

13ª JORNADA DE INICIAÇÃO CIENTÍFICA

I N F O R M Á T I C A

ESTUDO SOBRE ANÁLISE DE DESEMPENHO DE ALGORÍTIMOS CRIPTOGRÁFICOS APLICADOS A TECNOLOGIA VOIP

¹Leonardo dos Anjos Tetéo (IC-UNIRIO); ¹Geiza M. H. da Silva (Orientadora)

1 – Departamento de Informática Aplicada; Centro de Ciências Exatas e Tecnologia; Universidade Federal do Estado do Rio de Janeiro.

Apoio Financeiro: UNIRIO

Palavras-chave: Criptografia; Informação; Segurança.

INTRODUÇÃO

Atualmente, as tecnologias relacionadas a transmissão de dados tem se inserido cada vez mais na vida cotidiana e corporativa. Um dos fatores preponderantes a adesão por estes setores é o crescimento da internet e a sua utilização como meio de comunicação através de dispositivos móveis e fixos em qualquer tipo de situação. Entretanto, junto com os avanços tecnológicos há a inserção de vulnerabilidades, principalmente no que diz respeito a transmissão de informações. Deste modo, é necessário o desenvolvimento de ferramentas que garantam a comunicação segura, entre as partes interessadas, protegendo assim as informações transmitidas.

Para garantir a segurança desejada é necessário a utilização de conceitos importantes da segurança da informação, sendo eles: confidencialidade, integridade, autenticação, disponibilidade, controle de acesso e auditoria [1]. Para que estes sejam aplicados de forma adequada, julga-se necessário um sistema de autenticação e a utilização de algoritmos criptográficos. No entanto, as soluções para uma segurança eficaz enfrenta o desafio relacionado com a diminuição de desempenho em processamentos e transmissões de qualquer tipo, inclusive através de rede.

Neste contexto o projeto SACIS[5][3], objetiva o desenvolvimento de ferramentas para o armazenamento e transmissão de informações com segurança, e este subprojeto visa o estudo do desempenho de algoritmos criptográficos utilizando o protocolo IPSec junto a tecnologia VoIP (Voice over Internet Protocol)[2][8]. Dado que a tecnologia VoIP requer transmissão de dados em tempo real, o desempenho da mesma se torna um fator ainda mais crítico.

OBJETIVO

Neste projeto está sendo realizado estudos sobre criptografia e a segurança de redes[4] com o objetivo de adquirir o conhecimento e a maturidade necessários para auxiliar no desenvolvimento e na avaliação de desempenho dos algoritmos criptográficos e protocolos aplicados a VoIP, utilizando como plataforma de teste o projeto sobre a transmissão de voz com segurança na plataforma Windows phone[6].

METODOLOGIA

O estudo sobre os diferentes tópicos foi realizado através de livros[4][8] e artigos científicos[1][3][7], nos quais foram compreendidos os conceitos básicos de criptografia e redes. Esta base é fundamental para o entendimento sobre a análise de desempenho dos algoritmos e a transmissão dos dados.

A análise de desempenho dos algoritmos criptográficos foi realizada através da comparação dos resultados teóricos apresentados na literatura. No entanto, estes serão testados na prática em [6], para a comprovação dos resultados e a contribuição de possíveis evoluções no sistema[6]. Será estudado metodologias de avaliação para que as análises possam ser realizadas da melhor maneira possível.

Seguindo a literatura [2][6][7], houve o cuidado de selecionar casos diferentes para que a análise fosse o mais real possível. Foram anotadas os principais pontos de cada estudo, o que eles tinham em comum e quais eram as divergências entre eles, tudo isso levando em consideração os diferentes ambientes em que os experimentos estudados foram realizados. Serão estudados, também, artigos de conferências internacionais para que os resultados sejam ainda mais consistentes.

RESULTADOS

No estudo pode-se perceber que há um certo consenso de que o uso de cabeçalho ESP[4] em modo túnel no protocolo IPSec seria o mais indicado para a transmissão de voz. Os artigos [2] e [7] provaram que, o uso de algoritmos criptográficos tem como consequência uma diminuição no desempenho da transmissão dos pacotes de dados pela rede, seja pelo retardo causado pelo próprio processo de cifragem, como também pelo acréscimo no tamanho dos pacotes devido a adição de cabeçalhos adicionais. Para isso, uma forma de compactação dos cabeçalhos pode ser estudada para que se possa atingir o desempenho esperado.

Também foi observado que na fase de processamento dos pacotes, onde a criptografia é realizada, o mecanismo de criptografia pode se tornar um “gargalo” para

13ª JORNADA DE INICIAÇÃO CIENTÍFICA

a transmissão em tempo real utilizando o IPSec [2]. Isto se deve ao fato de não existir uma forma de priorizar os pacotes que serão processados pelo mecanismo e, em um momento de grande tráfego, tem como consequência a perda de pacotes contribuindo para uma menor qualidade do sinal de voz ao chegar no destinatário.

Embora o desempenho seja notavelmente prejudicado pelo uso dessa arquitetura de segurança, o uso de diferentes técnicas, tais como a compactação de cabeçalhos e o uso de protocolos de QoS (Quality of Service)[8] pode melhorar o desempenho à padrões aceitáveis. Como exemplo, a tabela 1 ilustra os benefícios da compactação de cabeçalho realizada por [2] em relação ao uso de banda. Deste modo, este projeto continuará nesse caminho, analisando novos casos e buscando soluções.

Uso de banda em Kbps	
IP comum	30
IPSec	45
cIPSec (compactado)	33

Tabela 1: Comparação de uso de banda em Kbps [2]

CONCLUSÃO

Este é um estudo auxiliar para os projetos desenvolvidos por outros membros do grupo que implementa a ferramenta SACIS[5], principalmente no que diz respeito a transmissão de voz com segurança em plataforma Windows phone, a viabilidade de implementação da tecnologia VoIP [6] e o protocolo IPSec. O estudo ainda está em andamento e será possível oferecer soluções para os problemas relatados através de uma pesquisa mais aprofundada dos protocolos e mecanismos envolvidos, sendo a pesquisa em artigos de conferências nacionais e internacionais uma forma sólida de obter resultados ainda mais relevantes.

Vale ressaltar que este projeto possibilitou o estudo de um tópico extremamente importante para a área de Sistema de Informação, a Segurança da informação e o Desempenho na transmissão dos dados, que não faz parte diretamente da grade curricular, além da experiência no campo da pesquisa científica.

REFERÊNCIAS

- [1] ALENCAR, E. S.; RODRIGUES, W. - Segurança Aplicada a VoIP: Aspectos e Soluções.
- [2] BARBIERI, R.; BRUSCHI, D.; ROSTI, E. - Voice over IPsec: Analysis and solutions. In: Computer Security Applications Conference, 2002. Proceedings. 18th Annual. IEEE, 2002. p. 261-270.
- [3] Teixeira, F.A.A. - Sistema para Armazenamento e Comunicação de Mensagens com Segurança no Ambiente Windows – XI Jornada de Iniciação Científica- UNIRIO, 2013.
- [4] STALLINGS, W.- Criptografia e segurança de redes: princípios e práticas. Pearson Prentice Hall, 2008.
- [5] Teixeira, F.A.A, Souza, R. R., Silva, G.M.H. - Solução de Armazenamento e Comunicação de Informações com Segurança na Plataforma Windows - X Jornada de Iniciação Científica- UNIRIO, 2012.
- [6] SOUZA, R. R., SANTOS, D. A. – Estudo sobre a Transmissão de Voz com Segurança na Plataforma Windows - XI Jornada de Iniciação Científica- UNIRIO, 2013.
- [7] PASSITO, A.et al.- Análise de desempenho de tráfego VoIP utilizando o Protocolo IP Security. In: Anais do I Workshop de Ciência da Computação e Sistemas de Informação da Região Sul. Florianópolis. 2004.
- [8] SYED A. A., ILYAS M. - VoIP HANDBOOK: Applications, Technologies, Reliability, and Security – CRC Press, 2008.