Construção de uma *Interface Gráfica* para o OpenSSL em GTK+

Proposta de Projeto

Orientador: Pedro R. M. Inácio

1 Objetivos

O OpenSSL é a implementação *open source* em Linguagem C dos vários algoritmos e procedimentos que compõem os protocolos Secure Sockets Layer (SSL) e Transport Layer Security (TLS). Para além de se poder fazer uso das bibliotecas para funções de segurança em aplicações informáticas, são também disponibilizados uma série de comandos que encabeçam uma Client Line Interface (CLI) muito completa e poderosa. Com esta CLI é possível cifrar e decifrar ficheiros, calcular valores de *hash*, produzir e verificar assinaturas ou certificados digitais e implementar autoridades de certificação. Como reflexo da sua utilidade, foram também surgindo algumas *Graphical User Interfaces* (GUIs) para esta ferramenta ao longo do tempo, normalmente focadas em aplicações específicas, sobretudo no que toca à geração e manuseamento de certificados digitais.

O objetivo deste projeto é o de completar uma GUI contruida em GTK+ para o OpenSSL. A implementação atual precisa de ser melhorada de forma a incorporar melhor futuras versões do `OpenSSL` e a disponibilizar, de forma amigável para o utilizador, o maior número possível de funcionalidades fornecidas com a ferramenta, nomeadamente:

- Cifra e decifra de ficheiros;
- Cálculo de valores de *hash*;
- Geração, cifra e transmissão de chaves de cifra;
- Geração e verificação de selos temporais;
- Geração de chaves RSA, elaboração e verificação de assinaturas digitais;
- Geração de números aleatórios;
- Criação, configuração e gestão de autoridades de certificação;
- Verificação de cadeias de certificados;
- Criação de listas de revogação de certificados;
- Outras funcionalidades.

O desenvolvimento deve ser especialmente focado na criação de uma aplicação intuitiva e estruturada, dada a quantidade de funcionalidades que pode vir a acumular. Como objetivos secundários, pretende-se ainda que se preparem os pacotes de instalação da ferramenta para várias distribuições de Linux e uma página *web* de apresentação da aplicação. Com este trabalho pretende-se que o(a) aluno(a) melhore os seus conhecimentos no sistema operativo Linux, em programação e em segurança informática.

O projeto deverá ser desenvolvido preferencialmente no laboratório do grupo *Multimedia Signal Processing* (MSP) `http://floyd.di.ubi.pt/nmcg/`. O(A) aluno(a) terá oportunidade de interagir com outros investigadores do grupo e exercitar a sua capacidade crítica.

2 Tarefas a Realizar

T1 Estudo do problema e da versão preliminar da aplicação desenvolvida.

T2 Definição de funcionalidades a implementar. Engenharia de software.

T3 Implementação e teste da aplicação.

T4 Preparação de pacotes de instalação para duas distribuições de Linux e de uma página *web* de apresentação e *download* da aplicação.

T5 Escrita do relatório de projeto (de preferência em língua inglesa).

3 Cronograma

T1 1 mês (0,5 meses sobreposto a T2)

T2 1 mês

T3 2 mês

T4 0,5 meses

T5 1 mês

4 Requisitos Técnicos

Vontade de aprender novas tecnologias. Demonstrar alguma fluência na Língua Inglesa. Familiarização com uma distribuição de Linux.

5 Requisitos Académicos

Boas notas nas unidades curriculares de Segurança Informática, Programação, Sistemas Operativos e Matemática para a Informática.

6 Grau de Dificuldade

Difícil.

7 Resultados esperados

- Uma interface gráfica em GTK+ para a ferramenta `OpenSSL`.
- Uma página web de apresentação da ferramenta.
- Pacotes de instalação para várias distribuições de Linux.
- Um relatório de projeto.

8 Contactos

Pedro R. M. Inácio (inacio@di.ubi.pt)