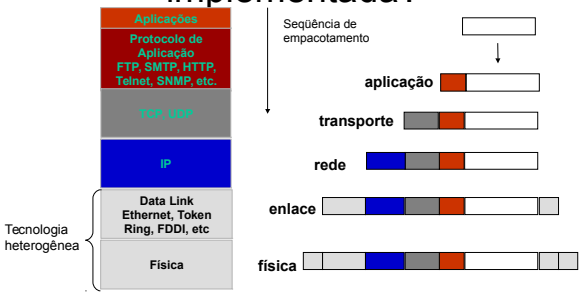
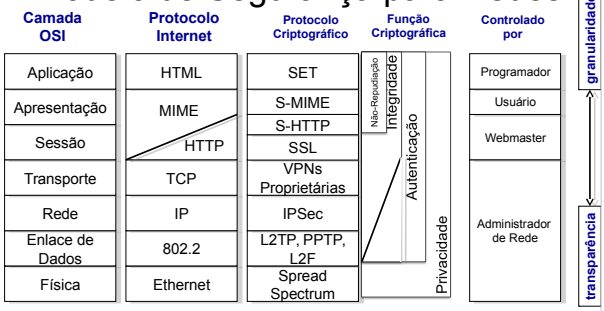
Protocolos para Comunicação Segura

Ricardo C. A. da Rocha

Como a criptografia pode ser implementada?



Modelo de Segurança para Redes



Jay Haiser. **"Three New Models for Application of Criptography"**. In: Information Security Management Handbook

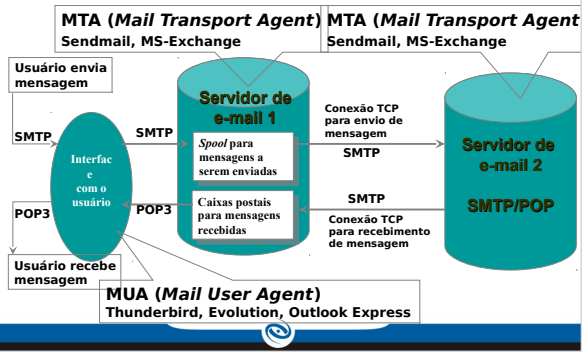
Protocolos para Comunicação Segura

Ricardo C. A. da Rocha

Roteiro

- E-mail Seguro
- Camada de Rede: IPSec
- Camada de Transporte: TLS
- VPN: Redes Virtuais Privadas
- Segurança em Redes sem Fio
- DNS Seguro: DNSSec

Sistema de Correio Eletrônico



Mensagem de Correio

Dividida em duas partes: cabeçalho e corpo

Cabeçalho

- Contém informações necessárias à transferência da mensagem
- Informa por quais servidores de correio a mensagem passou
- Informa a data de envio e de recebimento
- Contém os seguintes campos, dentre outros:
  - Endereço do remetente (campo “From: ”)
  - Endereço do destinatário (campo “to: ”)
  - Assunto da mensagem (campo “subject: ”)
  - Destinatários que receberão uma cópia da msg. (campo “cc: ”)
  - Destinatários que receberão uma cópia escondida (campo “bcc: ”)

Corpo

- Contém a mensagem propriamente dita

Endereço Eletrônico

Formato do Endereço Eletrônico

- São escritos através de um par de identificadores separados pelo símbolo @

nome_do_usuário@nome_do_dominio

- Exemplo

ricardo@inf.ufg.br

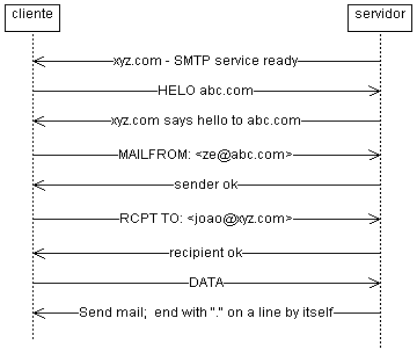
- **nome_do_usuário**
  - Identificação (*Login*) do usuário na rede
  - Não podem conter espaços e nem acentos
- **nome_do_domínio**
  - Identifica o domínio do usuário destinatário
  - Pode ser o nome do servidor de correio do domínio
  - Será usado para a procura do registro MX do DNS

SMTP

Simple Mail Transport Protocol

- Protocolo da família TCP/IP encarregado de transmitir mensagens de correio eletrônico
- Se assemelha ao sistema de correio comum
  - Confia integralmente nas informações passadas pelos agentes
- Utiliza o TCP
- Atende requisições de clientes na porta 25
- Utiliza o registro MX do DNS para descobrir o servidor de destino
- Paradigma comando/resposta
  - Para cada comando enviado do Emissor-SMTP para o Receptor-SMTP ocorrerá uma resposta do Receptor com um código numérico seguido de um texto
  - Comandos básicos obrigatórios
    - **HELO**, **MAIL FROM**, **RCPT TO**, **DATA**, **NOOP**, **QUIT** e **RSET**

SMTP



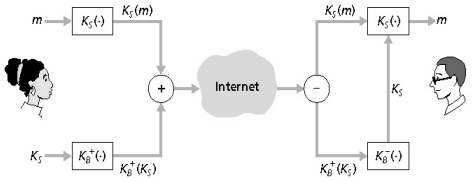
Exemplo de Sessão de Comunicação

Cliente estabelece comunicação via sockets TCP com a porta 25 do servidor de SMTP

Cliente	Servidor
	← 220 smtp2go.com ESMTP Exim
→ HELO mydomain.com	
	← 250 Hello mydomain.com
→ MAIL FROM:<sender@mydomain.com>	
	← 250 Ok
→ RCPT TO:<recipient@anotherdomain.com>	
	← 250 Accepted
→ DATA	
	← 354 Enter message, ending with "." on a line by itself
→ Subject: sample message	
→ From: sender@mydomain.com	
→ To: recipient@anotherdomain.com	
→	
→ Greetings,	
→ Typed message (content)	
→ Goodbye.	
→ .	
	← 250 OK
→ QUIT	
	← 221 www.sample.com closing connection

E-mail seguro

- Alice quer enviar e-mail confidencial e-mail, m, para Bob.



Alice envia uma mensagem de e-mail, *m*

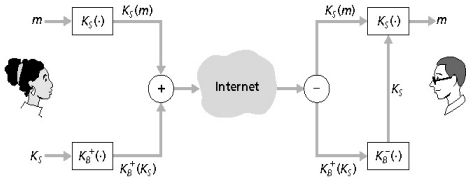
Bob recebe uma mensagem de e-mail, *m*

Alice:

- Gera uma chave privada *simétrica*, K_S
- Codifica mensagem com K_S (por eficiência)
- Também codifica K_S com a chave pública de Bob
- Envia tanto $K_S(m)$ como $K_B(K_S)$ para Bob

E-mail seguro

- Alice quer enviar e-mail confidencial e-mail, m, para Bob.



Alice envia uma mensagem de e-mail, *m*

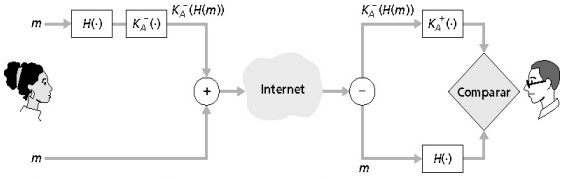
Bob recebe uma mensagem de e-mail, *m*

Bob:

- Usa sua chave privada para decodificar e recuperar K_S
- Usa K_S para decodificar $K_S(m)$ e recuperar m

E-mail seguro

- Alice quer fornecer autenticação de emissor e integridade de mensagem.



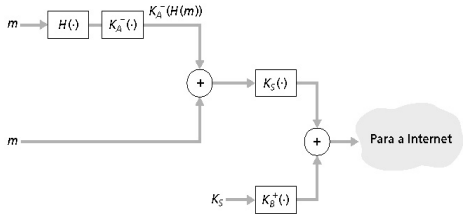
Alice envia a mensagem de e-mail *m*

Bob recebe a mensagem de e-mail *m*

- Alice assina digitalmente a mensagem
- Envia tanto a mensagem (aberta) quanto a assinatura digital

E-mail seguro

- Alice quer fornecer confidencialidade, autenticação de emissor e integridade de mensagem



Alice usa três chaves: sua chave privada, a chave pública de Bob e uma nova chave simétrica

Soluções para E-mail Seguro

- Padrão OpenPGP (RFC 4880) – padrão de fato
  - PGP – Pretty Good Privacy
  - GPG – Gnu Privacy Guard
- S/MIME (RFC 2633)
  - Aplicável em qualquer cenário de envio de dados usando MIME, não apenas e-mail.
  - Tipo de dado: **`application/pkcs7-mime`**

Pretty good privacy (PGP)

Esquema de codificação de e-mail da Internet, padrão de fato

Usa criptografia de chave simétrica, criptografia de chave pública, função de hash e assinatura digital, como descrito

Fornece confidencialidade, autenticação do emissor, integridade

Uma mensagem PGP:

```
---BEGIN PGP SIGNED
MESSAGE---
Hash: SHA1

Bob:My husband is out of
town tonight.Passionately
yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4
vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

Protocolos para Comunicação Segura

Ricardo C. A. da Rocha

Roteiro

E-mail Seguro
Camada de Rede: IPSec
Camada de Transporte: TLS
VPN: Redes Virtuais Privadas
Segurança em Redes sem Fio
DNS Seguro: DNSSec

IPsec: Segurança de camada de rede

Confidencialidade na camada de rede:
- Hospedeiro transmissor criptografa os dados no datagrama IP
- Segmentos TCP e UDP; mensagens ICMP e SNMP

Autenticação na camada de rede
- Hospedeiro de destino pode autenticar o endereço IP da origem

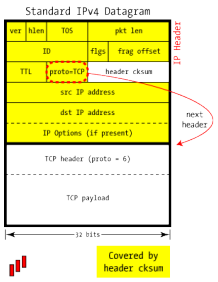
Dois protocolos principais:
- Protocolo de autenticação de cabeçalho (AH)
- Protocolo de encapsulamento seguro dos dados (ESP)

Tanto o AH quanto o ESP realizam uma associação da fonte e do destino:
- Cria um canal lógico de camada de rede denominado associação de segurança (SA – Security association)

Cada SA é unidirecional

Unicamente determinado por:
- Protocolo de segurança (AH ou ESP)
- Endereço IP de origem
- ID de conexão de 32 bits

Datagrama IP



Protocolo de autenticação de cabeçalho (AH)

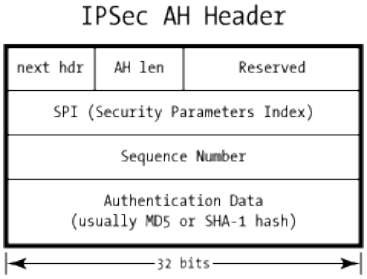
Oferece autenticação de fonte, integridade dos dados, mas não confidencialidade

- Cabeçalho AH é inserido entre o cabeçalho IP e o campo de dados
- Campo de protocolo 51
- Roteadores intermediários processam o pacote na forma usual

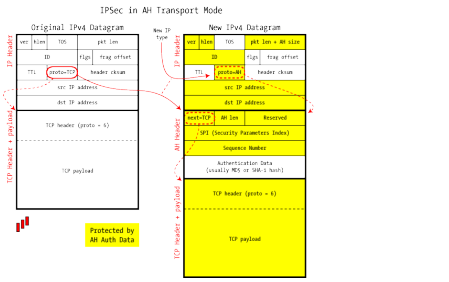
Cabeçalho AH inclui:

- Identificador de conexão
- Dados de autenticação de dados: resumo da mensagem assinado pela fonte calculado sobre o datagrama IP original.
- Campo de próximo cabeçalho: especifica tipo de dado (ex.: TCP, UDP, ICMP)

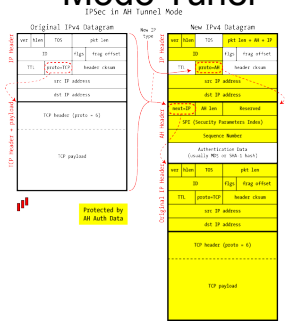
Modo AH - Autenticação



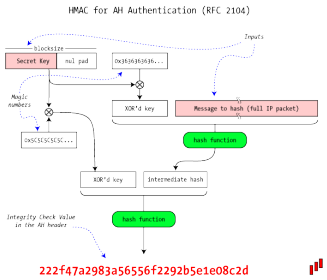
Modo de Transporte



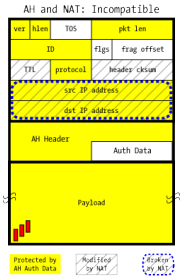
Modo Tunel



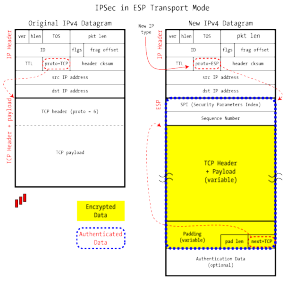
Autenticação baseada em HMAC



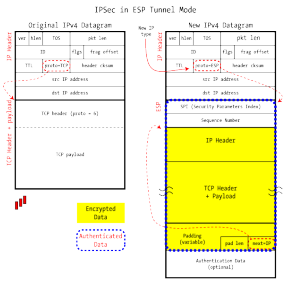
AH e NAT



Encriptação



Modo Tunel com Tunelamento



Protocolos para Comunicação Segura

Ricardo C. A. da Rocha

Roteiro

E-mail Seguro
Camada de Rede: IPSec
Camada de Transporte: TLS
VPN: Redes Virtuais Privadas
Segurança em Redes sem Fio
DNS Seguro: DNSSec

Camada de sockets segura (SSL)

Segurança de camada de transporte para qualquer aplicação baseada no TCP usando serviços SSL
- Usado entre browsers Web e servidores para comércio eletrônico (https)

Serviços de segurança:
- Autenticação de servidor
- Criptografia de dados
- Autenticação de cliente (opcional)

Servidor de autenticação:
- Browser com SSL habilitado inclui chaves públicas para CA confiáveis
- Browser pede certificado do servidor, emitido pela CA confiável
- Browser usa chave pública da CA para extrair a chave pública do servidor do certificado

SSL

Sessão SSL criptografada:

- Browser gera chave de sessão simétrica, criptografa essa chave com a chave pública do servidor e a envia para o servidor
- Usando a chave privada, o servidor recupera a chave de sessão

Browser e servidor conhecem agora a chave de sessão

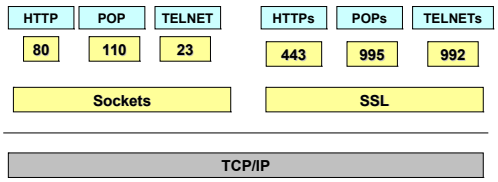
- Todos os dados são enviados para o socket TCP (pelo cliente e pelo servidor) criptografados com a chave de sessão

SSL: base do padrão Transport Layer Security (TLS) do IETF

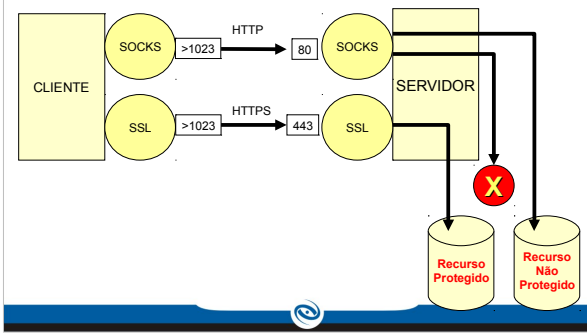
SSL pode ser usado por aplicações fora da Web; ex., IMAP.

SSL

SSL: Secure Sockets Layer



Exemplo: HTTPS



Secure Socket Layer (SSL) e Transport Layer Security (TLS)

O SSL/TLS permite executar duas funções básicas:

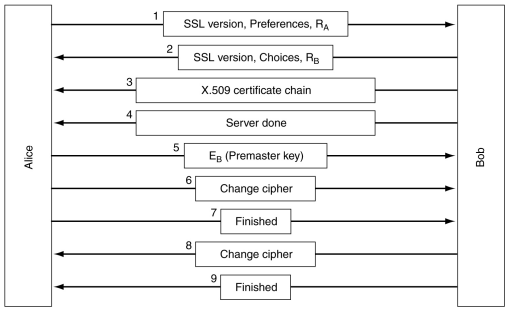
- autenticação entre o cliente e o servidor.
- criptografia na troca de mensagens.

O servidor se autentica para o cliente (obrigatório)

SSL/TLS

O cliente se autentica para o servidor (opcional)

Handshake SSL

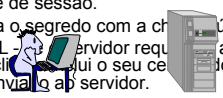


SSL Handshake

1. Do Cliente para o Servidor
   - versão do SSL
   - configuração de criptografia
2. Do Servidor para o Cliente
   - versão do SSL
   - configuração de criptografia
   - certificado do servidor
   - (opcionalmente, requisita o certificado do cliente)

SSL Handshake

3. O Cliente:
   - Usa as informações recebidas para autenticar o servidor.
   - Se a autenticação falhar, o usuário é alertado sobre o problema e a conexão é abortada.
   - Se o servidor for autenticado, o cliente:
     - Cria um segredo que futuramente será usado para criar uma chave de sessão.
     - Criptografa o segredo com a chave pública do servidor.
     - OPCIONAL - Se o servidor requisitar autenticação do cliente: o cliente inclui o seu certificado junto com o segredo enviado ao servidor.



SSL Handshake

4. O Servidor:
   - (OPCIONAL: se o certificado do cliente foi solicitado) o servidor verifica a identidade do cliente.
     - Se a verificação falhar, a sessão é terminada.
   - O servidor usa sua chave privada para decifrar o segredo e segue uma série de procedimentos para gerar a chave de sessão/chave secreta.
   - O servidor informa ao cliente que completou a geração da chave de sessão/chave secreta.

SSL Handshake

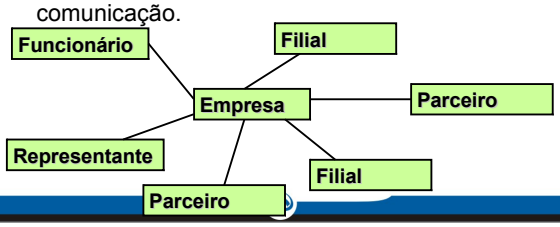
5. O Cliente:
   - Gera a chave de sessão (secreta) a partir do segredo, utilizando os mesmos procedimentos que o servidor.
   - O cliente informa ao servidor que completou a chave de sessão.
6. O handshake está completo.
   - Cliente e servidor criptografam suas mensagens usando a chave de sessão.

Roteiro

E-mail Seguro
Camada de Rede: IPSec
Camada de Transporte: SSL
VPN: Redes Virtuais Privadas
Segurança em Redes sem Fio
DNS Seguro: DNSSec

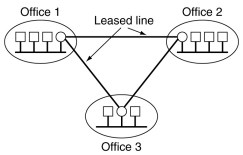
Motivação

Como construir sistemas de informação de grande amplitude geográfica sem arcar com custos excessivos com a infra-estrutura de comunicação.

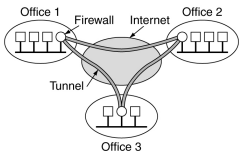


Duas possíveis arquiteturas gerais

Linha Dedicada



Tunelamento na Internet



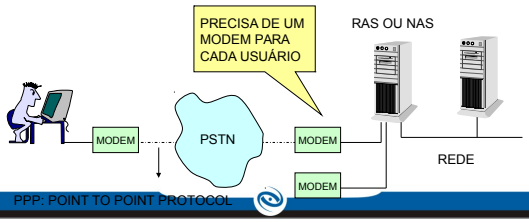
Soluções Usuais

Utilizar o enlaces de comunicação temporários
- LINHAS DISCADAS:
  - sistema público de telefonia

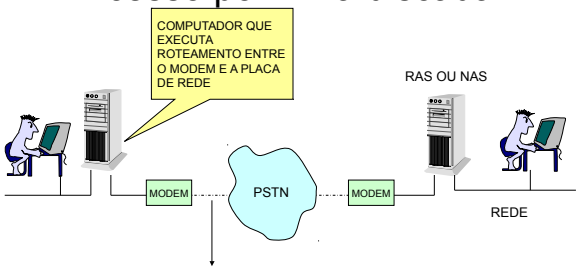
Utilizar enlaces de comunicação permanentes
- LINHAS DEDICADAS ou PRIVATIVAS:
  - Serviços disponibilizados por empresas de telecomunicação.

Acesso por linha discada

Serviço de Acesso Remoto:
- Implementado pelos sistemas operacionais comerciais mais difundidos.
- Permite que um usuário acesse um servidor por linha discada.



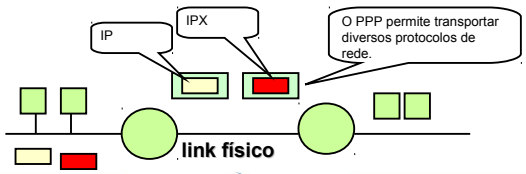
Acesso por linha discada



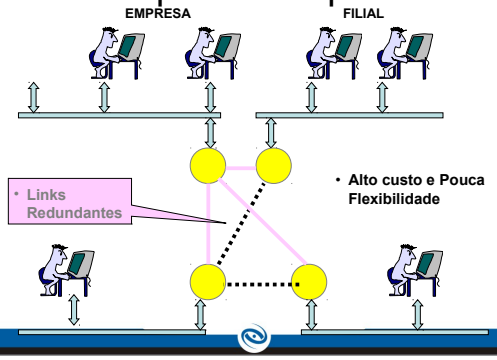
PPP: Point to Point Protocol

Permite criar conexão de rede através de links ponto a ponto.

- **O PPP é um protocolo do nível de enlace destinado a transportar mensagens ponto a ponto.**
- **O PPP supõem que o link físico transporta os pacotes na mesma ordem em que foram gerados.**



Acesso por linhas privativas



Tecnologias para Linhas Privativas

Linhas privativas podem ser implementadas com:

- ATM ou Frame-Relay
  - Comunicação Orientada a Conexão

Ambas as tecnologias permitem dividir a banda de um enlace físico através de circuitos virtuais

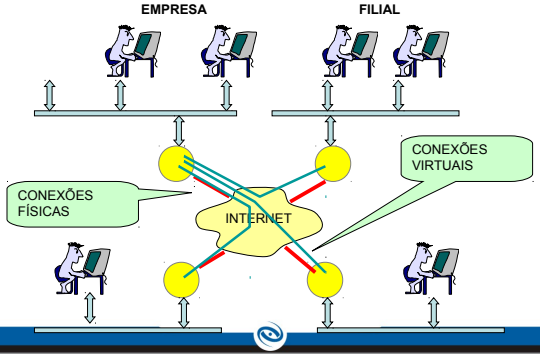
Garantia de largura de banda

Linhas Privadas X Linhas Discadas

Acesso Discado
- Serviço caro
- Velocidade limitada pela tecnologia das centrais telefônicas e pelos meios físicos utilizados.
- Sujeito a interrupções de funcionamento.

Linhas Privativas:
- Segurança por isolação física dos enlaces de comunicação.
- Custos elevados de implantação e manutenção, principalmente para longas distâncias.
- O custo aumenta com o número de pontos que compõe a linha privativa.

Redes Virtuais Privadas



VPN: Virtual Private Networks

Uma rede virtual privada (VPN) é um meio de simular uma rede privada sobre uma rede pública.
- **REDE VIRTUAL**: rede formada por conexões virtuais
- **CONEXÃO VIRTUAL**: conexões temporárias, não físicas, estabelecidas entre os pontos que se deseja estabelecer uma comunicação segura.

VPN sobre Internet = Extranet

A principal motivação para as VPN's é a possibilidade de utilizar a Internet como meio físico de comunicação, sendo uma alternativa muito mais viável que a alocação de linhas privativas.

Linhas Virtuais Privadas

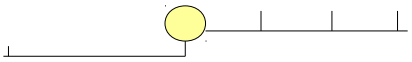
Linhas Virtuais Privativas:

- ✓segurança por criptografia e autenticação.
- ✓permite criar redes privativas com uma infinidade de enlaces sem aumento de custo significativo.
- ✓Permite transportar diversos tipos de protocolos de rede através de técnicas de tunelamento.

Tipos de VPN

ENTRE DUAS MÁQUINAS

ENTRE UMA MÁQUINA E UMA REDE



ENTRE DUAS REDES

Formas de Implementação das VPNs

- VPN de Acesso
- Intranet VPN
- Extranet VPN

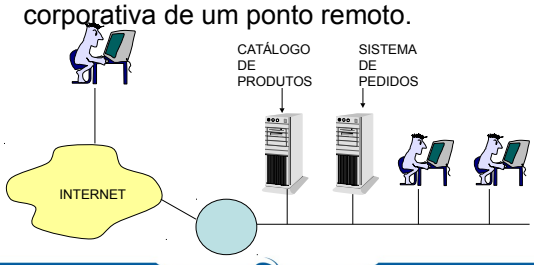
VPN de Acesso

Acesso remoto de usuários móveis e pequenos escritórios à uma rede corporativa
- mesmas políticas de segurança de uma rede privada.

Método de Acesso
- MODEM, IDSN, ADSL, CABO, etc.

Exemplo

Vendedor que precisa acessar a rede corporativa de um ponto remoto.

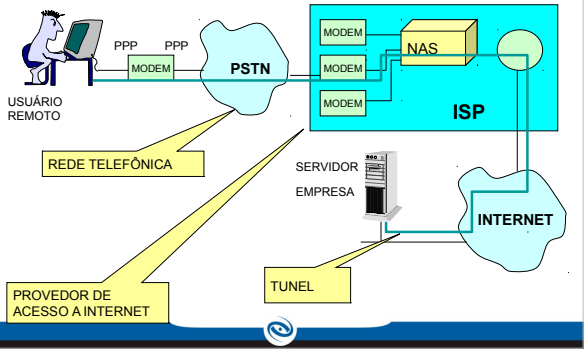


Tipos de VPN de Acesso

As VPNs de acesso podem ser de dois tipos, dependendo do ponto onde começa a rede segura:

1. Iniciada pelo Cliente
2. Iniciada pelo Servidor de Acesso a Rede (NAS)

Iniciada pelo Cliente

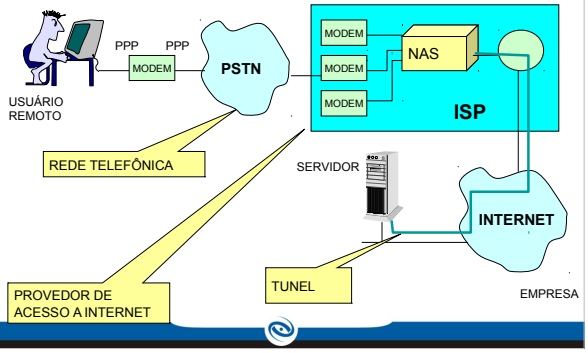


Iniciada pelo Cliente

O tunelamento acontece fim-a-fim (entre a máquina do cliente e o destino final).

- O computador do usuário necessita de um aplicativo ou sistema operacional que suporte a VPN.
- Os computadores do cliente e servidor perdem recursos de processamento.

Iniciada pelo NAS



Iniciada pelo Servidor de Acesso a Rede (NAS)

O tunelamento acontece a partir do servidor que atende a chamada do usuário no provedor (NAS).

- Configuração transparente para o usuário remoto.
- Não existe segurança nos dados até eles chegarem no ISP.

Conclusões para VPN de Acesso

Iniciada pelo cliente

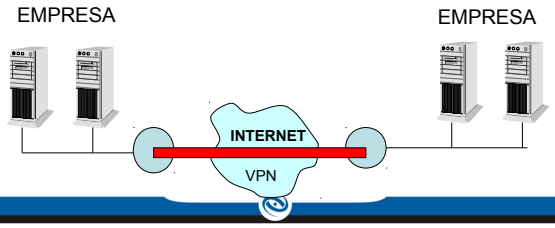
- A rede segura é fim-a-fim
- O computador do usuário precisa de suporte fim a fim.
- A informação de cada usuário deve ser roteada separadamente.

Iniciada pelo NAS

- O computador do usuário não precisa de suporte a VPN.
- Não garante segurança até chegar no ISP.

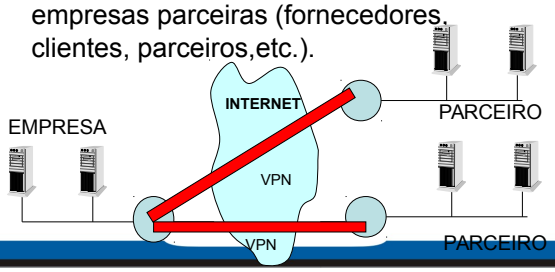
Intranet VPN

Permite construir uma intranet utilizando recursos de uma infra-estrutura de comunicação pública (e.g. Internet).



Extranet VPN

Permite construir uma rede que compartilha parcialmente seus recursos com empresas parceiras (fornecedores, clientes, parceiros,etc.).



Requisitos das VPN's

Uma tecnologia de VPN deve atender aos seguintes requisitos básicos:

- Isolamento em relação a rede pública.
- Acesso a rede virtual apenas para usuários autorizados.
- Confidencialidade das informações.

Conceitos Básicos de uma VPN

- TUNELAMENTO
- AUTENTICAÇÃO
- CRIPTOGRAFIA

Requisitos: Isolamento em Relação à Rede Pública

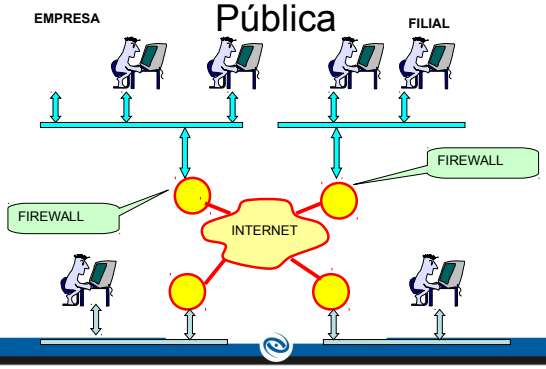
Isolamento em relação a rede pública:

- As redes internas e a rede pública devem estar fisicamente conectadas, mas logicamente separadas
- Deve-se ter controle sobre quais informações podem atravessar a fronteira entre a rede interna e externa.

IMPLEMENTAÇÃO:

- **FIREWALL E TUNELAMENTO**

Isolamento em Relação a Rede Pública

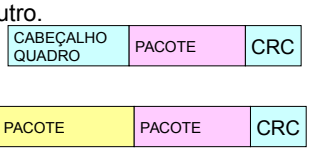


Tunelamento

"Tunelar" (tunneling):

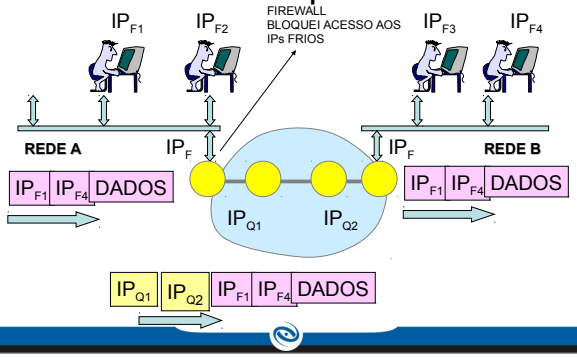
– Colocar as estruturas de dados de um protocolo da mesma camada do modelo OSI dentro do outro.

Exemplo:



TUNELAMENTO DA CAMADA 3

Exemplo



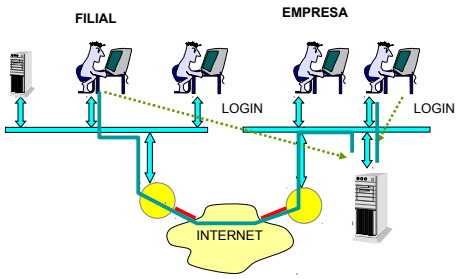
Requisitos para uma VPN

B) Acesso a rede virtual apenas para usuários autorizados

– A identidade do transmissor e do receptor deve ser provada de um para o outro.

IMPLEMENTAÇÃO: AUTENTICAÇÃO

Autenticação



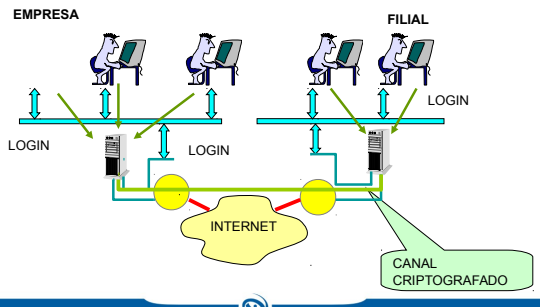
Requisitos da VPN

C) Confidencialidade das informações

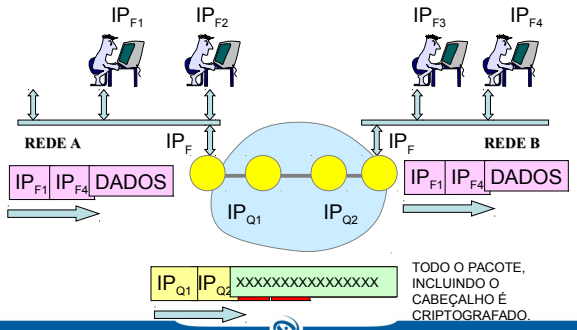
– Apenas as máquinas ou redes envolvidas diretamente na comunicação podem interpretar o conteúdos das mensagens trocadas.

IMPLEMENTAÇÃO: CRIPTOGRAFIA

Criptografia



Criptografia



Protocolos para VPN

PPTP
- Tunelamento de Camada 2
- Point-to-Point tunneling Protocol

L2TP
- Level 2 Tunneling Protocol (L2TP)
- Combinação do L2F e PPTP

IPSec
- Tunelamento de Camada 2

SSL
- Tunelamento na Camada de Transporte

Tipos de Tunelamento

Tunelamento de Camada 2
- Os pacotes são encapsulados no protocolo PPP (camada 2), e depois recebem o cabeçalho de tunelamento.
  - Exemplos PPTP e L2TP

Tunelamento de Camada 3
- Os pacotes recebem diretamente o cabeçalho de tunelamento.
  - Exemplo: IPSec.

PPTP: Point-to-Point tunneling Protocol

Desenvolvido por PPTP Forum:

- Ascend Communication, U.S. Robotics, 3Com Corporation, Microsoft Corporation e ECI Telematics
- Padronizado por RFC

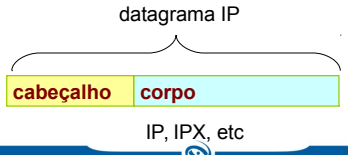
Requisitos para Utilização:

- Os sistemas operacionais do cliente e do servidor devem suportar PPTP
- PPTP é o protocolo de tunelamento mais difundido no mercado:
  - Windows, Linux, Roteadores, etc...

Tunelamento em PPTP

Princípio de tunelamento:

- Encapsular datagramas do protocolo de rede inteiros dentro de um envelope IP.
  - Protocolos de Rede: TCP/IP, IPX/SPX
- Oferece recursos de:
  - Autenticação e Criptografia



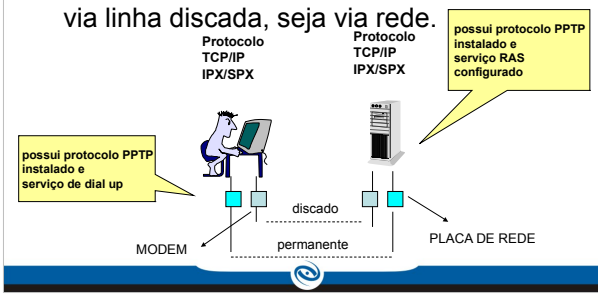
Cenários de Utilização do PPTP

Cenários:

1. Acesso por modem:
   - O cliente estabelece uma conexão com um provedor (ISP) e depois com o servidor de VPN.
1. Acesso por placa de rede:
   - O cliente já está na Internet, ele se conecta diretamente ao servidor de VPN.
   - O cliente e o servidor da VPN se encontram na mesma rede corporativa.

Tipos de Conexão

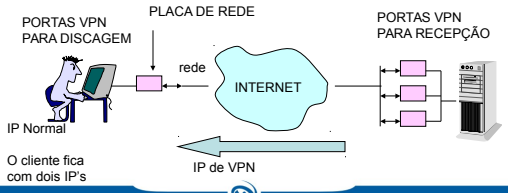
O cliente tem acesso direto ao servidor, seja via linha discada, seja via rede.



Acesso por linha permanente

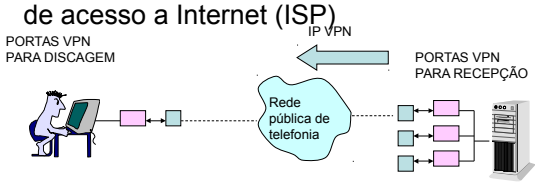
O computador do cliente já possui um IP da sua rede Internet.

O cliente disca para o número IP do servidor, e ganha um segundo IP.



Acesso por Linha Discada

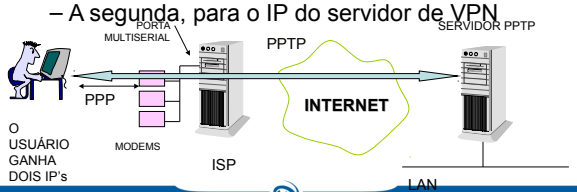
O acesso por linha discada via PPTP pode ser feito de forma direta ou via provedor de acesso a Internet (ISP)



Acesso Via Provedor (ISP)

No acesso via provedor, o cliente precisa estabelecer duas conexões:

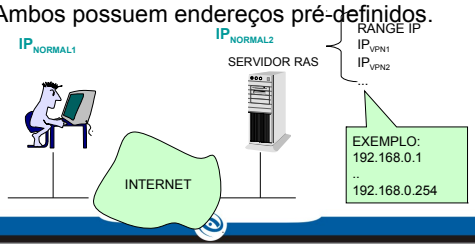
- A primeira para o provedor
- A segunda, para o IP do servidor de VPN



Exemplo

1) Situação Inicial

- Considere um cliente e um servidor conectados por uma rede TCP/IP.
- Ambos possuem endereços pré-definidos.



IPs de tunelamento

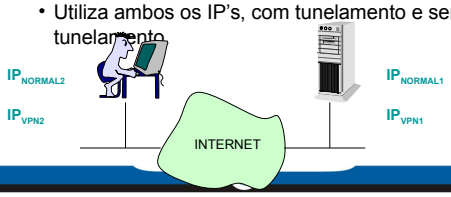
Uma conexão PPTP que encapsula protocolos TCP/IP em outro datagrama IP envolve a utilização de 2 pares de IP:

- IP sem tunelamento
  - cliente: $IP_{NORMAL2}$ (200.17.98.217)
  - servidor: $IP_{NORMAL1}$ (200.134.51.6)
- IP com tunelamento
  - cliente: IP_{VPN2} (192.168.0.2)
  - servidor: IP_{VPN1} (192.168.0.1)

IP's de tunelamento

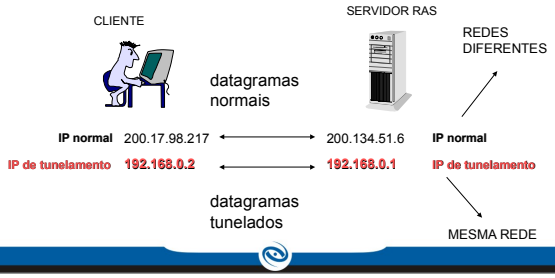
As rotas adicionadas aos computadores permitirão dois tipos de comunicação:

- Comunicação fora da VPN
  - Utiliza apenas os IP's sem tunelamento.
- Comunicação dentro da VPN
  - Utiliza ambos os IP's, com tunelamento e sem tunelamento.



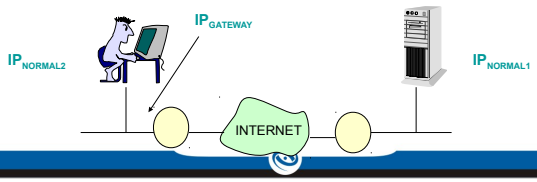
Situação após o estabelecimento da conexão

Cada computador possui dois IP's



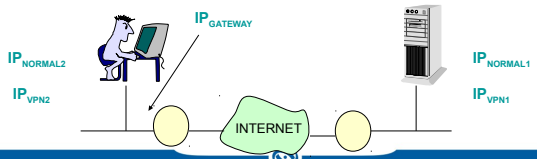
Rotas do Cliente antes da Conexão VPN

DESTINO	GATEWAY	INTERFACE
INTERNET	$IP_{GATEWAY}$	$IP_{NORMAL2}$
$IP_{NORMAL2}$	LOOPBACK	LOOPBACK
REDELOCAL	$IP_{NORMAL2}$	$IP_{NORMAL2}$



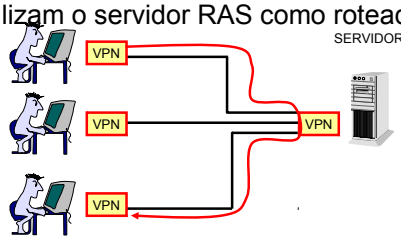
Rotas do Cliente após a Conexão VPN

DESTINO	GATEWAY	INTERFACE
REDE VPN	IP_{VPN2}	IP_{VPN2}
IP_{VPN2}	LOOBACK	LOOBACK
INTERNET	$IP_{GATEWAY}$	$IP_{NORMAL2}$
$IP_{NORMAL2}$	LOOPBACK	LOOPBACK
REDELOCAL	$IP_{NORMAL2}$	$IP_{NORMAL2}$



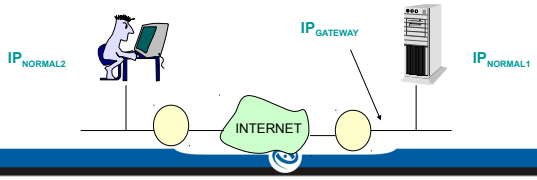
Rede Virtual

Os clientes conectados a rede virtual utilizam o servidor RAS como roteador.



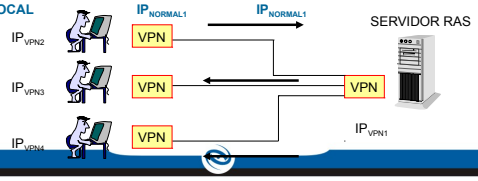
Rotas do Servidor antes da Conexão VPN

DESTINO	GATEWAY	INTERFACE
INTERNET	$IP_{GATEWAY}$	$IP_{NORMAL1}$
$IP_{NORMAL1}$	LOOBACK	LOOBACK
REDELOCAL	$IP_{NORMAL1}$	$IP_{NORMAL1}$

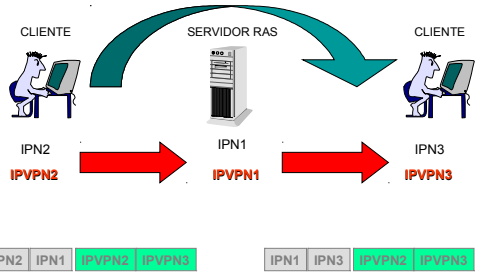


Rotas do Servidor após a Conexão VPN

DESTINO	GATEWAY	INTERFACE
IP_{VPN1}	LOOPBACK	LOOBACK
IP_{VPN2}	IP_{VPN1}	IP_{VPN1}
IP_{VPN3}	IP_{VPN1}	IP_{VPN1}
IP_{VPN4}	IP_{VPN1}	IP_{VPN1}
INTERNET	$IP_{GATEWAY}$	$IP_{NORMAL1}$
$IP_{NORMAL2}$	LOOPBACK	LOOPBACK
REDELOCAL	$IP_{NORMAL1}$	$IP_{NORMAL1}$

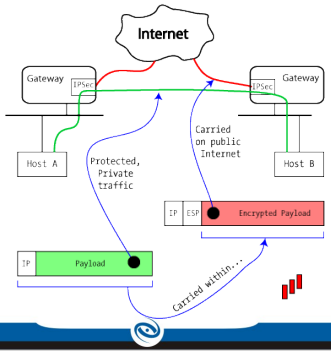


Comunicação com Tunelamento

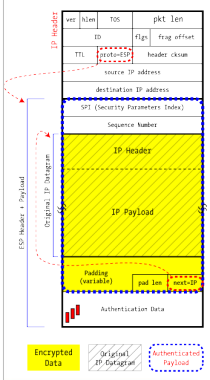


VPNs com IPSec

Virtual Private Network



ESP Authenticated Mode
– Traditional VPN



VPNs com IPSec

Roteiro

E-mail Seguro
Camada de Rede: IPSec
Camada de Transporte: SSL
VPN: Redes Virtuais Privadas
Segurança em Redes sem Fio
DNS Seguro: DNSSec

Requisitos

Autenticação entre cliente e AP
- Baseada em chave compartilhada

Confidencialidade dos dados
- Troca de mensagens por disseminação → não existe confidencialidade "física"

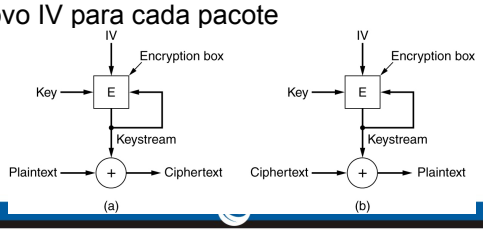
Dois mecanismos: WEP e WPA

Encriptação no WEP

Cada pacote é encriptado em separado

Utiliza um gerador de keystream

Novo IV para cada pacote



Encriptação WEP

Remetente calcula Integrity Check Value (ICV) do dado

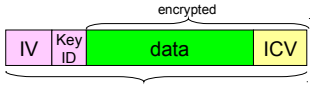
- 4 bytes: hash/CRC

Cada lado tem chave 104 bits compartilhada

Remetente cria IV de 24 bits e concatena com chave: chave de 128 bits

Remetende inclui keyID (campo 8 bits)

Dado do pacote encriptado com RC4



Geração do Dado Encriptado

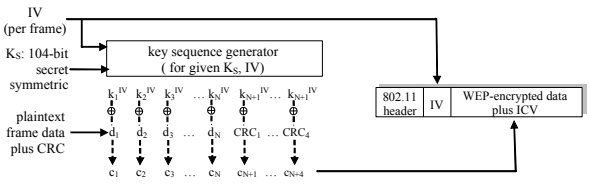


Figure 7.8-new1: 802.11 WEP protocol

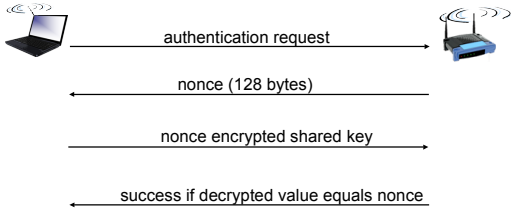
Kurose&Ross

Autenticação com nonces

AP desafia cliente para encriptar um *nonce* (número aleatório) com a chave

Se cliente é capaz, então ele possui a chave e a autenticação é finalizada

Autenticação WEP



Kurose&Ross

Falhas na Encriptação 802.11 WEP

Vulnerabilidade

IV 24 bits, 1 por pacote → em algum momento IV é reutilizado

IV é transmitido em texto plano e a reutilização é detectada

Ataque:

- Ataque do texto plano conhecido
- Atacante descobre k_i^{IV}
- Quando IV é reutilizado, atacante descobre chaves

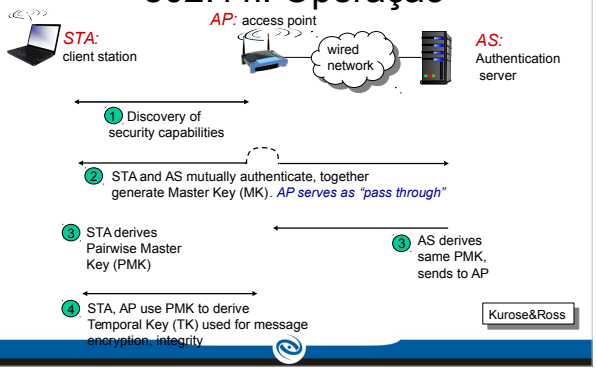
802.11i

Substituição ao WEP (802.11) para corrigir vulnerabilidades críticas

Permite autenticação flexível

– Se necessário, pode ser feita fora do AP

802.11i: Operação



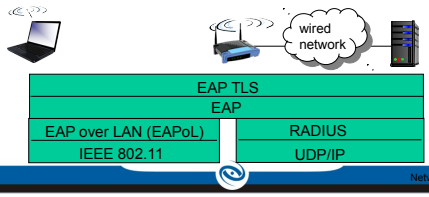
EAP: extensible authentication protocol

EAP: protocolo de autenticação fim-a-fim com cliente móvel

EAP usa tunelamento

– mobile-to-AP (EAP over LAN)

– AP para servidor de autenticação (RADIUS over UDP)



Encriptação no 802.11i

802.11i popularmente conhecido pelas siglas WPA e WPA2
- WPA → 802.11i-draft
- WPA2 → 802.11i (final)

Encriptação fornecida (AP→Cliente→AP)
- TKIP: funciona em hardware legado WEP
- CCMP: encriptação mais forte (AES)

TKIP

TKIP: Temporal Key Integrity Protocol

Projetado para funcionar com hardware legado baseado no WEP
- Exige atualização de firmware
- Exigências de poder de processamento limitadas

Projeto: evitar injeção de pacotes, ataques de replay, descoberta de chaves por análise estatísticas (todas fraquezas maiores do WEP)

TKIP: Message Integrity Code

Message Integrity Code visa dificultar a injeção de pacotes sem que seja detectado
- Oferece mecanismo para checagem da integridade dos pacotes transmitidos
- Substitui mecanismo falho do CRC

TKIP MIC

Chave de 64 bits dividida em 2 de 32 bits (X e Y)

MAC origem e destino, e QoS adicionados no payload do pacote

Mensagem quebrada em pacotes de 32 bits (M_1, M_2,M_3,... M_i)

- X=X⊕Mi
- X e Y recalculados com função leve

TKIP: Verificação MIC

Pacotes gerados não são previsíveis

Destinos podem calcular integridade dos pacotes

- Se duas falhas no MIC são encontradas nos pacotes em 60 segundos, então considera-se que um ataque está em ação
  - Nova reassociação com o AP
  - Novas chaves são geradas

Pacotes ainda encapsulados no WEP

- Erros de transmissão dificilmente causam falha no MIC
- CRC continua existindo

TKIP: Mecanismos Adicionais

Proteção contra ataques de replay

- Número de sequência TKIP para cada MAC PDU

Algoritmo de mistura de chaves

- Evita problema do reuso de chave do WEP, quando IV é repetido.
- TTAK (TKIP-mixed Transmit Address and Key)
  - 80 bits $= f(chave_{128}, MAC, TSC_{32\text{-}mais\text{-}sig})$

CCMP

CCMP: Counter Mode with Cipher Block Chaining (CBC) Message Authentication Code Protocol

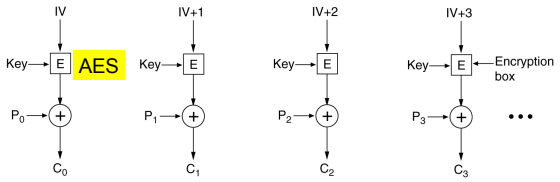
Utiliza chaves de 128-bits, com um bloco de 128 bits de encriptação

Usa número único (PN) de 48 bits por pacote, incrementado em cada frame

- Modo contator

CCMP: Revisão do Modo Contador

IV → 104 bits nonce + 24 bits do contador

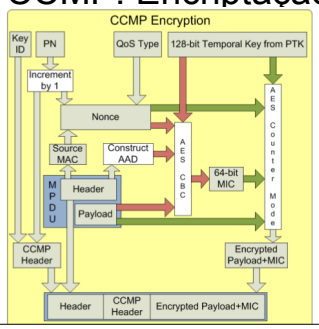


CCMP: Integridade da Mensagem

Campo AAD adicionado ao pacote

- Considera endereços, número fragmento, QoS
- Concatenado ao payload e encriptado
- Qualquer mudança em 1 bit de qualquer parte do pacote muda o dado encriptado
  - Funciona como verificador do MIC

CCMP: Encriptação



Kevin Benton. The Evolution of 802.11 Wireless Security. INF 795. UNLV Informatics-Spring 2010

Roteiro

E-mail Seguro
Camada de Rede: IPSec
Camada de Transporte: SSL
VPN: Redes Virtuais Privadas
Segurança em Redes sem Fio
DNS Seguro: DNSSec

Revisão de DNS

DNS – Domain Name System

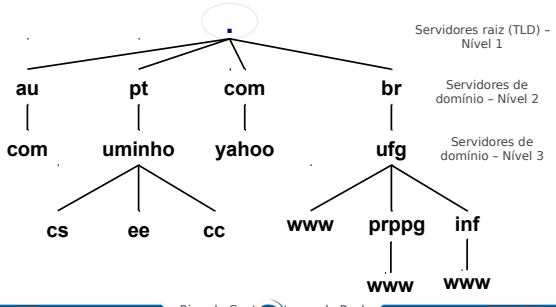
- Camada de transporte e rede só entendem endereços IP
  - Identificador 32 bits (v.4): 200.137.221.69, 208.67.222.222, 139.82.24.231
- Dificuldade para uso de endereços IP por usuários e aplicações
  - Endereços IP não possuem um significado claro para usuário: propósito, localização da estação
  - Difíceis de lembrar e validar
  - Endereços IP podem mudar
- DNS – mapeia endereços IP em nomes hierárquicos e significantes
  - Consulta: qual é o IP da estação ***www.inf.ufg.br***?

DNS - Domain Name System

- Padrão Aberto para Resolução de Nomes Hierárquicos
  - Agrupa nomes em domínios;
  - Base de dados distribuída implementada em uma hierarquia de servidores DNS;
  - Protocolo de aplicação que permite as máquinas consultarem essa base de dados distribuída.
  - Atende requisições na porta 53
    - Utiliza UDP e TCP
- Especificações do DNS (RFCs)
  - RFCs 1034, 1035, 1101, 1123, 1183 e 1536.
- Principal implementação dos servidores DNS:
  - Berkeley Internet Name Domain (BIND)
    - Implementação desenvolvida na Berkeley University

Hierarquia de Domínios

- Estrutura hierárquica de nomes



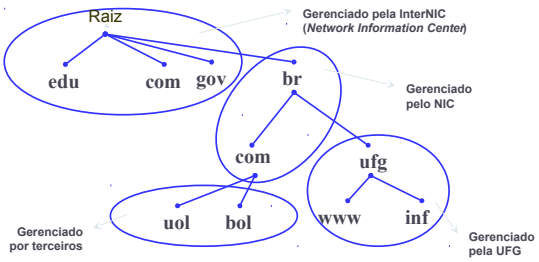
Organização dos Domínios

•O espaço de domínio de nomes é dividido em duas áreas principais:

- Domínios Genéricos:
  - 3 caracteres para indicar a atividade.
    - .com, .edu, .gov, .int, .mil, .net, .org
    - .int: organizações internacionais
    - .mil: organizações militares
    - .org: organizações não comerciais
- Domínios Geográficos:
  - 2 caracteres para identificar o país.
    - .br, .fr, .jp, etc.

Descentralização

•A descentralização e delegação de autoridade simplifica o gerenciamento, limita o tráfego e aumenta a confiabilidade.



Registro de Recursos

•RR é um tupla que contém

- Domain_name, Time_to_Live, Type, Value

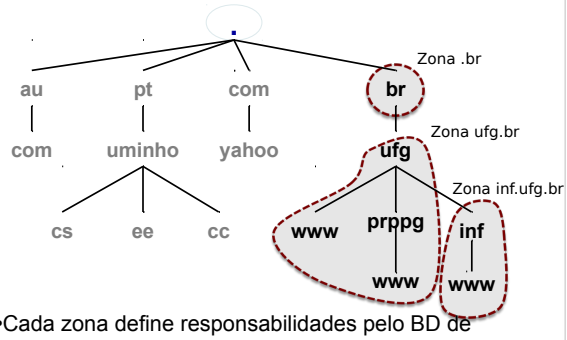
Tipo	Significado	Valor
SOA	Start of authority	Parâmetros da zona
A	IP de um host	Inteiro 32-bits (IPv4)
MX	Servidor e-mail	Prioridade, domínio aceitando e-mail
NS	Servidor de nomes	Nome do servidor to domínio
CNAME	Nome canônico	Nome do domínio
PTR	Ponteiro	Apelido para endereço IP
HINFO	Descrição da estação	Texto ASCII com CPU, OS, ..
TXT	Texto	Texto ASCII não-interpretado

Registros de Recursos

```
; Authoritative data for cs.vu.nl
cs.vu.nl.        86400  IN  SOA     star boss (952771,7200,7200,2419200,86400)
cs.vu.nl.        86400  IN  TXT     "Divisie Wiskunde en Informatica."
cs.vu.nl.        86400  IN  TXT     "Vrije Universiteit Amsterdam."
cs.vu.nl.        86400  IN  MX      1 zephyr.cs.vu.nl.
cs.vu.nl.        86400  IN  MX      2 top.cs.vu.nl.

flits.cs.vu.nl.  86400  IN  HINFO   Sun Unix
flits.cs.vu.nl.  86400  IN  A       130.37.16.112
flits.cs.vu.nl.  86400  IN  A       192.31.231.165
flits.cs.vu.nl.  86400  IN  MX      1 flits.cs.vu.nl.
flits.cs.vu.nl.  86400  IN  MX      2 zephyr.cs.vu.nl.
flits.cs.vu.nl.  86400  IN  MX      3 top.cs.vu.nl.
www.cs.vu.nl.    86400  IN  CNAME   star.cs.vu.nl
ftp.cs.vu.nl.    86400  IN  CNAME   zephyr.cs.vu.nl

rowboat                 IN  A       130.37.56.201
                        IN  MX      1 rowboat
                        IN  MX      2 zephyr
                        IN  HINFO   Sun Unix

little-sister           IN  A       130.37.62.23
                        IN  HINFO   Mac MacOS

laserjet                IN  A       192.31.231.216
                        IN  HINFO   "HP Laserjet IIISi" Proprietary
```

Exemplo parcial de registros no BD do domínio cs.vu.nl

Zonas

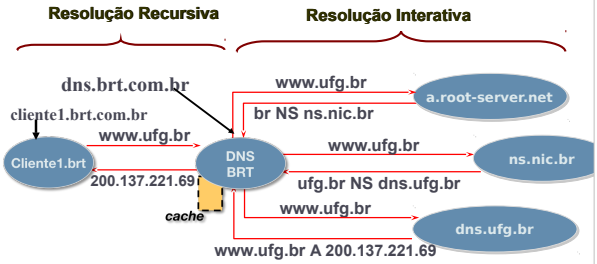


- Cada zona define responsabilidades pelo BD de domínio

Tipos de Servidores de DNS

- **Primário**
  - É o servidor autoritário para zona. A inclusão, alterações ou exclusão dos registros da zona são feitas através deste servidor.
  - O servidor primário envia uma cópia dos seus arquivos de dados para o servidor secundário através de um processo denominado **"zone transfer"**
- **Secundário**
  - Funciona como backup. Apenas lê os arquivos de dados do servidor primário, e responde as requisições dos clientes quando requisitado.
- **Caching-Only**
  - São servidores DNS que apenas efetuam consultas e guardam o resultado numa cache e retornam os resultados.
  - Um servidor DNS realiza consulta a outros servidores sempre que tiver que localizar um nome externo as zonas que controla.

Resolução de Requisições DNS



- Resolução do IP da estação ***www.ufg.br***

Requisição/Resposta

Identificação	Flags	12 bytes
Número de perguntas	Número de RRs de resposta	
Número de RRs com autoridade	Número de RRs adicionais	
Perguntas (número variável de perguntas)		Nome, campos de tipo para uma consulta
Respostas (número variável de registros de recursos)		RRs de resposta à consulta
Autoridade (número variável de registros de recursos)		Registros para servidores com autoridade
Informação adicional (número variável de registros de recursos)		Informação adicional 'útil', que pode ser usada

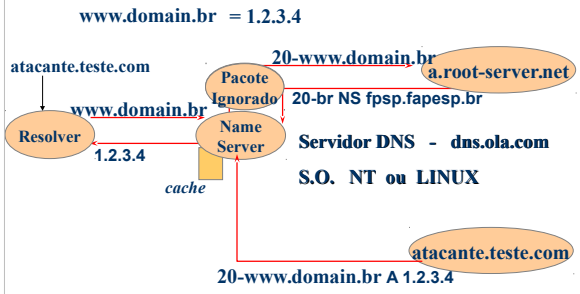
Usos Adicionais

- Características interessantes
  - Simples paradigma request-response
  - Bancos de dados textuais simples
  - Cache distribuído automaticamente mantido pela Internet
- Balanceamento de carga baseado em DNS
  - Manutenção de mais um registro A (IP) para mesmo nome
  - Respostas alternam a sequência dos IPs da resposta
- Bancos de dados simples textuais
  - Ex: Lista negra de IPs mantida por SPAMHAUS
- Validação de origem de mensagens no DomainKeys
  - DNS mantém chave pública de autenticação de origem de mensagens de um domínio

Limitações e Problemas

- Próprio RFC estabelece
  Resposta não pode ser considerada segura!
- Problemas
  - Validação de respostas
    - Fortemente dependente da aleatoriedade do id da requisição
      - Histórico 'rico' e recente de problemas de segurança
    - Confiabilidade dos resultados em cache
    - Solução parcial: certificados SSL autenticados
    - Solução: DNSSec – extensão segura do DNS
  - Validação de domínios
    - Nomes de domínios não devem ser considerados confiáveis
    - Solução: uso de EV-Certificates
- Não permite consultas mais complexas

DNS Spoofing
Envenenamento de Cache



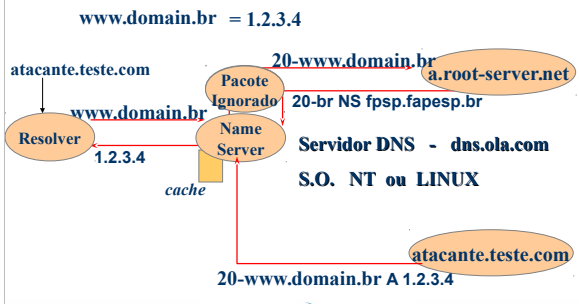
Dns Spoofing

Conseqüências:

- Alterar a Origem da Informação
- Driblar mecanismos de defesa que estabelecem uma relação de confiança baseada no nome dos hosts

Visualizando página Web indesejada

DNS Spoofing
Envenenamento de Cache



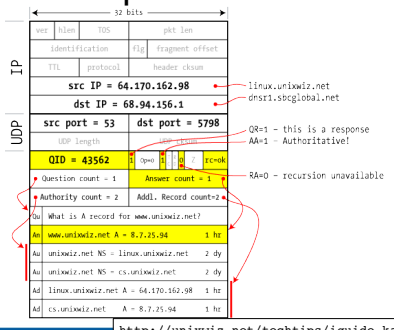
DNS Spoofing

Conseqüências:

- Alterar a Origem da Informação
- Driblar mecanismos de defesa que estabelecem uma relação de confiança baseada no nome dos hosts

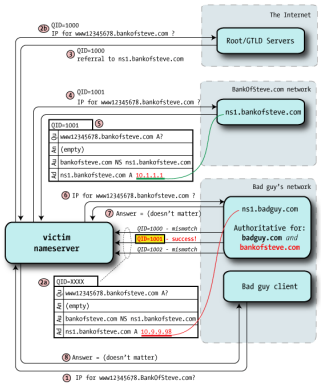
Visualizando página Web indesejada

Exemplo de Pacote Resposta

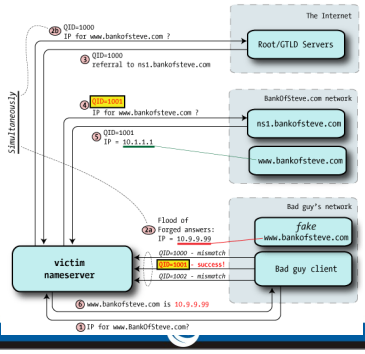


http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

- Ataque descoberto por Dan Kaminsky em 2008
- Geração de inúmeras consultas para nomes aleatório dentro do domínio
  - Facilita a descobert do Qid
- Campo QueryId é 16 bits: 65535 variações



Revendo o Ataque



Solução Efetiva

- Uso de DNSSec
- Implementa integridade das respostas de servidores de DNS
- Respostas validadas por chaves de cada servidor

Trabalho da Disciplina

Referências Iniciais Sugeridas Ataques DNS e DNSSec

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
http://registro.br/suporte/tutoriais/dnssec.html