

Segurança Operacional

Autenticação e Biometria

Gustavo Vilar



- Mini – CV
 - PPF / DPF – Papiloscopista Policial Federal
 - Pós-Graduado em Docência do Ensino Superior – UFRJ
 - Graduado em Ciência da Computação e Processamento de Dados – ASPER/PB
 - Aprovações: PRF 2002, PF 2004, MPU 2010, ABIN 2010, PCF-PF 2013

Gustavo Vilar

- Contatos:



<http://www.itnerante.com.br/profile/GustavoPintoVilar>

<http://www.provasdeti.com.br/index.php/por-professor/gustavo-vilar.html>



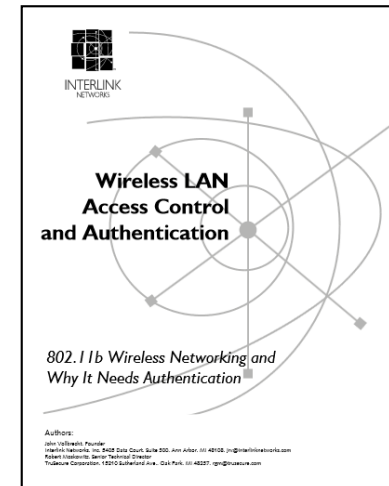
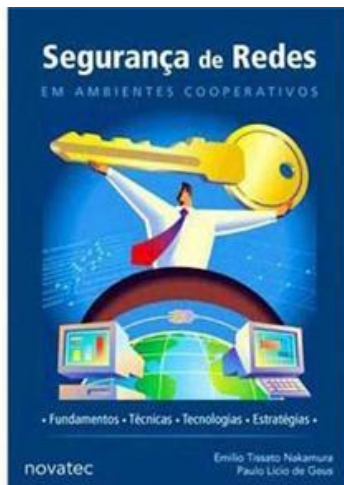
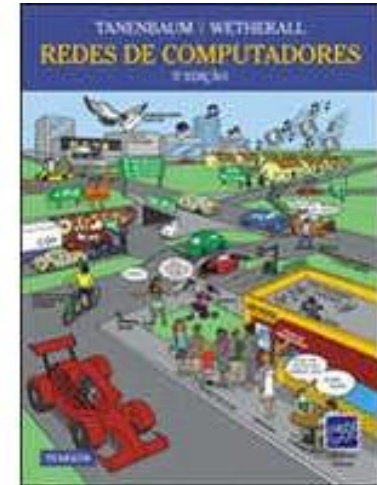
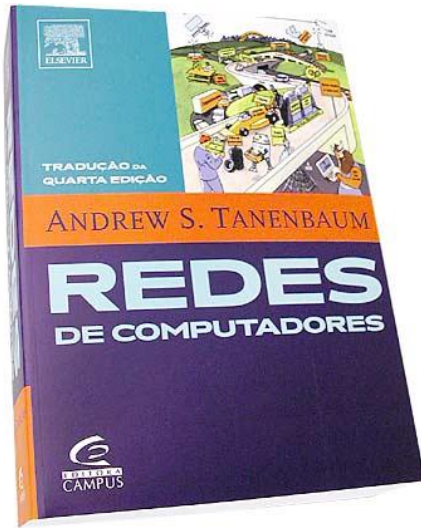
gustavopintovilar@gmail.com

p3r1t0f3d3r4l@yahoo.com.br

Escopo

- Abordar os assuntos mais recorrentes e com fortes tendências para concursos atuais
- Familiarizar o concursando com os tipos de questões mais frequentes.
- Abordar as metodologias de resolução de questões das principais bancas

Bibliografia



Autenticação e Biometria – Carga Horária

- **12 vídeo aulas (03h41m01s / 00h18m25s)**
 - Conceitos e pilares da autenticação
 - O eu sei
 - O que tenho
 - O que sou
 - SSO, Sincronização de senhas
 - Biometria
 - Estágios
 - Índices
 - Espécies
 - Primeira bateria de questões de aprendizagem
 - 802.1x e EAP
 - PAP, CHAP
 - TACACS, XTACACS, TACACS+, KERBEROS, RADIUS, DIAMETER
 - Segunda bateria de questões de aprendizagem
 - Terceira bateria de questões de aprendizagem



Segurança Operacional

Autenticação

Terminologia e conceitos

•Identificação

- Usuário declara uma identidade para um sistema
- Ator: usuário

•Autenticação

- Responsável pela validação de identidade do usuário, processo ou dispositivo
- Ator: Sistema
- O que sou, o que tenho, o que sei. Apenas o usuário legítimo deverá ter acesso aos sistemas e recursos
- Geralmente os métodos de controle de acesso se baseiam na autenticação



Terminologia e conceitos

• Autorização

- Após a autenticação ocorre a autorização para acesso aos recursos
- Ator: Sistema
- Permissão dada direta ou indiretamente pelo dono do recurso ou pelo sistema para utilização do mesmo
 - Garantir que usuários consumam os recursos definidos segundo um perfil

• Acesso

- Habilidade de realizar algo com os recursos computacionais
- Controle de acesso externo
 - Firewalls
 - dial-back modem



Pilares/fatores da autenticação

- **O que sei**

- Senha, Chave, PIN
- Método alternativo: Identificação positiva (bancos)
- Segurança depende do sigilo
 - Mais simples
- Problemas minimizados com OTP
 - mesmo assim é suscetível ao MITM
- SO não deve se manifestar se o usuário ou a senha estão inválidos
 - Unix não mostra nada
 - Windows mostra asteriscos
- Resposta a um desafio



Pilares/fatores da autenticação

•O que sei

—Ataques

- Password Guessing
- Pesca de senhas
- Quebra do sigilo
 - pelo próprio usuário
- Sniffers de rede
- Acesso ao arquivo de senhas do usuário
- Ataques de replay
 - Mesmo criptografadas podem ser reutilizadas
- Ataque de dicionário
- Força bruta
- Keylogger
- etc...



Pilares/fatores da autenticação

•O que tenho

–Token

- Apenas armazenam as informações sem processá-las
- Quase sempre usados em conjunto com as senhas
- "Cartão com valor armazenado"
- Menos de 1 KB
- Não há CPU no cartão. Valores nele contidos devem ser alterados por processadores externos
- Ex: Cartões telefônicos pré-pagos



–Smart Card

- Circuitos integrados
- Possuem certo grau de processamento
- CPUs de 4 Mhz associado a alguma memória ROM ou RAM, tudo entre 512 bytes e 16 KB
- "Cartões inteligentes"
- geralmente empregado como: Objeto + senha



Pilares/fatores da autenticação

- **O que sou / biometria**

- Características físicas ou comportamentais (permanentes ou pouco variáveis)

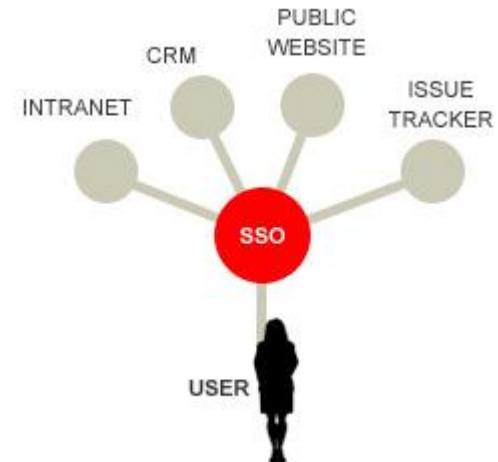
- **Fatores a considerar**

- Nível de intrusão
 - Nível de esforço
 - Nível de precisão
 - Custo



SSO - Single Sign On

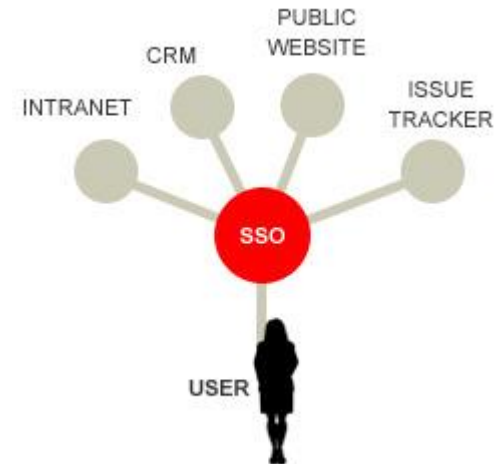
- Proposta de resolução do problema de senhas
- Realidade indesejada
 - Aumento do número de senhas para gerenciamento pelo usuário e administradores
 - Aumento da possibilidade de armazenamento em locais "seguros"
- Realidade proposta
 - Acesso a vários sistemas diferentes, de modo transparente e unificado, por meio de ÚNICA autenticação



SSO - Single Sign On

- Características

- Combinação de Usuários e Senhas Únicos
- Único método de administração, mudanças propagadas em todos sistemas
- Sólida segurança nas sessões de logon e armazenamento de senhas
- Integração das regras de autorização nas múltiplas aplicações
- Elimina necessidade de múltiplas autenticações



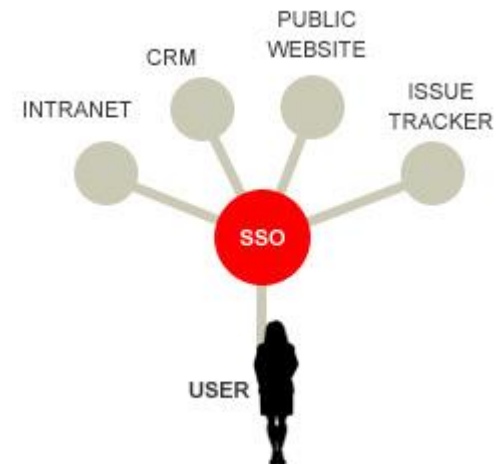
SSO - Single Sign On

- Implicações negativas

- Descoberta da senha = acesso a todos serviços
- Repositório central dos dados do usuário constitui único ponto de invasão, acesso de todos usuários ficará comprometido

- Implicações positivas

- Aumento de produtividade
- padronização da política de nomes de acesso/senhas
- Aplicação consistente na política de segurança



Sincronização de senhas

- Alternativa ao SSO
- Solução menos complexa
- Difere da SSO pelo fato do usuário precisar se autenticar em cada serviço por meio de senha única
- Senha alterada = propagação em todos servidores
- Não requer instalação de software no cliente
- Não constitui único ponto de falha
- Necessidade de autenticação individual em cada sistema



Biometria

- “O que sou”
- Biometria é o método de identificação de pessoas através de suas características físicas e comportamentais
- É hoje um dos principais métodos existentes para identificação e autenticação de pessoas



Biometria

- Passou a ser utilizada em áreas como
 - Identificação criminal,
 - Controle de ponto,
 - Controle de acesso e segurança de instalações
 - Eleições



Biometria

• Os sistemas chamados biométricos podem basear o seu funcionamento em características de diversas partes do corpo humano como

- os olhos,
- a face,
- a palma da mão,
- as impressões digitais,
- a retina ou íris dos olhos,
- as veias e
- a voz



Biometria

- Um sistema biométrico tem como objetivo fornecer uma das seguintes funções
 - Verificação (1:1): "Sou quem afirmo ser?"
 - Comparação de uma dada identidade contra uma única identidade
 - A autenticação dos utilizadores é efetuada considerando um registro previamente efetuado
 - O template capturado no processo de verificação é comparado com a informação biométrica existente na base de dados ou no smart card
 - Identificação (1:n): "Quem sou eu?"
 - comparação de uma dada identidade contra várias identidades
 - O template biométrico gerado é comparado com TODOS os registros existentes na base de dados do sistema biométrico e o resultado dessa comparação é retornado

Biometria

- Fatores a considerar
 - Nível de intrusão
 - Nível de esforço
 - Nível de precisão
 - Custo



Biometria

- Estágios da biometria
 - Captura
 - Extração
 - Comparação
 - Combinação/Não-Combinação



Biometria - Estágios

- Captura

- Um exemplo físico ou comportamental é capturado pelo sistema durante o cadastramento



Biometria - Estágios

- Extração

- Um dado único é extraído do exemplo e um template é criado

- Criação do template



Biometria - Estágios

- Comparação
 - O template é então comparado com um novo exemplo



Biometria - Estágios

- Combinação/Não-Combinação
(Match / Non Match)

- O sistema decide se o atributo extraído do novo exemplo constitui um par ou não



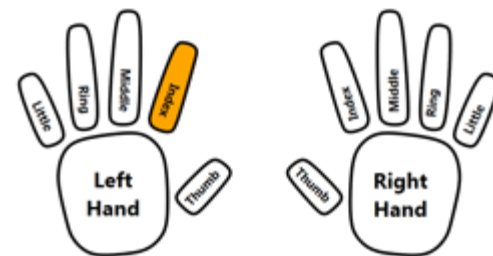
Biometria - Estágios

- Segundo Tanenbaum

- Um sistema biométrico é formado por 2 partes: Cadastramento e Identificação
- O nome de usuário é necessário, uma vez que as medidas não são exatas, dificultando a busca 1:n
- A característica escolhida deve ter uma variabilidade suficiente que o sistema distinga, sem erro, uma entre várias pessoas
- Projetistas devem decidir o nível de semelhança que configurará o "match"

Biometria – Índices Envolvidos

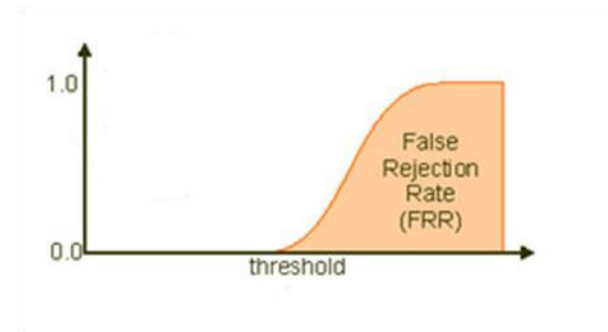
- FTE - Failure To Enrol Rate
 - Falha no registro dos atributos físicos
 - Os registros podem ser armazenados num BD centralizado ou armazenado num cartão inteligente



Biometria – Índices Envolvidos

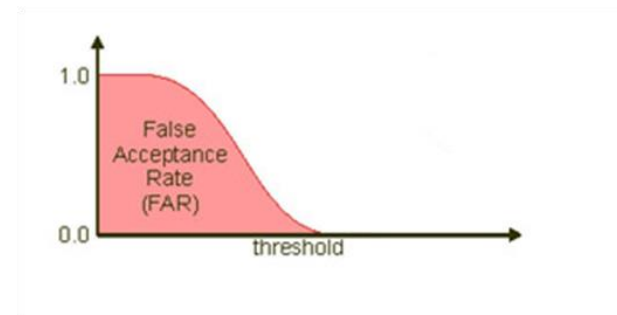
- FNMR False Non-Match Rate ou FRR False Reject Rate

- Não aceitação de um indivíduo correto
- Mocinho é barrado, similar ao falso positivo
- Índice no qual as pessoas autênticas e registradas são rejeitadas como pessoas não identificadas ou não verificadas por um sistema biométrico



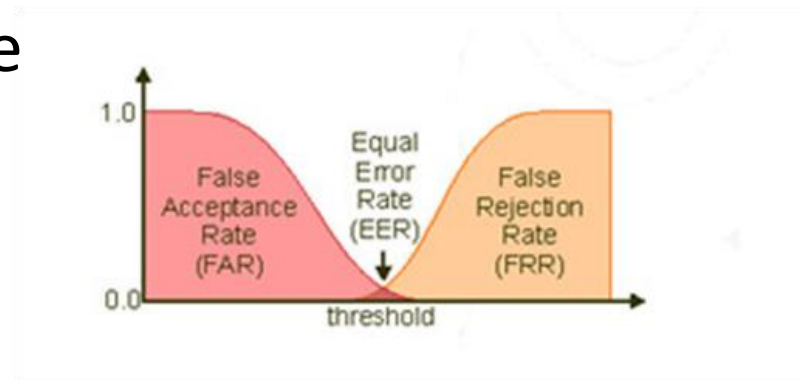
Biometria – Índices Envolvidos

- FMR False Match Rate ou FAR - False Accept Rate
 - Impostor passa
 - Bandido é autorizado, similar ao falso negativo
 - Índice na qual as pessoas não autênticas e não registradas são aceitas como pessoas identificadas e aceitas pelo sistema biométrico



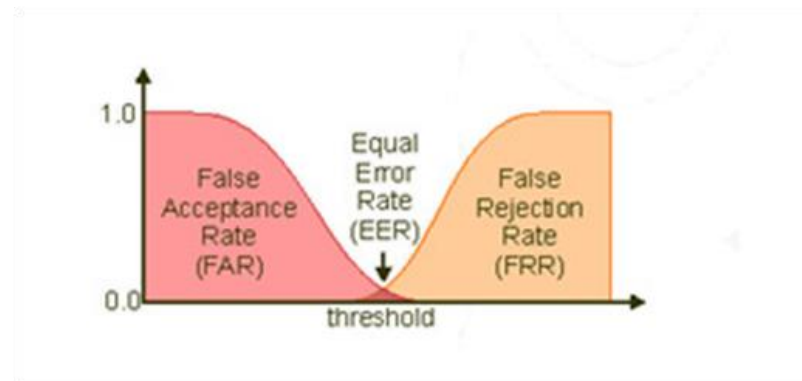
Biometria – Índices Envolvidos

- Índice de Interseção de Erros
 - (EER - Equal Error Rate ou CER - Crossover Error Rate)
 - É o ponto em que o índice de falsas rejeições e o índice de falsas aceitações são iguais
 - Balanceamento da FAR com FRR



Biometria – Índices Envolvidos

- Precisão do crossover
 - Retina
 - Íris
 - Impressão digital
- Três características que podem ser consideradas únicas são a retina, íris e a impressão digital



Biometria – Impressão Digital

- Método atualmente mais utilizado, devido ao baixo custo dos leitores (scanners) e o seu grau de precisão
- Uso de impressões digitais em documentos de identidade não requer aparelhagens sofisticadas
- O reconhecimento é feito com base nas pequenas linhas que há na pele



Biometria – Impressão Digital

- O software destaca alguns pontos dessas linhas (encontro de duas listras, bifurcações e "vales") e forma o desenho de um polígono
- O sistema armazena, então, não a fotografia do dedo, mas só o polígono das minúcias, tática que economiza espaço nos discos e aumenta a agilidade das buscas



Biometria – Impressão Digital

- Características

- Formada no feto e constante ao longo da vida
- Usadas ha mais de mil anos como forma de identificação
- Tecnologia mais utilizada atualmente

- Pontos fracos

- Equipamentos normalmente utilizados para a captura dos padrões não distinguem, eficientemente, um dedo vivo de um dedo morto



Biometria – Impressão Digital

- As limitações

- Impossibilidade de registrar alguns indivíduos,
- Resolução de alguns equipamentos disponíveis,
- Percepção de intrusão

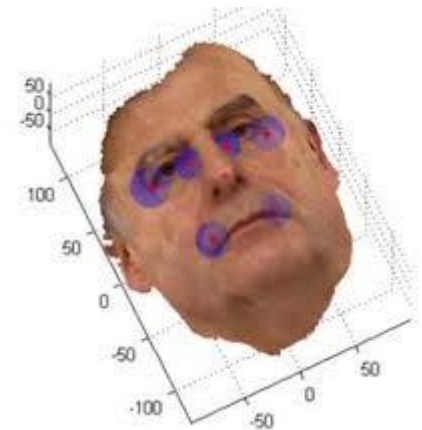
- Principais usos

- Identificação criminal
- Controle de acesso
- Identificação civil
- Segurança de redes de computadores
- Autenticação em pontos de vendas
- Autenticação telefônica e comércio eletrônico
- Vigilância e filtragem



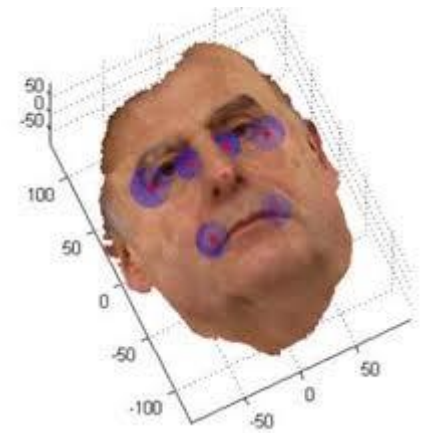
Biometria – Reconhecimento facial

- Método mais natural de identificação biométrica
 - Mapeamento em 128 números denominados coeficientes
 - Expressões, pelos e óculos influenciam no resultado
- Identificação automática é uma tarefa difícil porque a aparência facial tende a mudar a todo tempo
 - Expressões faciais, mudanças no estilo do cabelo, posição da cabeça, ângulo da câmara, condições de luz, etc.



Biometria – Reconhecimento facial

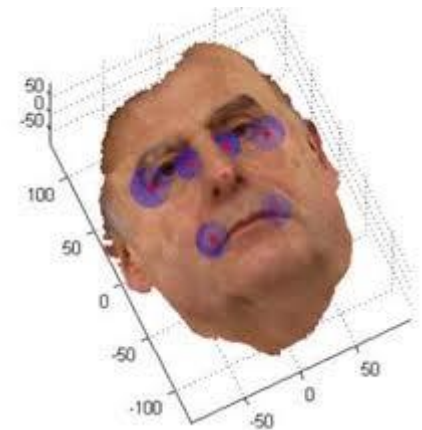
- Estes sistemas utilizam medidas da face como distâncias entre os olhos, nariz, queixo, boca e linha dos cabelos como meio de verificação.
- Alguns sistemas também podem executar testes "animados" para evitar que o sistema seja fraudado por uma fotografia



Biometria – Reconhecimento facial

- Pontos fortes

- Existe larga aceitação pública, já que fotos de faces são usadas rotineiramente em documentos.
- Os sistemas de reconhecimento de face são os menos intrusivos, não exigindo qualquer contato e nem mesmo a colaboração do usuário.
- Os dispositivos de aquisição de imagens 2D são de baixo custo.
- Usado em cassinos com sucesso



Biometria – Reconhecimento facial

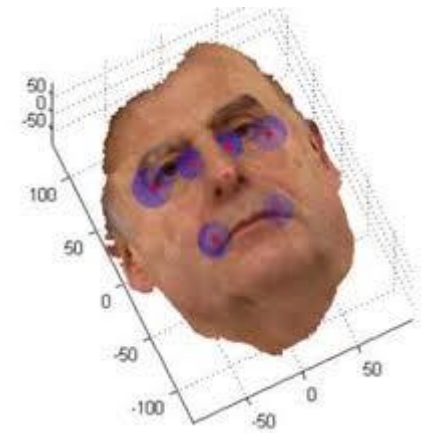
- Pontos fracos

- As condições de iluminação precisam ser controladas. Outros desafios técnicos ainda precisam ser vencidos.

- Boa apenas para aplicações de verificação de pequena escala. Biometria pobre para aplicações de identificação de larga escala.

- Fácil de fraudar o sistema, utilização de disfarces

- Variáveis como óculos de sol, bigode, barba, expressões faciais entre outras, podem causar falsas rejeições nesses sistemas



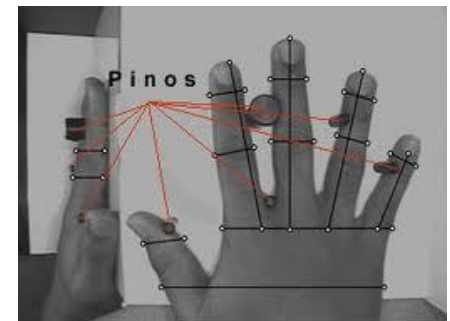
Biometria – Veias das mãos

- Amplia as possibilidades da segurança e controle de acesso a sistemas e locais restritos
- Os padrões das veias das mãos são muito consistentes para a identificação
- Cada mão possui um padrão de veias único e que não se alteram com a idade nem com trabalho pesado
- O sistema adquire uma imagem bastante detalhada do padrão de veias pela utilização de lentes infravermelhas



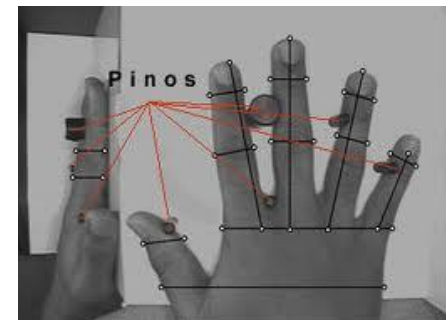
Biometria – Geometria das mãos e dedos

- Analisar e medir o formato da mão
- Uma câmera CCD e espelhos capturam a informação 3D da mão
- Virtualmente não existem duas pessoas com mãos idênticas. O formato da mão não sofre mudanças significativas após certa idade
- É razoavelmente rápida
- Requer pouco espaço de armazenamento



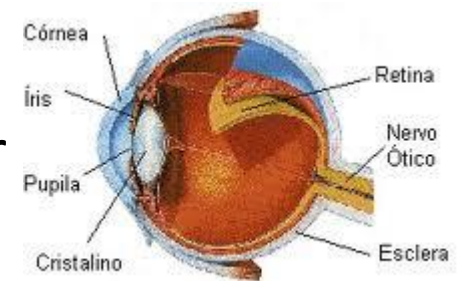
Biometria – Geometria das mãos e dedos

- Tamanho do dedo, largura e área são as principais características usadas nas análises
- Resulta de uma análise das características da mão como a forma, o comprimento dos dedos e as suas linhas características
- Não é uma característica própria de cada indivíduo.
- Pouco utilizada, a tecnologia esta longe da maturidade.
- Melhora a assertividade, quando combinada com outros fatores inerentes a mão, como as linhas da palma



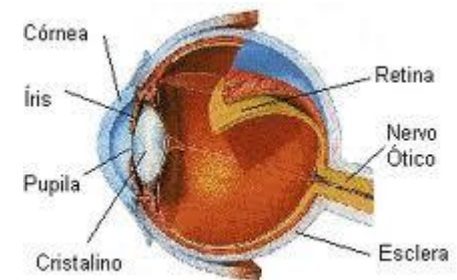
Biometria – Retina

- Analisa a camada de vasos sanguíneos localizada na parte posterior do olho através da utilização de uma fonte de luz de baixa intensidade
- O padrão de veias da retina é a característica com maior garantia de unicidade que uma pessoa pode ter
- É considerada um dos métodos biométricos mais seguros
- Elas são afetadas por doenças, incluindo doenças das quais o paciente pode não estar ciente



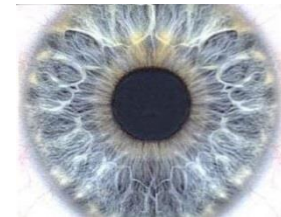
Biometria – Retina

- Esta técnica impulsionou o caminho da utilização da análise da íris
- Mais invasiva do que a análise de íris
 - Requer que o utilizador olhe para dentro de um receptáculo e foque um determinado ponto
- Pouco utilizada.
- Alto custo do equipamento.
- Soluções proprietárias



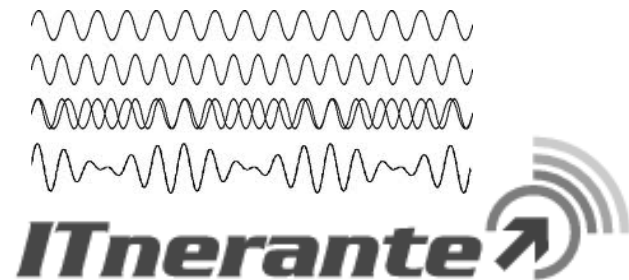
Biometria – Íris

- É o anel colorido que circunda a pupila do olho
- A captura da imagem é feita por uma câmara em preto e branco
- Padrão complexo
 - Pode ser uma combinação de características específicas como coroa, glândula, filamentos, sardas, sulcos radiais e estrias
- Extrai certas características por meio da transformação de uma ondoleta de Gabor e comprime o resultado até 256 bytes
 - Cadeia é compartilhada com o valor obtido no momento do cadastramento
 - Se a distância de Hamming estiver abaixo de um limiar crítico, a pessoa é autenticada
- Eficácia adequada para identificação.
- Baixo custo do equipamento.
- Uma das tecnologias biométricas mais precisas



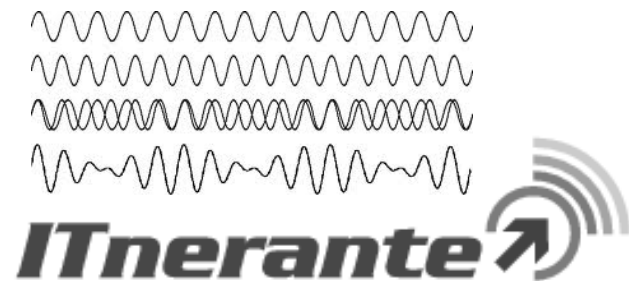
Biometria – Voz

- É um dos sistemas menos invasivos
- O som da voz humana é produzido pela ressonância na região vocal, em função de seu comprimento e do formato da boca e das cavidades nasais
- A forma da onda das frases é medida usando-se análises de Fourier
- Uma vez que as pessoas formam seus padrões de fala através da combinação de fatores físicos e comportamentais, a imitação é impossível
- Os aspectos da voz medida pelos sistemas não são os mesmos que os seres humanos costumam perceber



Biometria – Voz

- Existem problemas com as condições do ambiente onde se encontram os sensores, uma vez que é difícil filtrar o ruído de fundo
- Outros problemas incluem a variação da voz devido às condições físicas do usuário, como gripes e resfriados, estados emocionais,
- Baixo custo hardware: microfone. O resto é software
- Aplicação limitada – baixo nível de segurança (variações na voz)
- Baixa precisão dos sistemas de autenticação
- Sistemas mais avançados dizem ao usuário o que ele deve pronunciar, evitando gravações de uma frase padrão, por exemplo



Biometria – Assinatura manuscrita

- O ritmo necessário para escrever uma assinatura pode ser usado em um sistema de identificação automático
- Os dispositivos utilizados para análise dinâmica são canetas ópticas e superfícies sensíveis
- As assinaturas estão sujeitas ao humor do usuário, ao ambiente, à caneta, ao papel, e assim por diante



Biometria – Assinatura manuscrita

- Métodos

- Um método examina a assinatura já escrita

- A maior desvantagem deste método é que ele não pode detectar fotocópias das assinaturas

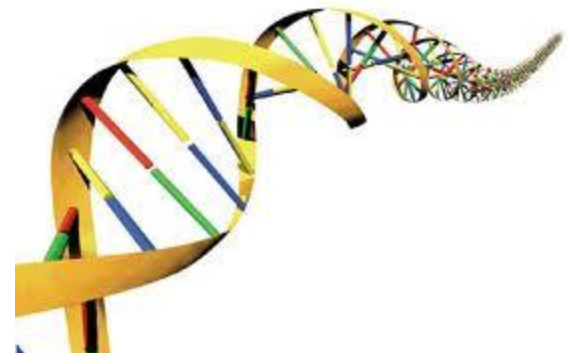
- Outro método estuda a dinâmica da assinatura

- Analisa o processo dinâmico da realização de uma assinatura, o ritmo de escrita, contato com a superfície, tempo total, pontos de curva, laços, velocidade e aceleração



Biometria – Outros fatores

- Outros fatores
 - Odores do corpo
 - DNA
 - Arquitetura da orelha
 - Ondas cerebrais
 - Termografia



Biometria – Concluindo...

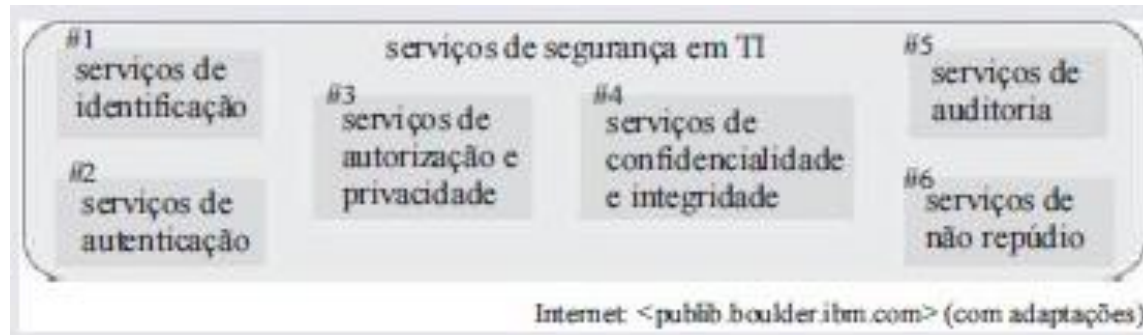
- Existe uma relação inversamente proporcional entre popularidade e custo
- Qualquer esquema de autenticação deve ser psicologicamente aceitável à comunidade de usuários
- Existem problemas culturais
 - Pessoas mais velhas
 - Identificação criminal
 - Invasividade
- Vantagens gerais dos recursos biométricos
 - Não podem ser forjados facilmente
 - Não podem ser esquecidos como acontece com senhas,
 - Obriga que a pessoa a ser autenticada esteja fisicamente presente no ponto de autenticação,
 - Eliminam o problema de roubo de senhas ou a transferência de senhas para outras pessoas.

Questões de Aprendizagem I

Autenticação e Biometria

1. Julgue os itens seguintes, que tratam de gestão de segurança da informação.

[69] Em um sistema de controle de acesso, os usuários podem ser autenticados usando-se biometria, que necessariamente consiste em fazer a digitalização e o reconhecimento de impressões digitais e é considerada uma das formas mais precisas e efetivas de autenticação



2. Considerando a figura acima, que apresenta um conjunto de serviços de segurança de TI, numerados de #1 a #6, assinale a opção correta acerca desses serviços e de suas relações com mecanismos e políticas de segurança.

- A biometria é um mecanismo tipicamente usado para apoiar serviços do tipo #2, mas não do tipo #1.

3. Acerca de segurança da informação, julgue os itens a seguir.

I A biometria é a ciência que verifica e estabelece a identidade de um indivíduo, a partir de características físicas ou comportamentais.

II A identificação descreve o método que garante que o sujeito é a entidade que ele afirma ser, enquanto que a autenticação realiza a verificação de identidade do sujeito.

SSP-CE – UECE 2003 – Perito Criminal Informática

4. A autenticação de mensagens:

- A. somente pode ser verificada pelo legítimo remetente;
- B. pode ser implementada através de senhas ou biometria;
- C. garante que a informação não será corrompida durante o processo;
- D. torna a mensagem transmitida ininteligível a terceiros.

MP MA – FCC 2013 – Analista Ministerial – Seg Info

5. Para permitir que seja possível aplicar medidas de segurança na internet, é necessário que os serviços disponibilizados e as comunicações realizadas por este meio garantam alguns requisitos básicos, como Identificação, Autenticação e Autorização. A Autorização visa

- A. proteger uma informação contra acesso não autorizado.
- B. proteger a informação contra alteração não autorizada.
- C. determinar as ações que a entidade pode executar.
- D. evitar que uma entidade possa negar que foi ela quem executou uma ação.
- E. garantir que um recurso esteja disponível sempre que necessário.

Gabarito

1.E

5.C

2.E

3.C, C

4.B

Padrão 802.1X

- É um método de controle de acesso baseado em portas, definido pelo IEEE
- Pode ser configurado para exigir autenticação mútua entre o cliente e a rede
- Utiliza o Extensible Authentication Protocol (EAP) para autenticar o cliente para a rede e vice-versa
 - Se não houver autenticação, as comunicações não são permitidas
- Modo EAP do WPA e do WPA2 utiliza autenticação 802.1X em vez de chaves PSK
 - Dá a cada usuário ou cliente as suas próprias credenciais de login: nome de usuário e senha e/ou um certificado digital

Padrão 802.1X

- O IEEE 802.1X é o padrão adotado para autenticação, em nível de "porta", em redes IEEE 802 cabeadas ou sem fio, atendendo à arquitetura AAA
 - O padrão define porta como sendo um ponto de conexão à LAN, podendo ser uma porta física, em redes cabeadas, ou uma porta lógica, como no caso da associação entre um dispositivo sem fio e o ponto de acesso
- Um nó wireless precisa autenticar-se antes de poder ter acesso aos recursos da LAN

802.1x – Partes envolvidas

- No modelo 802.1x padrão a autenticação da rede consiste de três partes:
 - O requerente (cliente),
 - Via de regra é um software
 - O autenticador (ponto de acesso, switch)
 - Atua como uma proteção secundária à rede
 - Servidor de autenticação (radius, diameter, etc...)
 - Guarda a base de dados

Processo de uma autenticação 802.1x-EAP

1. O cliente solicita a associação com o ponto de acesso
2. O ponto de acesso responde ao pedido de associação com uma requisição de identidade EAP.
3. O cliente envia uma resposta da identidade EAP para o ponto de acesso
4. A identidade EAP do cliente é encaminhada ao servidor de autenticação
5. O servidor de autenticação envia um pedido de autorização ao ponto de acesso
6. O ponto de acesso encaminha o pedido de autorização ao cliente
7. O cliente envia uma resposta da autorização EAP para o ponto de acesso
8. O ponto de acesso encaminha a resposta de autorização EAP para o servidor de autenticação
9. O servidor de autenticação envia uma mensagem EAP bem sucedida ao ponto de acesso
10. O ponto de acesso encaminha essa mensagem ao cliente e coloca a porta do cliente em modo ENCAMINHANDO.



autenticador



ponto de acesso



requerente

Processo de uma autenticação 802.1x-EAP

- Resumo
 - Fisicamente, o cliente se comunica com o Access Point (AP) através do protocolo Extensible Authentication Protocol over LAN (EAPOL)/802.1X.
 - O AP, por sua vez, se comunica com o servidor de autenticação através do protocolo usado pelo servidor de autenticação sobre UDP/IP

Processo de uma autenticação 802.1x-EAP



EAP TLS

EAP

EAP POR LAN (EAPoL)

RADIUS

IEEE 802.11

UDP/IP

Extensible Authentication Protocol

- O protocolo de autenticação extensível (EAP) possui a responsabilidade de criar um canal lógico de comunicação seguro entre o cliente (supplicant) e o servidor de autenticação, por onde as credenciais irão trafegar
- Uso de um servidor de autenticação isolado
 - Radius
 - Diameter
 - etc...
- O padrão 802.1x é relativamente novo, e os dispositivos que o suportam tem a habilidade de permitir a conexão para a rede na CAMADA 02, somente se a autenticação do usuário for bem sucedida

Extensible Authentication Protocol

- Uma vantagem do uso do protocolo EAP é o aumento de vida útil dos equipamentos que possuem suporte ao protocolo IEEE 802.1x, pois os mesmos passam a funcionar como intermediários entre o host cliente e o servidor de autenticação, não sendo necessário implementar mecanismos adicionais de segurança no próprio equipamento

Extensible Authentication Protocol

- Tipicamente a autenticação do usuário é realizada usando um servidor RADIUS e algum tipo de base de dados de usuários (RADIUS, NDS, Active Directory, LDAP) para validação dos mesmos
- Apenas define o formato das mensagens
 - Cada protocolo que usa o EAP define uma forma de encapsular mensagens EAP dentro de suas próprias mensagens

Tipos de autenticação EAP

•Por senhas

- EAP-MD-5 Challenge
- EAP-Cisco Wireless (LEAP)
- EAP-SPEKE (Simple Password-authenticated Exponential Key Exchange)
- EAP-SRP (secure remote password)

•Por certificados digitais

- EAP-TLS (segurança na camada de transporte) / Por certificados de segurança
- EAP-TTLS (segurança na camada de transporte encapsulada)
- PEAP (Protected EAP)

Tipos de autenticação EAP – Por Senhas

- **EAP-MD-5 Challenge**

- O mais antigo dos tipos de autenticação
- A senha é transmitida de forma cifrada através do algoritmo MD5
- Não fornece um nível de segurança alto, pois pode sofrer ataques de dicionário
- Uso de Chave Secreta
- Não há como autenticar o servidor e não gera chaves WEP dinâmicas

Tipos de autenticação EAP – Por Senhas

- **EAP-Cisco Wireless (LEAP)**

- Usado somente em APs Cisco
- Fornece segurança durante a troca de credenciais, criptografa os dados transmitidos usando chaves WEP dinâmicas e suporta autenticação mútua
- Utiliza nome de usuário e senha e suporta chaves WEP dinâmicas. Por ser uma tecnologia proprietária da Cisco exige que os equipamentos sejam da Cisco e que o servidor RADIUS seja compatível com o LEAP.

Tipos de autenticação EAP – Por Senhas

- EAP-SPEKE

- Faz uso do método SPEKE (Simple Password-authenticated Exponential Key Exchange), que permite ao cliente e servidor compartilhar uma senha secreta o que proporciona um serviço de autenticação mútua sem o uso de certificados de segurança.

Tipos de autenticação EAP – Por Senhas

- EAP-SRP (senha remota segura)
 - Protocolo baseado em senha e troca de chaves seguro
 - Ele soluciona o problema de autenticar o cliente ao servidor de uma forma segura em casos em que o usuário do software cliente deve memorizar um pequeno segredo
 - O servidor carrega um verificador para cada usuário o que permite a ele autenticar o cliente
 - Se o verificador for comprometido, não é permitido a um hacker por exemplo, se fazer passar pelo cliente

Tipos de autenticação EAP – Por Certificados de Segurança

- EAP-TLS (segurança na camada de transporte) / Por certificados de segurança
 - É baseada no uso de certificados, proporciona autenticação mútua do cliente e da rede
 - Certificado em ambos os lados
 - Confia nos certificados do lado cliente e do servidor para realizar a autenticação usando chaves WEP geradas dinamicamente baseadas na sessão e no usuário
 - Tanto o Windows XP quanto o Windows 2000 suportam o EAP-TLS
 - Uso de Criptografia Assimétrica

Tipos de autenticação EAP – Por Certificados de Segurança

- EAP-TTLS (segurança na camada de transporte encapsulada)
 - É uma extensão do EAP-TLS
 - Diferentemente do EAP-TLS, necessita somente de certificados no lado servidor
 - Pode ser usado com sistemas de autenticação existentes tais como: Active Directory e NDS
 - Chaves WEP são distribuídas e geradas dinamicamente para proteger a conexão
 - A autenticação do cliente por parte do servidor faz-se após estabelecer uma sessão TLS utilizando outro método como PAP, CHAP, MS-CHAP ou MS-CHAP v2.

Tipos de autenticação EAP – Por Certificados de Segurança

- PEAP

- Similar ao EAP-TTLS pois somente requer certificado de segurança no servidor. Foi desenvolvido por Microsoft, Cisco e RSA Security.

Outros protocolos utilizados: PAP

- Password Authentication Protocol
- O mais comum entre os provedores de Internet
- Identificação é feita no sentido utilizador para o autenticador: Nome + palavra-chave
- No sentido inverso espera-se a aceitação ou rejeição
- Usado APENAS no início do estabelecimento da ligação

Outros protocolos utilizados: PAP

- PAP
 - A autenticação inicia-se quando o cliente envia um pacote authenticate-request com elementos de autenticação constituído pela combinação do nome do utilizador e palavra chave. Depois que o servidor recebe estes dados, compara-os com os que estão armazenados na sua base de dados e responde com pacote authenticate-ack se forem válidos, ou authenticate-nack se não forem.

Outros protocolos utilizados: PAP

Código	Nome	Sentido	Descrição
1	Authenticate-request	C→S	Pacote de início do protocolo PAP
2	Authenticate-ack	S→C	Confirmação do User/Password
3	Authenticate-nack	S→C	Rejeição do User/Password

Outros protocolos utilizados: CHAP

- Challenge Handshake Authentication Protocol
- Usado no início do estabelecimento da ligação ou posteriormente a qualquer momento
- Um resumo/hash da senha do usuário, em vez da própria senha, é enviada durante o processo de autenticação
- Pressupõe a existência de um desafio enviado pelo servidor ao cliente.
- Chave compartilhada é usada no cálculo

Outros protocolos utilizados: CHAP

1. Servidor de acesso remoto envia um desafio ao cliente de acesso remoto
 - A. Função deve ser complexa o suficiente
 - B. Função é calculada nos dois extremos e comparada
 - C. Só a resposta trafega na rede, não restando ajuda para a próxima vez
2. O cliente de acesso remoto utiliza um algoritmo de hash para calcular um resultado hash MD5 baseado no desafio.
3. O cliente de acesso remoto envia o resultado hash MD5 ao servidor de acesso remoto
4. Esse servidor, que também tem acesso ao resultado hash da senha do usuário, realiza o mesmo cálculo usando o algoritmo de hash e compara o resultado com o enviado pelo cliente
5. Se os resultados corresponderem, as credenciais do cliente de acesso remoto serão consideradas autênticas

Outros protocolos utilizados: CHAP

Código	Nome	Sentido	Descrição
1	Challenge	S→C	Enviado pelo servidor de autenticação a qualquer momento
2	Response	C→S	Valor será comparado com o produzido pelo servidor
3	Success	S→C	Aceitação caso a resposta do desafio seja correta
4	Failure	S→C	Rejeição caso a resposta do desafio seja incorreta



requerente



autenticador



autenticador



ponto de acesso



requerente

TACACS

- Terminal Access Controller Access-Control System

- Protocolo de autenticação remota para UNIX Like

 - Modelo cliente/Servidor

- TCP ou UDP na porta 49

- Possui datagramas em 2 versões

 - TACACS

 - Formato do pacote de request diferente do pacote de reply

- Entre 6 e 16 bytes

 - XTACACS

 - Uso do SLIP

 - Entre 26 e 516 bytes

 - Possuem o mesmo formato para request e reply

- Usuário e senha transmitidos em claro

TACACS+

- Terminal Access Controller Access-Control System **PLUS**
- Surgiu já com a finalidade de substituir o TACACS e XTACACS
- Apesar do nome é um protocolo completamente novo e não mantém compatibilidade com TACACS ou XTACACS
- TCP ou UDP na porta 49

Kerberos

- Protocolo desenvolvido para fornecer poderosa autenticação em aplicações usuário/servidor
- Funciona como a terceira parte neste processo, oferecendo autenticação ao usuário
- Para garantir a segurança, ele usa criptografia de chave simétrica sem estar necessariamente vinculado a um protocolo específico
- TCP e UDP na porta 88



Kerberos

- Premissas

- Em um ambiente distribuído aberto, é necessário autenticar requisições e restringir acesso a usuários autorizados
- É difícil garantir a segurança de muitos servidores em uma rede, mas é viável garantir alta segurança de um único servidor



Kerberos

- Ponto de falha único: É necessária uma alta disponibilidade contínua do servidor central
- Necessita que os relógios internos dos clientes estejam sincronizados com o dele
 - Os Tickets têm um tempo de vida, e se o relógio do cliente não estiver sincronizado com o do servidor, a autenticação irá falhar
 - Na configuração padrão, é necessário que os relógios dos clientes não tenham uma diferença maior do que 10 minutos
 - Na prática, servidores NTP são utilizados para manter os relógios do servidor e dos clientes sincronizados



Kerberos

- Senha nunca trafega pela rede
 - Não sofre com o MITM
- Clientes devem implementar o protocolo
 - Todos sistemas e aplicações devem aceitar tickets em vez do sistema tradicional de senhas



Kerberos

- O sistema de confiança tripla é chamado de Centro de Distribuição de Chaves (CDC / KDC)
- Toda entidade de rede – tanto clientes como servidores – compartilham uma chave secreta que é apenas conhecido por eles mesmos e pelo CDC
- Para a comunicação entre as entidades o CDC gera uma chave de sessão temporária, que serve para garantir a privacidade das informações



Kerberos - Partes

- SA = Servidor de Autenticação / Authentication Server (AS)
 - Confirma a Id dos usuários durante login
 - Responsável pela autenticação em si do usuário, pois a partir de um pedido a este servidor, ele receberá um ticket e uma chave de sessão, podendo assim continuar tentando se conectar com o sistema
 - Kerberos: servidor de autenticação central que contém e valida a senha (chave) e autorizações de todos os usuários e servidores da rede



Kerberos - Partes

- SCT = Servidor de Concessão de Ticket / Ticket -Granting Server (TGS)
 - Emite bilhetes de comprovação de identidade
 - É o responsável pela concessão dos tickets para os serviços que utilizam o Kerberos
 - Uso de tickets e credenciais
 - Conexão inicial é feita com servidor central (SA)



Kerberos - Partes

- SS = Servidor de Serviço
 - Servidor de arquivos ou qualquer outro recurso/serviço



Kerberos - Partes

- Cliente = Aplicação cliente do kerberos no sistema



Kerberos - Partes

- KADM - Servidor de Administração
 - Responsável pelo controle das chaves secretas, cadastrando-as tanto no cliente quanto no servidor. Para isso o usuário precisa fazer o seu cadastramento, escolhendo um username e uma senha

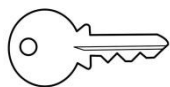


Kerberos

- Funcionamento

- O Cliente requisita ao SA o ticket inicial, o Ticket-Granting Ticket (TGT) para o Kerberos
- O Kerberos retorna ao cliente o TGT requisitado, juntamente com o Session Key
- O cliente requisita o ticket de um determinado serviço para o Ticket-Granting Server (TGS).
- O TGS retorna ao cliente o ticket do serviço requisitado
- O cliente utiliza o ticket para utilizar o serviço





HTTP

SA



Cliente



TGS



FTP

Radius

- Remote Authentication Dial In User Service
 - Provê um sistema de segurança Cliente/Servidor aberto e escalonável.
 - O servidor RADIUS pode ser adaptado facilmente para trabalhar com produtos de segurança de terceiros ou em sistemas de segurança proprietário
 - Qualquer mecanismo de comunicação, seja um software ou um hardware que utilize o protocolo cliente RADIUS pode se comunicar com um servidor RADIUS.

Radius

- Amplamente usado em provedores de acesso a internet
- É importante ressaltar que toda a comunicação entre o host e o cliente RADIUS é realizada na camada de enlace do modelo OSI. Entre o cliente e o servidor RADIUS, a comunicação se dá na camada de aplicação. Somente após o acesso ser autorizado ao host, é que o mesmo tem acesso concedido à camada de rede e superiores

Radius

- Serviço baseado em UDP de pergunta e resposta
 - O RADIUS tem uma porta para autenticação (UDP 1645 ou UDP 1812) e outra para contabilidade (UDP 1646 ou UDP 1813)
- As requisições e respostas seguem um padrão de tabelas (variável=valor)
 - A variável não possui um nome e sim um número.

Radius

- Numa rede que usa RADIUS, há funções distintas para os equipamentos:
 - Cliente
 - host que deseja usufruir de um recurso da rede
 - por exemplo, uma estação que deseja se associar a um Access Point
 - NAS (Network Authentication Service)
 - host que recebe uma solicitação do cliente (o Access Point por exemplo) e autentica esse pedido no servidor RADIUS.

Radius

—Servidor Radius

- host que validará o pedido do NAS
- Resposta Positiva ou negativa
 - (Access-Accept) acompanhada da tabela de parâmetros de resposta
 - » usados para orientar o NAS de como tratar o cliente
 - » tempo máximo de conexão permitida
 - » chave de criptografia que deverá ser usada no canal de comunicação entre o cliente e o NAS
 - (Access-Reject) sem nenhum parâmetro

• A comunicação entre cliente e servidor é encriptada por meio de chave secreta que nunca é enviada pela rede

Radius - Protocolo AAA

- Autenticação

- Confirma a validade do usuário que realiza a requisição de um serviço
- Apresentação de uma identidade junto com uma ou mais credenciais
- Permite autenticação tanto de usuários quanto de dispositivos conectados à rede.
- Requer que tanto o cliente quanto o servidor tenham, cada um, uma cópia da chave de autenticação.
- O servidor RADIUS suporta muitos mecanismos de autenticação, entre esses PPP PAP, PPP CHAP, Unix login, entre outros

Radius - Protocolo AAA

- Autorização

- Concessão de uso para determinados tipos de serviço, dada a um usuário previamente autenticado

- Accounting

- Coleta da informação relacionada à utilização de recursos de rede pelos usuários

- Faz a contabilidade (accounting) do serviço ao qual provê acesso.

- A única forma de confidencialidade a que ele se propõe é a das senhas transmitidas no processo de autenticação

Radius - Mensagens

1. **Access-Request** : Enviada por um cliente RADIUS para solicitar autenticação e autorização de uma tentativa de conexão.
2. **Access-Accept**: Enviada por um servidor RADIUS em resposta a uma mensagem Access-Request. Esta mensagem informa o cliente RADIUS que a tentativa de conexão foi autenticada e autorizada.
3. **Access-Reject**: Enviada por um servidor RADIUS em resposta a uma mensagem Access-Request. Esta mensagem informa o cliente RADIUS que a tentativa de conexão foi rejeitada. Um servidor RADIUS envia esta mensagem se as credenciais não forem autênticas ou se a tentativa de conexão não for autorizada.
4. **Access-Challenge**: Enviada por um servidor RADIUS em resposta a uma mensagem Access-Request. Esta mensagem é um desafio para o cliente RADIUS que exige uma resposta.
5. **Accounting-Request**: Enviada por um cliente RADIUS para especificar as informações de estatísticas para uma conexão que foi aceita.
6. **Accounting-Response**: Enviada pelo servidor RADIUS em resposta a uma mensagem Accounting-Request. Esta mensagem confirma o recebimento bem-sucedido e o processamento da mensagem Accounting-Request.

Radius

- Pode atuar como um proxy para outro servidor RADIUS externo
 - Vantagem para sistemas embarcados

Diameter

- "Raio é a metade do diâmetro"
- Protocolo AAA sucessor do Radius
 - O Diameter é um protocolo baseado no RADIUS, que tenta consertar as deficiências apresentadas no mesmo
 - Não é totalmente compatível com o RADIUS, mas apresenta muitas semelhanças

Diameter x Radius

- TCP ou do SCTP 3868, em vez do UDP
- Maior espaço de endereçamento para atributos e para identificadores
- Melhor controle nas mensagens de erro e notificações de erro, se comparado ao RADIUS (silencioso)
- Segurança provida pelo IPSec ou TLS (fim-a-fim)
- Pacote = cabeçalho + vários Attribute-Value Pairs, or AVPs

Questões de Aprendizagem II

Autenticação e Biometria

1. Julgue os itens que se seguem, referentes a técnicas de comunicação, topologias, arquiteturas e protocolos relacionados às redes de computadores.

[69] Utilizado em dispositivos de acesso a redes sem fio, o padrão IEEE 802.1x provê um mecanismo de autenticação para dispositivos que se conectam a uma porta em uma LAN. Esse padrão envolve três partes: o cliente (também conhecido como suplicante), um dispositivo autenticador e o servidor de autenticação (por exemplo, o Radius).

2. A respeito de segurança lógica em ambientes de redes, julgue os itens a seguir.

[69] Equipamentos de rede modernos tais como roteadores e switches de núcleo de rede suportam o Radius e o TACACS com autenticação de usuários por meio de bases de usuário do tipo LDAP (lightweight directory access protocol).

3. No que concerne a antivírus, antispam e radius, julgue os itens que se seguem.

[62] O free radius, um projeto open source compatível com o Ubuntu Linux, permite realizar autenticação de usuários remotos em redes que necessitem de autenticação centralizada ou serviço de contabilidade para suas estações de trabalho.

Prefeitura SP – FCC 2012 – Auditor Fiscal Tributário

4. Sobre o Kerberos é correto afirmar:

- A. O Ticket Granting Server (TGS) e o Kerberos Authenticator Server (AS) são equivalentes, mas não podem residir na mesma máquina.
- B. A função do Kerberos Authenticator Server (AS) é a seguinte: antes de acessar qualquer serviço, o usuário requisita um ticket para contatar o AS, como se ele fosse um serviço qualquer. Este ticket é chamado de Ticket Authenticator Ticket (TAT).
- C. É um protocolo de autenticação seguro que utiliza criptografia de chave assimétrica. É usado quando um usuário em uma rede tenta utilizar determinado serviço e este quer assegurar-se de que o usuário é realmente quem diz ser.
- D. Usa um processo de requisição de ticket, utilizando criptografia de chave assimétrica para autenticação, que serve para uma requisição em particular a um servidor. Nesse processo o ticket e a senha do usuário são enviados pela rede.
- E. Inicialmente, pelo processo de autenticação do Kerberos, o cliente (que deseja obter autenticação no servidor) deve obter um bilhete de autenticação TGT (ticket-granting ticket) em um servidor de bilhetes que faz parte do sistema de autenticação TGS (ticket-granting server).

5. O protocolo de transporte utilizado pelo RADIUS é

- A. UDP**
- B. TCP**
- C. DCCP**
- D. SCTP**
- E. RSVP**

6. A respeito dos protocolos RIP, OSPF, BGP, TCP/IP e RADIUS, julgue os próximos itens

[76] RADIUS (remote authentication dial in user service) é um protocolo AAA (authentication, authorization e accounting) que permite aplicações para acesso à rede de computadores e mobilidade por meio de rede IP.

7. A respeito de conceitos de RAID e radius, julgue os itens consequentes.

[89] Uma desvantagem do radius é que ele suporta apenas o mecanismo de autenticação PPP.

[93] O radius é um sistema utilizado para prover autenticação centralizada em redes dial-up, VPN e redes sem fio. Ele é responsável por receber pedidos de conexão, autenticar o usuário e repassar ao NAS as informações necessárias para que o usuário acesse a rede.

ALE SP – FCC 2010 – Agente Técnico Administrativo Seg Redes

8. A tecnologia Microsoft Active Directory é um serviço de diretório que
- A. oferece autenticação unificada de usuários para acesso aos recursos da rede, mas não oferece autenticação baseada no protocolo Kerberos.
 - B. oferece tanto autenticação unificada de usuários para acesso aos recursos da rede quanto autenticação baseada no protocolo Kerberos.
 - C. oferece autenticação baseada no protocolo Kerberos mas não oferece autenticação unificada de usuários para acesso aos recursos da rede.
 - D. não oferece sincronização de diretórios entre diferentes servidores.
 - E. oferece seus serviços por meio do armazenamento distribuído dos dados das aplicações.

Gabarito

1.C

5.E

2.C

6.C

3.E

7.E, C

4.E

8.B

Questões de Aprendizagem III

Autenticação e Biometria

ALE SP – FCC 2010 – Agente Técnico Administrativo Seg Redes

1. Considere as seguintes afirmações.

I. Uma das funcionalidades do protocolo RADIUS é a de fazer a contabilidade (accounting) do serviço ao qual provê acesso.

II. O protocolo RADIUS permite autenticação tanto de usuários quanto de dispositivos conectados à rede.

III. O protocolo CHAP requer que tanto o cliente quanto o servidor tenham, cada um, uma cópia da chave de autenticação.

Está correto o que se afirma em

- A. III, apenas.
- B. II e III, apenas.
- C. I e III, apenas.
- D. I e II, apenas.
- E. I, II e III.

2. NÃO é uma característica do TACACS+

- A. utilizar a porta 49.
- B. oferecer suporte ao AppleTalk.
- C. utilizar o TCP como protocolo de transporte.
- D. separar a operação de autenticação da autorização.
- E. ser compatível com o TACACS.

3. Em uma rede de computadores, deseja-se configurar um servidor com as seguintes funções: um serviço de gerenciamento de nomes, um serviço de concessão dinâmica de endereços IPs, um protocolo de autenticação remota e um banco de dados (diretório) para consultas. Os serviços necessários neste servidor, seriam, respectivamente?

- A. DNS, DHCP, NTP, LDAP
- B. DNS, DHCP, TACACS, LDAP
- C. DNS, DHCP, TACACS, HTTPS
- D. NFS, SSH, TACACS, LDAP
- E. NAT, SSH, TACACS, LDAP

ANATEL – CESPE 2009 – Analista Administrativo (adaptada)

4. Com relação a segurança física e lógica, mecanismos de autenticação (TACACS, RADIUS), certificação digital, criptografia e tratamento de incidentes de segurança, julgue os itens a seguir.

[86] As transações entre um cliente e um servidor RADIUS são autenticadas por meio do uso de um segredo compartilhado, o qual nunca é enviado pela rede. A mensagem Access-Request é enviada ao servidor RADIUS através da rede. Se alguma condição não for satisfeita, o servidor RADIUS retorna a mensagem Access-Reject, indicando que a solicitação do usuário é inválida.

SERPRO – CESPE 2008 – Técnico Operação de Redes

5. A respeito de VPN, listas de acessos, criptografia e mecanismos de autenticação, julgue os próximos itens.

[84] Na administração centralizada do controle de acesso, uma entidade é responsável por manter o acesso aos recursos da empresa. Este tipo de administração fornece um método consistente e uniforme de controlar os direitos de acesso por parte dos usuários. Um exemplo de uma administração centralizada é o sistema RADIUS (remote authentication dial-in user service), que utiliza uma autenticação cliente servidor para autorizar usuários remotos.

[85] O TACACS (terminal access controller access-control system) é um protocolo de autenticação remota usado para comunicação com servidores de autenticação. TACACS permite que um cliente remoto, sem necessidade de um servidor de acesso, se comunique com um servidor de autenticação para verificar se o usuário tem acesso à rede.

6. Considerando o protocolo Kerberos, utilizado pelo MS-Exchange Server 2003, para se ter certeza que não haverá problema de conexão com esse protocolo, deve-se liberar no Firewall a porta de número

- A. 21.
- B. 25.
- C. 80.
- D. 88.
- E. 90.

7. Uma das alternativas que pode ser utilizada para autenticar clientes e servidores de uma rede é o protocolo

- A. Kerberos
- B. RPC
- C. MAC Address
- D. PHP Injection
- E. Phishing

Gabarito

1.E

5.C, E

2.E

6.C

3.B

7.A

4.C