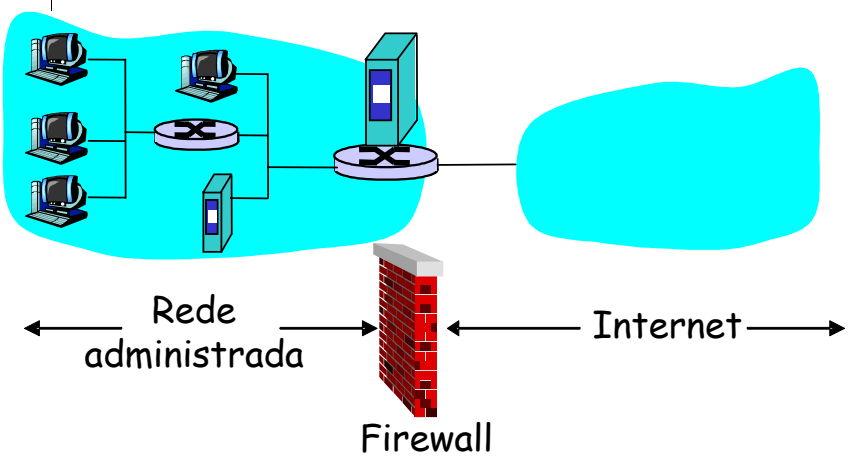
Unidade 3
Dispositivos e Tecnologias

Firewalls

firewall

Isola a rede interna de uma organização da rede pública (Internet), permitindo a passagem de certos pacotes, bloqueando outros.



Firewalls: Por quê?

Evita ataques de destruição de serviço (DoS):

- ✓ *enchente* SYN: hacker estabelece muitas conexões TCP "falsas", sem deixar recursos para conexões "reais".

Impede modificações/acessos ilegais aos dados internos.

- ✓ hacker substitui a homepage oficial por outra qualquer.

Permite somente o acesso autorizado à rede interna

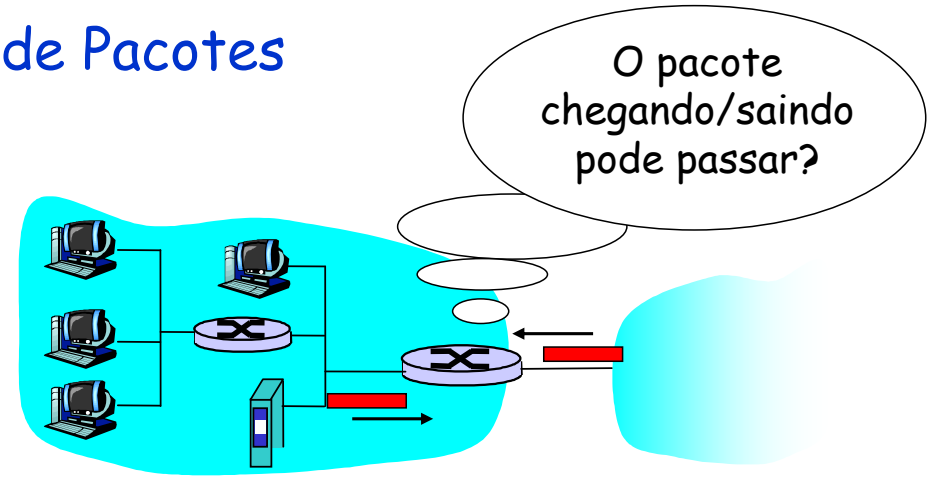
- ✓ grupo de usuários/servidores autenticados

Tipos de firewalls:

- ✓ filtragem de pacotes
- ✓ nível de aplicação

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

Filtragem de Pacotes



Rede interna conectada a Internet através roteador (firewall).

roteador filtra pacote por pacote, a decisão de permitir/impedir a sua passagem é baseada em:

- ✓ endereço fonte IP, endereço destino IP
- ✓ número das portas TCP/UDP fonte e destino
- ✓ tipo de mensagem ICMP
- ✓ TCP SYN e ACK bits

Filtragem de Pacotes

Exemplo 1: Bloquear datagramas de entrada e saída com campo de protocolo IP = 17 e porta fonte ou destino = 23.

- ✓ Todo fluxo UDP de entrada e saída e todas as conexões Telnet são bloqueadas.

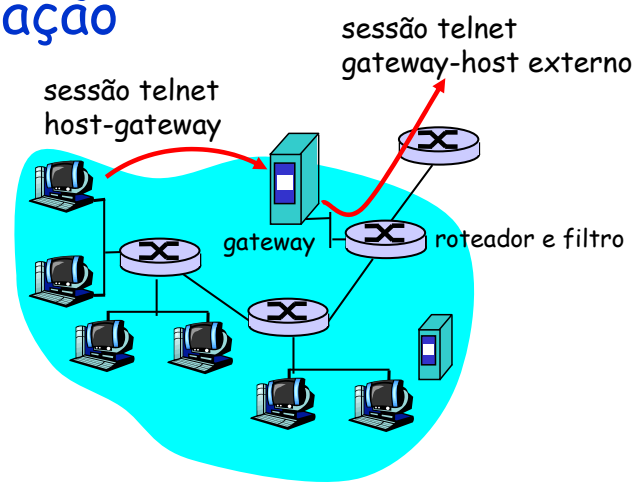
Exemplo 2: Bloquear segmentos TCP de entrada com ACK=0.

- ✓ Impede que clientes externos estabeleçam conexões TCP com clientes internos, mas permite que clientes internos conectem com o exterior.

Gateway no nível de aplicação

Filtra os dados da camada de aplicação dos pacotes , como também os campos IP/TCP/UDP.

Exemplo: permite que certos usuários internos realizem sessões telnet com o exterior.



1. Requer que as sessões telnet sejam feitas através do gateway.
2. Para os usuários autorizados, o gateway estabelece a conexão telnet com o host de destino e comuta os dados das 2 conexões.
3. Filtro do roteador bloqueia todas conexões telnet não originadas a partir do gateway.

Limitações dos firewalls e gateways

IP spoofing:

O roteador não pode saber se os dados "realmente" vêm da fonte alegada.

Se múltiplas aplicações requerem tratamento especial, cada uma deve ter o seu gateway.

Software aplicativo deve saber como contatar o gateway.

- ✓ p.ex., end. IP do serviço proxy no Web browser

Compromisso: grau de liberdade de comunicação com o mundo externo, nível de segurança.

Internet: considerações sobre segurança

Mapeamento:

- ✓ Pré- ataque
  - descobre quais os serviços que estão implementados na rede.
- ✓ Usa `ping` para determinar quais são os sistemas que têm endereços na rede.
- ✓ Varredura de portas:
  - tenta estabelecer conexão TCP com cada porta em seqüência (veja o que acontece).

Contramedidas?

Internet: considerações sobre segurança

Mapeamento: contramedidas

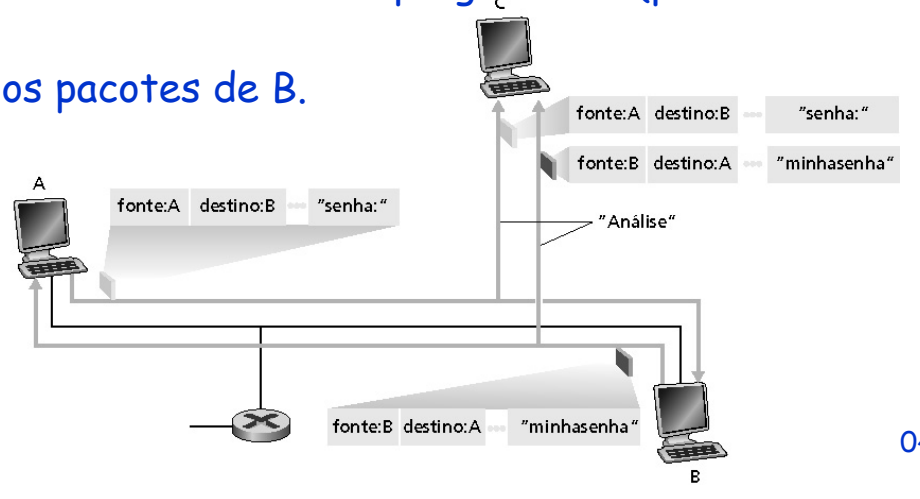
- ✓ Monitoramento do tráfego entrando na rede.
- ✓ Detecção de atividades suspeitas
  - endereços IP e portas sendo varridas seqüencialmente

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

Internet: considerações sobre segurança

Farejamento de pacotes (packet sniffing):

- ✓ Meio de transmissão "broadcast".
- ✓ Interface de rede em modo "promíscuo" grava todos os pacotes que trafegam no meio.
- ✓ Pode-se ler todos os dados não criptografados (p.ex. senhas)
- ✓ Ex.: C fareja os pacotes de B.



Contramedidas?

Internet: considerações sobre segurança

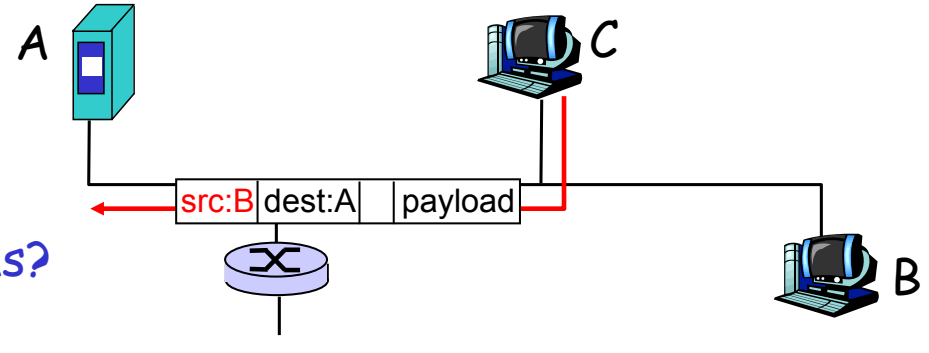
Packet sniffing: contramedidas

- ✓ Todos os computadores da organização executam software que verifica periodicamente se as suas interfaces de rede não estão em modo promíscuo.
- ✓ Um computador por segmento do meio de transmissão (Ethernet comutada)

Internet: considerações sobre segurança

IP Spoofing:

- ✓ Pode gerar pacotes IP "crus" diretamente a partir da aplicação, colocando qualquer valor no campo de endereço IP do remetente.
- ✓ O receptor não sabe se o remetente é falso.
- ✓ Ex.: C se faz passar por B.

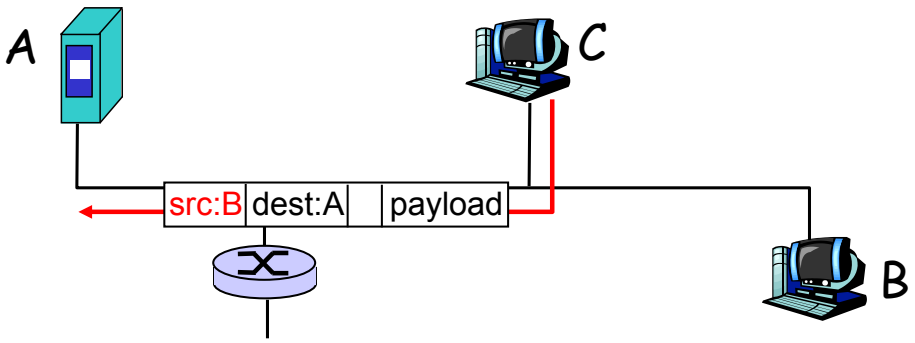


Contramedidas?

Internet: considerações sobre segurança

IP Spoofing: filtragem de ingresso

- ✓ Roteadores não devem deixar sair pacotes com endereços do remetente inválidos. Ex.: endereço fonte inexistente na sub-rede do roteador)
- ✓ o.k., mas filtragem de ingresso não pode ser garantida em todas as redes.

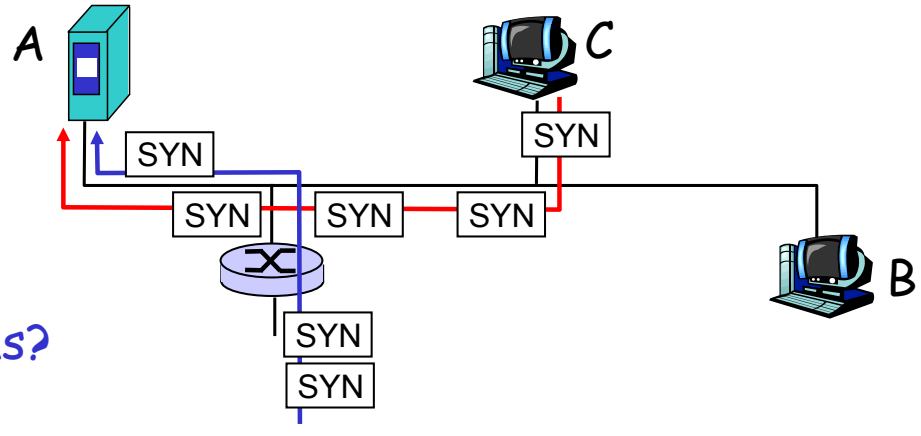


Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

Internet: considerações sobre segurança

Destruição de Serviço (DoS):

- ✓ Tráfego intenso de pacotes gerados maliciosamente "inunda" o receptor.
- ✓ DoS Distribuído (DDoS): fontes múltiplas e coordenadas inundam o receptor. Ex.: C e host remoto promovem um ataque SYN ao host A.

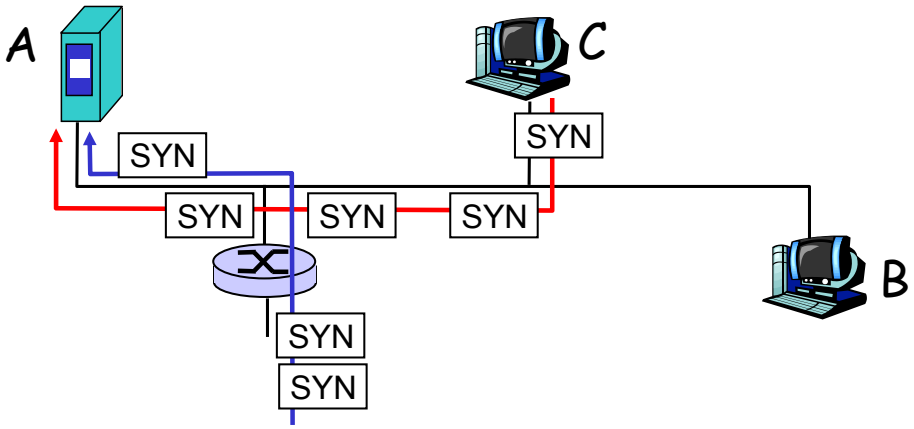


Contramedidas?

Internet: considerações sobre segurança

DoS: contramedidas

- ✓ Filtrar pacotes inundados (Ex.: SYN) antes que atinjam o host: descarte de pacotes bons e ruins.
- ✓ Seguir a rota até a fonte da inundação (provavelmente uma máquina inocente, comprometida).



DNS: Domain Name System

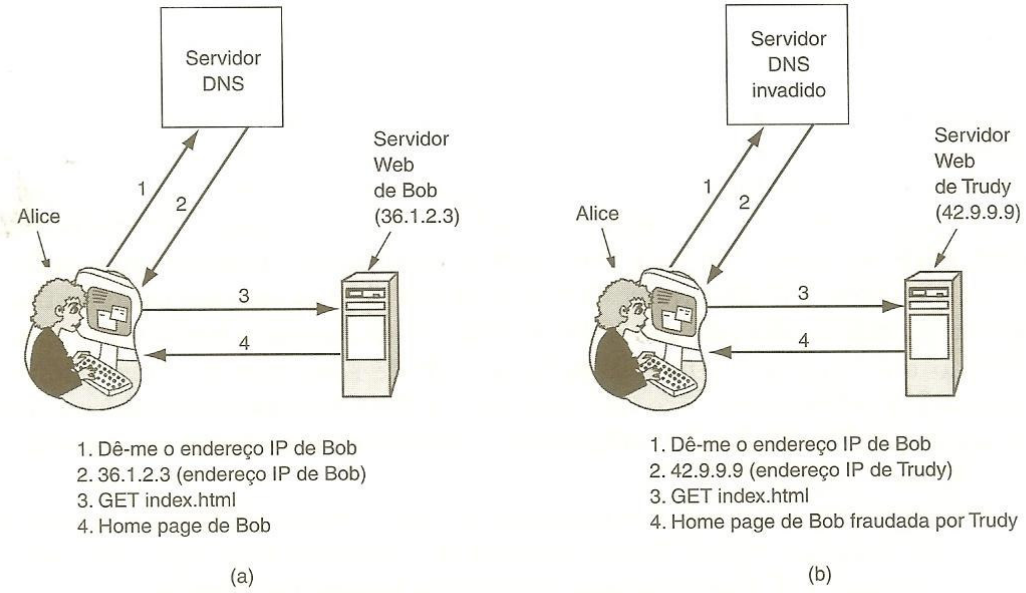


Figura 8.46 (a) Situação normal. (b) Um ataque baseado na invasão do DNS e na modificação do registro de Bob

Fonte: Tanenbaum

DNS Seguro

Exemplo de RRSet (resource record set) para *bob.com*:

Fonte: Tanenbaum

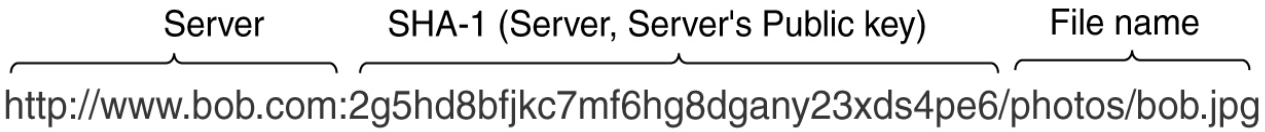
Domain name	Time to live	Class	Type	Value
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7B73F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A8B848F5272E53930C...

O registro *KEY* é a chave pública de Bob. O registro *SIG* é o *hash* de assinatura dos registros *A* e *KEY* do servidor *com* de nível mais alto, permitindo verificar as suas autenticidades.

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

Auto-certificação de URL

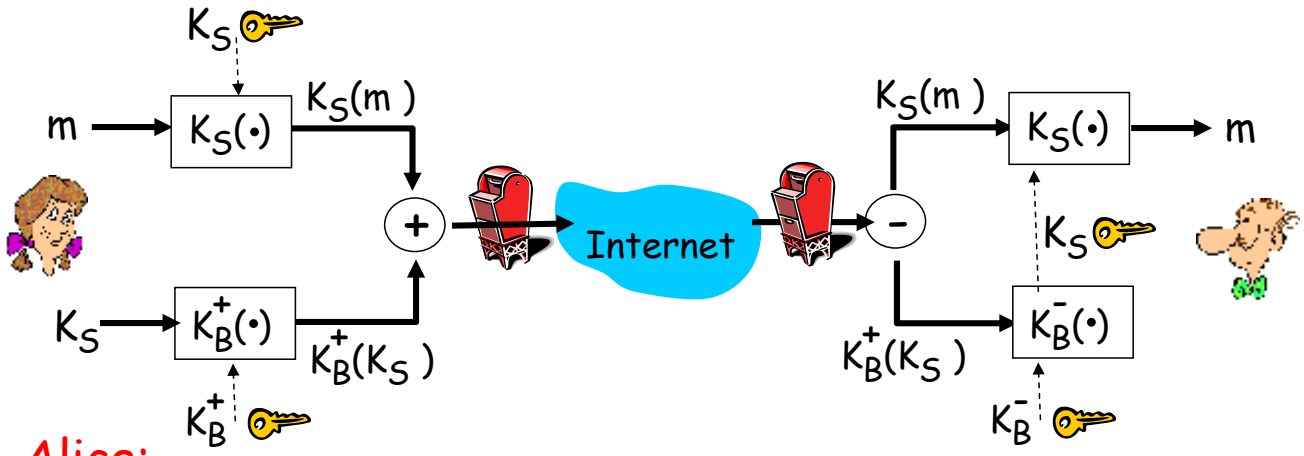
Uma URL auto-certificada contendo a assinatura do nome do servidor e da chave pública:



Fonte: Tanenbaum

E-mail seguro

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



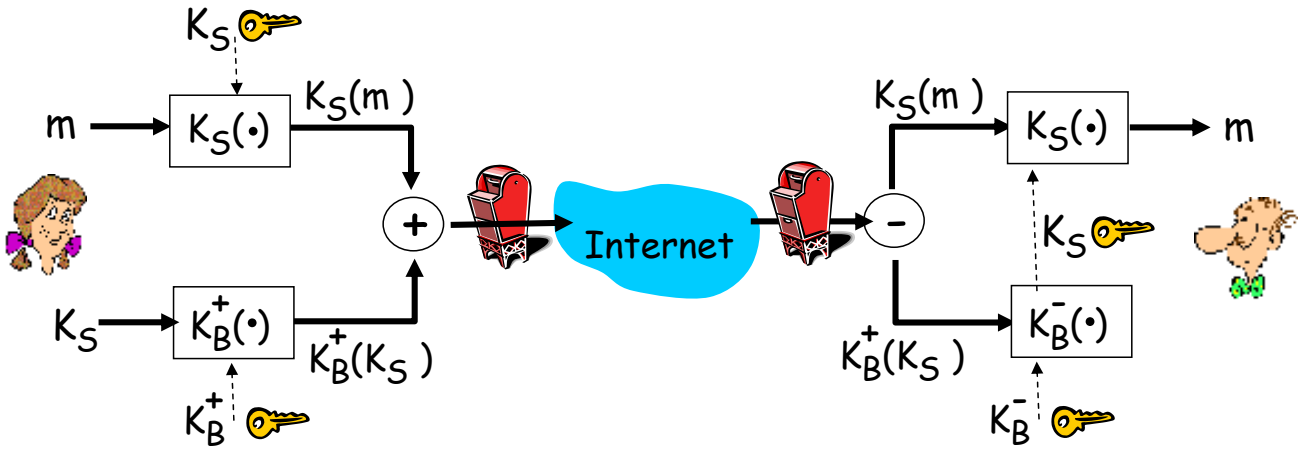
Alice:

- gera, aleatoriamente, uma chave secreta *simétrica* , K_S.
- cifra a mensagem com K_S (para eficiência)
- também cifra K_S usando a chave pública de Bob.
- envia ambos criptogramas $K_S(m)$ and $K_B(K_S)$ para Bob.

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

E-mail seguro

- Alice enviou um e-mail confidencial, m, para Bob

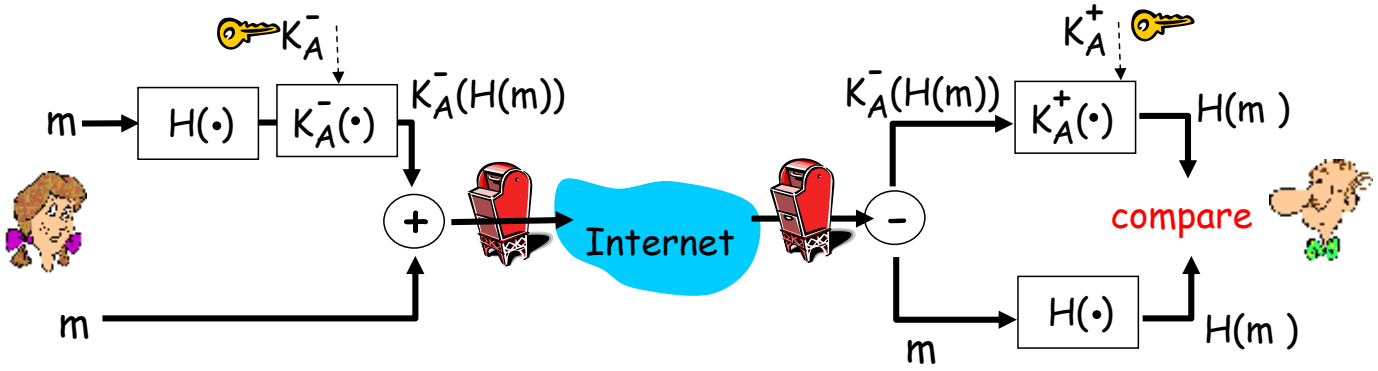


Bob:

- usa sua chave privada para decifrar e obter K_S.
- usa K_S to decifrar $K_S(m)$ para recuperar m.

E-mail seguro (cont.)

- Alice quer enviar uma mensagem autenticada para Bob.



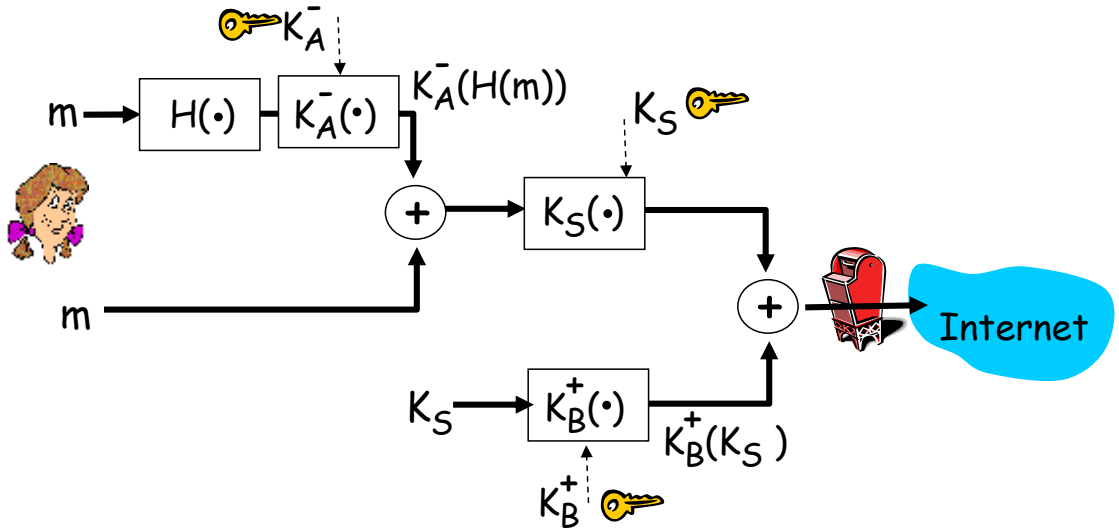
Alice:

- assina digitalmente a mensagem.
- envia a mensagem (em claro) e a assinatura digital.

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

E-mail seguro (cont.)

- Alice quer garantir confidencialidade, autenticação do remetente e integridade da mensagem.



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

Pretty Good Privacy (PGP)

Esquema para criptografia de e-mail na Internet, padrão-de-fato.

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

Fornece sigilo, autenticação do remetente e integridade dos dados.

O inventor, Phil Zimmerman, foi alvo de investigação federal (FBI) por 3 anos.

Uma mensagem PGP assinada:

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

Bob:
   Meu marido está fora da cidade
esta noite.
   Eternamente sua, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZ
P9t6n7G6m5Gw2
---END PGP SIGNATURE---
```


Secure Sockets Layer (SSL)

Segurança na camada de transporte para qualquer aplicação TCP usando serviços SSL.

Usado entre Web browsers e servidores de comércio eletrônico (shttp).

Serviços de segurança:

- ✓ autenticação de servidor
- ✓ criptografia
- ✓ autenticação de cliente (opcional)

Autenticação de servidor:

- ✓ browser com SSL inclui chaves públicas para CAs de confiança.
- ✓ o browser requer o certificado do servidor, emitido por uma CA.
- ✓ o browser usa a chave pública da CA para extrair a chave pública inclusa no certificado.

Secure Sockets Layer (SSL)

Sessão SSL criptografada:

Browser gera *chave de sessão simétrica*, cifra-a com a chave pública do servidor e envia a chave cifrada para o servidor.

Usando a chave privada, o servidor decifra a chave de sessão.

O browser e o servidor têm uma chave de sessão em comum.

- ✓ Todos os dados enviados no soquete TCP (pelo cliente ou servidor) são cifrados com a chave de sessão.

SSL: base do Transport Layer Security (TLS) do IETF (Internet Engineering Task Force).

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

IPsec: Segurança da Camada de Rede

Confidencialidade:

- ✓ host fonte cifra os dados do datagrama IP;
- ✓ segmentos TCP e UDP, mensagens ICMP e SNMP.

Autenticação :

- ✓ host de destino pode autenticar endereço IP da fonte.

Dois protocolos principais:

- ✓ protocolo *authentication header* (AH)
- ✓ protocolo *encapsulation security payload* (ESP)

Para ambos, AH e ESP, a sinalização entre fonte e destino:

- ✓ cria um canal lógico da camada de rede chamado de associação de segurança (security association - SA)

Cada SA é unidirecional.

Unicamente determinado pelo:

- ✓ protocolo de segurança (AH ou ESP)
- ✓ endereço IP da fonte
- ✓ ID da conexão de 32 bits

Protocolo AH

Fornece autenticação da fonte, integridade de dados. (*sem* confidencialidade)

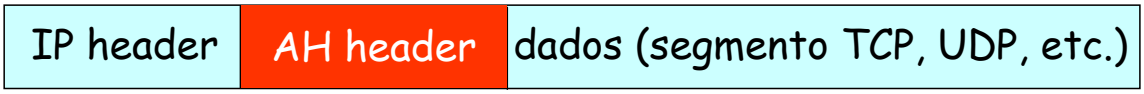
Cabeçalho AH inserido entre o cabeçalho IP e o campo de dados.

Campo de protocolo: 51

Roteadores intermediários processam os datagramas normalmente.

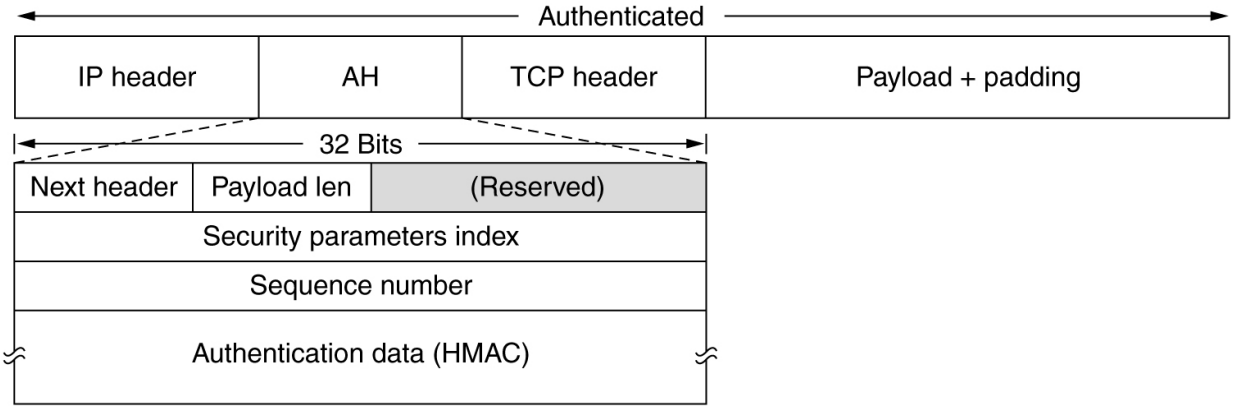
Cabeçalho AH inclui:

- ✓ identificador de conexão.
- ✓ dados de autenticação : resumo de mensagem assinado pela fonte e calculado a partir do datagrama IP original.
- ✓ campo "Next Header": especifica o tipo dos dados (p.ex., TCP, UDP, ICMP)



Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

Protocolo AH: detalhes



Fonte: Tanenbaum

Protocolo ESP

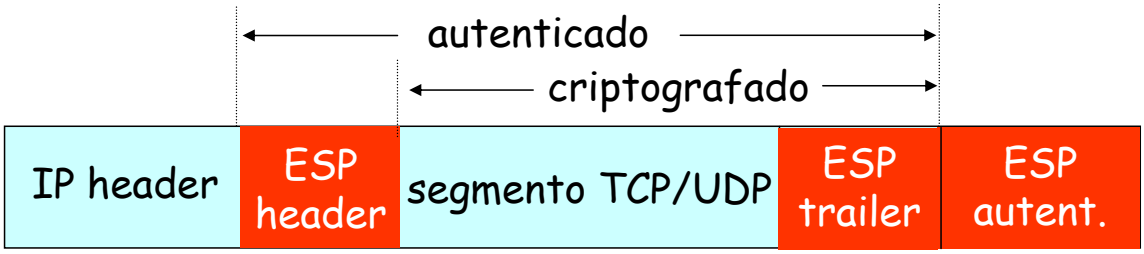
Fornece confidencialidade, autenticação e integridade dos dados.

Dados e trailer ESP são criptografados.

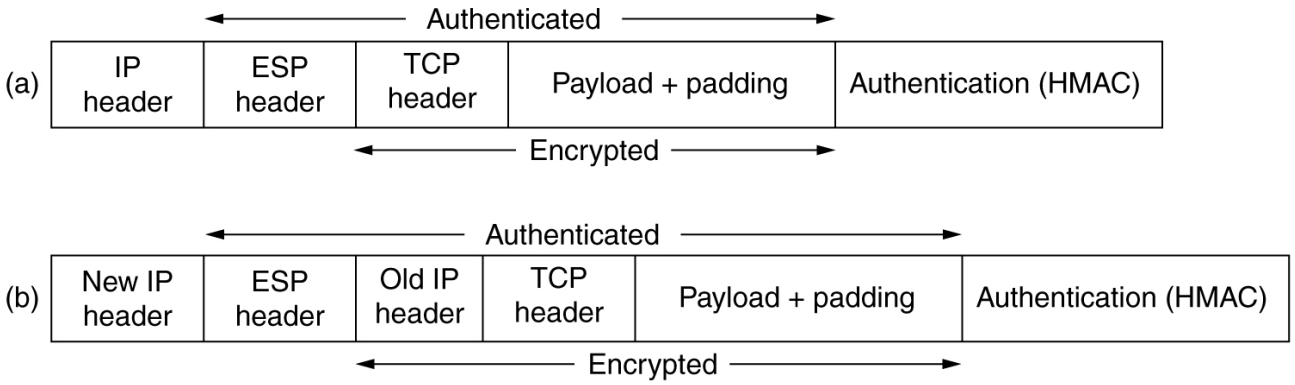
Campo "Next Header" fica no trailer ESP.

Campo de autenticação ESP similar ao campo de autenticação AH.

Protocolo = 50.



Protocolo ESP: detalhes



Fonte: Tanenbaum

(a) ESP no modo de transporte. (b) ESP no modo túnel.

Segurança IEEE 802.11

Wired Equivalent Privacy (WEP):

Autenticação como no protocolo *ap4.0.*

- ✓ Host requer autenticação do ponto de acesso (AP);
- ✓ Ponto de acesso envia *nonce* de 128 bits;
- ✓ Post cifra o *nonce* usando chave simétrica;
- ✓ Ponto de acesso decifra o *nonce* e autentica o host.

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

Segurança IEEE 802.11

Wired Equivalent Privacy (WEP):

Criptografia

- ✓ Host/AP compartilham uma chave simétrica de 40 bits (semi-permanente).
- ✓ Host adiciona vetor de inicialização (IV) de 24 bits para criar uma chave de 64 bits.
- ✓ Chave de 64 bits usada para gerar uma seqüência de chaves, k_i^{IV}.
- ✓ k_i^{IV} usada para cifrar o i-ésimo byte, d_i, do quadro:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- ✓ IV e os bytes cifrados, c_i são enviados no quadro.

Quebrando a cifragem 802.11 WEP

Furo na segurança:

IV de 24 bits, um IV por quadro → IV's são reusados.

IV transmitido em claro → reuso do IV detectável.

Ataque:

- ✓ Trudy faz Alice cifrar um texto em claro conhecido d_1 d_2 d_3...
- ✓ Trudy grava: $c_i = d_i$ XOR k_i^{IV}
- ✓ Trudy sabe c_i d_i, logo pode calcular k_i^{IV}
- ✓ Trudy conhece a seqüência das chaves k_1^{IV} k_2^{IV} k_3^{IV} ...
- ✓ Próxima vez que o mesmo IV for usado, Trudy poderá decifrar o quadro!

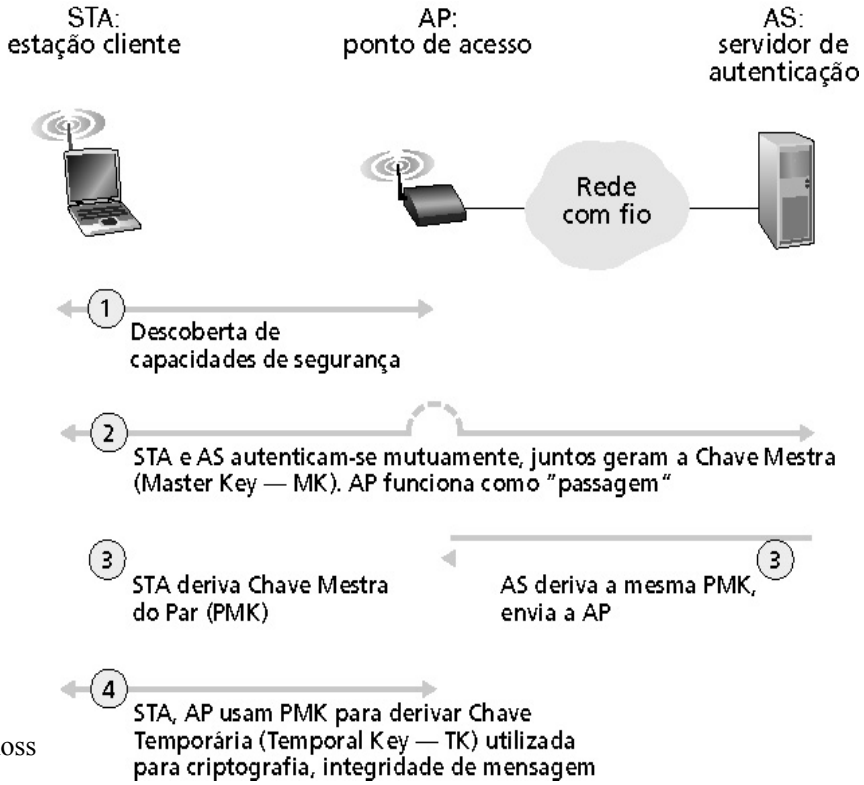
Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

802.11i

Versão aprimorada do WEP - 2004

- ✓ WEP
  - Criptografia relativamente fraca
  - Somente um modo de autenticação
  - Nenhum mecanismo de distribuição de chaves
- ✓ 802.11i
  - Numerosas formas de criptografia (e mais fortes) são possíveis
  - ✓ Oferece distribuição de chave
  - ✓ Usa autenticação de servidor separada do ponto de acesso

802.11i: quatro fases de operação



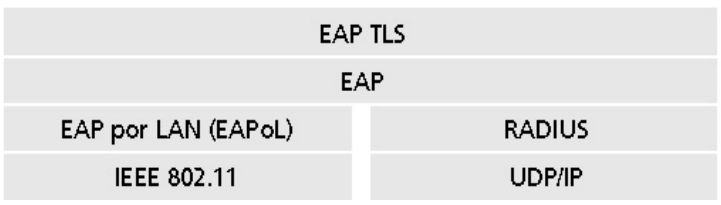
Fonte: Kurose e Ross

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

EAP: protocolo de autenticação extensível

- ✓ EAP: protocolo fim-a-fim entre o cliente (móvel) e o servidor de autenticação
- ✓ EAP envia sobre "enlaces" separados
  - Móvel para AP (EAP sobre LAN)
  - AP para servidor de autenticação (RADIUS sobre UDP)

Fonte: Kurose e Ross



WPA (Wi-Fi Protected Access)

- ✓ Lançado pela Wi-Fi Alliance, implementa um subconjunto de funcionalidades do IEE802.11i
- ✓ É um protocolo de encriptação mais bem elaborado com o objetivo de substituir o WEP
- ✓ Possui uma chave temporária TKIP (Temporal Key Integrity Protocol)
- ✓ IV de 48 bits
- ✓ Autenticação no modo pre-shared key no lugar de um servidor de autenticação para aplicações caseiras e de pequenos escritórios.
- ✓ Em grandes empresas, o WAP deve ser utilizado em conjunto com um servidor de autenticação.

Inatel
Instituto Nacional de Telecomunicações
Dispositivos e Tecnologias – Unid. 3

WPA2

- ✓ Implementação full do IEEE802.11i
- ✓ A principal mudança entre o WPA2 e o WPA é o método criptográfico utilizado.
- ✓ Enquanto o WPA utiliza o TKIP com o RC4, o WPA2 utiliza o AES (*Advanced Encryption Standard*) em conjunto com o TKIP com chave de 256 bits, que é um método de criptografia muito mais poderoso.
  - O AES permite a utilização de chaves de 128, 192 e 256 bits, constituindo-se assim em uma ferramenta poderosa de criptografia.
  - A utilização de chave de 256 bits no WPA2 é padrão.

Lista de Exercícios 03