

## 13ª JORNADA DE INICIAÇÃO CIENTÍFICA

# INFORMÁTICA

### PROPOSTA INICIAL DE IMPLEMENTAÇÃO PARA TRANSMISSÃO DE VOZ COM SEGURANÇA NA PLATAFORMA WINDOWS

<sup>1</sup>Rodrigo Ramos de Souza (IC-UNIRIO); <sup>1</sup>Davi de Araújo dos Santos (IC-UNIRIO); <sup>1</sup>Geiza Maria Hamazaki 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: Segurança da Informação; Dispositivos móveis; Criptografia.

#### INTRODUÇÃO

O crescente avanço da tecnologia e informatização dos processos gerou novas tendências na Gestão Corporativa em vigor em todo o mundo. É comum que assuntos importantes sejam resolvidos em chamadas telefônicas ou de vídeo, e com as descobertas sobre espionagem na rede, a segurança da informação trocada entre o remetente e o destinatário é de extrema importância.

Existem poucos sistemas para dispositivos móveis que realizam chamadas de forma segura. Esta foi a motivação para esse projeto, que propõe a criação de uma aplicação que permite a comunicação de voz criptografada entre dispositivos móveis.

Nesta aplicação a segurança da chamada é realizada através da criptografia de voz, que transforma a voz de forma que esta só possa ser compreendida pelo destinatário, e da identificação dos remetentes e destinatários, além da proteção contra modificação dos dados enviados pela rede. Para o desenvolvimento deste, é necessário conhecimentos nas áreas de redes, criptografia e manipulação de voz.

#### OBJETIVO

No projeto está sendo desenvolvido uma aplicação VoIP (voz sobre IP)[5] que permitirá a realização de chamadas entre dispositivos móveis (Windows phone) com o objetivo de garantir a segurança da conversa através da cifração simétrica (AES) da voz dos participantes da conversa. Além disso, a aplicação visa garantir a identidade do remetente e do destinatário.

#### METODOLOGIA

No desenvolvimento do projeto já foi executado o Módulo de Análise, onde foi estudado o sistema operacional Windows Phone e qual tecnologia seria utilizada para captura e transmissão da voz. Nesta etapa decidiu-se, então, pela utilização da tecnologia VoIP e o protocolo G711[5] para codificação da voz em sinal digital. Em seguida foi implementado o Módulo de Modelagem, onde foi realizado o levantamento dos requisitos e a modelagem da aplicação, definindo a arquitetura, as linguagens utilizadas na implementação dos sistemas e suas interfaces.

No Módulo de Desenvolvimento de Sistemas, a aplicação estava sendo desenvolvida com base na biblioteca OPAL[7], que implementa os protocolos para VoIP em C++. A biblioteca, no entanto, apresentou inúmeros problemas e foi necessário substituí-la. A aplicação agora está sendo desenvolvida usando a biblioteca H323+[8]. As aplicações para Windows Phone devem ser implementadas em C#, o que torna necessário a criação de uma DLL para as funções da biblioteca. Para garantir que a execução do projeto seja realizada com sucesso, todos os artefatos gerados estão documentados, visando facilitar a assimilação das tecnologias tanto por parte da equipe quanto por parte dos futuros participantes.

#### RESULTADOS

Inicialmente o objetivo era aplicar diretamente uma camada de criptografia sobre as chamadas controladas pelo Sistema Operacional Windows phone, entretanto devido ao controle de segurança do sistema, isto não é possível. Então foi decidido utilizar a tecnologia VoIP, na qual todos os aspectos da chamada estariam sobre o controle da aplicação a ser desenvolvida. O protocolo escolhido para implementar a aplicação VoIP foi o H323, devido a sua compatibilidade com o Windows Phone. O H323 é conjunto de protocolos para a transmissão de voz sobre ip. Ele é formado por outros protocolos, como o G711 que codifica a voz em sinal digital. Para auxiliar na implementação, foi escolhida a biblioteca OPAL[7] que implementa o protocolo H323 para transmissão de voz sobre IP. Esta biblioteca é uma biblioteca Open Source, mas ao tentar utilizá-la, a biblioteca apresentou várias falhas e incompatibilidades com as ferramentas sendo utilizadas. Depois de tentar, sem sucesso, resolver os problemas encontrados, foi decidido mudar de biblioteca. A nova escolha foi a H323+, uma versão mais recente e melhorada da OPAL.

Após esta fase foi iniciando o estudo sobre a captura da voz, a sua conversão em sinal de digital, o estabelecimento da conexão com o destino, a cifração dos dados e o envio para o destino (figura 1). No destino é preciso fazer o processo contrário para decifrar a informação e torná-la compreensível ao receptor.

## 13ª JORNADA DE INICIAÇÃO CIENTÍFICA

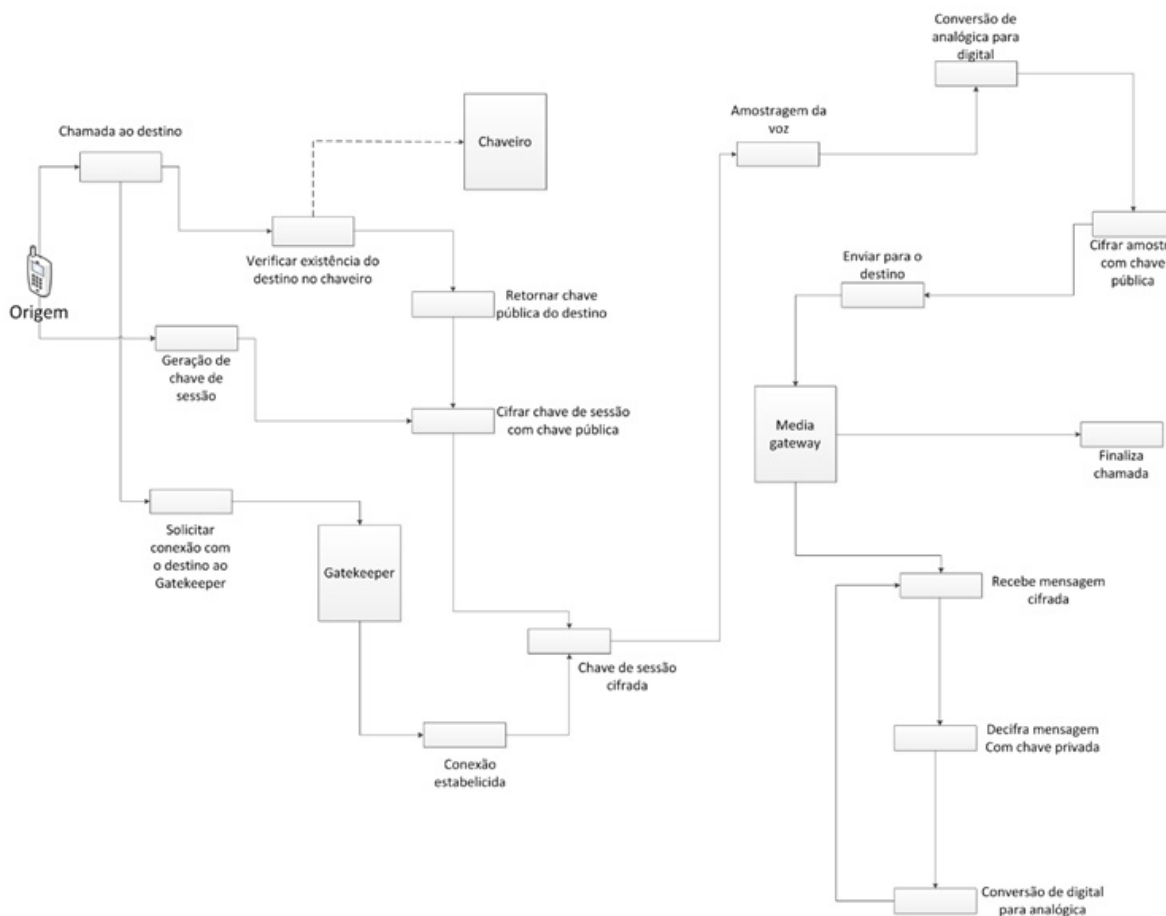


Figura1- Esquema da realização, envio e recepção de mensagens utilizando a aplicação VoIP [12]

Entre os principais resultados obtidos, pode-se ressaltar o ganho de conhecimento em áreas que não constam diretamente na grade curricular (Segurança da Informação, VoIP e Dispositivos Móveis), através do desenvolvimento de uma aplicação com tecnologia de ponta em um ambiente de pesquisa colaborativo. Além do aprendizado na elaboração e apresentação de trabalhos de pesquisa.

### CONCLUSÃO

O objetivo final do projeto é o desenvolvimento de uma aplicação VoIP que permita a troca de mensagens de voz de forma segura através de criptografia. O projeto está em fase de desenvolvimento da aplicação VoIP na qual será aplicada a criptografia. Atualmente está sendo desenvolvida uma solução para a troca de mensagens de voz, que inclui estabelecer uma conexão, capturar a voz e codificá-la para enviar digitalmente. A troca de mensagens de voz é o passo inicial, depois devem ser implementados as funcionalidades para enviar com sucesso uma mensagem criptografada da origem até o destino. Em seguida é necessário capturar a voz e codificá-la, criptografá-la e enviá-la para o destino, onde deve ser descryptografada obtendo assim a mensagem original.

Este projeto terá como produto um programa, que será integrado com outro subprojeto do projeto principal SACIS[11], o qual realiza o armazenamento e o envio de mensagens, em texto, criptografadas nos sistema operacional Windows.

### REFERÊNCIAS

- [1] DOUGLAS, R. Stinson. Cryptography Theory and Practice, Chapman & Hall/CRC Press, 3rd. edition, Nov 2005.
- [2] SCHNEIER, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. Editora John Wiley and Sons.
- [3] STAMP, M. Information Security: Principles and Practice. John Wiley and Sons.2007, McClure, S. Hacking Exposed, McGraw-Hill Osborne Media, 2005.
- [4] KELLY, V.T - Voip for Dummies - Wiley Publishing Inc. 2005.
- [5] SYED A. A., ILYAS M. VoIP HANDBOOK: Applications, Technologies, Reliability, and Security – CRC Press, 2008.



### **13ª JORNADA DE INICIAÇÃO CIENTÍFICA**

- [6] HANKERSON D., MENEZES A., VANSTONE S. Guide to Elliptic Curve Cryptography - Springer, 2003.
- [7] <http://www.opalvoip.org/> acessado em 13/05/2014.
- [8] <http://www.h323plus.org/> acessado em 13/05/2014
- [9] LOPEZ Research, Final Mobile Deployments Require Robust Security May 09.pdf - <http://www.lopezresearch.com/> acessado em 28/02/2013.
- [10] WAI C. C., Speech Coding Algorithms: Foundation and Evolution of Standardized Coders - Wiley-Interscience, 2003
- [11] 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.
- [12] Souza, R. R. , Santo D. A., Silva, G.M.H - Estudo sobre a Transmissão de Voz com Segurança na Plataforma Windows- XII Jornada de Iniciação Científica – UNIRIO, 2013.