém, fundamentam-se em três metodologias principais.

Quadro 6 – Metodologias de autenticação

Metodologia	Exemplo
Algo que você sabe	Senha, resposta
Algo que você tem	Token, certificado digital
Algo que você é	Biometria

A autenticação por **algo que você sabe** é com certeza o método mais conhecido e o mais utilizado nas organizações e na internet. Baseia-se no conhecimento prévio do usuário para permitir a entrada dele em determinado sistema. Login e senha de acesso são os elementos mais comuns. O login (número ou nome) fica registrado no sistema de autenticação de usuário do mecanismo de acesso (servidor de acesso). A senha é cadastrada ou alterada pelo usuário; somente ele a conhece.

Esse método apresenta alguns problemas. Moraes (2010) menciona, por exemplo, a questão da segurança do acesso, que depende da manutenção da senha em segredo, ou seja, depende da consciência do usuário em protegê-la, evitando revelá-la a alguém e estando atento a furtos por invasão e técnicas de engenharia social. As organizações aplicam punições severas para os funcionários que emprestam suas senhas de acesso ou que, por negligência, permitem que sejam descobertas.

Outra dificuldade está ligada ao fato de que, na maioria dos sistemas de autenticação, as senhas trafegam sem nenhuma codificação por criptografia, o que facilita a ação de crackers. Estes utilizam ferramentas de análise de tráfego para rastrear as redes e obter acesso a senhas. Tais ferramentas são chamadas de **sniffers**.

Outra forma muito utilizada para a quebra de senhas de acesso são os ataques de força bruta, nos quais o atacante escolhe o alvo e, com o auxílio de um programa denominado **robô**, testa milhares de senhas possíveis (palavras de dicionário, nomes, números sequenciais). Quanto mais trivial for a senha, mais rapidamente ela será quebrada. O Sans Institute afirma que é possível minimizar o risco por meio de políticas de criação e manutenção de senhas.

Quadro 7 – Políticas de senha segura

Política	Evita
Todas as senhas devem ser mudadas num intervalo de no máximo 30 dias	Ataque de força bruta e engenharia social
As contas de usuário devem ser bloqueadas após três tentativas malsucedidas de usar a senha	Ataque de força bruta
As senhas devem conter caracteres alfanuméricos e numéricos	Ataque de força bruta
Não deve ser permitido o uso das últimas cinco senhas anteriormente cadastradas	Ataque de força bruta
Devem-se utilizar sistemas que criptografem as senhas antes de enviá-las pelas redes	Ataque de interceptação ou ação de sniffers
Todas as senhas devem conter caracteres maiúsculos e minúsculos	Ataque de força bruta
Todas as senhas devem ter no mínimo oito caracteres	Ataque de força bruta
As senhas não podem ser palavras de dicionário ou jargões	Ataque de força bruta
As senhas não podem ser baseadas em informações pessoais, nomes de familiares ou números de telefone	Ataque de força bruta e engenharia social
As senhas nunca devem ser escritas ou armazenadas em papéis ou arquivos	Furto e engenharia social

Adaptado de: Moraes (2010, p. 49).

Existem casos em que o usuário perde a senha acidentalmente, por esquecimento. Por causa disso, é necessário criar um processo bem definido para o recadastramento dela. Em geral, esse processo é realizado presencialmente, a fim de reduzir o risco de fraude. Quando isso não é possível, criam-se mecanismos que atestem a identidade do usuário, como desafio/resposta.

Ataques a senhas são muito comuns e podem ser realizados off-line. O fraudador consegue acesso ao arquivo em que as senhas estão armazenadas e tenta quebrar a criptografia empregada nesse arquivo.

A instalação de vírus no computador da vítima (usuário) também é uma forma de ataque. Os chamados **trojans**, ou **cavalos de troia**, são instalados com o consentimento do usuário. Daí vem o nome de **código malicioso**, que remete à instalação obtida através de alguma forma de engenharia social – por exemplo, supostas promoções imperdíveis enviadas por e-mail.

Exemplo de aplicação

Engenharia social é o nome que se dá a um golpe que explora valores e sentimentos humanos – ganância, medo, curiosidade, preguiça, confiança, entre outros – para conseguir informações confidenciais (pessoais e corporativas). O usuário, enganado, é levado a fornecer essas informações ou a clicar num link que permite a instalação de códigos maliciosos (vírus) no computador.

Reflita sobre esse golpe. É mais fácil desenvolver mecanismos tecnológicos de invasão ou enganar as pessoas e fazê-las entregar o acesso espontaneamente?

Saiba mais

Para conhecer mais a fundo a atuação prática de um engenheiro social, leia:

MITINIK, K.; SIMON, W. L. *A arte de enganar*: ataques de hackers: controlando o fator humano na segurança da informação. Tradução Kátia Aparecida Roque. São Paulo: Pearson, 2003.

A autenticação **por algo que você tem** baseia-se na posse de algum objeto, como um cartão ou um dispositivo (MORAES, 2010).

Não é aconselhável que esta seja a única forma de autenticação, pois um objeto pode ser repassado, por meio de furto, geração de duplicidade ou negligência.

Nesses casos, a combinação de dois fatores de autenticação seria a melhor solução – por exemplo, senha e token.

Figura 4 – Token

Por meio de tokens, mesmo que o fraudador consiga a senha do usuário, sem o dispositivo físico, sua ação será dificultada. Algumas tecnologias aceitam programação de repúdio para os casos em que são realizadas várias tentativas frustradas. Isso é possível pela utilização de servidores que rastreiam o usuário que está de posse do mecanismo físico.

Esses dispositivos costumam apresentar um visor de LCD e um teclado. Em alguns casos, podem ser compostos de um circuito lógico que gera um cálculo de senhas validadas uma única vez. Possuem um relógio interno que sincroniza com um servidor e mostram uma numeração válida por apenas alguns segundos.

Em relação aos smart cards, a solução mais conhecida é o cartão de crédito, ativa desde 1967. Segundo Moraes (2010), existem atualmente mais de 50 milhões de smart cards em circulação, usados como cartões telefônicos, carteira de identidade, carteira de motorista, controle de acesso físico etc.

Os smart cards são dispositivos que têm memória incorporada e criptografia no chip, o que garante a segurança. Esses cartões são autenticados por meio de leitoras.

Figura 5 – Smart card e leitora de smart card

Existem três tipos de smart card:

- **Protegido por senha**: é necessário conhecer uma senha para utilizá-lo. Sua principal característica é a impossibilidade de clonagem.

- **Criptografado**: há uma chave criptográfica armazenada no cartão, usada através de um desafio/resposta enviado ao servidor de autenticação.

- **Sem contato**: trabalha como uma calculadora criptografada. Não existe a necessidade de o cartão estar diretamente ligado à leitora. O usuário digita um PIN (um código) e, em seguida, o smart card devolve uma sequência de números que libera o acesso.

A autenticação **por algo que você** é, segundo Moraes (2010, p. 53),

> [...] baseia-se em alguma característica física ou de comportamento única do indivíduo. O sistema biométrico trabalha com o conceito de verificação e identificação, comparando a característica lida com uma anteriormente armazenada.

A biometria é a ciência que mensura as diferenças entre os seres humanos. Transforma uma característica, seja ela física ou comportamental, em métrica indicadora da unicidade de um ser humano, e utiliza essa unicidade em mecanismos de segurança.

A vantagem desse sistema é não ser preciso lembrar uma senha ou carregar determinado objeto. Basta ser você mesmo e estar previamente cadastrado no sistema.

Quase todos os sistemas biométricos operam da mesma forma: o usuário cadastra suas características num banco de dados e, no momento da leitura, essas características são comparadas com o que foi previamente armazenado; quando há equivalência, ocorre a autenticação. Sempre existe a necessidade da presença física do indivíduo no momento da autenticação.

Há várias técnicas de controle de acesso biométrico. O reconhecimento pode ser feito por impressão digital, retina, voz, íris, geometria das mãos, assinatura, entre outros.

O quadro a seguir mostra vantagens, desvantagens e aplicações de diversos mecanismos biométricos.

Quadro 8 – Comparação entre os mecanismos biométricos

Mecanismo	Vantagem	Desvantagem	Aplicação
Impressão digital	Estabilidade no tempo Unicidade Leitor pequeno e barato	Resistência por parte dos usuários Requer treinamento	Controle de acesso Soluções de autenticação de aplicações
Íris	Estabilidade no tempo Alta precisão	Alta resistência por parte dos usuários Requer treinamento	Acesso físico Caixa de banco Passagem área
Retina	Estabilidade no tempo Unicidade Altíssima precisão	Alta resistência por parte dos usuários Requer treinamento Tempo de leitura	Controle de acesso
Geometria das mãos	Template pequeno Baixa taxa de erro na criação Não é afetado pela condição da pele Não é intrusivo	Tamanho do dispositivo	Controle de acesso Ponto eletrônico

Voz	Facilidade de uso Requer pouco treinamento Não é intrusivo Pode ser usado por telefone	A voz é afetada pelo tempo ou por condições emocionais Pouca precisão Fácil de ser fraudado	Controle de acesso Telefones celulares Banco por telefone
Assinatura	Alta aceitação pelos usuários Treinamento mínimo Conveniente para transações financeiras	Instável Não estabilidade no tempo Requer várias leituras	Dispositivos portáteis Cartão de crédito

Adaptado de: Moraes (2010, p. 62).

2.2 Autorização

De acordo com Moraes (2010), a autorização determina os diversos serviços que o usuário pode acessar na rede. É a etapa posterior à autenticação.

Quadro 9 – Autorização de acesso

Função	Objetivo
Alocação de privilégios de acesso	Alocar o mínimo possível de permissões
Administração de privilégios	Verificar se os privilégios condizem com as atividades atuais do usuário
Registro de privilégios	Organizar e armazenar logs para a auditoria
Limitação do tipo de acesso	Restringir o acesso ao necessário para que o usuário execute suas atividades
Prevenção de acessos não autorizados	Evitar e registrar tentativas de acesso indevidas
Revogação de privilégios de acesso	Excluir acessos quando houver transferências ou demissões

Adaptado de: Moraes (2010, p. 62).

No ambiente de rede, existem diversas formas de autorizar o acesso às bases de dados (lógicas e físicas). Quando falamos de controles de autorização lógicos, referimo-nos a vários métodos para autorizar os usuários a acessarem apenas aquilo que realmente faz parte de sua atribuição. Esses métodos podem ser combinados para aumentar a segurança. Apresentamos os mais utilizados a seguir.

2.2.1 Autorização por serviços de diretório

Serviços de diretório, nativos dos sistemas operacionais para servidores, são repositórios de informações sobre diversos ativos, geralmente de TI, armazenadas de maneira centralizada com o propósito de permitir seu compartilhamento. Normalmente, é possível armazenar num diretório contas de usuário, podendo haver alteração no formato desse armazenamento a fim de suportar aplicações futuras.

Os principais componentes dos serviços de diretório estão amparados na estrutura de armazenamento X.500, nos protocolos de acesso padrão e no LDAP (lightweight directory access

protocol). Também é possível utilizar o protocolo SSL (secure sockets layer) para encapsular a comunicação LDAP de maneira segura e garantir a confidencialidade, a integridade e a autenticação da comunicação.

Para esses serviços, criam-se primeiro as pastas de acesso (os diretórios), geralmente uma para cada setor ou área do negócio; depois, criam-se as estruturas de diretório (as subpastas dentro da pasta principal). Cada usuário fará parte de um ou mais grupos com acesso aos diretórios criados. Pode-se ainda excluir ou acrescentar um acesso, conforme a necessidade.

2.2.2 Autorização por SSO (single sign-on)

É uma simplificação do processo de logon dos usuários. Permite que, após uma única autenticação, o usuário acesse todos os recursos a que tem direito sem a necessidade de repetir o procedimento. A partir do momento em que o usuário valida seu acesso ao ambiente da rede, todos os demais acessos são liberados. Isso facilita muito o dia a dia, mas também pode trazer riscos à segurança da informação, se o gerenciamento não for adequado e se o usuário não estiver ciente da importância de proteger a senha de acesso.

Os tipos de SSO são:

- **Enterprise SSO**: autentica o usuário no serviço de diretório.
- **WAM (web access management)**: permite ao usuário acessar diversos aplicativos web com apenas uma autenticação.
- **Federation**: viabiliza a uma aplicação validar a identidade de um usuário para outra aplicação.
- **Kerberos**: possibilita a autenticação de um usuário em meios inseguros de comunicação, prevenindo problemas de interceptação e ataques do tipo replay.

2.2.3 Autorização por AMS (account management system)

Os modelos de AMS são usados na definição de regras para o acesso aos recursos do sistema e das redes.

- **DAC (discretionary access control)**: o proprietário (owner) do recurso (um arquivo, por exemplo) é quem tem a responsabilidade de atribuir permissões para o acesso.
- **ACL (access control list)**: define, para determinado recurso, quais usuários podem acessá-lo e quais ações estes podem praticar (leitura, escrita etc.).
- **Capability table**: em vez de o usuário passar por um identificador e informar quem é toda vez que for solicitar o acesso a um arquivo, o que demanda verificação por parte do reference monitor, ele recebe as chamadas **capacidades**, referências para o acesso aos arquivos, semelhantes a file descriptors, que já incluem as permissões do usuário para aquele arquivo.

- **MAC (mandatory access control)**: o proprietário de um recurso não diz diretamente quais usuários podem acessá-lo. Em vez disso, ele atribui um rótulo de classificação aos recursos. Na outra ponta, o administrador do sistema cria contas para os usuários e define quais credenciais de segurança eles têm. Caberá ao sistema implementar o conjunto de regras que definirá exatamente quais credenciais podem acessar quais rótulos.

- **RBAC (role-based access control)**: o proprietário pode apenas atribuir permissões a papéis previamente definidos, que representam cargos funcionais, como vendedor ou enfermeiro.

Lembrete

Podemos configurar a autorização unindo os métodos de gestão de acesso dos usuários. Isso aumenta a segurança no controle e na administração.

2.3 Auditoria

O terceiro A do AAA é a auditoria. Todos os passos do usuário dentro da rede devem ser monitorados e gerar evidências. O processo de auditoria é um método de coleta de informações sobre o que é realizado pelo usuário durante o período de acesso à rede de dados. Aos arquivos que armazenam essas informações damos o nome de **logs de acesso**.

Os logs são importantes para a segurança da informação porque, ao registrarem o comportamento do usuário na rede, revelam acessos indevidos feitos por ele ou até mesmo ações de crackers tentando acessar as informações. Outro ponto em que as auditorias auxiliam está ligado ao estudo do comportamento da rede e de suas capacidades.

Arima (1994) define a auditoria de redes de comunicação como a adequação, a avaliação e as recomendações para o aprimoramento dos controles internos da empresa na utilização dos recursos humanos e dos materiais tecnológicos envolvidos na transmissão de informações dentro das redes.

A auditoria de redes verifica se as permissões de acesso condizem com o informado nas atribuições do usuário, se houve tentativas de acesso a diretórios aos quais o usuário não está autorizado ou se ocorreu qualquer tipo de comportamento anormal na rede. Podemos afirmar que o processo de auditoria tem características preventivas, detectivas e corretivas.

Para sistemas em desenvolvimento, a auditoria consiste na revisão e na avaliação do processo de construção de sistemas de informação. Para eventos específicos, abarca a análise da causa, da consequência e da ação corretiva cabível.

Os trabalhos de auditoria abrangem todo o ambiente de tecnologia da informação, em termos de infraestrutura, normas e procedimentos, custos, nível de utilização de recursos e planos de segurança e de contingência.

Os pontos de controle de um processo de auditoria indicam situações que precisam ser validadas, segundo determinados parâmetros internos.

Os resultados dos pontos de controle são demonstrados através de documentos, relatórios, arquivos, pontos de integração, estrutura lógica e física do sistema, modelo entidade-relacionamento etc.

O ciclo de auditoria se inicia com a auditoria de posição, que diagnostica como a organização está atuando em relação aos controles definidos. Após a avaliação dos pontos de controle, eles são selecionados e testados a fim de verificar a existência de fraquezas. Caso haja alguma, os pontos de controle tornam-se pontos de auditoria.

O planejamento e o controle do ciclo de auditoria referem-se à definição da necessidade de recursos humanos, tecnológicos, materiais e financeiros, em função do enfoque, da abrangência e da delimitação da rede a ser auditada, bem como do prazo estabelecido pela alta administração. Devem-se formar equipes de trabalho para a coordenação, a execução e a elaboração de cronogramas, quadros de recursos, orçamentos etc.

Na fase de levantamento, deve ser feita uma caracterização abrangente, em nível macro, para alcançar um entendimento pleno e global do perfil da rede. É necessário analisar a documentação para elaborar um diagrama hierárquico de permissões de acesso.

O inventário de pontos de controle identifica os diversos pontos que o auditor poderá avaliar, os quais podem ser agrupados por meio de processos informatizados, processos manuais e resultados de processamento.

Exemplos de pontos de controle: documentos de entrada, relatórios, arquivos magnéticos, rotinas, programas de computador e pontos de integração.

A eleição dos pontos inventariados relaciona-se com o estabelecimento de prioridades. São aspectos comumente observados: a análise de riscos, a disponibilidade de recursos, os prazos e os cronogramas de trabalho, a decisão gerencial, a relevância do que vai ser avaliado, a natureza da avaliação e o foco dos trabalhos de auditoria.

A revisão e a avaliação consistem em executar testes de validação dos pontos de controle segundo parâmetros internos para a auditoria da rede. Aplicam-se as técnicas de auditoria que evidenciem as falhas ou fraquezas do controle interno. Detectando-se falhas ou fraquezas, elabora-se o relatório de fraqueza de controle interno, apontando soluções que minimizem ou até eliminem os problemas.

O ponto de controle, como visto, transforma-se em ponto de auditoria. Uma vez corrigido, passa por um novo inventário ou uma segunda auditoria.

Na conclusão, apresenta-se, por meio do relatório de auditoria, a opinião final sobre o estado do controle interno dos acessos na rede, que pode ser satisfatório, em baixo, médio ou alto risco, ou não satisfatório.

É possível que alguns pontos elencados não sejam avaliados em sua totalidade, ou que o processo de avaliação não forneça elementos que deem suporte à opinião do auditor. Nesse caso, o status do parecer será **não avaliado**, e na sequência se apresentarão os motivos pelos quais isso ocorreu.

O follow-up consiste em revisar, dentro de um novo projeto de auditoria, os pontos de controle que apresentaram deficiências em trabalhos anteriores. A atividade de follow-up tem por finalidade:

- Identificar se os problemas foram resolvidos, isto é, se as medidas propostas foram adotadas para eliminar as deficiências.
- Adequar e atualizar as recomendações diante das novas realidades tecnológicas e organizacionais.
- Avaliar o comprometimento da administração com a segurança computacional.

A introdução de ferramentas que gerenciem os logs é uma alternativa para administrar a imensidão de dados gerados nos processos de auditoria, o que, de outro modo, demandaria muitas horas de trabalho e incrível capacidade de síntese dos administradores de rede.

Segundo Moraes (2010), as soluções AAA, em geral, estão integradas com algum tipo de produto ou solução de billing, que permite a auditoria completa dos usuários de acordo com seu uso da rede.

Observação

A palavra **billing** significa "cobrança", "tarifação". Na auditoria de redes, dizemos que uma solução de billing vai tarifar (ou seja, armazenar) o comportamento do usuário na rede.

2.4 Exemplos de solução AAA

As soluções AAA são fundamentais para a segurança da informação e das redes. Vamos exemplificá-las por meio das soluções baseadas no protocolo Radius (remote authentication dial-in user service) e no protocolo Kerberos.

A solução baseada no protocolo Radius foi criada na metade dos anos 1990 e padronizada em 1996 pela RFC 2139. Tem como principal característica o conceito de cliente/servidor. Logo no início, mostrou-se eficiente para o acesso remoto conhecido como NAS (network access server), em que esse equipamento é um cliente do protocolo Radius e se comunica via rede com o servidor Radius.

O processo de acesso, autenticação e auditoria funciona da seguinte forma: o NAS solicita ao servidor Radius a autenticação dos usuários que estão tentando o acesso; o servidor Radius coleta uma série de informações do NAS, como o login do usuário, a senha de acesso e a porta a que ele está conectado, e depois verifica se essas informações correspondem ao anteriormente armazenado; se o resultado for positivo, o servidor Radius, através do ACK (acknowledgment), retornará para o NAS a confirmação;

se o resultado for negativo, o servidor Radius, através do NAK (non-acknowledgment), negará o acesso e a conexão será derrubada.

Um Radius pode atender vários clientes. Pode ainda servir de proxy para a autenticação em outros Radius.

Toda a comunicação ocorre com uma chave secreta, ou seja, os dados são criptografados para evitar o acesso indevido.

A autorização pode utilizar mais de cinquenta atributos do Radius, o que possibilita criar múltiplas formas de filtragem no NAS.

Nas auditorias, o servidor Radius permite a criação de logs de acesso que podem ser armazenados. Com isso, mantém um histórico dos acessos dos usuários e provê informações para soluções de billing.

Vários equipamentos e dispositivos de rede podem ser clientes Radius, como roteadores, servidores de acesso, firewalls e switches de rede, o que maximiza sua utilização e auxilia na segurança das informações.

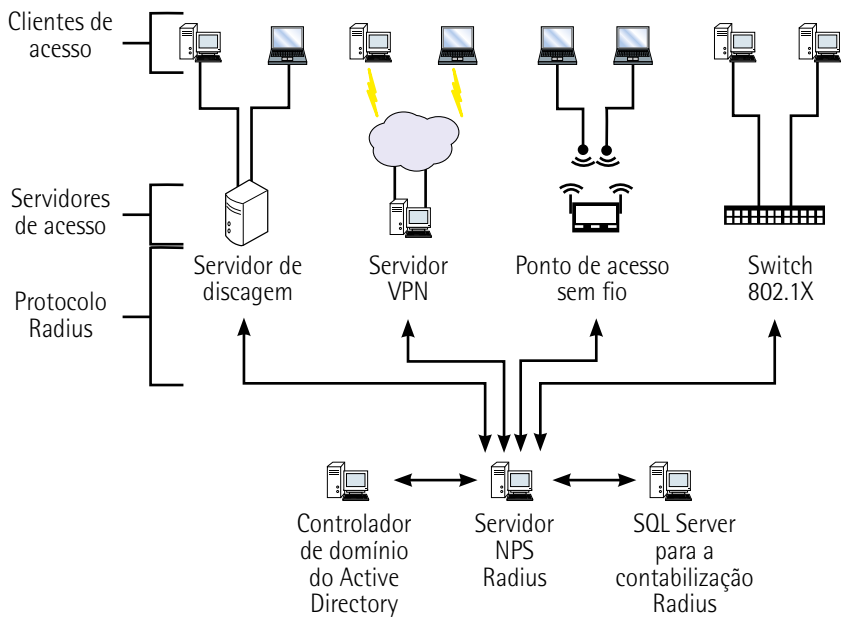

Figura 6 – Sistema de autenticação Radius

O sistema de AAA baseado no protocolo Kerberos trabalha de maneira diferente, mas também segura. Seu padrão, definido pela RCF 1510, foi criado pelo projeto Athena do MIT (Massachusetts Institute of Technology). Trata-se de uma solução confiável para a autenticação de rede, nativa dos sistemas operacionais Microsoft Windows, da versão 2000 em diante. Utiliza criptografia de chave simétrica.

O Kerberos usa um processo de requisição de tíquete criptografado para a autenticação. Nesse processo, o que é enviado pela rede é o tíquete, e não a senha do usuário. Assim, se você deseja acessar um servidor através de uma estação, deve primeiramente pegar o tíquete Kerberos para ser atendido.

Para conseguir esse tíquete, é necessário fazer uma requisição ao servidor de autenticação segura do Kerberos, o qual cria uma chave de sessão, baseada em sua senha, e um valor randômico, que representa o serviço requisitado. Essa chave de sessão é um TGT (ticket-granting ticket). De posse do TGT, você deve enviá-lo ao TGS (ticket-granting server), o qual retorna o tíquete que deve ser enviado ao servidor para a requisição do serviço. O servidor pode aceitar ou rejeitar o acesso. Os tíquetes têm um carimbo de tempo, podendo ser utilizados pelo usuário apenas por determinado período.

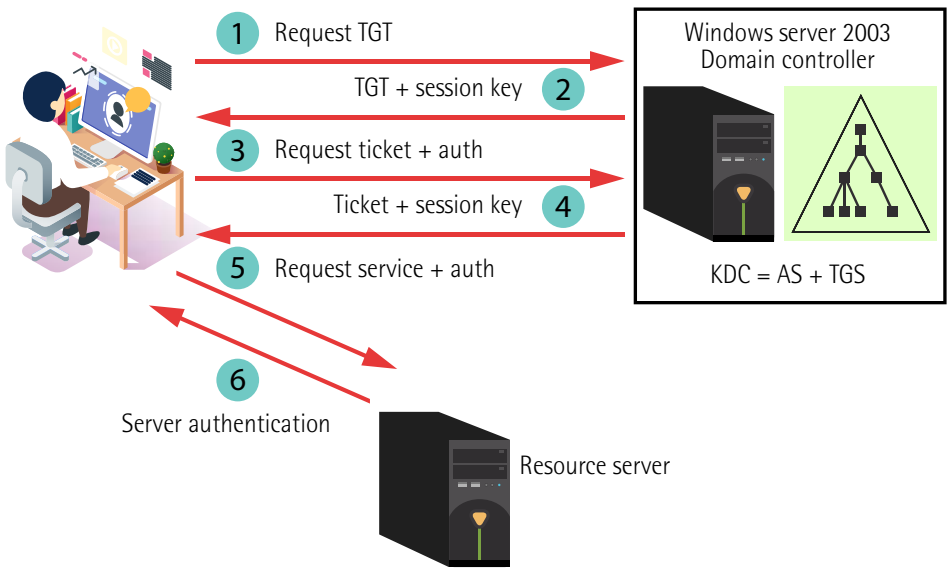

Figura 7 – Sistema de autenticação Kerberos

Saiba mais

Os RFC (Request for Comments) são documentos criados para registrar anotações não oficiais padrão no que diz respeito à descrição de métodos, comportamentos, pesquisa e inovação na internet. Para conhecer melhor o assunto, acesse:

<http://www.rfc-editor.org>.

Resumo

Nesta unidade, tratamos dos sistemas de autenticação em redes. Eles são baseados em três elementos, chamados de triple A ou simplesmente AAA: autenticação, autorização e auditoria.

Na autenticação, verifica-se a identidade da pessoa que está tentando o acesso, ou seja, se ela é realmente quem diz ser. Vimos alguns métodos de

autenticação, como senha, smart card e biometria. Abordamos as políticas de senha segura, apresentamos os tipos de smart card e fizemos uma comparação entre os mecanismos biométricos.

Na autorização, certifica-se o acesso da pessoa ao ambiente de rede. Examinamos os três métodos de autorização mais utilizados, a saber, por serviços de diretório, por SSO e por AMS.

Na auditoria, monitoram-se os passos do usuário no tempo em que ele esteve na rede. A auditoria confere se as permissões de acesso condizem com o informado nas atribuições do usuário, se houve tentativas de acesso a diretórios aos quais o usuário não está autorizado ou se ocorreu qualquer tipo de comportamento anormal na rede.