

13ª JORNADA DE INICIAÇÃO CIENTÍFICA

INFORMÁTICA

PROPOSTA DE IMPLEMENTAÇÃO DE UM SISTEMA PARA ARMAZENAMENTO E COMUNICAÇÃO DE INFORMAÇÕES COM SEGURANÇA PARA O SISTEMA OPERACIONAL ANDROID

¹ Cecília de Almeida Soares (IC- UNIRIO); ¹ 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; Criptografia; Android.

Palavras-chave: ontologia; alinhamento; complexidade.

INTRODUÇÃO

As instituições estão cada vez mais inseridas em um cenário digital, integrado e complexo, onde uma das principais preocupações está em garantir a segurança e integridade de seus processos através da utilização de novas tecnologias. Existem vários aplicativos para dispositivos fixos e móveis, por exemplo: [1], [3], [4] e [5] que podem ser utilizados para a proteção da informação através de cifras, sejam elas simétricas ou assimétricas, bem como para a verificação de integridade [7].

Dentre as vulnerabilidades mais comuns em dispositivos móveis, pode-se citar: vírus propagados através de conexões com algum computador ou telefone infectado, aplicativos maliciosos que prejudicam o usuário através de permissões não pertinentes a eles e também acesso não permitido a informações armazenadas ou transferidas.

Este projeto propõe o desenvolvimento de novas tecnologias, confiáveis e flexíveis, para transmissão de informações sigilosas através de um ambiente de suporte “automático” para o armazenamento e transmissão de documentos criptografados para um conjunto significativo de dispositivos móveis que possua o sistema operacional Android. Este sistema propõe:

- Tornar mais seguros os dados armazenados no aparelho e em cartões de memória através de criptografia dos mesmos.
- A segurança na transmissão dos dados através da identificação dos remetentes e destinatários, além da proteção contra modificação dos pacotes enviados pela rede.

No primeiro momento serão utilizados algoritmos criptográficos públicos simétricos e assimétricos clássicos [6]. Para permitir a interoperabilidade da aplicação, o armazenamento dos documentos será realizado no formato XML [8]. A aplicação terá uma versão para dispositivos fixos e móveis que possuam o Sistema operacional Windows [12], com a qual será testada a interoperabilidade.

OBJETIVO

Este projeto está desenvolvendo uma aplicação com objetivo de garantir a segurança da informação em dispositivos móveis com o sistema operacional Android. Será utilizada a cifração simétrica (AES) e assimétrica (RSA) [6] dos documentos armazenados ou transmitidos. Além disso, visa garantir a integridade das informações enviadas por um emissor a um determinado receptor.

A aplicação terá características não comuns a outras pertencentes ao mesmo grupo, como a possibilidade de inserção de algoritmos proprietários sem a necessidade de conhecimento intrínseco dos mesmos. Permitirá a interoperabilidade da aplicação entre diversas plataformas, sejam elas de dispositivos móveis ou fixos.

Além dos objetivos técnicos científicos, pode-se ressaltar a possibilidade de integração de múltiplos conhecimentos na solução de um dado problema, gerando inovações tecnológicas promissoras. Este ganho de conhecimento proporciona aos alunos envolvidos no projeto um diferencial para trabalhos futuros – seja no mercado profissional, seja como pesquisador.

METODOLOGIA

No desenvolvimento do projeto, os Módulos de Análise (no qual foram levantados os requisitos e a modelagem da aplicação) e Modelagem (onde foi definida a arquitetura, a implementação dos sistemas e suas interfaces) já foram realizados pela professora responsável, juntamente com os bolsistas do Projeto. Após a aquisição dos conhecimentos necessários, o Módulo de Desenvolvimento, deste projeto, foi inicializado pelos bolsistas em Dezembro de 2012. Para garantir a compatibilidade entre as diferentes versões do sistema operacional, o desenvolvimento da aplicação está sendo realizada utilizando a Linguagem de Programação JAVA e tendo como ambiente de desenvolvimento o software open source [10].

Após a primeira versão da aplicação estar concluída, será implementado o Módulo de Avaliação, no qual serão realizados testes sobre a usabilidade e serão identificados os requisitos não atendidos. As não-conformidades serão analisadas novamente, retornando ao módulo de Desenvolvimento, onde a equipe

13ª JORNADA DE INICIAÇÃO CIENTÍFICA

propará novas soluções para resolver os problemas levantados. A fim de garantir que a execução do projeto seja realizada com sucesso, todos os artefatos gerados serão documentados, visando facilitar a assimilação das tecnologias pelos integrantes do grupo.

Regularmente reuniões são realizadas para a sincronização do andamento dos projetos, bem como direções futuras e linhas de pesquisa de interesse comum.

RESULTADOS

O projeto atualmente está na fase de desenvolvimento não oferecendo resultados práticos. A interface inicialmente estava sendo implementada com a biblioteca Greendroid [11] para a plataforma Android. Como o autor desta biblioteca resolveu descontinuar o projeto, optou-se por outra, a ActionBarSherlock [13]. Esta, após algum tempo de uso no projeto, demonstrou ser um problema, pois não era compatível com algumas funcionalidades já implementadas anteriormente, fazendo com que o mesmo aparentasse estar sem layout caso a API não estivesse devidamente incorporada ao projeto. Atualmente este está sendo desenvolvido com interface própria para evitar futuros problemas com as bibliotecas que podem, inesperadamente, terem o seu desenvolvimento descontinuado. No projeto foi finalizado a cifração/decifração simétrica de arquivos, a cifração/decifração assimétrica esta sendo desenvolvida em paralelo com a interfaces para acesso de administrador e usuário, envio e recebimento de mensagens e documento, além da verificação da integridade dos mesmos. A integração com o Webservice será implementada logo após os testes das cifrasões/decifrações.

Como resultado principal vale ressaltar a aquisição e aplicação de conhecimentos na área de segurança da informação, modelagem de software, desenvolvimento e documentação de projetos.

CONCLUSÃO

Existe a carência de ferramentas que transmitam os dados do usuário de forma sigilosa, que tenham uma interface intuitiva e simplificada, que permitam a inserção de algoritmos proprietários para o processo de cifração/decifração (simétrico ou assimétrico) e a interoperabilidade da aplicação entre diversas plataformas. Neste cenário, a ferramenta está sendo implementada de forma a atender as características citadas, sendo este trabalho a parte da ferramenta implementada para o Sistema Operacional Android.

É importante ressaltar ainda a existência do projeto “Sistema de Armazenamento e Compartilhamento de Informações com Segurança – Ambiente Windows PC” [14] que foi finalizado. Neste projeto foi implementado o web service, solução que irá permitir que novas aplicações possam interagir com aquelas já existentes, e que os sistemas desenvolvidos em plataformas diferentes sejam compatíveis, o que é de suma importância para o projeto SACIS, que ainda encontra-se sendo desenvolvido em outras plataformas, e terá a validação da Interoperabilidade da ferramenta sendo feita através dessa solução implementada.

REFERÊNCIAS

- [1] PGP- <http://www.pgp.com/>, acessado em 09/01/2014
- [2] RSA- <http://www.rsa.com/>, acessado em 09/01/2014
- [3] TRUECRYPT - <http://www.truecrypt.org/>, acessado em 09/01/2014
- [4] GOLD LOCK 3G - <https://www.gold-lock.com/en/home/> acessado em 09/01/2014
- [5] SYMANTEC ENCRYPTION - <http://www.symantec.com/pt/br/products-solutions/families/?fid=encryption> acessado em 10/01/2014