apontamentos para o teste 14-04

Criptografia Simétrica e Assimétrica

- A criptografia simétrica e assimétrica são dois métodos diferentes de criptografia utilizados para proteger informações sensíveis durante a transmissão ou armazenamento.

- A criptografia simétrica usa uma única chave para criptografar e descriptografar informações. A chave é mantida em segredo entre as partes que se desejam comunicar, e a mesma chave é usada tanto para criptografar quanto para descriptografar a mensagem. Embora a criptografia simétrica seja relativamente rápida e eficiente, o grande desafio é garantir que a chave secreta seja mantida em segredo e partilhada apenas entre as partes autorizadas.

- Já a criptografia assimétrica usa um par de chaves: uma chave pública e uma chave privada. A chave pública pode ser distribuída livremente, enquanto a chave privada é mantida em segredo pelo proprietário. Quando uma mensagem é criptografada com a chave pública de alguém, somente o proprietário da chave privada correspondente pode descriptografá-la. A criptografia assimétrica é geralmente mais segura que a criptografia simétrica, pois as chaves privadas não são partilhadas e, portanto, são menos suscetíveis a serem comprometidas.

- Em geral, a criptografia simétrica é mais adequada para transmissão de dados em massa, enquanto a criptografia assimétrica é mais adequada para comunicações seguras entre duas partes ou para autenticação de identidade em sistemas de segurança mais robustos.

Analogia da Alice e Bob tendo em conta os dois tipos de criptografias

- A analogia de Alice e Bob é frequentemente usada para ilustrar a criptografia e as comunicações seguras entre duas partes. Em geral, Alice e Bob representam duas entidades que se desejam comunicar de forma segura, e a criptografia é usada para proteger a privacidade e a integridade das informações que estão a ser partilhadas.

- Na criptografia simétrica, Alice e Bob concordam em uma chave secreta que será usada tanto para criptografar quanto para descriptografar as mensagens. Por exemplo, Alice pode enviar uma mensagem criptografada para Bob usando a chave secreta que eles concordaram. Bob, por sua vez, usa a mesma chave secreta para descriptografar a mensagem e ler o conteúdo. Nesse cenário, a chave secreta deve ser compartilhada de forma segura e confiável entre Alice e Bob, a fim de garantir que a criptografia seja eficaz.

- Na criptografia assimétrica, Alice e Bob usam um par de chaves públicas e privadas para se comunicar de forma segura. Alice compartilha sua chave pública com Bob, e Bob compartilha sua chave pública com Alice. Quando Alice envia uma mensagem para Bob, ela criptografa-a usando a chave pública de Bob. Somente Bob pode descriptografar a mensagem usando a sua chave privada correspondente. Acontece o mesmo no caso do Bob enviar uma mensagem à Alice. Nesse cenário, as chaves privadas são mantidas em segredo pelos seus proprietários, o que significa que a comunicação entre Alice e Bob é segura e confiável.

Vantagens e Desvantagens da criptografia Simétrica

Vantagens:

1. *Eficiente*: A criptografia simétrica é muito rápida e eficiente, pois usa uma chave única para cifrar e decifrar a mensagem.
2. *Fácil de implementar*: A criptografia simétrica é relativamente fácil de implementar e pode ser usada em variadas aplicações.
3. *Segurança*: Se a chave for mantida em segredo, a criptografia simétrica é segura.

Desvantagens:

1. *Chave de segurança:* A chave de criptografia simétrica deve ser mantida em segredo absoluto para garantir a segurança da mensagem. Se a chave for comprometida, toda a segurança do sistema é comprometida.
2. *Compartilhamento de chaves*: A chave deve ser compartilhada com qualquer pessoa que precise acessar a mensagem, o que pode ser difícil em algumas situações.
3. *Escalabilidade*: A criptografia simétrica é difícil de escalar para grandes sistemas, pois uma chave separada deve ser compartilhada com cada pessoa que precisa acessar a mensagem. Isso pode se tornar muito complicado em sistemas maiores com muitos utilizadores.

Vantagens e Desvantagens da criptografia Assimétrica

Vantagens:

1. Chave pública: A criptografia assimétrica usa uma chave pública para cifrar a mensagem, o que significa que a chave pode ser compartilhada amplamente sem comprometer a segurança da mensagem.
2. Segurança: A chave privada é mantida em segredo absoluto pelo destinatário, o que garante a segurança da mensagem.
3. Flexibilidade: A criptografia assimétrica é flexível e pode ser usada em várias aplicações, incluindo autenticação, assinatura digital e troca de

chaves.

Desvantagens:

1. *Desempenho*: A criptografia assimétrica é mais lenta do que a criptografia simétrica, pois envolve operações matemáticas complexas.
2. Complexidade: A criptografia assimétrica é mais complexa do que a criptografia simétrica e requer mais processamento para gerar e gerenciar as chaves públicas e privadas.
3. *Vulnerabilidade a ataques de homem no meio*: Como a chave pública é compartilhada amplamente, ela pode ser interceptada e substituída por um atacante mal-intencionado, comprometendo assim a segurança da mensagem.

apontamentos para o teste 21-04

Para que servem e em que contextos se tornam úteis as cifras homomórficas?

- As cifras homomórficas permitem que dados criptografados sejam processados de forma segura e eficiente sem a necessidade de decifrá-los primeiro. Permitem que dados criptografados possam ser manipulados sem que o seu conteúdo original precise ser revelado. Pode ser útil em muitos contextos, tais como:

1. **Computação em nuvem**, sendo possível realizar cálculos nos dados armazenados na nuvem sem expor os dados reais.
2. **Análise de dados privados**: quando empresas ou organizações desejam compartilhar dados privados entre si, mas precisam manter esses dados confidenciais, as cifras homomórficas podem ser utilizadas para realizar análises em conjunto sem expor os dados reais.

O que é a esteganografia? Como pode ser feita ao nível da camada de rede da pilha protocolar TCP/IP?

- A esteganografia é a prática de ocultar informações dentro de outros dados de forma que a presença da informação oculta não seja detectada facilmente, passando despercebida.

  Ao nível da camada de rede da pilha protocolar TCP/IP, a esteganografia pode ser feita de várias maneiras. Uma das maneiras é a ocultação da mensagem dentro dos pacotes de dados da rede. A outra é a utilização de protocolos de comunicação que permitem a inserção de dados ocultos. Por exemplo, é possível usar o protocolo DNS para ocultar informações em nomes de domínio.

No entanto, é importante notar que a esteganografia na camada de rede pode ser detectada por técnicas de análise de tráfego, que procuram por padrões incomuns ou suspeitos no tráfego de rede. Por essa razão, a esteganografia é frequentemente combinada com a criptografia para aumentar a segurança e proteção dos dados ocultos.

Ilustre, justificando, com recurso a um trecho de configuração, uma vantagem que o controlo de permissões de execução de comandos baseado em vistas possui face aos níveis de prioridade em Cisco IOS?

O controlo de permissões de execução de comandos baseado em vistas é uma técnica de segurança em redes que permite limitar o acesso dos utilizadores aos comandos do router. Assim, é possível restringir o acesso a determinados comandos, garantindo que apenas utilizadores autorizados possam executá-los.

Permite um controlo mais flexível sobre os comandos que podem ser executados pelos utilizadores. O controlo de permissões de execução de comandos baseado em vistas permite criar permissões personalizadas com base em critérios específicos.

```
parser view PedroMartins
    secret cisco
    commands interface include shutdown
    commands interface include ip address
    commands interface include ip
    commands configure include interface
    commands exec include configure terminal
    commands exec include configure
    commands exec include all show
    commands configure include-exclusive all interface Ethernet0/1
```

apontamentos para o teste 28-04

Blue Teams → grupo de profissionais de segurança responsáveis por defender os sistemas de informação de uma organização contra ataques de rede. O objetivo principal do Blue Team é prevenir e detectar ameaças, bem como responder a incidentes de segurança de forma rápida e eficaz.

Eles têm várias funções importantes, tais como:

1. Monitorar sistemas e redes para detetar atividades suspeitas ou potenciais ameaças.
2. Realização de análises para identificar e corrigir vulnerabilidades de segurança.
3. Reportar as empresas sobre as ameaças sofridas e sugestão às mesmas sobre as medidas a adotar para mitigar os dados.

Principio de Kerckoff e Shannon

"Um sistema criptográfico deve ser seguro, mesmo que tudo sobre o sistema, exceto a chave, seja conhecido publicamente." Essa afirmação realça a importância da chave secreta num sistema criptográfico e destaca que a segurança do sistema deve ser baseada num segredo bem protegido, em vez de depender da suposta segurança do algoritmo ou método de criptografia em si. A ideia por trás desse princípio é que, mesmo que um adversário tenha conhecimento completo do algoritmo ou método de criptografia utilizado, ele não deve ser capaz de comprometer a segurança do sistema sem acesso à chave secreta. Portanto, é importante que os sistemas criptográficos sejam

projetados para proteger a chave secreta, em vez de confiar na obscuridade do algoritmo ou do método de criptografia.

A teoria da informação de Shannon fornece ferramentas matemáticas para avaliar a segurança do sistema criptográfico em termos de entropia e informações transmitidas. Assim, enquanto o princípio de Kerckhoff destaca a importância da chave secreta, a teoria da informação de Shannon fornece um quadro matemático para avaliar a eficácia do sistema criptográfico em proteger a informação. Juntos, esses dois conceitos são fundamentais para a criptografia moderna e a segurança da informação.

Para que servem Blue Teams, quem os integra e que funções desempenham estes elementos?

Blue Teams são equipes de cybersegurança responsáveis por defender uma organização contra ataques. Constituída por analistas e engenheiros de segurança e administradores de sistemas. Desempenham uma variedade de funções, como:

1. Monitorar a rede e os sistemas da organização para detectar possíveis ameaças e vulnerabilidades.
2. Em caso de incidente de segurança, a equipa conduzirá uma investigação para determinar a sua causa e tomar medidas para remediar os danos.
3. Realizar análises de risco para identificar possíveis pontos fracos na infraestrutura e desenvolver planos para mitigar esses riscos.

Primeiro Kerckhoffs (1883) e depois Shannon (1949) identificaram o pressuposto fundamental da criptografia moderna. A que pressuposto aludem ambos os cientistas e que motivação lhe assiste?

Kerckhoffs e Shannon identificaram o pressuposto fundamental da criptografia moderna, que é o seguinte:

"Um sistema criptográfico deve ser seguro, mesmo que tudo sobre o sistema, exceto a chave, seja conhecido publicamente."

Por outras palavras, a segurança de um sistema criptográfico deve depender exclusivamente da chave criptográfica, e não do algoritmo criptográfico em si. Isso significa que, mesmo que um atacante conheça o algoritmo criptográfico utilizado, ele não deve ser capaz de decifrar a mensagem criptografada sem a chave correta.

Essa abordagem é motivada pela necessidade de garantir a segurança das comunicações num ambiente onde a interceptação de mensagens é cada vez mais comum. Além disso, a chave criptográfica pode ser facilmente trocada quando necessário, tornando mais difícil para um atacante que interceptou uma mensagem criptografada em um momento específico decifrá-la posteriormente.

apontamentos para o teste 05-05

1. **O alfabeto português possui 26 letras.**

a) Qual a entropia associada à escolha verdadeiramente aleatória (e.g., equiprovável) de um carater deste alfabeto?

Se considerarmos a escolha verdadeiramente aleatória de um caracter do alfabeto português, onde cada letra tem a mesma probabilidade de ser escolhida, a entropia associada é dada por:

H = log2(26) ≈ 4,7 bits

b) Assuma agora que nos teclados normais é possível obter pelo menos maiúsculas, minúsculas e algarismos. Em quanto sobe a entropia de uma escolha feita nas mesmas condições sobre este domínio mais alargado?

Se considerarmos agora um domínio mais amplo que inclui maiúsculas, minúsculas e algarismos, temos um total de 62 caracteres possíveis. Nesse caso, a entropia associada a uma escolha verdadeiramente aleatória de um caractere é dada por:

H = log2(62) ≈ 5,95 bits

c) Pelos parâmetros atuais uma senha considera-se segura se possuir um entropia de 50 bits. Quantos carateres deverá uma senha possuir (na última modalidade mencionada) para nos oferecer tal segurança?

Para uma senha com entropia de 50 bits no domínio mais amplo (com 62 caracteres possíveis), o número mínimo de caracteres necessários pode ser

calculado a partir da seguinte equação:

50 = n * log2(62)

onde "n" é o número de caracteres na senha. Resolvendo para "n", temos:

n = 50 / log2(62) ≈ 8,4

Isso significa que a senha deve ter pelo menos 9 caracteres para oferecer uma entropia de segurança de 50 bits. Na prática, é recomendável usar senhas ainda mais longas e complexas para aumentar a segurança.

2. **Explique, no âmbito da criptografia moderna, os objetivos dos principios:**

a) Confusão

Procura tornar a relação entre a chave de criptografia e o texto cifrado o mais complexa possível, dificultando assim a análise criptográfica e o trabalho de decifrar o texto cifrado. Isso é alcançado por meio da utilização de técnicas criptográficas que baralham os dados de entrada de tal forma que a relação entre a entrada e a saída se torne extremamente complexa e difícil de ser compreendida.

b) da Difusão.

Procura espalhar a influência de cada bit do texto original através de todo o texto cifrado. Isso é alcançado por meio da utilização de técnicas criptográficas que distribuem a informação de forma homogênea ao longo do texto cifrado. A criptografia fica menos suscetível a ataques que exploram redundâncias no texto original.

3. **Nas cifras por blocos:**

   a) qual o principal problema (de segurança) que decorre do uso de blocos pequenos?

   A possibilidade de ataques de criptoanálise. Numa cifra por blocos, cada bloco de entrada é cifrado independentemente dos outros, e um bloco

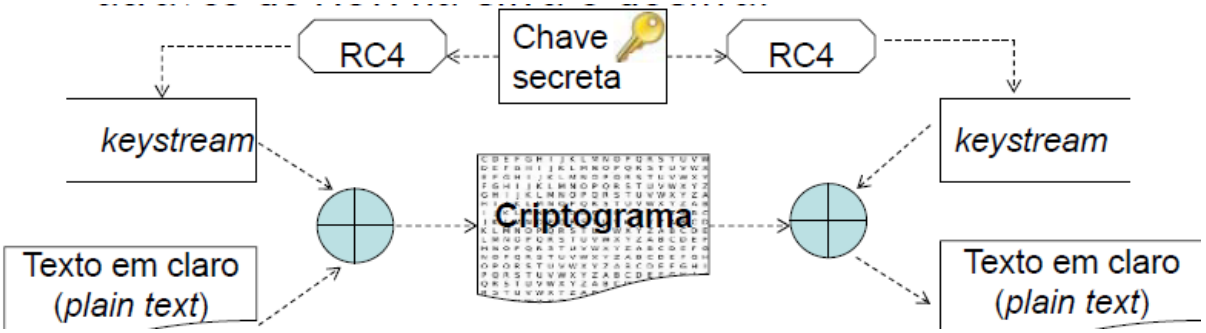
pequeno pode ter um número limitado de combinações possíveis. Isso significa que um atacante pode tentar todas as combinações possíveis de chave para um bloco de tamanho pequeno e, assim, descobrir a chave de criptografia.

b) como pode ainda assim ser muito atenuado esse problema?

Utilizando funções de hash criptográficas para ampliar o tamanho do bloco de entrada. Isso permite que um bloco pequeno de entrada seja estendido para um tamanho maior, dificultando a busca exaustiva por uma chave de criptografia.

apontamentos para o teste 12-05

Com o apoio de um diagrama mostre como é aplicada o RC4 na cifra de uma mensagem. Por que motivo esta cifra é denominada continua?



A cifra RC4 funciona gerando uma sequência de bytes pseudoaleatórios, que são combinados com os bytes da mensagem usando uma operação XOR.

A chave secreta é usada como entrada para um algoritmo de geração de chave, que produz uma sequência pseudoaleatória de bytes chamada de fluxo de chave. O fluxo de chave é então combinado com a mensagem clara usando uma operação XOR para produzir a mensagem cifrada.

A cifra RC4 é considerada "contínua" porque o fluxo de chave pode ser gerado continuamente sem interrupção e usado para cifrar uma quantidade ilimitada de dados. Diferente das cifras de bloco, que operam em blocos fixos de dados, a cifra RC4 é capaz de cifrar dados de comprimentos variáveis de forma eficiente.

Programe a firewall stateless de um router Cisco para que uma rede A se possa realizar com sucesso ping aos terminais da rede B e, simultaneamente, em sentido inverso tal não seja permitido.

```
R1# configure terminal
R1(config)# access-list 101 permit icmp 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255 echo
R1(config)# access-list 101 deny icmp 192.168.200.0 0.0.0.255 192.168.100.0
0.0.0.255 echo
R1(config)# access-list 101 permit ip any any

R1(config)# interface int e0/0
R1(config-if)# ip access-group 101 out

R1(config)# interface  int e0/1
R1(config-if)# ip access-group 101 in
```

Apontamentos para o teste 02-06

1. **Descreva, indicando o tipo de dispositivo de segurança, o local (na topologia da rede) e respetiva configuração (resumida e apenas verbalmente escrita), que é necessário e suficiente (ou seja, se for suficiente usar uma firewall stateless deve ser esse o dispositivo indicado e não outro que consuma mais recursos ou atrase mais o processamento de tráfego como uma firewall stateful ou mesmo um IDS) condiderar mitigar cada um dos seguintes ataques:**

a) um ataque externo de spoofing IP à rede de uma organização que transporte no campo Source Address um endereço de espaço público da mesma.

Para mitigar um ataque externo de spoofing IP à rede de uma organização, o dispositivo de segurança necessário e suficiente seria uma Firewall Stateless. A configuração seria bloquear todo o tráfego que chega com endereços IP de origem que pertencem ao espaço público da organização, mas que não são originados internamente. Ao bloquear o tráfego de spoofing IP, a firewall impede que pacotes falsificados cheguem à rede da organização, protegendo-a contra esse tipo de ataque.

b) um ataque externo com tráfego forjado (fake) dirigido ao servidor web público da organização.

Para mitigar um ataque externo com tráfego forjado (fake) dirigido ao servidor web público da organização, o dispositivo de segurança necessário e suficiente seria um IPS ou uma Firewall Stateful. Ambos os dispositivos são capazes de inspecionar o tráfego em tempo real e tomar medidas para bloquear atividades suspeitas. A configuração consistiria em definir regras que identifiquem o tráfego forjado e bloqueiem ou descartem os pacotes correspondentes. O IPS é especialmente projetado para detectar

e prevenir ataques, enquanto a Firewall Stateful pode manter um estado de conexão para monitorar o tráfego de forma mais eficaz.

c) um ataque externo de reconhecimento que varra todos os endereços públicos da organização (ex. nmap 194.65.52.1-254).

Para mitigar um ataque externo de reconhecimento que varra todos os endereços públicos da organização, o dispositivo de segurança necessário e suficiente seria uma IDS. A configuração seria configurar o IDS para analisar e monitorar o tráfego de entrada em busca de comportamento suspeito. O IDS pode alertar os administradores da rede sobre essas atividades de reconhecimento, permitindo que medidas adicionais sejam tomadas para proteger a rede.

2. **Indique um protocolo comum, no âmbito das redes IP, que use Message authentication Codes (MAC). No âmbito desse protocolo como é criado o MAC? No âmbito desse protocolo que serviços de segurança fornece a utilização do MAC? Que limitações possuem os MAC?**

   Um protocolo comum que utiliza Message Authentication Codes (MAC) no âmbito das redes IP é o Protocolo de Integridade de Mensagem (MIP).

   No MIP, o MAC é criado através da aplicação de uma hash a uma combinação de uma chave secreta compartilhada e a mensagem que precisa ser autenticada. O resultado da função de hash é o MAC, que é anexado à mensagem original.

   A utilização do MAC no MIP fornece serviços de segurança importantes, como autenticação e integridade. A autenticação é alcançada através da verificação do MAC pela parte receptora, garantindo que a mensagem não tenha sido modificada no caminho e tenha sido realmente enviada pela parte que alega tê-la enviado. A integridade é garantida porque qualquer modificação na mensagem resultaria num MAC diferente, fazendo com que a verificação falhe.

No entanto, os MACs possuem algumas limitações. Uma limitação é que eles não fornecem confidencialidade, ou seja, o conteúdo da mensagem ainda pode ser lido por qualquer pessoa que a intercepte. Além disso, o uso de uma chave compartilhada implica que ambas as partes envolvidas no protocolo precisem de ter acesso a essa chave. Isso pode ser problemático em cenários em que as partes não têm um canal seguro para trocar a chave ou quando há muitas partes envolvidas.

3. **Como é produzida a assinatura digital de um documento pelo seu autor? Que serviços de segurança presta a mesma? Como deve proceder o consumidor do documento para validar a mesma?**

   A assinatura digital é produzida por meio de algoritmos criptográficos que garantem a autenticidade e a integridade de um documento eletrónico. O autor do documento gera um par de chaves criptográficas, composto por uma chave privada e uma chave pública. A chave privada é mantida em sigilo e não deve ser compartilhada, enquanto a chave pública é divulgada para que outras pessoas possam verificar a autenticidade das assinaturas. Em seguida, o autor utiliza sua chave privada para criptografar o resumo do documento, formando assim a assinatura digital.

   A assinatura digital oferece serviços de segurança importantes, como autenticidade, uma vez que a assinatura digital permite verificar a identidade do autor do documento, pois somente a chave privada correspondente à chave pública utilizada para verificar a assinatura é capaz de produzir uma assinatura válida e integridade, já que qualquer modificação no conteúdo do documento, mesmo que seja uma única letra alterada, resultará em uma assinatura digital inválida. Portanto, a assinatura digital garante que o documento não tenha sido alterado desde a sua assinatura.

   Para validar a assinatura digital de um documento, o consumidor deve ter acesso à chave pública do autor do documento, geralmente fornecida junto com o documento, uma vez que necessita para realizar a verificação da assinatura digital. Isso envolve descriptografar a assinatura com a chave pública para obter o resumo do documento original e compará-lo com o

resumo atual do documento. Após verificar a assinatura, o consumidor pode confirmar que o documento foi realmente assinado pelo autor, garantindo a autenticidade do mesmo.