ADMINISTRAÇÃO DE REDES DE COMPUTADORES

Segurança

5/12/2005

Engª de Sistemas e Informática
Licenciatura em Informática

UALG/FCT/DEEI 2005/2006

Classes de criptografia

- Criptografia simétrica ou de chave secreta
  - Existência de uma mesma chave secreta entre os intervenientes.

- Criptografia assimétrica ou de chave pública
  - Existência de uma chave provada a cada interveniente e uma chave pública de conhecimento público.

- Criptografia mista (simétrica e assimétrica)
  - Usando criptografia assimétrica para troca de chaves de criptografia e simétrica em posterior utilização.

Criptografia simétrica (DES)

Características

- Uma chave é utilizada para encriptar e des-encriptar dados.
- Necessidade de partilha da chave pelos intervenientes.

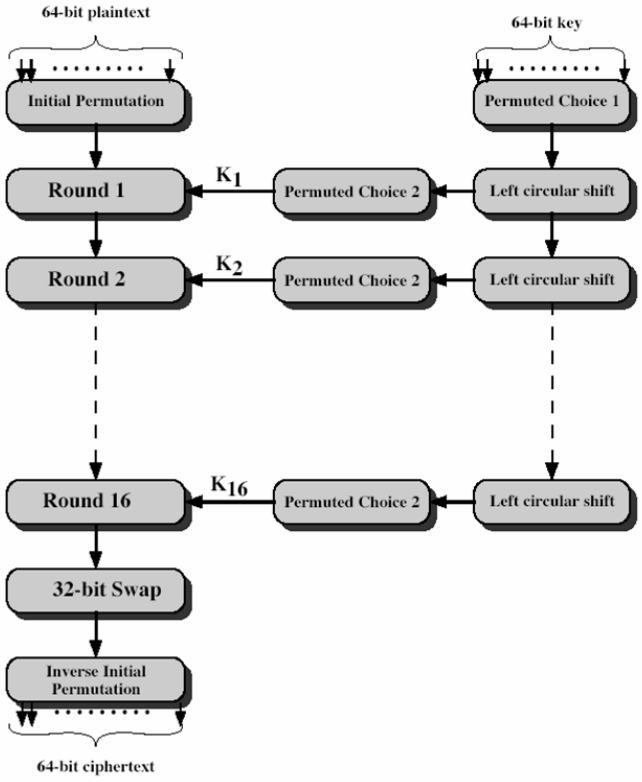
Limitações

- Como transmitir a chave de maneira segura através da rede.

Ex: Algoritmo mais utilizado
DES-Data Encryption Standard (IBM 1977)

- Algoritmo de cifragem de bloco de dados de 64 bits
- Chaves de 56 bits
- Concebido para implementações sobre hardware

Criptografia simétrica (DES)



Criptografia asimétrica

- Diferentes chaves para cifrar e decifrar

  -uma chave pública K_{pub}
  -uma chave privada K_{priv}

- Uma menssagem cifrada com K_{pub} só pode ser decifrada com K_{priv} e vice versa.

$$c = encrypt(K_{pub}, m)$$
$$m = decrypt(K_{priv}, encrypt(K_{pub}, m))$$

Criptografia asimétrica (Algoritmo RSA- Rivest, Shamir e Adleman

1- Escolhe dois números primos , p e q (o produto de p e q deve de ser da ordem de 1024 para empresas e 768 para particulares).

2- Calcule $n=pq$ e $z=(p-1)(q-1)$

3- Escolhe um número, e, menor que n, que não tenha factores comuns (diferente de 1) com z.

4- Encontre um número d tal que $ed-1$ seja divísivel por z.

n e e chave pública

n e d chave privada

Alice para enviar uma mensagem a BOB cifra a mensagem com a chave pública e BOB decifra a mensagem com a chave privada.

Criptografia asimétrica (Algoritmo RSA- Rivest, Shamir e Adleman

- Alice cifra a mensagem

$c=m^e \bmod n$

letra	Representação númerica	m^e	$c=m^e \bmod n$
l	12	248832	*17*
o	15	759375	*15*
v	22	5153632	*22*
e	5	3125	*10*

- Bob decifra a mensagem

$m=c^d \bmod n$

Texto cifrado	c^d	$m=c^d \bmod n$	Texto recebido
17	48196857210675091509141182522307169 7	*12*	*l*
15	12783403948858939111232757568359375	*15*	*o*

PGP-Pretty Good Privacy

Características desejadas
-confidencialidade
-autenticação do emissor
-integriadade da mensagem
-autenticação do receptor

Confidencialidade (Alice quer enviar uma mensagem confidencial a Bob)
- Utiliza encriptação asimétrica (algoritmo RSA)
- Bob disponibiliza a sua chave pública.
- Alice cifra a sua mensagem utilizando a chave pública de Bob e envia mensagem através de uma ligação normal SMTP.
- Bob decifra a mensagem com a sua chave privada.

Problema: requer muito tempo

Solução: Chave de sessão
-Alice envia uma chave simétrica a Bob, cifra essa mensagem com a chave pública de Bob.
-Alice cifra a sua mensagem com a chave simétrica.
- Bob decifra a chave simétrica com a sua chave privada e a mensagem com a chave simétrica.

PGP-Pretty Good Privacy

Autenticação

- Bob assina digitalmente um documento *m*
- Calcula a sua assinatura digital *Ad* com a sua chave privada K_{priv}.
- Para provar que o documento recebido foi enviado por Bob, Alice faz $K_{pub}(Ad(m))$
-Também é possível provar que o documento original não foi alterado.

PGP-Pretty Good Privacy

Técnica de encriptação de e-mail criada por Philip R. Zimmermann em 1991.

PGP é a técnica de encriptação de e-mail mais utilizada no mundo

Criar o par (chave pública, chave privada)

#gpg –gen-key

No Debian vais encontar a chave pública e privada em

~/.gnupg/secring.gpp

~/.gnupg/pubring.gpp

Podes importar para o ficheiro pubring.gpp chaves públicas de outras pessoas

gpg – import chave_publica.gpp

PGP-Pretty Good Privacy

Para assinares um texto com a tua chave privada.

gpg –clearsign texto.txt

Para verificares a autenticidade de um texto com uma assinatura digital executa o comando

gpg –verify mensagem.txt.asc

SSL- Secure Sockets Layer

-Motivação: comércio electrónico

-SSL é um protocolo (inventado pela Netscape) que funciona num nível intermédio entre a camada de transporte e a camada das aplicações. É utilizado para garantir transmissões seguras de dados em vários serviços. O mais popular é o serviço HTTPS (HTTP em cima de SSL).

- o cliente (browser) garante a identidade do servidor através da chave pública deste.

-o cliente gera uma chave secreta única para cada transação. Encripta-a com a chave pública e envia-a para o servidor.

- a partir deste momento o cliente encripta os dados com a chave secreta.

A chave pública do servidor tem de ser assinada digitalmente por uma entidade idónea que garante a sua autenticidade (Verisign)

SSL- Secure Sockets Layer

- Criação do par (chave pública, chave privada)

openssl genrsa –des3 1024 > server.key

o ficheiro server.key contem o par de chaves utilizando o algoritmo RSA

-Criação de um certificado x509 para o servidor HTTS assinado com a chave privada, válida por 365 dias.

openssl req –new –key server.key –x509 –days 365 –out server.crt

A chave pública, no formato x509, encontra-se no ficheiro server.crt

SSH- Secure Shell

Como funciona:

- o cliente liga-se à porta 22 do servidor e solicita a chave pública deste. Também envia ao servidor a sua chave pública.
-depois de autenticados mutuamente o cliente gera uma chave para a sessão, encripta-a com a chave pública do servidor e envia-a.
-os dados da sessão são encriptados com a chave simétrica de sessão.

SSH- Secure Shell

As opções de configuração de servidor ssh e do cliente ssh encontram-se em:

/etc/ssh/sshd_config para o servidor
/etc/ssh/ssh_config para o cliente

Na fase de instalação do servidor este gera o par de chaves que se encontram em

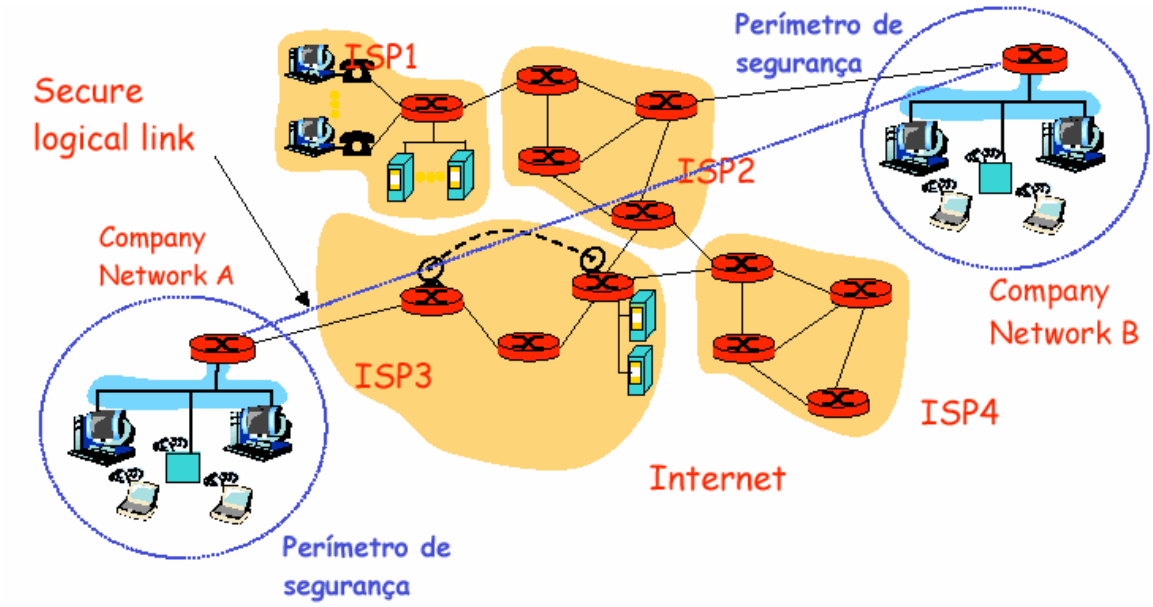
/etc/ssh/ssh_host_key chave privada
/etc/ssh/ssh_host_key.pub chave pública

O par de chaves no cliente é criado pelo próprio utilizador com o comando.

ssh –keygen

E encontram-se em
~/.ssh/identity chave privada
~/.ssh/identity.pub chave pública

Virtual Private Networks



Virtual Private Networks

- Um túnel em IP é implementado encapsulando IP sobre IP. A rede normal transporta os pacotes IP externos com um número de protocolo especial.Quando estes chegam ao destino, são analisados e aparece um novo pacote IP, o interno.

Cabeçalho IP 1	Cabeçalho IP 2	Dados

- Numa rede privada (VPN) é todo o pacote que é encapsulado.
- O processo de encriptação e de-encriptação funciona ao nível dos routers, e é totalmente transparente ao utilizador
- Os routers intermédios não analisam o pacote interno.

Virtual Private Networks

IPSec é um conjunto de RFCS que especificam tudo o que é necessário para encaminhar tráfego de forma segura ao nível rede e transporte

Envolve:

- Authentication header Protocol (AH)
- Encapsulated security payload Protocol (ESP)
- Troca de chaves e gestão de associações de segurança
- Muitos RFCs (RFC 2401, 2402, 2406, 2408, 2409, 2411, ...)

Providenciam autenticação, confidencialidade e protecção contra replay replay.

Free SWAN – Free Secure Wide Area Network

- Free SWAN é uma implementação Open Source do protocolo de encriptação standard IPSEC

- Os routers que implementam uma rede virtual partilham entre si uma chave secreta, ou utilizam as suas chaves públicas para se autenticarem entre si.

- Os routers configuram a rede VPN através de dois ficheiros

  1) /etc/ipsec.secrets – contém a chave simétrica préviamente partilhada, ou a chave pública do router no outro extremo do 'túnel'

  ipsec ranbits 256 cria a chave simétrica

  ipsec rsasigkey cria o par de chaves públicas

  2) o ficheiro
  /etc/ipsec.conf contém as configurações epecíficas da ligação: identificação das interfaces, identificação das redes privadas, identificação dos routers, método de autenticação.

Free SWAN – Free Secure Wide Area Network

Autenticação e integridade da mensagem
- Assinatura digital
-Bob utiliza a sua chave privada para assinar digitalmente um texto.
-Alice vai buscar a chave publica de Bob e corre a chave pública no documento para verificar a autenticidade do emissor e a integridade do texto.