Sistema para Armazenamento e Transmissão de Informação com Segurança no Ambiente Windows[1]

Fabio A. A. Teixeira[1], Roberto Assakura[1] ,Geiza M. H. da Silva[1]

[1]Universidade Federal do Estado do Rio Janeiro - (UNIRIO)
Avenida Pasteur, 458 – Urca – Rio de Janeiro / RJ – CEP:22290-240

{fabio.teixeira,roberto.assakura, geiza.hamazaki}@uniriotec.br

Abstract. *The advance of technology and automation of processes are developing new trends in Corporate Management. One of the major concern is related to the storage and transmission of sensitive information through mobile and fixed devices. There are several systems that guarantee the security of information stored locally, such as [PGP] and [TRUECRYPT]. In the case of transmitting information securely, either through fixed or mobile devices, it becomes necessary to use several independent tools. This scenario motivated the design of a system for transmitting sensitive information through an environment of support "automatic" for storage and encrypted transmission of documents for fixed and mobile devices. At this work is presented a tool for a device that has the Windows operating system, using cryptographic algorithms for symmetric and asymmetric keys. The application will have a desktop version, allowing synchronization with Windows Mobile smartphones.*

Resumo. *O crescente avanço da tecnologia e informatização dos processos gerou novas tendências na Gestão Corporativa. Ao visualizar a complexidade da infra-estrutura tecnológica que sustenta as organizações [Stamp 2006], uma das principais preocupações está relacionada ao armazenamento e transmissão de informações sigilosas através de dispositivos móveis e fixos. Existem vários sistemas que garantem a segurança das informações armazenadas localmente, como o [PGP] e o [TRUECRYPT]. No caso da transmissão da informação de forma segura, seja através de dispositivos fixos ou móveis, torna-se necessária a utilização de diversas ferramentas independentes entre si. Tal cenário motivou o projeto de um sistema para transmissão de informações sigilosas através de um ambiente de suporte "automático" para o armazenamento e transmissão de documentos criptografados para dispositivos fixos e móveis. No primeiro momento, a base de testes é um dispositivo que tem como sistema operacional Windows, utilizando algoritmos criptográficos públicos simétricos e assimétricos. A aplicação terá uma versão para desktops, permitindo assim a sincronização com smartphones com o Sistema Operacional Windows Mobile.*

[1] Este artigo é parte de pesquisa do Projeto Financiado pela FAPERJ - Soluções de Armazenamento e Comunicação de Informações com Segurança - SACIS.

1. Introdução

Com a inserção de novas tecnologias, e das ameaças e vulnerabilidades que as acompanham, uma das preocupações principais na Gestão Corporativa está relacionada à comunicação de dados sigilosos, ao acesso controlado aos dados, a sua transmissão e a integridade através de dispositivos digitais, dentre diversas plataformas e protocolos de rede.

Existem vários aplicativos como, por exemplo: [RSA] e [TRUECRYPT], que podem ser utilizados para a proteção da informação através de cifras, sejam elas simétricas ou assimétricas, bem como para a verificação de integridade para dispositivos fixos [Douglas 2005] [Schneier 1996]. No caso de dispositivos móveis, esse contexto se torna restrito a computadores portáteis.

Este trabalho propõe como solução um conjunto de inovações tecnológicas que compõe uma nova infra-estrutura para transmissão de informações sigilosas através de um ambiente de suporte "automático" para o armazenamento e transmissão de documentos criptografados através de dispositivos móveis e fixos que possuem o *Windows* como sistema operacional.

A aplicação é composta de:

1. Um sistema de gerenciamento de chaves;
2. Um sistema para a administração de usuários;
3. Um sistema para uso do usuário;
4. Segurança dos dados através da sua criptografia armazenando-os no aparelho e em cartões de memória removíveis;
5. Segurança na transmissão dos dados através da identificação dos remetentes e destinatários, além da proteção contra modificação dos dados enviados pela rede.

2. Desenvolvimento

Este projeto implementa uma aplicação para a família de dispositivos que possuem sistema operacional *Windows*. Para garantir a compatibilidade entre as diferentes versões do sistema operacional a implementação da aplicação foi realizada em C# utilizando como ambiente de desenvolvimento o *software* [VISUAL STUDIO 2008]. Para transmissão da informação é estabelecida uma conexão segura utilizando o protocolo HTTPS para conectar, transmitir e visualizar as mensagens armazenadas no servidor.

A aplicação é dividida em dois sistemas: um para o administrador e outro para o usuário conforme ilustrado na figura 1. O sistema para o usuário é subdividido em duas funcionalidades: o armazenamento local de dados criptografados e envio de mensagens e arquivos criptografados.

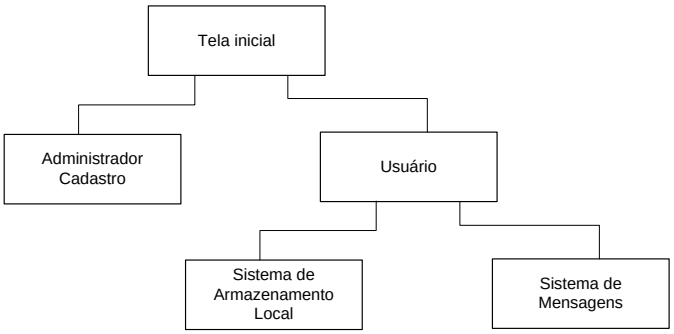

Figura 1. Organograma geral do sistema

2.1. Sistema Administrador

Neste sistema, o administrador irá inserir os dados solicitados no cadastro de usuário (nome, *login* e senha - Figura 2) e, além disso, incluir a chave pública informada pelo usuário e a sua validade. A chave pública fornecida pelo usuário poderá ser certificada ou gerada por um gerador de pares de chaves assimétricas, por exemplo, com o [OPENSSL].

Ao realizar o cadastro, o sistema irá verificar a existência do *login* inserido no formulário. Caso este não exista, os dados serão inseridos no banco de dados MySQL[MYSQL], o qual armazenará as informações de cadastro do usuário (nome do usuário, *login*, *hash* da senha, chave pública, validade da chave pública). Caso contrário será informado ao administrador à existência do usuário e o primeiro será questionado se deseja a alteração dos dados.

Após o cadastro no banco de dados, o sistema irá criar uma pasta individual no servidor para o usuário. Esta contém subpastas para as mensagens recebidas, enviadas, chave pública e contatos particulares. Ainda nesta fase, o sistema irá padronizar a chave pública certificada para que ele possa utilizá-la de forma mais eficiente no processo de cifração e decifração.

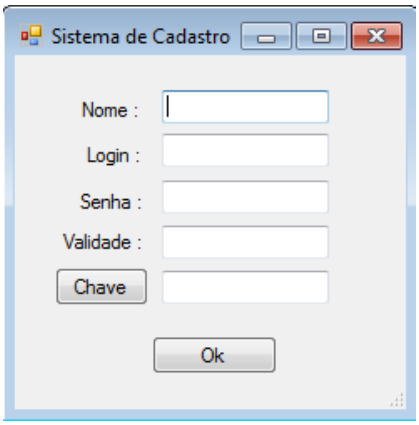

Figura 2. Tela do sistema de cadastro do administrador

2.2. Sistema Usuário

Este sistema é dividido em duas funcionalidades: cifrar/decifrar arquivos locais (Sistema de Armazenamento Local) e envio/recebimento de mensagens com ou sem anexos, os quais poderão ser cifrados ou não (Sistema de Mensagens).

2.2.1. Sistema de Armazenamento Local

O Sistema de Armazenamento Local serve para a cifração e decifração de arquivos locais. Para entrar no sistema é necessário um *login* (nome e senha) "semi-independente" da conexão com o servidor, pois para utilizar o sistema o usuário deverá ter realizado ao menos um acesso ao servidor *web* para que possa ser registrado localmente. Neste processo os dados do servidor são copiados para uma pasta local no dispositivo.

Dado que o usuário esteja registrado localmente será aberta a tela com o gerenciador de arquivos. Uma vez selecionado(s) o nome do(s) arquivo(s) e as ações de remover, cifrar/decifrar e cancelar serão apresentadas ao usuário.

2.2.2. Sistema de Mensagens

O sistema para envio e recebimento de mensagens entre os usuários do sistema possui um *login* que é verificado através da consulta ao banco de dados central (servidor). Ao ser garantido seu acesso, o sistema irá verificar localmente a existência do registro do usuário. Caso não exista o registro, este será realizado copiando dados do servidor para uma pasta local no dispositivo.

Ao entrar no sistema uma tela de gerenciamento de mensagens é exibida, mostrando as pastas de mensagens (entrada e enviados) e o *menu* contendo as opções de nova mensagem, catálogo e fechar (figura 3). Os dados são visualizados do servidor, permitindo sua manipulação (visualização e remoção) na caixa de entrada e enviados. Quando for solicitado que uma mensagem seja aberta, o sistema verificará se há partes da mensagem cifradas (corpo da mensagem ou anexos) e automaticamente decifra-as. Os anexos poderão ser salvos localmente na pasta determinada pelo usuário.

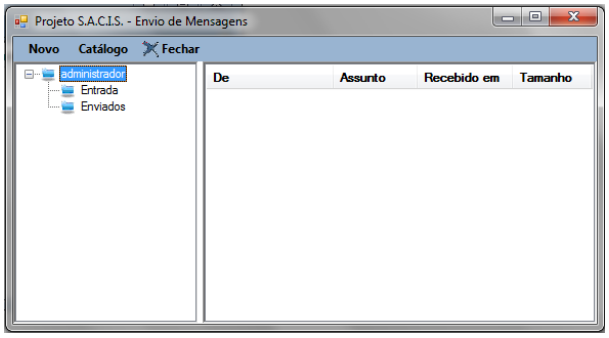

Figura 3. Tela principal do sistema de mensagens

Ao criar, encaminhar ou responder uma mensagem é exibida uma tela para seleção dos contatos e edição do assunto (figura 4). Para anexar um documento é apresentado uma nova tela indicando quais serão criptografados (com chaves simétricas AES [Schneier 1996] e assimétricas [RSA]). A seleção dos contatos poderá ser realizada através do chaveiro criado pelo usuário e armazenado no servidor, no qual o usuário poderá adicionar ou remover contatos, ou através do chaveiro central.

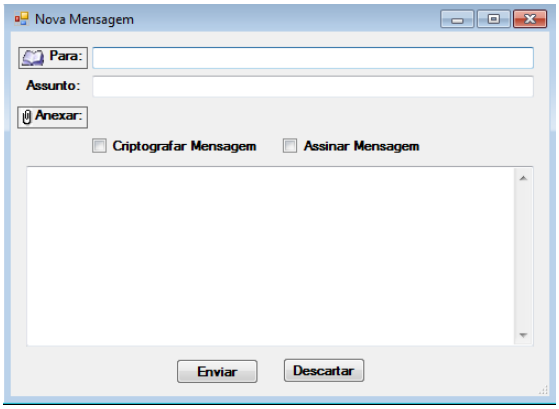

Figura 4. Tela da nova mensagem

Ao solicitar o envio da mensagem, o sistema irá verificar quais arquivos anexados deverão ser cifrados e se a mensagem deverá ser cifrada. Estes dados serão armazenados em um arquivo no formato [XML], conforme ilustrado na figura 5, e enviados para o destinatário.

```
<message>
    <header>
        <from>webmaster@gowansnet.com</from>
        <to>webmaster@xml.org</to>
        <subject>ZZZZ </subject>
    </header>
    <attachment> arquivo anexado </attachment>
    <body> XXXX</body>
</message>
```

Figura 5. Formato XML para mensagens

A geração de chaves simétricas é realizada utilizando um algoritmo baseado no [MERSENNE].

3. Conclusão

Este trabalho propõe uma ferramenta para a transmissão e armazenamento de informações sigilosas em dispositivo (fixos ou portáteis) que possuem como Sistema Operacional o ***Windows***. Esta ferramenta permite a sincronização das informações entre os dispositivos e a inserção de algoritmos proprietários para o processo de cifração/decifração (simétrico ou assimétrico).

Esta aplicação está em fase de implementação. Em paralelo está sendo realizado o estudo para a implementação da mesma para o sistema operacional Android, bem como a utilização de técnicas vindas da área de métodos formais para verificar propriedades da aplicação e dos protocolos de comunicação móvel.

AGRADECIMENTOS

A FAPERJ, por ter possibilitado e financiado esta pesquisa e ao Analista Ronaldo Cesar dos Santos.

4. Referências Bibliográficas

Douglas, R. S. (2005) "Cryptography Theory and Practice", Chapman & Hall/CRC Press, 3rd. edition.

Schneier, B. (1996) "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition. Editora John Wiley and Sons.

Stamp, M. (2006) "Information Security: Principles and Practice". John Wiley and Sons. Editora Wiley Interscience.

PGP- http://www.pgp.com/ acessado em 23/04/2011

RSA- http://www.rsa.com/ acessado em 23/04/2011

TRUECRYPT - http://www.truecrypt.org/ acessado em 23/04/2011

XML - http://www.w3.org/XML/ acessado em 23/04/2011

MYSQL – http://www.mysql.com/ acessado em 28/08/2011

MERSENNE - http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html acessado em 28/08/2011

OPENSSL - http://www.openssl.org/ acessado em 28/08/2011

VISUAL STUDIO 2008 - http://www.microsoft.com/portugal/msdn/visualstudio08/default.mspx acessado em 08/10/2011