UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FEELT – FACULDADE DE ENGENHARIA ELÉTRICA

ENGENHARIA DE COMPUTAÇÃO

LUCAS ALBINO MARTINS

12011ECP022

REDES DE COMPUTADORES I: RELATÓRIO SEGURANÇA EM REDES DE COMPUTADORES: CRIPTOGRAFIA.

UBERLÂNDIA

2021

Relatório: Segurança em redes de computador – Criptografia.

1. Introdução

O conceito de segurança pode ser definido como um conjunto de medidas assumidas para proteger-se de quaisquer atos de ataques, ou seja, segurança implica a qualidade ou o estado de estar seguro. Em redes de computadores não seria diferente, e muito importante ressaltar a segurança de redes, visto que há milhares de dados e informações partilhas dentre elas algumas classificadas como dados sensíveis ou informações confidenciais, e o vazamento ou divulgação dos mesmos podem ter como destino o cyber crime. A partir dessa ideia do compartilhamento de informações e a segurança das mesmas, podemos pegar como exemplo informações que eram enviadas a tropas na segunda guerra mundial, surgiu a ideia de se codificar, encriptar e fazer com os dados ou informações enviadas mesmo sendo interceptados por pessoas não autorizadas continuassem protegidos. Iniciou-se então a ideia de produzir uma camada pra esconder a informação original através da criptografia. Com base na ideia de segurança de redes esse relatório traz informações sobre os princípios da criptografia, falando dos conceitos, história, tipos e algoritmos na criptografia, além de citar também sobre diversos conceitos das chaves assimétricas vulgarmente conhecidas de chave pública e da chave simétrica ou chave privada.

2. **Criptografia e seus princípios**.

2.1 Criptografia como conceito

A criptografia e defina como a maneira de como encriptamos uma mensagem ou informação de modo que apenas a pessoa na qual foi direcionada

a mensagem consiga desencriptar, sendo que para efetuar esse processo de leitura o destinatário teria que estar de posse do mesmo algoritmo que o remetente utilizou para encriptar a mensagem, de maneira análoga com o nosso cotidiano basta imaginar um determinado remetente envia uma carta em um idioma não muito popular na região aonde pretende contactar o destinatário, então ao decorrer do percurso caso a carta for extraviada ou violada por qualquer individuo durante esse percurso as informações estariam protegidas a menos que a pessoa que violou tivesse o domínio sob o idioma que foi escrito a carta, da mesma maneira o destinatário também teria que saber o idioma que a carta foi escrita para poder desencriptar a mensagem. Mas o fator linguístico não garantiria a segurança da informação, para garantir essa segurança questões como integridade da informação com base em permissões, autenticidade com base na origem do remetente, confiabilidade na questão apenas o destinatário poderia ter a chave para leitura e a rejeição que o fator que nem remetente e nem destinatário podem negar que uma mensagem foi enviada em algum momento.

2.2 Criptografia é sua história dentro das redes de computadores

A criptografia tem suas origens ligadas a ideia de comunicar-se ou passar informações entre um remetente e um destinatário. A origem da palavra criptografia surgiu com a fusão entre duas palavras gregas “kryptós” e “gráphein”, que tem seus respectivos significados por “oculto” e “escrever”. Pesquisadores sobre criptografia coloca que o primeiro uso de um documento criptografado datado no ano de 1900 a.C. com origem no Egito. Com a evolução dos meios de criptografia começaram a surgir algoritmos de criptografia datados no ano de 600 a.C. e 500 a.C. Os Hebreus utilizavam cifras de substituição simples que levou

a surgir a Cifra de César que nada mais é a técnica mais clássica de criptografia, basicamente consiste no deslocamento do alfabeto, avançando três casam. O uso dessa criptografia gerou um algoritmo ainda mais robusto que chama Cifra de Vigenère que nada mais é o uso de várias cifras de César em sequência, com diferentes valores de deslocamento ditados por uma palavra chave. Com o passar dos anos as técnicas de criptografia foram se modernizando, no século XX no ano de 1938 Arthur Scherbius desenvolveu a Enigma, uma máquina de criptografia, utilizada pela marinha Alemã principalmente na segunda guerra mundial, que em meados de 1938 com uma pesquisa em conjunto com uma universidade norte americana o inglês Alan Turing iniciou estudos para quebrar as cifras geradas pela Enigma; 1948 Teoria da Informação (Claude Shannon); 1970 DES (Data Encryption Standard), 1976 Diffie-Hellman, 1978 RSA, 2002 AES (Advanced Encryption Standard).

2.3 Tipos e algoritmos de criptografias.

A criptografia traz em sua estrutura dois tipos, assimétrica ou chave pública e a simetria ou chave privada. Ambos tipos de criptografias são utilizados em algoritmos de encriptação.

2.3.1 Criptografia de chaves assimétricas.

A criptografia assimétrica conhecida como a chave pública, basicamente ela faz o uso de duas chaves, uma pública e uma privada, nesse método então o remetente cria uma chave de codificação e envia ao destinatário, no caso essa é a chave pública, logo a outra chave usada na descodificação é secreta é apenas o destinatário tem sua posse, conhecida como chave privada. Essa teoria foi proposta por Diffie-Hellman em 1976, somente para a troca de chaves,

sua motivação para o surgimento da criptografia das chaves foi o problema da troca de chaves. Os algoritmos que utilizavam essa criptografia além de garantirem o sigilo garantiam a integridade, autenticidade e a não rejeição no que diz respeito a troca de informações.

O algoritmo mais utilizado com esse tipo de criptografia é o RSA (Rivest, Shamir and Adleman), desenvolvido em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman pesquisadores do MIT (Massachusetts Institute of Technology). Nele os números primos são usados da seguinte forma: dois números são multiplicados para se obter um terceiro valor, ou seja, a assimétrica ou chave pública são os números primos multiplicados e a simétrica ou chave privada é o valor obtido. Há também o algoritmo ElGamal, desenvolvido por Taher ElGamal, esse por sua vez faz o uso de um problema matemático conhecido por “logaritmo discreto” para se tornar seguro. Esse algoritmo é frequentemente utilizado em assinaturas digitais, segundo o um redator da infowester Emerson Alecrim. Outros algoritmos também são usados em assinaturas digitais, como o DAS (Digital Signature Algorithm) e o Schnorr.

2.3.2 Criptografia de chaves simétricas.

Criptografia de chaves simétricas ou chaves privadas é considerado um tipo de criptografia muito simples em que o remetente e o destinatário compartilham da mesma chave, ou seja, a chave é única, usada tanto para codificar pelo remetente quanto para descodificar pelo destinatário. Essas chaves por sua vez possuem os algoritmos extremamente velozes no quesito execução, seu intuito e prover sigilo das informações. Existem vários tipos de algoritmos que utilizam as chaves simétricas, dentre eles temos o DES (Data

Encryption Standard), IDEA (International Data Encryption Algorithm), RC (Ron's Code ou Rivest Cipher), AES (Advanced Encryption Standard).

Começando pelo DES, foi desenvolvido em 1977 pela IBM, seu algoritmo faz o uso de chaves de 56 bites, o que corresponde a 72 quatrilhões de combinações. Mesmo com esse valor bastante grande de combinações esse algoritmo com o tempo foi quebrado em um desafio na internet, através de uma técnica conhecida por "brute-force" (força bruta), basicamente essa técnica utilizada da ideia de tentativa erro ao acerto. O IDEA, desenvolvido em 1991 por James Massey e Xuejia Lai, esse algoritmo consiste em um conjunto de chaves de 128 bits e que tem uma estrutura semelhante ao DES. Já o RC, desenvolvido em 1994 por Ron Rivest na empresa RSA Data Security, seu algoritmo é bem mais utilizado para e-mails e faz o uso de chaves que vão de 8 a 1024 bits. Possui diversas versões: RC2, RC4, RC5 e RC6 e se diferem uma da outra por trabalharem com chaves maiores. Por último o AES, desenvolvida depois dos anos desde 1997 por Vincent Rijmen e Joan Daemen e publicada em 2001 pelo NIST (National Institute of Standards and Technology), esse algoritmo foi baseado no DES, logo possui uma chave de criptografia que pode ter 128, 192 ou 256 bits, e é aplicada em unidades de dados, chamados blocos, cada um com 128 bits, esse por sua vez é um dos algoritmos mais utilizados na encriptação das senhas de redes.

3. Funções de Hash

Funções de hash pelo conceito são funções que aceita uma mensagem de comprimento variável como entrada e produz uma saída de comprimento fixo, conhecido como código de hash. Essa função garante autenticação e sigilo. A função de hash é uma função criptográfica

que gera uma saída de tamanho fixo geralmente 128 a 256 bits independente do tamanho da entrada.

3.1 Algoritmos da função de Hash

Existem diversos algoritmos dentro de funções de Hash, dentre eles os mais famosos são o MD5 e o SHA1 e o SHA2. O MD5 (Message Digest Algorithm RDA-MD5), definido na RFC 1321, é uma versão melhorada de MD4. Basicamente é um algoritmo não descodificável, isto é uma vez codificado não se consegue descodificar a informação, esse por sua vez e bastante utilizado na encriptação das senhas dos utilizadores de determinados sistemas informáticos, pois caso houver alguma penetração e interceptação dos dados do banco de dados essa codificação garantiria que a senha do utilizador não será exposta. Já o SHA1 é um algoritmo que implementa uma hash sem chave, que pega uma mensagem de até 264 bits e produz um resumo da mensagem de 160-bits e é utilizado para a verificação de integridade da mensagem, baseado nos princípios do algoritmo do MD4 e MD5 o SHA1 e considerado o sucessor do MD5, processando blocos de 512 bits. E por último o SHA2, bem semelhante ao SHA1, mas diferencia-se no número de blocos, no número de rodadas das funções de compressão, ou uso de deslocamentos de bits para esquerda e para direita e no tamanho da constante que define as mensagens de entrada e saída do algoritmo.

4. Conclusão

Podemos concluir que o uso da criptografia é uma camada extra de proteção na segurança de redes de computadores, pois ela tem o objetivo de proteger você dos riscos de falhas e invasões e vazamentos de seus

dados pessoais ou arquivos importantes e privados, porém vale ressaltar que além de codificar suas informações com algoritmos ou configurar os padrões de senhas da sua rede sem fio de maneira mais segura possuem muito mais medidas a adotar, para que a sua rede possa ser considerada segura, além do fato que toda tecnologia sendo de criptografia ou não sempre deve ser atualizada para as versões mais atuais.

5. Referências.

[1] ALECRIM, E. CRIPTOGRAFIA. 12 de outubro de 2005 – Atualizado em 11 de julho de 2009; INFORWESTER.Disponível em <http://www.infowester.com/criptografia.php>. Acesso em 06 de junho de 2021.

[2] SEGURANÇA EM REDES DE COMPUTADORES. Disponível em< https://www.ic.unicamp.br/~nfonseca/arquivos/3ed/cap08>. Acessado em 06 de junho de 2021.

[3] MIANI, P. R. PRINCIPIOS DE CRIPTOGRAFIA. FACOM/UFU. Disponível em: <http://www.facom.ufu.br/~miani/site/teaching_files/seguranca/>. Acessado em 06 de junho de 2021.

[4] FUNÇÃO HASING. Disponível em <https://www.gta.ufrj.br/grad/09_1/versao-final/assinatura/hash.htm>. Acessado em 06 de junho de 2021.

[5] KUROSE, James F. Redes de computadores e a Internet: uma abordagem top-down. São Paulo: Pearson Education do Brasil, 2013. xxii, 634 p., il. Inclui bibliografia e índice. ISBN 9788581436777.