Capítulo 8 – Segurança na Rede

Objetivos:

- Entender os princípios de segurança em redes:
  - Criptografia e seus *muitos* usos, além de "confidencialidade"
  - Autenticação
  - Integridade de mensagens
  - Distribuição de chaves
- Segurança na prática:
  - *firewalls*
  - Segurança nas camadas de aplicação, transporte, rede e enlace

Capítulo 8 - Segurança

O que é segurança na rede?

Confidencialidade: apenas o emissor e o receptor desejado devem "entender" o conteúdo da mensagem
- Emissor cifra a mensagem
- Receptor decifra a mensagem

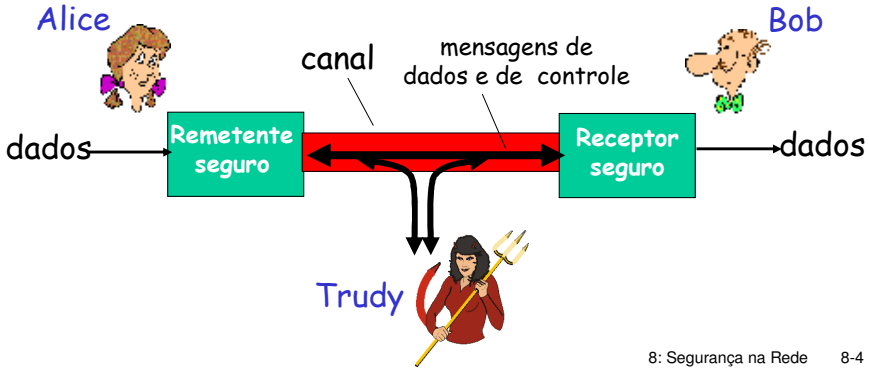
Autenticação: emissor e receptor querem confirmar a identidade um do outro

Integridade e não-repudiação de mensagens: emissor e receptor querem assegurar que o conteúdo da mensagem não foi alterado (em trânsito ou posteriormente)

Disponibilidade e Controle de Acesso: serviços devem estar acessíveis e disponíveis a usuários autorizados

Amigos e inimigos: Alice, Bob, Trudy

- Bob, Alice querem se comunicar com "segurança"
- Trudy (intrusa) pode interceptar, apagar e adicionar mensagens



Quem podem ser Bob e Alice?

- … Bobs e Alices reais!
- Navegadores/Servidores Web em transações eletrônicas
- Cliente /Servidor em bancos *on-line*
- Servidores DNS
- Roteadores trocando atualizações de tabelas de roteamento
- Outros exemplos?

Intrusos

Q: O que pode um intruso fazer?

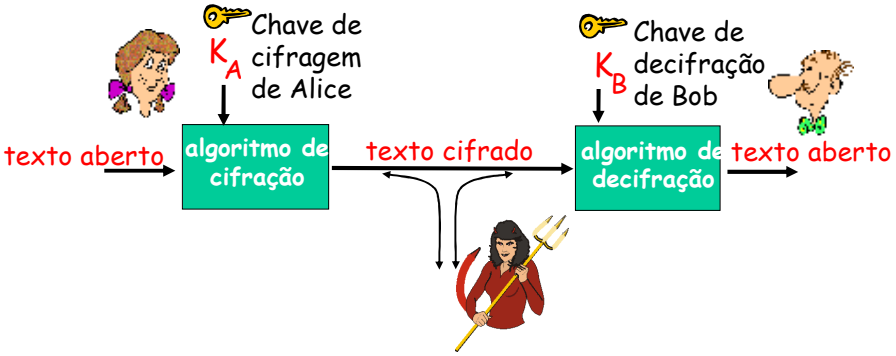
R: muito!

- *Espiar (eavesdrop):* interceptar mensagens
- *Inserir* mensagens na conexão
- *Personificação (impersonation):* fraudar (*spoof*) o endereço fonte de um pacote (ou outro campo)
- *Seqüestrar (hijacking):* "assumir" uma conexão em curso, inserindo-se no lugar do emissor ou o do receptor
- *Negação de serviço (denial of service)*: impedir que um serviço seja usado pelos outros (p.ex. sobrecarregando os recursos)

Capítulo 8 - Segurança

8.1 O que é segurança na rede?
8.2 Princípios de criptografia
8.3 Autenticação
8.4 Integridade
8.5 Distribuição de chaves e certificação
8.6 Controle de acesso: *firewalls*
8.7 Ataques e contramedidas
8.8 Segurança em muitas camadas

A linguagem da criptografia



criptografia de chave simétrica: chaves do emissor e do receptor são *idênticas*

criptografia de chave pública: chave de cifração publica; chave de decifração secreta (privada)

lat.mod. *cryptographia*, formado de *cript(o)-* (gr. *kruptós* 'oculto, secreto, obscuro,ininteligível') + *-grafia* (gr. *-graphía*, com o sentido de 'escrita', do v. gr. *gráphó* 'escrever'); f.hist. 1844 *cryptographia*

Criptografia de chave simétrica

cifra de substituição: substituir uma coisa por outra

- Cifra monoalfabetica : substituir uma letra por outra

```
textoabertp:   abcdefghijklmnopqrstuvwxyz
                ↓                       ↓
textocifrado:  mnbvcxzasdfghjklpoiuytrewq
```

Ex.: `Texto aberto: bob. i love you. alice`
`Texto cifrado: nkn. s gktc wky. mgsbc`

Q: Quão difícil é quebrar esta cifra simples?

Fig. 8.3

Quão difícil é quebrar a cifra monoalfabetica?

- 26! (~10^{26}) pares de letras
  - Trabalhoso quebrar com ataque de "força bruta"
  - Contudo, análise estatística do texto pode ajudar
- Ataque exclusivo a texto cifrado
  - O intruso têm apenas acesso ao texto cifrado
- Ataque com texto aberto conhecido
  - O intruso conhece alguns dos pares de letras
- Ataque com texto aberto escolhido
  - O intruso é capaz de fazer cifrar texto conhecido

Criptografia de chave simétrica: cifra polialfabetica

Plaintext letter:	a b c d e f g h i j k l m n o p q r s t u v w x y z
$C_1(k = 5)$:	f g h i j k l m n o p q r s t u v w x y z a b c d e
$C_2(k = 19)$:	t u v w x y z a b c d e f g h i j k l m n o p q r s

Figure 8.4 ♦ A polyalphabetic cipher using two Caesar ciphers

Ex. modelo de repetição C1, C2, C2, C1, C2:

Texto aberto: bob. i love you.
Texto cifrado: ghu. n etox dhz.

Fig. 8.4

Criptografia de chave simétrica : DES

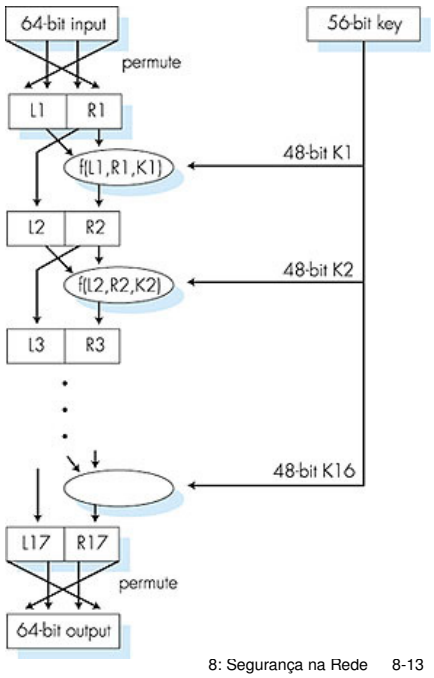
DES: Data Encryption Standard

- Padrão dos EUA [NIST 1993]
- Chave simétrica de 56 bits (mais 8 de paridade, um para cada 7+1 bits), aplicada a porções de texto aberto de 64 bits
- Quão segura é o DES?
  - DES Challenge (1997): a frase "Strong cryptography makes the world a safer place" foi decifrada usando força bruta em 4 meses
  - DES Chalenge III (1999): vencido em 22 horas
- Tornando o DES mais seguro:
  - Usar três chaves seqüencialmente (3-DES)
  - Encadeamento de blocos de cifras

Criptografia de chave simétrica: DES

DES

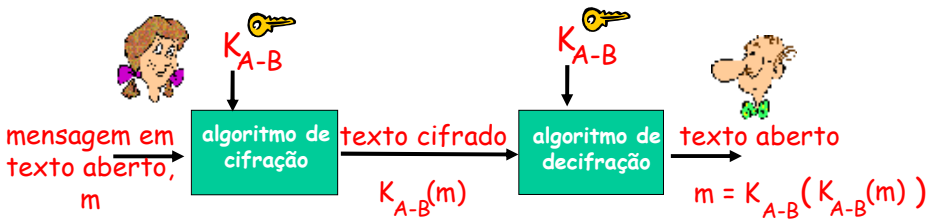
permutação inicial
16 rodadas idênticas envolvendo a aplicação de uma função, usando uma chave diferente de 48 bits
permutação final



AES: Advanced Encryption Standard

- Novo (Nov. 2001) padrão de chave simétrica do NIST, substituindo o DES
- Processa dados em blocos de 128 bits
- Chaves de 128, 192, ou 256 bits
- Decifração por força bruta (tentar cada chave),
  - se levar 1 s no DES com chave de 56 bits ...
  - ... levará 149 trilhões de anos no AES com chave de 128 bits

Criptografia de chave simétrica



- Q: como Bob e Alice chegam a um acordo sobre o valor da chave?

Chave Simétrica X Chave Pública

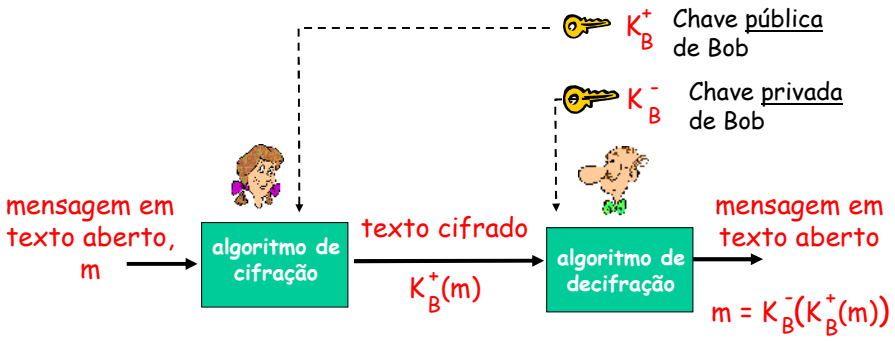
Criptografia de chave simétrica

- Requer que o emissor e o receptor recebam a chave secreta
- Como definir a chave? (particularmente se o emissor e o receptor nunca se "encontrarem")

Criptografia de chave pública

- [Diffie-Hellman76, RSA78]
- Chave *pública* de cifração conhecida por *todos*
- Chave *privada* de decifração conhecida apenas pelo receptor

Criptografia de chave pública



Algoritmos de criptografia de chave pública

Requisitos:

1. $K_B^+(\cdot)$ e $K_B^-(\cdot)$ tais que
$$K_B^-(K_B^+(m)) = m$$

2. dada a chave pública K_B^+, deve ser impossível computar a chave privada K_B^-

RSA: algoritmo de Rivest, Shamir, Adelson

RSA: Escolha das chaves

1. Escolha dois números primos grandes *p, q.* (p.ex. de 1024 bits cada)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Escolha $e < n$ que não tem fatores comuns com z (exceto 1) -> *e, z* são primos entre si.
4. Escolha d tal que $ed-1$ seja divisível exatamente por z. (ou seja : $ed \bmod z = 1$).
5. Chave *pública:* $\underbrace{(n,e)}_{K_B^+}$. Chave *privada:* $\underbrace{(n,d)}_{K_B^-}$.

RSA: Cifração, Decifração

0. Dados (n,e) e (n,d)
1. Para cifrar o padrão de bits, *m, tal que* $m < n$, computar
   $c = m^e \bmod n$
2. Para decifrar o padrão de bits recebido, *c*, computar
   $m = c^d \bmod n$

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

RSA: Exemplo

Bob escolhe $p=5$, $q=7$. Logo $n=35$, $z=24$.
$e=5$ (e,z primos entre si).
$d=29$ ($ed-1$ divisível exatamente por z.

	letra	m	m^e	$c = m^e \bmod n$
cifrar:	l	12	1524832	17

	c	c^d	$m = c^d \bmod n$	letra
decifrar:	17	481968572106750915091411825223071697	12	l

RSA: Por quê? $m = (m^e \bmod n)^d \bmod n$

Resultado da teoria dos números: Se p,q são primos e $n = pq$, então:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(usando o resultado acima)

$$= m^1 \bmod n$$

(usando $ed \bmod (p-1)(q-1) = 1$)

$$= m$$

(pois $m < n$)

RSA

Outra propriedade importante:

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

Por que o RSA é seguro?

- Dificuldade prática para fatorar números inteiros grandes
  - Neste caso, *n* em *p* e *q*

Capítulo 8 - Segurança

Autenticação

Objetivo: Bob quer que Alice prove a sua identidade

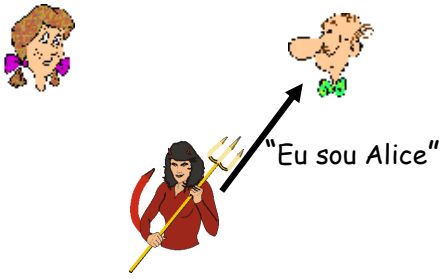
Protocolo pa1.0: Alice diz "Eu sou Alice"

Cenário de falha ?

Autenticação

Objetivo: Bob quer que Alice prove a sua identidade

Protocolo pa1.0: Alice diz "Eu sou Alice"



Numa rede, Bob não pode "ver" Alice, logo Trudy simplesmente se declara como Alice

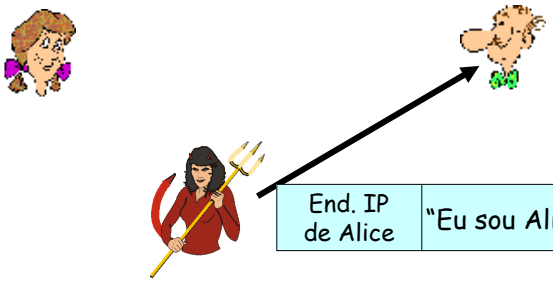
Autenticação : outra tentativa

Protocolo pa2.0: Alice diz "Eu sou Alice" num pacote IP contendo o seu endereço IP fonte

Cenário de falha??

Autenticação: outra tentativa

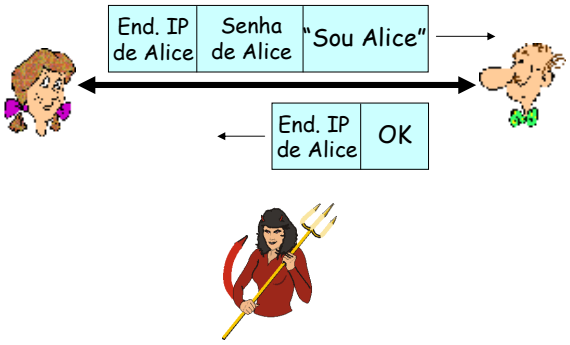
Protocolo pa2.0: Alice diz "Eu sou Alice" num pacote IP contendo o seu endereço IP fonte



Trudy pode criar um pacote "imitando" (*spoofing*) o endereço de Alice

Autenticação: outra tentativa

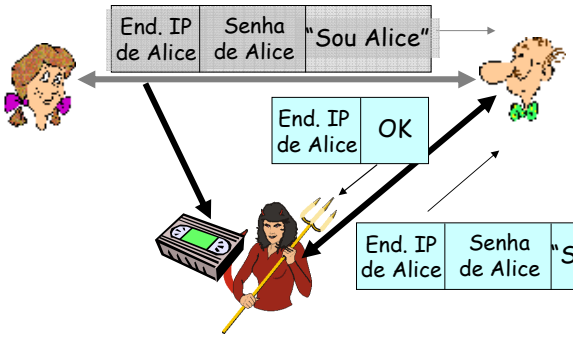
Protocolo pa3.0: Alice diz "Eu sou Alice" e envia a sua senha secreta para "provar"



Cenário de falha??

Autenticação: outra tentativa

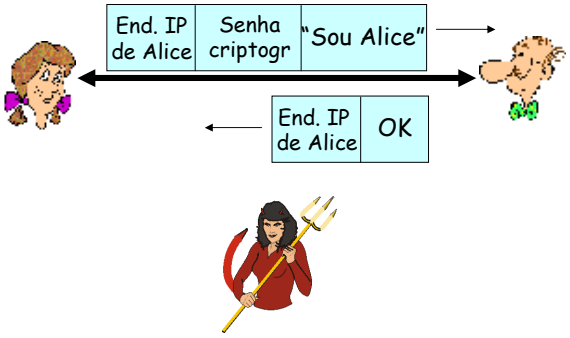
Protocolo pa3.0: Alice diz "Eu sou Alice" e envia a sua senha secreta para "provar"



Trudy espia e descobre a senha de Alice

Autenticação: mais uma tentativa

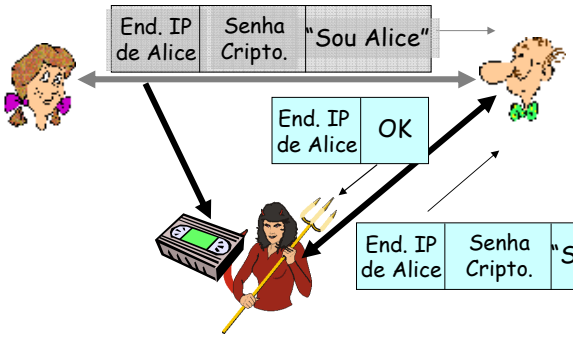
Protocolo pa3.1: Alice diz "Eu sou Alice" e envia a sua senha secreta *criptografada* para "provar".



Cenário de falha??

Autenticação: mais uma tentativa

Protocolo pa3.1: Alice diz "Eu sou Alice" e envia a sua senha secreta *criptografada* para "provar".



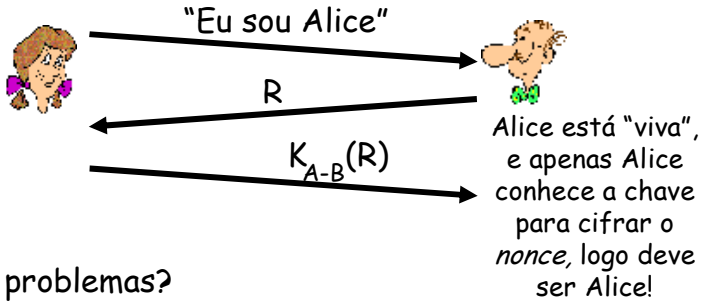
Ataque de reprodução: Trudy grava o pacote de Alice e posteriormente o reproduz para Bob

Autenticação: mais uma tentativa

Objetivo: evitar o ataque de reprodução

Nonce: número (R) usado apenas "uma *vez na vida*"

pa4.0: para provar que Alice está "viva", Bob envia a Alice um *nonce*, R. Alice deve retornar R, criptografado com uma chave secreta compartilhada



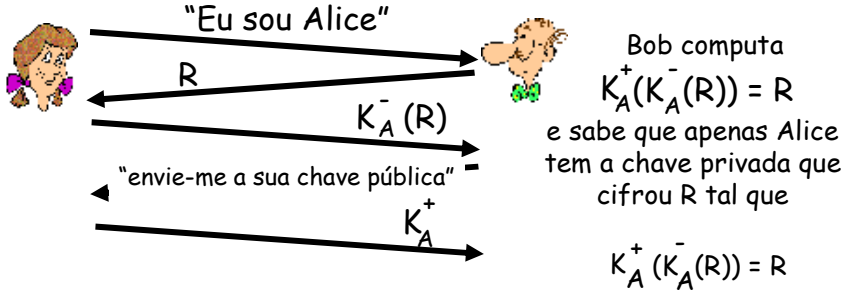
Falhas, problemas?

Autenticação: pa5.0

pa4.0 requer uma chave simétrica compartilhada

- Pode-se autenticar usando chaves públicas?

pa5.0: usa um *nonce* e criptografia de chave pública



pa5.0: falha de segurança

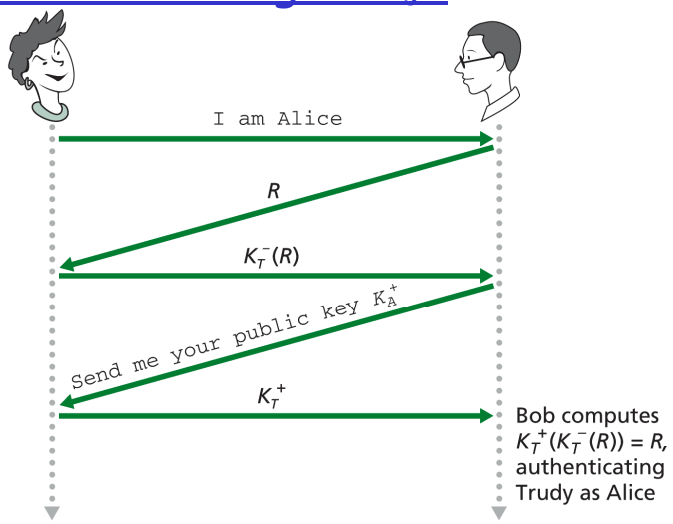


Figure 8.12 ♦ A security hole in protocol *ap5.0*

pa5.0: falha de segurança

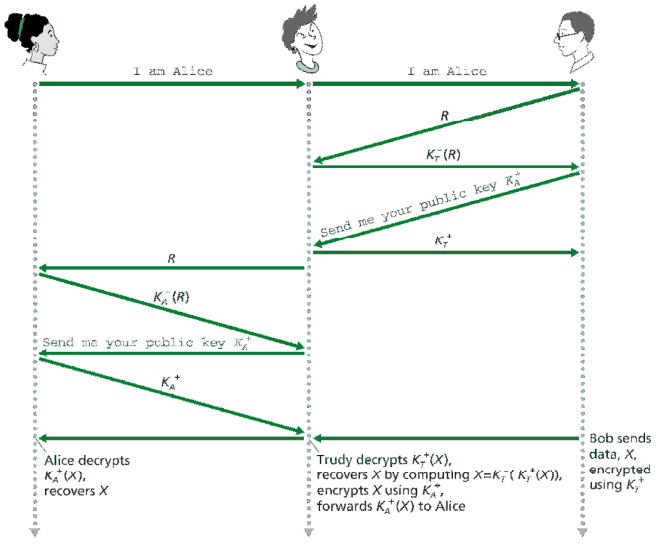


Figure 8.13 ♦ A man-in-the-middle attack

pa5.0: falha de segurança

Ataque do homem (mulher) no meio: Trudy se passa por Alice (para Bob) e por Bob (para Alice)

Difícil de detectar:

- Bob recebe tudo que Alice envia e vice-versa (eles podem se encontrar posteriormente e não perceber o que ocorreu)
- O problema é que Trudy também recebe todas as mensagens!
  - É necessário um mecanismo seguro de distribuição de chaves públicas

Capítulo 8 - Segurança

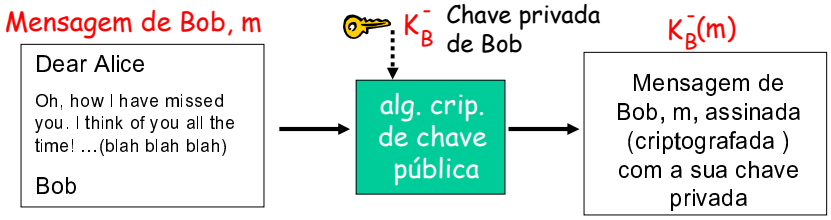
8.1 O que é segurança na rede?
8.2 Princípios de criptografia
8.3 Autenticação
8.4 Integridade
8.5 Distribuição de chaves e certificação
8.6 Controle de acesso: *firewalls*
8.7 Ataques e contramedidas
8.8 Segurança em muitas camadas

Assinaturas Digitais

Técnicas criptográficas são análogas a assinaturas a mão.

- Emissor (Bob) assina digitalmente o documento, indicando que ele é o proprietário/autor do documento
- Verificável, não falsificável e incontestável: receptor (Alice) pode provar que Bob, e ninguém mais (incluindo Alice), assinou o documento

Assinaturas Digitais



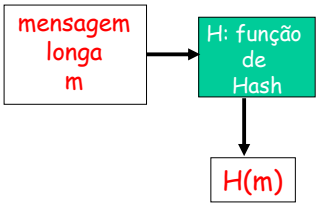
- Suponha que Alice recebe m e a assinatura digital $K^-_B(m)$
- Alice confirma que m foi assinada por Bob verificando se $K^+_B(K^-_B(m)) = m$.

Resumo de Mensagem

A criptografia de chave pública é computacionalmente dispendiosa para mensagens longas

Objetivo: "impressão digital" de tamanho fixo fácil de computar

- Aplicar uma função de *hash* H a m, para obter um resumo da mensagem de tamanho fixo, H(m)

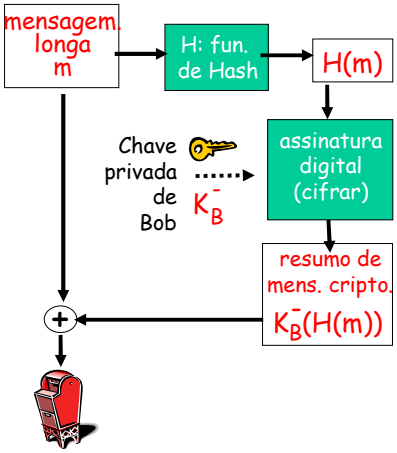


Propriedades da função de *hash*:

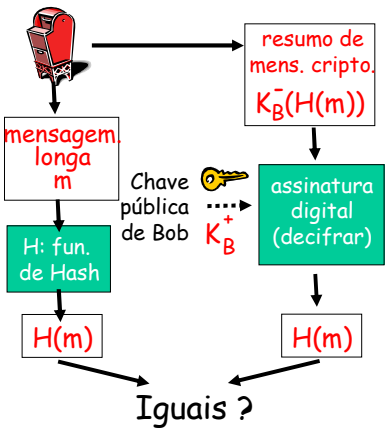
- H(m) fácil de calcular
- Muitos-para-um
  - Entrada de qq tamanho
  - Saída de tamanho fixo
- Dado H(m) é inviável encontrar m
- Dado m, é inviável encontrar m' tal que H(m) = H(m').
- Qualquer mudança na entrada (mesmo de apenas 1 bit) produz uma saída muito diferente

Assinatura Digital = Resumo de Mensagem Assinado

Bob envia mensagem assinada digitalmente:



Alice verifica a assinatura e a integridade da mensagem assinada digitalmente:



Algoritmos de Funções de Hash

Internet checksum: função de *hash* pobre

Checksum da Internet:

- fácil de calcular
- produz um resumo de mensagem de tamanho fixo
- muitos-para-um

Mas, dada uma mensagem com um valor de *hash,* é fácil encontrar outra mensagem como mesmo valor :

mensagem	ASCII
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 D2 42
	B2 C1 D2 AC

mensagem	ASCII
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 D2 42
	B2 C1 D2 AC

Mens. diferentes mas *checksums* idênticos!

Fig. 8.18

Algoritmos de Funções de Hash

- MD5 amplamente usado (RFC 1321)
  - Calcula resumo de mensagem de 128 bits
  - Conjectura-se que a dificuldade de produzir ...
    - duas mensagens que tenham o mesmo resumo seja da ordem de 2^{64} operações
    - uma mensagem que tenha um dado resumo seja da ordem de 2^{128} operações
- Secure Hash Algorithm (SHA-1)
  - Padrão dos EUA [NIST, FIPS PUB 180-1]
  - Resumo de 160 bits

Capítulo 8 - Segurança

8.1 O que é segurança na rede?
8.2 Princípios de criptografia
8.3 Autenticação
8.4 Integridade
8.5 Distribuição de chaves e certificação
8.6 Controle de acesso: *firewalls*
8.7 Ataques e contramedidas
8.8 Segurança em muitas camadas

Intermediários Confiáveis

Problema da Chave Simétrica:

- Como duas entidades estabelecem uma chave secreta através da rede?

Solução:

- Centro de distribuição de chaves confiável (*key distribution center* - KDC) atuando como intermediário entre as entidades

Problema da Chave pública:

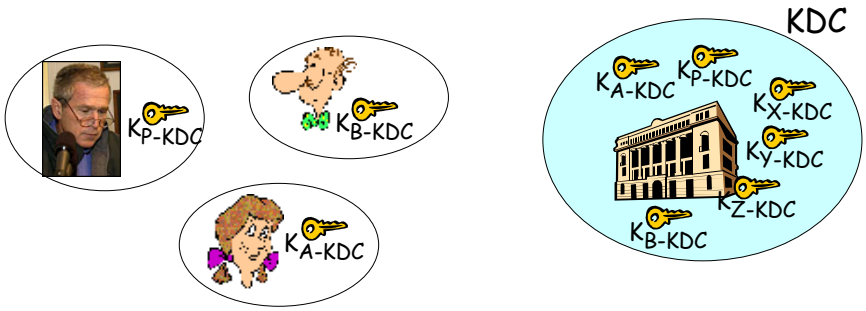
- Quando Alice obtém a chave pública de Bob (de página na Web, *e-mail*, disquete), como ela sabe que se trata realmente da chave pública de Bob, não de Trudy?

Solução:

- Autoridade certificadora confiável (*certification authority* - CA)

Key Distribution Center (KDC)

- Alice e Bob precisam de chave simétrica compartilhada
- KDC: servidor compartilha chaves secretas diferentes com *cada* usuário registrado
- Alice e Bob conhecem as suas chaves simétricas, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, para comunicar-se com o KDC.



Key Distribution Center (KDC)

Q: Como o KDC permite que Bob e Alice determinem chaves simétricas compartilhadas e secretas para se comunicar?

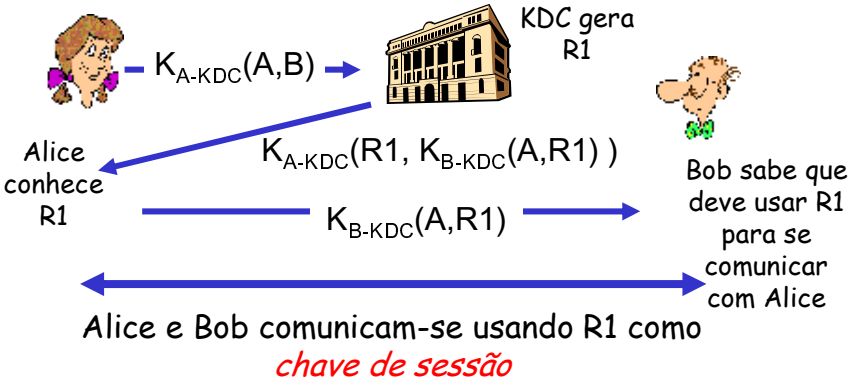
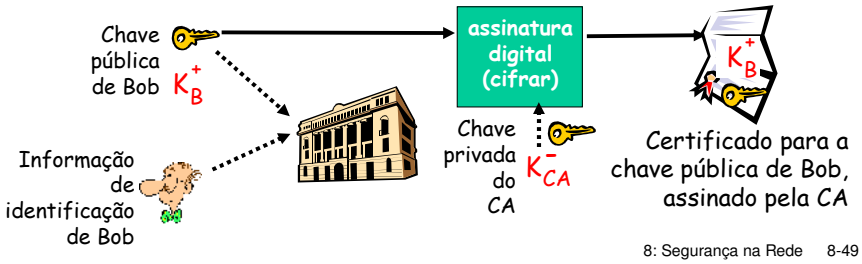


Figura 8.19

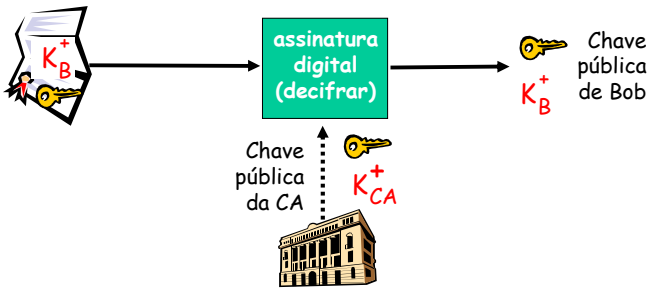
Autoridades de Certificação

- *Certification authority* (CA): associa uma chave pública a uma entidade particular, E.
- E (pessoa, roteador …) registra a sua chave pública na CA.
  - E fornece "prova de identidade" à CA.
  - CA cria certificado vinculando E à sua chave pública.
  - Certificado contém a chave publica de E assinada digitalmente pela CA



Autoridades de Certificação

- Quando Alice quer a chave pública de Bob:
  - Obtém certificado de Bob (através de Bob ou em outra parte).
  - Aplica a chave pública da CA ao certificado de Bob para obter a chave pública de Bob

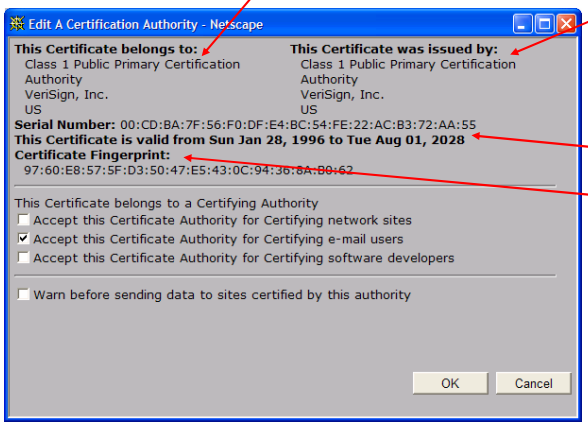


Field Name	Description
Version	Version number of X.509 specification
Serial Number	CA-issued unique identifier for a certificate
Signature	Specifies the algorithm used by CA to sign this certificate
Issuer Name	Identity of CA issuing this certificate, in distinguished name (DN) [RFC 2253] format
Validity period	Start and end of period of validity for certificate
Subject name	Identity of entity whose public key is associated with this certificate, in DN format
Subject public key	The subject's public key as well as an indication of the public key algorithm (and algorithm parameters) to be used with this key

Table 8.3 ♦ Selected fields in a X.509 and RFC 1422 public key

Conteúdo de um certificado:

- Número de série (único para o certificado/emissor)
- Informação sobre o proprietário do certificado, incluindo algoritmo e o valor da chave (não mostrada)



- Informação sobre o emissor do certificado
- validade
- Assinatura digital do emissor

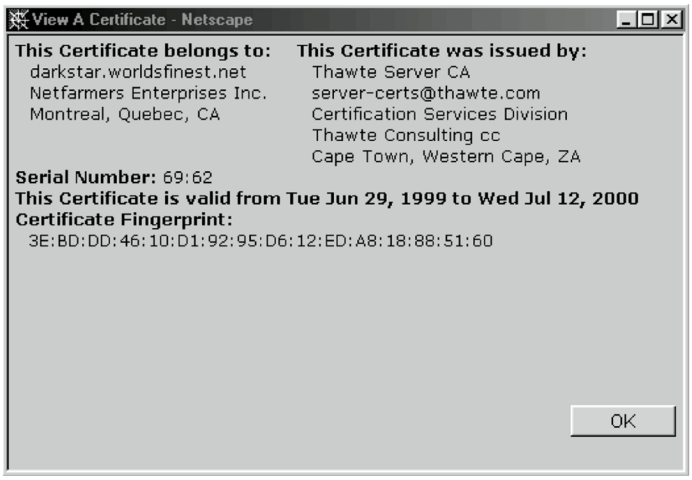


Figure 8.22 ♦ A certificate issued by Thawte Consulting to Netfarmers Enterprises, Inc.

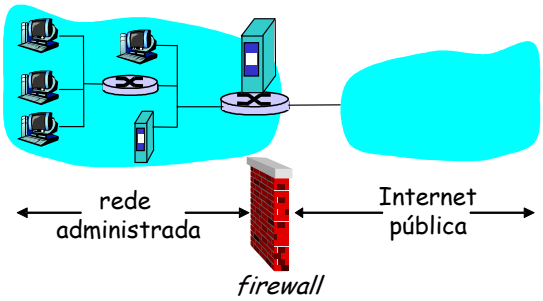
Capítulo 8 - Segurança

8.1 O que é segurança na rede?
8.2 Princípios de criptografia
8.3 Autenticação
8.4 Integridade
8.5 Distribuição de chaves e certificação
8.6 Controle de acesso: *firewalls*
8.7 Ataques e contramedidas
8.8 Segurança em muitas camadas

Firewalls

firewall

Isola a rede interna de uma organização da Internet pública, permitindo que alguns pacotes passem e bloqueando outros.



Firewalls:

Previnem ataques do "negação de serviço":

- *SYN flooding*: atacante estabelece muitas conexões TCP "falsas", não deixando recursos para conexões "reais".

Previnem acesso/modificação ilegal dos dados internos.

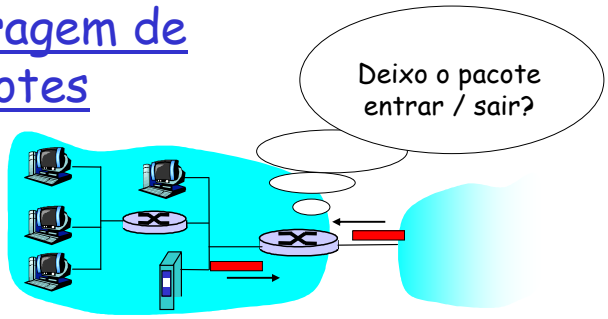
- Ex. atacante troca a página Web da organização

Permitem apenas acessos autorizados à rede interna (conjunto de usuários/hospedeiros autenticados)

Dois tipos de *firewalls:*

- *Gatway* de aplicação
- Filtragem de pacotes

Filtragem de Pacotes



- Rede interna conectada à Internet através de um roteador *firewall*
- Roteador filtra pacote-a-pacote. Decisão para repassar / descartar baseada em:
  - endereço IP fonte e destino
  - Portas origem e destino do TCP/UDP
  - Tipo de mensagem ICMP
  - Bits TCP SYN e ACK

Filtragem de Pacotes

- Exemplo 1: Bloquear datagramas de entrada e saída com:
  - IP.protocolo = 17 ou (porta fonte =23 ou porta destino= 23).
  - Todos os pacotes UDP de entrada e saída e conexões telnet são bloqueadas.
- Exemplo 2: Bloquear segmentos TCP de entrada com ACK=0.
  - Evita que clientes externos estabeleçam conexões TCP com servidores internos, mas permite que clientes internos se conectem com o exterior.

Rule	Source Address	Destination Address	Action	Comments
R1	111.11/16	222.22.22/24	permit	Let datagrams from Bob's university network into a restricted subnet.
R2	111.11.11/24	222.22/16	deny	Don't let traffic from Trudy's subnet into anywhere within Alice's network.
R3	0.0.0.0/0	0.0.0.0/0	deny	Don't let traffic into Alice's network.

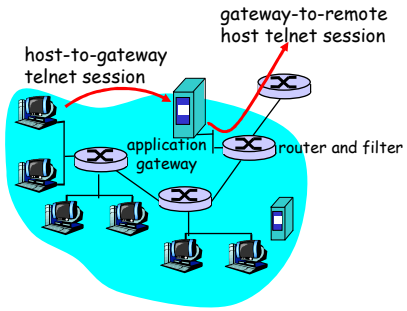
Table 8.4 ♦ Packet-filtering rules

Datagram Number	Source IP Address	Destination IP Address	Desired Action	Action Under R2, R1, R3	Action Under R1, R2, R3
P1	111.11.11.1 (hacker subnet)	222.22.6.6 (corp.net)	deny	deny (R2)	deny (R2)
P2	111.11.11.1 (hacker subnet)	222.22.22.2 (special subnet)	deny	deny (R2)	permit (R1)
P3	111.11.6.6 (univ. net, not the hacker subnet)	222.22.22.2 (special subnet)	permit	permit (R1)	permit (R1)
P4	111.11.6.6 (univ. net, not the hacker subnet)	222.22.6.6 (corp. net)	deny	deny (R3)	deny (R3)

Table 8.5 ♦ Results of packet filtering, according to rule order

Gateways de Aplicação

- Filtram pacotes usando também dados da aplicação.
- Exemplo: permitir que alguns usuários internos façam telnet para fora.



1. Requer que todos os usuários façam telnet através do gateway.
2. Para usuários autorizados, o *gateway* estabelece uma conexão telnet com o hospedeiro de destino. O *gateway* repassa os dados entre as duas conexões.
3. Roteador-filtro bloqueia todas as conexões que não se originem no *gateway*.

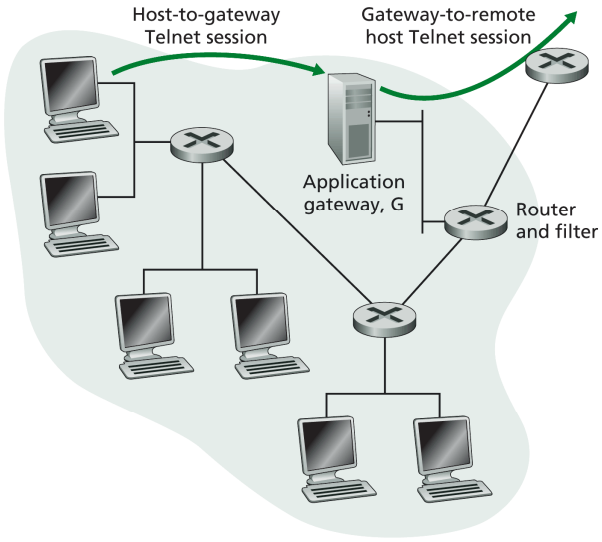


Figure 8.24 ♦ Firewall consisting of an application gateway and a filter

Limitações de *firewalls* e *gateways*

- *IP spoofing*: roteador não tem como saber se os dados "realmente" vem da fonte declarada
- Se várias aplicações precisam de tratamento especial, cada uma precisa de seu *gateway*.
- O software cliente deve saber como contatar o gateway.
  - ex., deve-se especificar o end. IP do *proxy* no navegador Web
- Geralmente filtros usam uma política de tudo ou nada (p.ex. para tráfego UDP).
- compromisso:
  grau de comunicação com o mundo exterior
  X
  nível de segurança
- Diversos sítios muito protegidos ainda sofrem com ataques.

Capítulo 8 - Segurança

8.1 O que é segurança na rede?
8.2 Princípios de criptografia
8.3 Autenticação
8.4 Integridade
8.5 Distribuição de chaves e certificação
8.6 Controle de acesso: *firewalls*
8.7 Ataques e contramedidas
8.8 Segurança em muitas camadas

Ameaças à Segurança na Internet

Mapeamento:

Antes de atacar: "reconhecer o terreno" – P.ex. endereços IP e serviços implementados

- `ping` para determinar os endereços IP presentes na rede
- Varredura de portas (*port-scanning*) : tentar contatar portas seqüencialmente (via conexões TCP ou datagramas UDP)
  - nmap (http://www.insecure.org/nmap/): "exploração de rede e auditoria de segurança"

Contramedidas?

Ameaças à Segurança na Internet

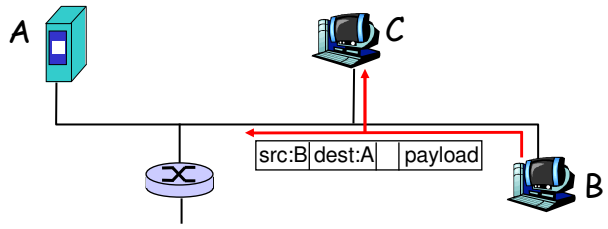
Mapeamento: contramedidas

- Registrar o tráfego entrando na rede
- Procurar atividades suspeitas (endereços IP, portas sendo varridas seqüencialmente)

Ameaças à Segurança na Internet

Análise de pacotes (*packet sniffing*):

- Canais de difusão
- NIC em modo promíscuo pode ler dados não criptografados (ex. senhas)
- ex. C analisa os pacotes de B



Contramedidas?

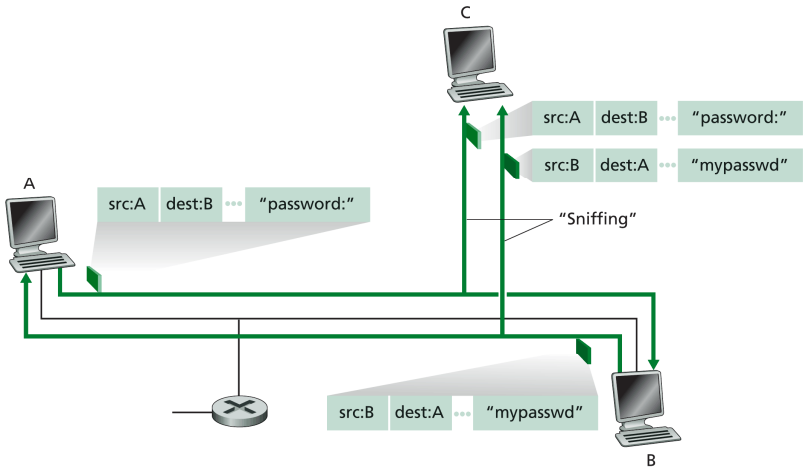
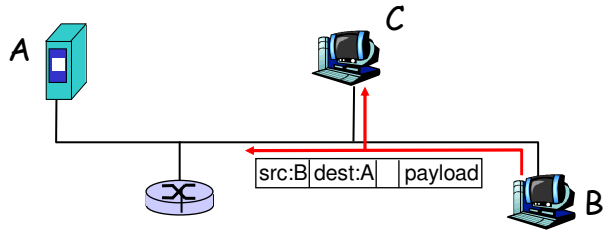


Figure 8.25 ♦ Packet sniffing

Ameaças à Segurança na Internet

Análise de pacotes: contramedidas

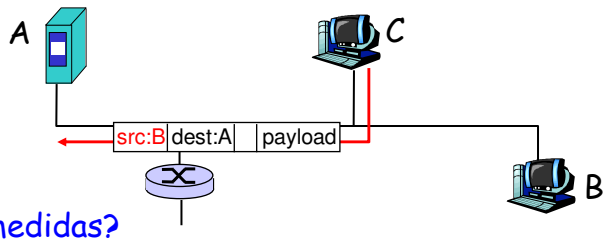
- Rodar em todos os hospedeiros da organização programa que verifica periodicamente se as interfaces estão em modo promíscuo.
- Um hospedeiro por segmento em enlaces de difusão (Ethernet comutada).
- Criptografia.



Ameaças à Segurança na Internet

Falsificação de endereço IP (*IP Spoofing*):

- Dependendo do controle que se tem sobre o equipamento, pode-se gerar pacotes IP, com qq. endereço fonte IP
- Receptor não tem como saber se a fonte é falsificada



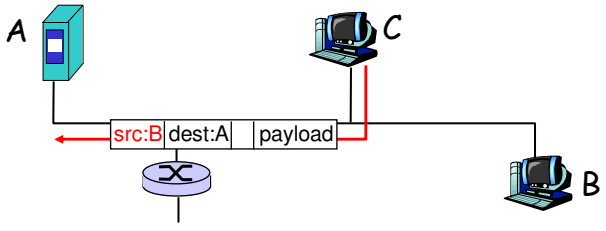
Contramedidas?

Ameaças à Segurança na Internet

IP Spoofing: Contramedidas

Filtragem de entrada

- Roteadores não devem repassar pacotes de saída com endereços fonte inválidos (ex. endereço fonte do datagrama não pertencente à rede do roteador)
- Boa prática na Internet, porém, não pode ser imposta a todas as redes



Ameaças à Segurança na Internet

Negação de Serviço (*Denial Of Service* - DOS):

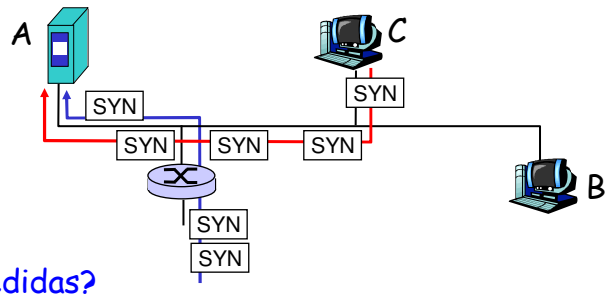
- Torrente de pacotes maliciosamente gerados para "alagar" um receptor. Exs.:
  - Inundação SYN com endereços IP fonte falsificados. A terceira via do *3-way hadshake* não é feita, deixando conexões parcialmente abertas.
  - Enviar fragmentos IP, mas sem completar um datagrama.
  - *Ataque smurf:* hospedeiros inocentes respondem a pacotes ICMP solicitando eco para um IP falsificado (a ser atacado)

Contramedidas?

Ameaças à Segurança na Internet

Negação de Serviço Distribuída (DDOS):

- Varias fontes coordenadas alagam o receptor
- ex., C e outro hospedeiro remoto fazem um ataque SYN a A



Contramedidas?

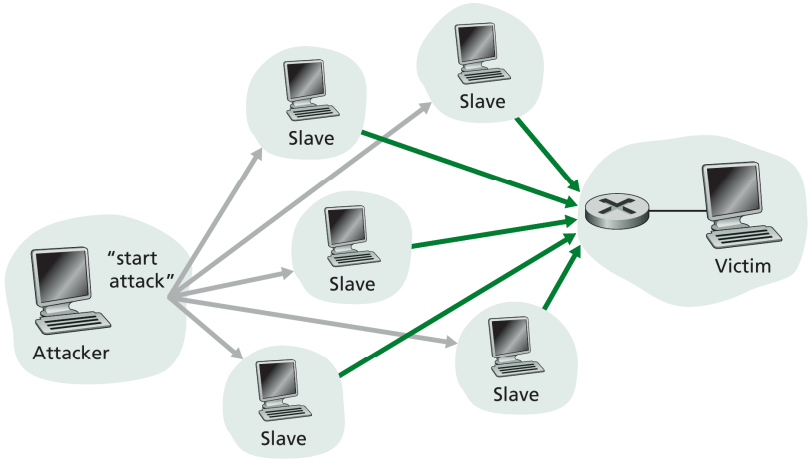


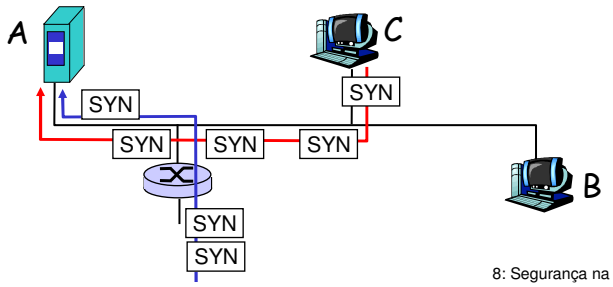
Figure 8.26 ♦ A DDoS attack

Ameaças à Segurança na Internet

Negação de Serviço: contramedidas

- Filtrar pacotes de inundação (ex. SYN) antes de que eles cheguem ao hospedeiro - descarte de bons com ruins
- Traçar o caminho de volta até a fonte da inundação - provavelmente um inocente, uma máquina comprometida

De modo geral, é difícil se proteger de ataques DoS, e especialmente de ataques DDoS



Capítulo 8 - Segurança

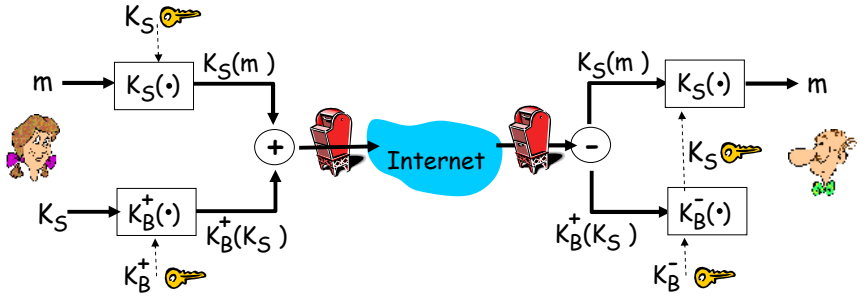
8.1 O que é segurança na rede?
8.2 Princípios de criptografia
8.3 Autenticação
8.4 Integridade
8.5 Distribuição de chaves e certificação
8.6 Controle de acesso: *firewalls*
8.7 Ataques e contramedidas
8.8 Segurança em muitas camadas
- 8.8.1. correio eletrônico seguro
- 8.8.2. soquetes seguros
- 8.8.3. IPsec
- 8.8.4. Segurança no 802.11

Segurança em muitas camadas, por quê?

- Segurança nas camadas inferiores nem sempre é suficiente para garantir a segurança nas camadas superiores
  - p.ex., a camada de rede pode criptografar os dados dos datagramas e autenticar os endereços IP, porém ela não é capaz de autenticar um cliente fazendo compras em um sítio de comercio-e.
- E mais fácil implantar novos serviços, inclusive de segurança, nas camadas superiores da pilha de protocolos

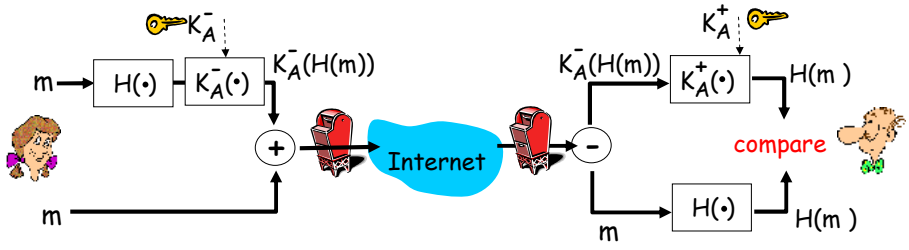
Correio Eletrônico Seguro

Alice quer enviar uma mensagem confidencial, m, a Bob.



Correio Eletrônico Seguro

Alice quer autenticação do remetente e integridade da mensagem.



Correio Eletrônico Seguro

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

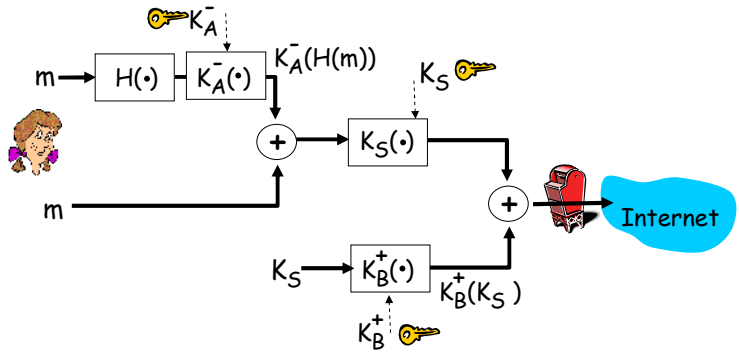


Figura 8.29

Pretty good privacy (PGP)

- Padrão *de facto* de criptografia para correio eletrônico na Internet.
- Usa chave criptografia de chave simétrica, criptografia de chave pública, função de *hash*, e assinatura digita.
- Fornece confidencialidade, autenticação do remetente e integridade.
- Phil Zimmerman, o inventor, foi alvo de uma investigação do governo dos EUA durante 3 anos.

Mensagem assinada com o PGP:

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

Bob:Can I see you tonight?
  Passionately yours,
  Alice

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

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.0
u2R4d+/jKmn8Bc5+hgDsqAewsDfrGdszX68liKm5F6Gc4sDfcXyt
RfdS10juHgbcfDssWe7/K=lKhnMikLo0+1/BvcX4t==Ujk9PbcD4
Thdf2awQfgHbnmKlok8iy6gThlp
-----END PGP MESSAGE
```

Figure 8.31 ♦ A secret PGP message

Secure sockets layer (SSL)

- Segurança na camada de transporte para aplicações baseada em TCP.
- Usado entre navegadores da Web e servidores para comercio eletrônico (https).
- Serviços de segurança:
  - autenticação de servidores
  - criptografia de dados
  - autenticação de clientes (opcional)
- Autenticação do servidor:
  - Navegadores habilitados para SSL incluem as chaves públicas de CAs de confiança.
  - Navegador requisita o certificado do servidor, emitido por um CA de confiança.
  - Navegador usa a chave pública do CA para extrair do certificado a chave pública do servidor.

SSL

Sessão SSL:

- Navegador gera uma *chave simétrica de sessão*, criptografa-a com a chave pública do servidor e a envia ao servidor.
- Usando a chave privada, o servidor decifra a chave de sessão.
- Todos os dados enviados através do soquete TCP são codificados usando a chave de sessão.

- SSL: base do *Transport Layer Security* (TLS) da IETF.
- SSL pode ser usado por aplicações não-Web, ex. IMAP.
- Autenticação do cliente pode ser feita com certificados do cliente.

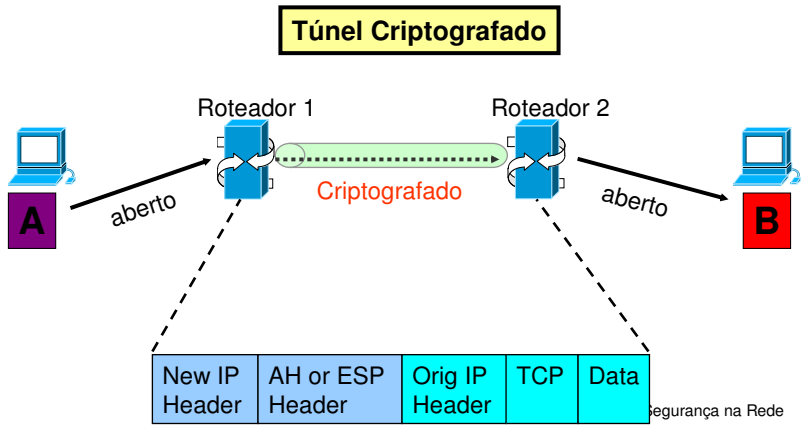
IPsec: Segurança na Camada de Rede

- Sigilo na camada de rede:
  - Hospedeiro emissor criptografa os dados do datagrama IP
    - Segmentos TCP e UDP; mensagens ICMP e SNMP.
- Autenticação na camada de Rede
  - Hospedeiro de destino pode autenticar end. IP fonte
- Protocolos principais:
  - authentication header (AH)
  - encapsulation security payload (ESP)
  - geração e distribuição de chaves (não discutidos aqui)

- Negociação inicial entre fonte e destino, para AH e ESP:
  - Criar um canal lógico em nível de rede chamado uma associação de segurança (*security association* - SA)
- Cada SA é unidirecional.
- Unicamente determinada por:
  - Protocolo de segurança (AH ou ESP)
  - Endereço IP destino
  - Id. de conexão de 32 bits (*Security Parameter Index - SPI*)

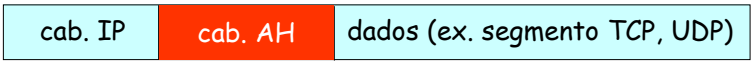
IPsec: Modo Transporte vs. Modo Túnel

- Transporte : hospedeiro -> hospedeiro
- Túnel: hospedeiro -> roteador ou roteador -> roteador



AH (*Authentication Header*)

- Fornece autenticação da fonte, integridade de dados, mas não confidencialidade
- Cabeçalho AH inserido entre o cabeçalho IP e o campo de dados (modo transporte)
- Campo protocolo: 51
- Roteadores intermediários processam o datagrama da forma usual

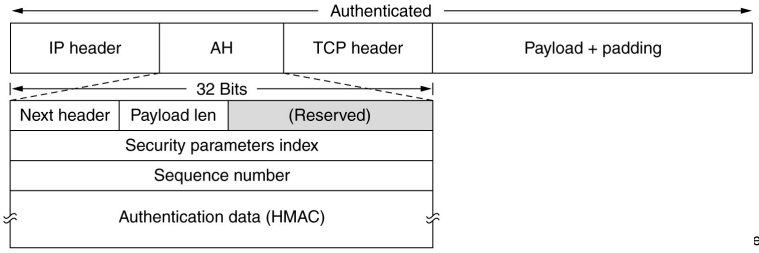


AH (*Authentication Header*)

Cabeçalho AH inclui:

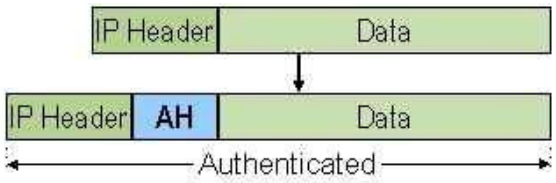
- Id. de conexão (SPI)
- Dados de autenticação (HMAC): resumo de mensagem assinado pela fonte, calculado a partir do datagrama IP original (exceto para os campos que podem mudar durante o trânsito).
- Campo 'próximo cabeçalho' : especifica o tipo de dados (ex. TCP, UDP, ICMP)

- O AH é incompatível com NAT: o NAT muda o end. IP fonte
  - NAT-T (RFC 3715, 3947, 3948) define mecanismos para encapsular mensagens IPsec de modo a permitir a coexistência IPSec-NAT

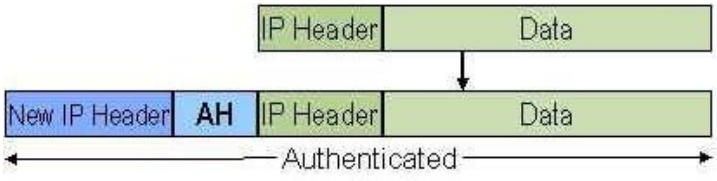


Modos de uso do IPSec - AH

- Modo de Transporte

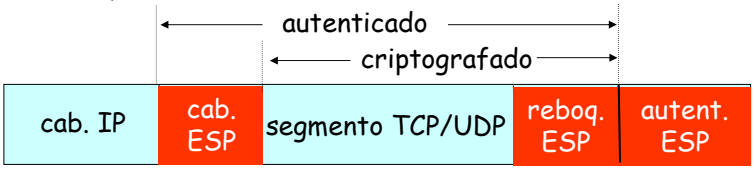


- Modo de Túnel



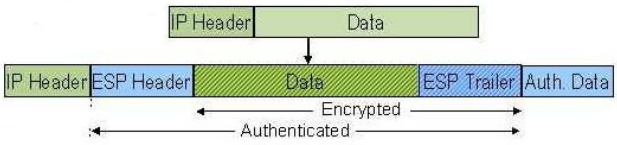
ESP (*encapsulation security payload*)

- Fornece confidencialidade, autenticação de hospedeiro e integridade dos dados.
- Dados e reboque (*trailer*) ESP criptografados .
- Campo 'próximo cabeçalho' no reboque ESP.
- Campo autenticação do ESP é similar ao campo autenticação do AH.
- Protocolo = 50.

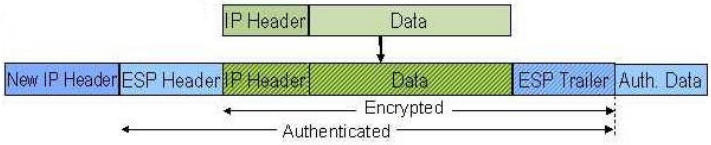


Modos de uso do IPSec - ESP

Modo transporte



Modo Túnel



Segurança no IEEE 802.1

- *War-driving:* deslocamento de carro pela Baia de São Francisco, durante 18 meses em 2001, com um *laptop* equipado com uma placa 802.11
  - Mais de 9000 redes acessíveis a partir das vias públicas
  - 85% não usa criptografia/autenticação (nem mesmo os frágeis mecanismos originais do padrão)
  - Fácil fazer análise de pacotes (*packet-sniffing*) e vários tipos de ataques!
- Segurança no 802.11
  - Criptografia, autenticação
  - Primeira tentativa de segurança no 802.11: *Wired Equivalent Privacy* (WEP): um fiasco
  - Tentativa atual: 802.11i

WEP (*Wired Equivalent Privacy*)

- Autenticação como no protocolo *pa4.0*
  - Hosp. requisita autenticação ao ponto de acesso
  - Ponto de acesso envia um nonce de 128 bits
  - Hosp. criptografa o *nonce* usando chave simétrica compartilhada
  - Ponto de acesso decifra o *nonce* e autentica o hosp.
- Não há mecanismo de distribuição de chaves
- Autenticação: conhecer a chave compartilhada é o suficiente

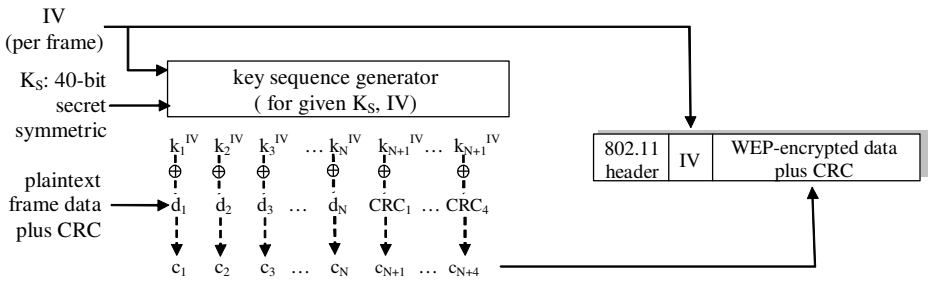
WEP: criptografia de dados

- Hosp./AP compartilham uma chave simétrica de 40 bits (semipermanente)
- Hosp. acrescenta um vetor de iniciação de 24 bits (IV) a fim de criar uma chave de 64 bits
- Chave de 64 bits é usada para gerar uma seqüência de chaves, k_i^{IV}
- k_i^{IV} usada para criptografar o i'ésimo byte, d_i, do quadro :

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

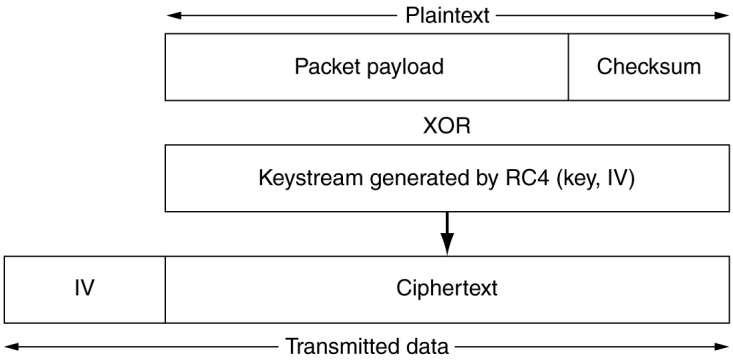
- IV e bytes criptografados, c_i enviados no quadro

802.11 WEP: criptografia de dados



WEP: criptografia do lado emissor

802.11 WEP: criptografia de dados



Quebrando a criptografia do 802.11 WEP

Falha de segurança:

- Um IV de 24 bits por quadro -> IVs eventualmente reusados
- IV transmitido em texto aberto -> reuso de IV detectado
- **Ataque:**
  - Trudy faz Alice criptografar um texto aberto conhecido d_1 d_2 d_3 d_4 … (ex. solicita uma página Web ou arquivo conhecidos)
  - Trudy vê: $c_i = d_i$ XOR k_i^{IV}
  - Trudy conhece c_i d_i, logo pode computar $k_i^{IV} = d_i$ XOR c_i
  - Trudy conhece a seqüência de chaves k_1^{IV} k_2^{IV} k_3^{IV} …
  - Na próxima vez que IV for usado, Trudy pode decritografar o quadro (assim como quadros passados)!
  - Como IVs são gerados aleatóriamente, uma vez que Trudy tenha determinado um par válido (IV, k_i^{IV}), ela pode gerar pacotes e interferir ativamente na comunicação

Quebrando a criptografia do 802.11 WEP

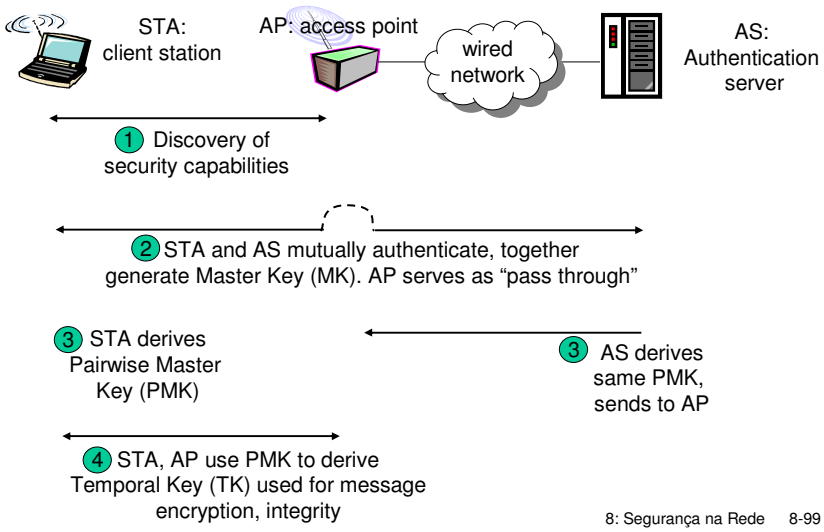
Em setembro de 2001, a IEEE responde ao fato de que o WEP havia sido completamente "quebrado":

- Nos dissemos que a segurança do WEB não era melhor que a do Ethernet !?
- Uma ameaça muito maior é não possibilitar segurança alguma.
- Tentem usar outro esquema de segurança (ex., segurança na camada de transporte).
- A próxima versão, 802.11i, terá um esquema de segurança melhor.
- Certificação futura irá exigir o uso do 802.11i.
- Nós vamos tentar pensar em algo a fazer até o 802.11i chegar!

802.11i: segurança aprimorada

- Várias formas (robustas) de criptografia possíveis
- Mecanismo de distribuição de chaves
- Servidor de autenticação separado do ponto de acesso
- Também conhecido por WPA2
- Wi-Fi Protected Access (WPA): solução intermediária da "Wi-Fi Alliance" para as falhas do WEP.

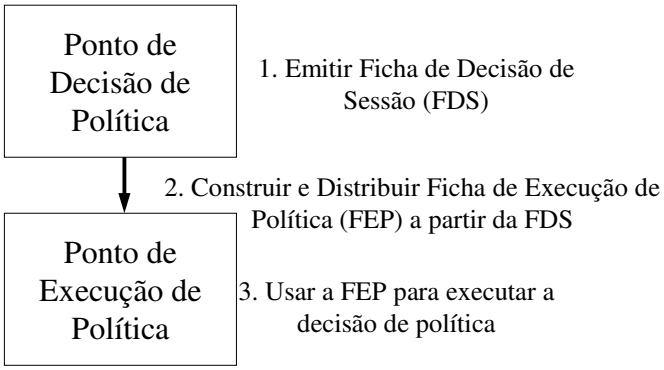
802.11i: quatro fases de operação



802.11i: Modelo Genérico de Política

- Policy Decision Point (PDP) = Componente Lógico responsável por tomar decisões de política
- Policy Enforcement Point (PEP) = Componente lógico responsável por aplicar decisões políticas
- Session Decision Token (SDT) = Estrutura de dados representando uma decisão política
- Session Enforcement Token (SET) = Estrutura de dados usada para implementar uma decisão política

802.11i: Operação do Modelo de Política



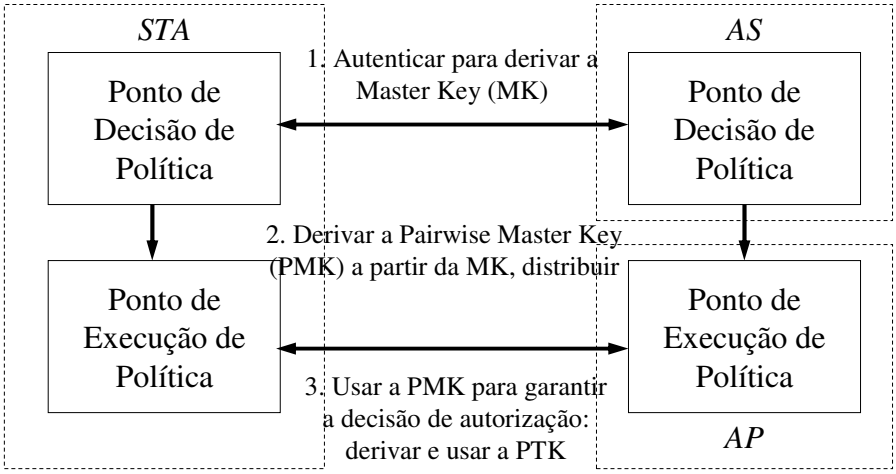
802.11i: Aplicação ao 802.11i (1)

- Dois pontos de Decisão de Política: STA e AS
- Decisão de Política: permitir acesso à rede 802.11?
- Decisão de Política decidida por autenticação
- Ficha de Decisão de Política do 802.11: ***Master Key*** (MK)
  - MK = ***chave simétrica*** representando a decisão da ***Estação*** (STA) e do ***Servidor de Autenticação*** para a ***sessão***
  - Apenas a STA e a AS podem possuir a MK
    - A posse da MK demonstra autorização para tomar decisões

802.11i: Aplicação ao 802.11i (2)

- Dois pontos de execução de Política: STA e AP
- Ficha de Execução de Política do 802.11: ***Pairwise Master Key*** (PMK)
  - PMK é uma ***nova chave simétrica que*** controla o acesso da ***STA*** e do ***AP*** ao canal 802.11 durante a ***sessão***
  - Apenas a STA e o AS podem produzir a PMK
    - PMK derivada da MK
    - AS distribui a PMK para o AP
  - A posse da PMK demonstra a autorização para acessar o canal 802.11 durante a sessão

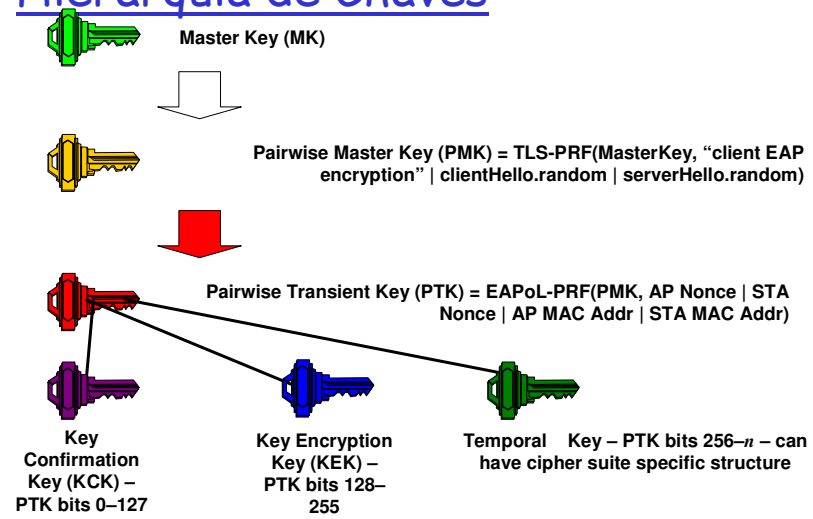
802.11i: Aplicação ao 802.11i (3)



802.11i: Observação sobre as chaves

- O AP e a STA devem tomar a mesma decisão de autenticação
  - Ou não haverá comunicação através do canal 802.11
- MK ≠ PMK
  - Ou o AP poderá tomar decisões de controle de aceso, em vez do AS
- PMK está vinculada a *esta* STA e a *este* AP
  - Ou outro participante poderá se passar or qualquer deles
- MK é nova e vinculada a *esta* sessão entre a STA e o *AS*
  - Ou uma MK de outra sessão poderá representar a decisão para a sessão
- PMK é nova e vinculada a *esta* sessão entre a STA e o *AP*
  - Ou uma PMK antiga poderia ser usada para autorizar a comunicação nesta sessão
- Quando AP ≠ AS, é necessário ***assumir*** que a AS ***não*** irá …
  - se passar pela STA ou pelo AP
  - revelar a PMK a outro participante que não o AP

802.11i: Hierarquia de Chaves



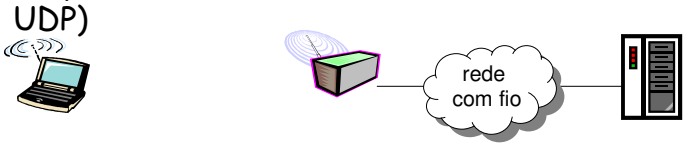
Fonte: Cam-Winget et al. 2007

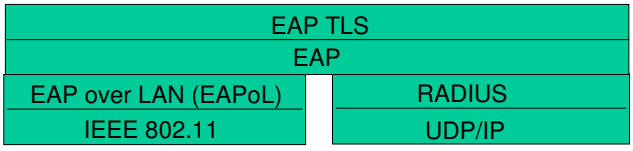
802.11i: Hierarquia de Chaves

- Master Key – representa uma decisão positiva de acesso
- Pairwise Master Key (PMK)– representa a autorização para acessar o meio 802.11
  - A PMK deve durar toda a sessão e ser exposta o mínimo possível.
  - É usado um protocolo (four-way handshake) para estabelecer a PTK.
- Pairwise Transient Key (PTK) – Coleção de chaves operacionais:
  - Key Confirmation Key (KCK) – usada para vincular a PTK ao AP, STA; usada para provar a posse da PMK
  - Key Encryption Key (KEK) – usada para distribuir a Group Transient Key (GTK)
  - Temporal Key (TK) – usada para proteger os dados
- Group Transient Key (GTK)
  - Usada para proteger o tráfego de dados multicast/broadcast

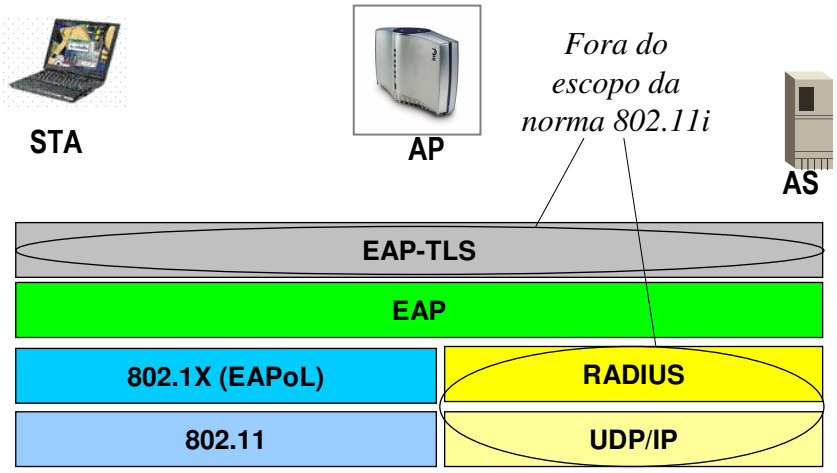
EAP (*Extensible Authentication Protocol*)

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





Arquitetura de Autenticação e Gerenciamento de Chaves (1)



Fonte: Cam-Winget et al. 2007

Arquitetura de Autenticação e Gerenciamento de Chaves (1)

- EAP é o transporte fim a fim para a autenticação feita entre STA e AS
- 802.1X é o tranporte para EAP sobre LANs 802
- Protocolo *backend* não está no escopo do 802.11
  - Porém RADIUS é o transporte *de facto* para EAP sobre redes IP
- Método concreto EAP de autenticação está fora do escolpo do 802.11
  - Porém EAP-TLS é o protocolo de autenticação *de facto*, porque os outros não funcionam

Segurança na Rede (sumário)

Técnicas básicas……

- criptografia (simétrica e pública)
- autenticação
- integridade de mensagens
- distribuição de chaves

…. usadas em diferentes cenários

- correio eletrônico seguro
- transporte seguro (SSL)
- IP sec
- 802.11

Bibliografia

- KUROSE, J. F.; ROSS, K. W.; Redes de Computadores e a Internet. 3a. edição, Pearson Education, 2005.
- TANENBAUM, A. S., Redes de Computadores, 4rd. Ed., Campus, 2003.
- Cam-Winget, N., Moore T. , Stanley, D. , Walker, J.IEEE 802.11i Overview. http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf, acesso maio 2007.