

13ª JORNADA DE INICIAÇÃO CIENTÍFICA

INFORMÁTICA

SISTEMA PARA ARMAZENAMENTO E COMUNICAÇÃO DE MENSAGENS COM SEGURANÇA NO AMBIENTE WINDOWS PHONE

¹Thiago M. Passos (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: FAPERJ, UNIRIO

Palavras-chave: Dispositivos móveis; Criptografia; Segurança da Informação.

INTRODUÇÃO

Nos dias de hoje os smartphones e tablets tem ganhado cada vez mais popularidade e tem feito cada vez mais parte do dia a dia dos usuários. Graças ao crescente poder computacional desses dispositivos, estes podem ter aplicações que antes só eram possíveis de serem executados em ambiente desktop. A aplicação do SACIS (Sistema para Armazenamento e Comunicação da Informação com Segurança) [1] para o Windows Phone 8 [2] acompanha esse momento suprimindo a necessidade de uma aplicação móvel capaz de garantir a segurança de arquivos armazenados localmente, e de mensagens – com arquivos em anexos. Este sistema, poderá acessar as mensagens e arquivos criptografados enviados pela aplicação desktop do SACIS [1].

OBJETIVO

O objetivo é de disponibilizar o aplicativo para o sistema operacional Windows Phone 8 [2] com o máximo de funcionalidades possíveis comparados a aplicação para desktop, respeitando as possíveis limitações inerentes ao sistema operacional mobile, oferecendo o acesso às informações transmitidas ou arquivadas independente do software do SACIS utilizado, seja para Windows Phone, Windows Desktop ou outras possíveis versões do SACIS para outros sistemas operacionais.

METODOLOGIA

Este projeto começou a ser implementado em julho de 2013 com uma análise do sistema SACIS existente para o desktop [1], assim como uma pesquisa sobre os sistemas criptográficos [5] e desenvolvimento de aplicações Windows Phone 8 [3] [4], cujo o paradigma de desenvolvimento se difere bastante do Windows Desktop.

Na implementação foi utilizado o Windows Phone SDK [4], disponibilizado pela Microsoft para a produção de aplicativos para o sistema [2], utilizando o software Visual Studio 2012 Express [7]. Como é o padrão do sistema móvel, foi adotada a arquitetura MVVM [8] de design pattern para o desenvolvimento do software.

Nas Reuniões com o grupo de desenvolvimento do projeto SACIS (alunos e professora orientadora) foram analisados o funcionamento do programa, especificação sobre as funcionalidades que a aplicação mobile deve ter, e discussão sobre cronogramas, dúvidas, resultados, direcionamento para o projeto além do compartilhamento dos conhecimentos adquiridos.

RESULTADOS

Após o estudo sobre desenvolvimento de aplicativos para o Windows Phone 8 [3] [4], foi realizado um levantamento de quais classes da plataforma .net [13] utilizadas na aplicação desktop [1] estariam disponíveis para o uso no sistema operacional Windows Phone 8 [2], e foi constatado que algumas classes da área criptográfica, além de toda a de interface, teriam que ser reimplementadas.

Para a área criptográfica foram utilizadas bibliotecas do Mono [14] e BouncyCastle [15] para suprir as deficiências do .net utilizado pelo Windows Phone 8, como hash SHA-512, cifra simétrica e cifra assimétrica [5].

Na implementação da interface gráfica foi utilizada a linguagem XAML [16], provendo uma experiência mais apropriada ao tamanho reduzido da tela do telefone, sem que perca a semelhança de uso do SACIS para desktop [1].

A comunicação do SACIS para o Windows Phone com o servidor do SACIS é feita utilizando o padrão WSDL [9], que faz a conversação usando SOAP [10] para trafegar as mensagens em XML [11] entre cliente-servidor. Com isso o XML recebido do servidor é tratado para controlar o conteúdo exibido na interface gráfica. Atualmente o projeto se encontra no acesso, leitura e envio de mensagens (figura 1).

13ª JORNADA DE INICIAÇÃO CIENTÍFICA

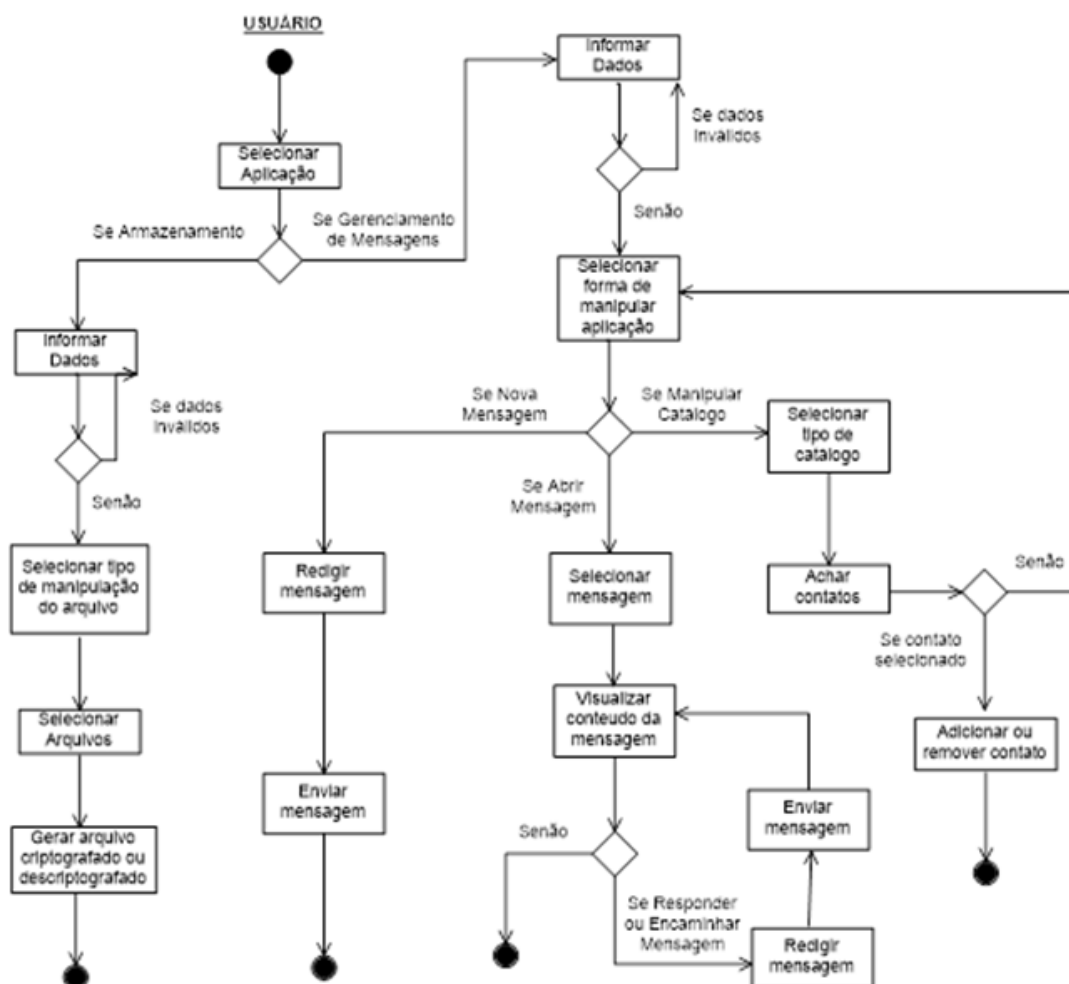


Figura 1 – Processo de negócio do SACIS para o usuário [1]

CONCLUSÃO

Este trabalho propõe um cliente totalmente funcional ao já existente servidor do SACIS [1] com um novo layout voltado às telas menores dos smartphones, com a mínima perda de recursos comparado a aplicação feita para o desktop.

Desta forma o SACIS poderá sempre acompanhar o usuário em seu smartphone, podendo armazenar arquivos e trocar mensagens com segurança sem a necessidade de ter um computador desktop ou notebook. O projeto já considera a inserção de novas tecnologias que serão incorporadas ao SACIS, como comunicação por voz [12]. O conhecimento adquirido no desenvolvimento da aplicação para o Windows Phone também poderá ser aplicada no desenvolvimento numa futura versão da aplicação para o sistema operacional Android. Vale ressaltar o aprendizado nas áreas de desenvolvimento mobile para Windows Phone, linguagem de programação C# [17], sistemas criptográficos [5] e estruturas de comunicação cliente-servidor [9].

REFERÊNCIAS

- [1] Teixeira, F.A.A, Souza, R. R. , Silva, G.M.H. - SOLUÇÃO DE ARMAZENAMENTO E COMUNICAÇÃO DE INFORMAÇÕES COM SEGURANÇA NO AMBIENTE WINDOWS - XI Jornada de Iniciação Científica - UNIRIO, 2013.
- [2] WINDOWS PHONE 8: [online] <<http://www.windowsphone.com/pt-br/how-to/wp8/basics/get-started-with-windows-phone>> acessado em 12/05/2014.
- [3] NOKIA DEVELOPER: [online] <<http://developer.nokia.com>> acessado em 12/05/2014.
- [4] WINDOWS PHONE DEV CENTER: [online] <<http://developer.windowsphone.com/en-us>> acessado em 12/05/2014.
- [5] STALLINGS, William - Criptografia e Segurança de Redes; 4ª Edição; Editora Prentice Hall, 2010.
- [6] WINDOWS PHONE SDK: [online] <<https://dev.windowsphone.com/en-us/downloadsdk>> acessado em 12/05/2014.



13ª JORNADA DE INICIAÇÃO CIENTÍFICA

- [7] VISUAL STUDIO 2012 EXPRESS: [online] <<http://www.visualstudio.com/pt-br/visual-studio-homepage-vs.aspx>> acessado em 12/05/2014.
- [8] Model-View-ViewModel (MVVM) Applications: General Introduction: [online] <http://blogs.msdn.com/b/ivo_manolov/archive/2012/03/17/10284665.aspx> acessado em 12/05/2014.
- [9] WSDL: [online] <<http://www.w3.org/TR/wsdl>> acessado em 12/05/2014.
- [10] SOAP: [online] <<http://www.w3.org/TR/soap/>> acessado em 12/05/2014.
- [11] XML: [online] <<http://www.w3.org/standards/xml/>> acessado em 12/05/2014.
- [12] Souza, R. R., Santos D. A., Silva, G.M.H. – ESTUDO SOBRE A TRANSMISSÃO DE VOZ COM SEGURANÇA NA PLATAFORMA WINDOWS - XI Jornada de Iniciação Científica - UNIRIO, 2013.
- [13] Microsoft .NET: [online] <<http://www.microsoft.com/net/>> acessado em 14/05/2014.
- [14] Mono: [online] <<http://www.mono-project.com/>> acessado em 14/05/2014.
- [15] BouncyCastle: [online] <<https://www.bouncycastle.org/>> acessado em 14/05/2014.
- [16] Visão geral de XAML (WPF): [online] <<http://msdn.microsoft.com/pt-br/library/ms752059%28v=vs.110%29.aspx>> acessado em 14/05/2014.
- [17] C# Language Specification: [online] <<http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-334.pdf>>; 4a edição; ECMA; Junho 2006.