1. Conceitos Básicos

Os projetos de segurança e de gerenciamento da rede devem ser completados antes do início da fase de projeto físico, para o caso de terem efeito sobre o desenvolvimento das especificações físicas.

Por exemplo, eles aumentam os requisitos de capacidade? É necessário um caminho de dados separado para gerenciamento da rede? É necessário que todo o tráfego passe através de dispositivos de criptografia? Talvez seja necessário também reconsiderar a topologia lógica! Lembre-se de que a metodologia de projetos de redes top-down é um processo interativo que lhe permite revisar soluções preliminares à medida que desenvolve planos cada vez mais detalhados.

2. Criptografia por Chaves Simétricas

A criptografia por chave simétrica usa uma única chave compartilhada pelo receptor e o emissor. Essa chave é usada tanto na encriptação e decriptação dos dados e é denominada chave secreta. Esse método é muito utilizado na transferência de grandes quantidades de dados, pois exige pouco processamento, ou seja, a encriptação e a decriptação dos dados são rápidas.

Apesar de ser um método bastante seguro e eficiente, ele se baseia na hipótese de que somente o emissor e o receptor possuem uma chave secreta que não pode ser obtida por terceiros. Quando as partes vão iniciar uma comunicação, a chave secreta precisa ser compartilhada por meio de um canal seguro. Muitas vezes essa troca é feita através de criptografia usando chave pública.

Se a chave secreta for inacessível para os hackers, a única alternativa para decriptografar os dados é através da adivinhação da chave. Porém esse método

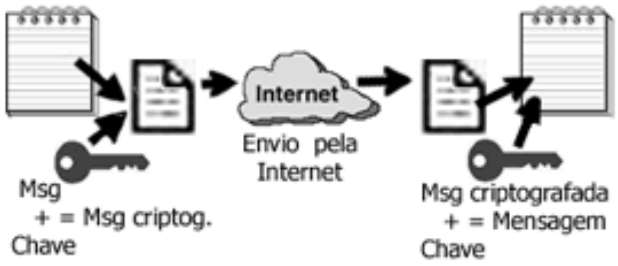
vai se tornando menos eficiente (em relação à performance) à medida que o tamanho dessa chave secreta aumenta. Um outro fator que aumenta a segurança é a utilização de múltiplas chaves. Usando uma chave secreta bem grande e um algoritmo de criptografia eficiente a quebra desse sistema de criptografia por chave simétrica torna-se praticamente inviável, mesmo feita por computadores muito poderosos.

Os três algoritmos mais utilizados para implementar a criptografia por chave simétrica são:

- **DES (*Data Encryption Standard*)**: o DES utiliza uma chave de 56 bits. Foi projetado inicialmente para ser utilizado em componentes de hardware, mas nos dias atuais, ele é usado na Internet em conexões Web seguras, com o SSL. Ele é um algoritmo seguro para a maioria das aplicações, entretanto, em aplicações altamente secretas, ele não deve ser usado, pois existe chance de violação.

- **RC2 e RC4**: mais rápidos do que o DES, esses códigos podem se tornar mais seguros com o simples aumento do tamanho das chaves. O RC2 pode substituir perfeitamente o DES com a vantagem de ser 2 vezes mais rápido, já o RC4 é 10 vezes mais rápido que o DES.

- **IDEA (*International Data Encryption Algorithm*)**: criado em 1991, ele foi projetado para ser facilmente programado. É forte e resistente a muitas formas de criptoanálise.



3. Criptografia por Chaves Assimétricas

A criptografia por chave pública utiliza-se de duas chaves: a chave pública e a chave privada. Essas chaves são matematicamente relacionadas, sendo também chamadas de chaves assimétricas. Nesse sistema, a chave pública é divulgada enquanto a chave privada permanece secreta. Desta forma, um dado criptografado com uma chave pública só pode ser decriptografado utilizando-se a chave privada e vice-versa. Por exemplo, se Maria criptografa um texto usando a chave pública de João, somente João com sua chave privada pode decriptografar esse texto.

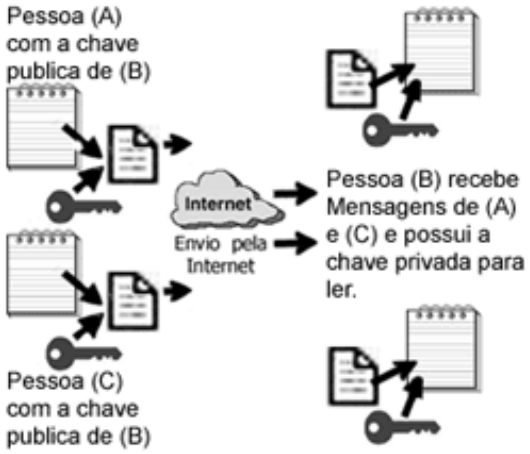
Diferente da criptografia com chave simétrica, o processamento necessário para criptografar e decriptografar dados usando chave pública é muito grande, pois um grande número de operações matemáticas complexas é feita utilizando-se, em geral, chaves bem grandes. Assim a criptografia por chave pública torna-se um método muito eficiente para criptografar pequenas quantidades de dados, como por exemplo, chaves simétricas secretas.

Os três algoritmos mais utilizados para implementar a criptografia por chave pública são:

- **RSA**: o algoritmo *Rivest-Shamir-Adleman* (RSA) é o mais utilizado hoje em dia, principalmente em dados enviados pela Internet. A incapacidade de se fatorar números muito grandes utilizando os sistemas computacionais atuais torna este algoritmo muito forte. O RSA é o único capaz de implementar assinatura digital e troca de chaves, entre os algoritmos mais comuns.

- **DSA**: esse algoritmo, desenvolvido pela NSA (*National Security Agency*) dos Estados Unidos, é utilizado somente para a implementação da assinatura digital. A força desse algoritmo está na dificuldade de calcular logaritmos discretos.

- **Diffie-Helman**: foi o primeiro algoritmo inventado para fazer troca de chaves. Sua segurança depende da dificuldade em calcular logaritmos discretos em um plano finito. Esse algoritmo é usado unicamente para troca de chaves.



4. Projeto de gerenciamento de redes

A ISO define cinco processos de gerenciamento de redes:

- Gerenciamento de Falhas;
- Gerenciamento de Desempenho;
- Gerenciamento de Configuração;
- Gerenciamento de Segurança;
- Gerenciamento de Contabilização.

4.1. Gerenciamento de Falhas

Utiliza dispositivos que permitam detectar, isolar e corrigir operações anormais do ambiente OSI. Questões:

- Onde está a falha?
- Isolamento da falha do resto da rede para que esta continue operando.
- Reconfiguração ou modificação da rede?
- Substituição dos componentes em falha e volta da rede a seu estado inicial.

4.2. Gerenciamento de Contabilização

Em várias situações é preciso cobrar pela utilização dos recursos de rede. Mesmo que isso não seja necessário, é preciso contabilizar a utilização dos recursos por diversas razões:

- Usuários abusam e sobrecarregam a rede.
- Uso ineficiente dos recursos de rede.
- Gerente de rede tomará melhores decisões (por exemplo, como expandir a rede) se estiver ciente das atividades de seus usuários.

4.3. Gerenciamento de Configuração

Sistemas modernos de comunicação são compostos por vários componentes físicos e lógicos. Um mesmo dispositivo pode ser configurado como um roteador ou um switch. Questões:

- Escolha do software e parâmetros apropriados.
- Inicialização e shutdown, atualização, adição de componentes, etc.

4.4. Gerenciamento de Desempenho

Necessidade de acompanhamento de limites de desempenho, monitoramento, rastreamento de atividades na rede. Questões:

- Qual a capacidade atual de utilização?
- Há tráfego em excesso?
- *Throughput* está diminuindo?
- Existem gargalos?

4.5. Gerenciamento de Segurança

Geração, distribuição e armazenamento de chaves de criptografia. Monitoramento e controle de acessos à rede. Manutenção de logs e arquivos de auditoria.

5. Modelo para Gerenciamento de Redes

O modelo utilizado para gerenciamento de redes TCP/IP é composto pelos seguintes elementos:

- Estação de Gerenciamento;
- Agente de Gerenciamento;
- Base de Informações de Gerenciamento (MIB);
- Protocolo de Gerenciamento de Redes (SNMP).

A estação de gerenciamento serve como interface para o administrador num sistema de gerenciamento de rede.

O agente de gerenciamento responde às solicitações de informações e de ações da estação de gerenciamento. Deve também prover assincronamente informações importantes que não foram solicitadas por esta estação (alarmes).

Os recursos a serem gerenciados são representados como objetos, sendo a coleção de objetos referenciada como a Base de Informações de Gerenciamento (MIB).

A forma de comunicação entre a estação de gerenciamento e o agente de gerenciamento é definido pelo protocolo de gerenciamento de rede (SNMP).