Desbloqueio de *Keyrings* usando Certificados Digitais

Proposta de Projeto

Orientador: Pedro R. M. Inácio

1 Objetivos

Devido à grande quantidade de credenciais de autenticação dos utilizadores de sistemas informáticos, a gestão das combinações *nome de utilizador* / *palavra-passe* é normalmente (e por vezes de modo transparente) deixada a cargo de módulos de *software* especializados com o nome sugestivo de *chaveiros* (*keyrings*). É também habitual estes chaveiros estarem protegidos por uma chave mestra, da qual deriva a chave de cifra que protege as palavras-passes e os nome de utilizadores guardados no chaveiro. Caso a chave mestra seja a mesma que é utilizada para autenticação no sistema operativo, o chaveiro pode ficar imediatamente desbloqueado aquando da entrada do utilizador no ambiente de trabalho. Caso contrário, o sistema operativo ou a aplicação que queria usufruir ou desbloquear o chaveiro pede a chave mestra ao utilizador interativamente. Navegadores como o *Firefox* ou o *Chromium* trazem os seus próprios chaveiros, facilitando a entrada repetida de nomes de utilizadores ou palavras-passe em sites visitados mais que uma vez.

Como antes dito, o desbloqueio dos chaveiros é normalmente feito através da inserção de uma chave mestra. O objetivo deste trabalho é o de implementar um sistema que desbloqueie chaveiros recorrendo a certificados digitais com função de autenticação. Numa primeira fase, a implementação pode recorrer apenas a certificados digitais gerados localmente usando o `OpenSSL`. Numa segunda fase, pode procurar-se a integração do sistema desenvolvido com o cartão do cidadão, visto este já trazer certificados de autenticação. A prova de conceito pode ser feita com o sistema final a desbloquear o chaveiro do, e.g., *firefox* após inserção do cartão do cidadão e do PIN de autenticação. O desenho do sistema deve ter em atenção o fato de que é sempre necessária uma palavra-passe para cifrar o chaveiro bloqueado, quer seja o utilizador a introduzi-la ou não. Para além de fazer a autenticação, o sistema deve definir a melhor forma de derivar essa palavra-passe.

Com este trabalho pretende-se que o(a) aluno(a) melhore os seus conhecimentos em sistemas operativos, programação e 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 familiarização com tecnologias envolvidas.

T2 Desenho e implementação do sistema inicial de autenticação e desbloqueio de chaveiros.

T3 Integração do sistema com chaveiros existentes (e.g., Firefox).

T4 Integração do sistema com o cartão do cidadão.

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

3 Cronograma

T1 1 mês (0.5 meses partilhados com a tarefa 2)

T2 1 mês

T3 1 mês

T4 1,5 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

- Um sistema de autenticação e desbloqueio de chaveiros seguro.
- Um programa capaz de correr em *background* e desempenhar as funcionalidades referidas nesta proposta.
- Um relatório de projeto.

8 Contactos

Pedro R. M. Inácio (inacio@di.ubi.pt)