Autenticação no Sistema Operativo com Códigos *Quick Response*

Proposta de Projeto

Orientador: Pedro R. M. Inácio

1 Objetivos

A possibilidade de fazer autenticação com códigos *Quick Response* (QR) é já referida há algum tempo, motivada principalmente por algumas aplicações úteis destes códigos em dispositivos móveis. Recentemente, a Google também testou a utilização destes códigos na autenticação ao serviço de Gmail. A ideia fundamental por detrás desta possível solução é a de codificar uma série de informações na forma de um código QR que, após ser lido por um leitor, é processado pelo dispositivo móvel e o resultado transmitido de novo ao codificador inicial (o autenticador). Se o dispositivo móvel pertencer à entidade que se quer autenticar deve conter o segredo que produz a resposta esperada pelo autenticador.

O objetivo deste projeto é construir um sistema que faça o *login* num sistema operativo (ou desbloqueie a proteção de ecrã) recorrendo a códigos QR e a mecanismos de criptografia de chave pública. Na fase de instalação, o sistema desenvolvido deve criar e instalar o material criptográfico (chaves assimétricas) necessário à sua correta operação. Quando em funcionamento, o sistema autenticador (computador) deve mostrar um código QR no ecrã, a ser lido pelo dispositivo móvel (e.g., telemóvel *android*). Após descodificação, o dispositivo móvel processa e produz os dados de autenticação, que são transmitidos de novo ao autenticador. A transmissão destes dados será alvo de estudo mas pode, por exemplo, ser feita na forma de novo código QR mostrado no ecrã do dispositivo móvel e lido pelo computador. Após validação bem sucedida, o computador desbloqueia. Após fase de desenvolvimento inicial, pode proceder-se à integração desta solução com certificados digitais para validação da entidade a autenticar e estudar a autenticação mutua de ambas partes.

Este trabalho é um pretexto para estudar a interação entre mecanismos de criptografia e dispositivos móveis pessoais. 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 das tecnologias e mecanismos envolvidos.

T2 Definição de funcionalidades a implementar.

T3 Implementação e teste da aplicação.

T4 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 2,5 mês

T4 1 mês

4 Requisitos Técnicos

Vontade de aprender novas tecnologias (nomeadamente programação para o sistema operativo Android). Demonstrar alguma fluência na Língua Inglesa. Familiarização com uma distribuição de Linux.

5 Requisitos Académicos

Boas notas nas unidades curriculares de Segurança Informática, Programação (nomeadamente Programação Orientada a Objetos), Sistemas Operativos e Matemática para a Informática.

6 Grau de Dificuldade

Difícil.

7 Resultados esperados

- Um sistema para autenticação no computador usando códigos QR ou protótipo de prova de conceito equivalente.
- Um relatório de projeto.

8 Contactos

Pedro R. M. Inácio (inacio@di.ubi.pt)