Proteção de Aplicações

1. Especificação

Um aspeto muito importante do desenvolvimento de aplicações é o controlo da integridade e o controlo de execução das aplicações desenvolvidas. Considerando que qualquer desenvolvimento possui um custo não desprezável, constituindo o meio de vida dos programadores, é simples compreender que muitos autores pretendam disponibilizar as aplicações por si desenvolvidas de forma não gratuita.

Considerando esta situação, é comum as aplicações incorporarem mecanismos destinados a comprovar que o utilizador tem de facto uma cópia autorizada da aplicação, e que as cópias apenas executam de acordo com os parâmetros acordados entre o autor e o utilizador, como por exemplo a restrição de execução num número limitado de dispositivos.

O processo pelo qual é realizado este controlo tem as suas raízes na utilização de cifras simétricas e assimétricas, assim como em funções de síntese (*hash*) e em assinaturas digitais. O princípio básico consiste na criação de uma licença que não é mais do que uma assinatura criada pelo autor ou distribuidor, de alguma forma relacionada com a aplicação em execução. É comum considerar-se o nome da aplicação e a sua versão, podendo igualmente considerar-se um identificador do sistema em que a aplicação executa ou mesmo uma síntese do binário em execução. Também é comum utilizarem-se dispositivos físicos, frequentemente denominados por *dongles* ou chaves de hardware, que restringem a execução da aplicação aos sistemas onde aquele dispositivo se encontre conectado.

1.1 Objetivos

O objetivo deste trabalho é o de desenvolver um sistema que permita distribuir aplicações de forma segura, garantindo que apenas são executadas pelos donos legítimos das mesmas.

Este sistema deverá ser composto por: (i) um conjunto de ferramentas que executam nas instalações do autor ou distribuidor da aplicação; e (ii) por uma biblioteca de controlo de execução que é incorporada nas aplicações a proteger.

Na concretização deste trabalho os alunos devem considerar proteger uma qualquer aplicação desenvolvida pelos mesmos ou por outros, numa qualquer linguagem de programação da sua preferência.

As ferramentas disponibilizadas ao autor devem permitir criar ficheiros de licenças que são fornecidos às aplicações, e que devem incluir uma especificação de execução e a identificação dos dados da licença. Estes ficheiros serão descritos na Secção 1.2.

A biblioteca de controlo de execução deverá ser constituída por um módulo contendo um conjunto de funcionalidades (ou métodos numa classe). É vital que esta biblioteca seja completamente independente da aplicação desenvolvida, no máximo partilhando a linguagem de programação.

Esta biblioteca deverá possuir o seguinte conjunto de métodos:

- `void init(string nomeDaApp, string versão)`: Este método corresponde à inicialização da biblioteca de controlo de execução. No caso de uma implementação orientada a objetos, este método pode corresponder ao construtor.
- `bool isRegistered()`: Uma aplicação deverá invocar este método no início da sua execução e sempre que ache necessário. Este método deverá executar de forma rápida e eficiente, validando a correta execução da aplicação atual. Caso se verifique que a aplicação executa de forma autorizada, ele não deverá imprimir qualquer valor e deverá devolver o valor `True`. Caso contrário deverá devolver o valor `False`.
- `bool startRegistration()`: Este método deve apresentar uma interface (da forma mais adequada à aplicação, o que pode ser utilizar o `stdout` ou uma interface gráfica) indicando que a aplicação não se

encontra registada e possibilitando iniciar o processo de registo de uma nova licença. Os detalhes sobre este processo encontram-se na secção 1.4.

- `void showLicenseInfo()`: Esta função apresenta os dados da licença atual (caso ela exista), ou informação de que a aplicação não se encontra registada. A apresentação desta informação, mais uma vez, deverá ser efetuada da maneira mais adequada à aplicação. Para uma aplicação de linha de comandos esta informação pode ser escrita para o terminal (`stdout`).

1.2 Ficheiros de Licença

Os ficheiros de licença de uma aplicação deverão conter diversa informação que permita identificar a aplicação, o utilizador autorizado e o ambiente de execução da máquina. É deixado ao critério dos alunos a escolha da informação, sugerindo-se pelo menos a seguinte:

- Informação que identifique o utilizador: o seu nome, endereço de email, número de identificação civil e certificado de chave pública do Cartão de Cidadão.
- Informação que identifique o sistema: um identificador do sistema obtido do conjunto de hardware presente tais como número e tipo de CPUs, placas de rede (endereços MAC), números de série do suporte de armazenamento, ou mesmo identificadores da BIOS.
- Informação que identifique a aplicação: nome da aplicação, versão atual, valor da síntese do seu ficheiro principal (ou ficheiros relevantes) e, se a biblioteca existir de forma separada, qual o valor da síntese do ficheiro contendo a biblioteca.
- Informação que identifique o intervalo temporal de validade da licença: data de início de validade da licença e data de expiração.

Toda esta informação deverá depois ser cifrada, sendo adicionado um controlo de integridade sobre a forma de uma assinatura efetuada pelo autor ou distribuidor. Para isso, devem ser utilizadas chaves simétricas e assimétricas da forma mais adequada.

1.3 Validação da Licença

Validar uma licença implica vários passos, verificando primeiramente o próprio ficheiro de licença e depois os diferentes componentes que ela codifica.

O primeiro passo consiste em validar a assinatura da mesma e decifrar o seu conteúdo (por esta ordem ou pela inversa). Pode-se assumir que cada aplicação distribuída contém uma chave que fornece à biblioteca de proteção aquando da sua inicialização. Pode igualmente considerar que a biblioteca deriva uma chave a partir dos dados da máquina ou aplicação, ou mesmo que existe uma chave pré-distribuída na biblioteca.

A informação relativa ao intervalo temporal de execução deve ser validado considerando a data atual do sistema.

A informação relativa à identificação do sistema deve ser calculada na inicialização da biblioteca e confrontada com a informação presente no ficheiro de licença. A biblioteca deve ser capaz de tolerar pequenas alterações ao sistema, o que é comum caso exista a troca de um CPU ou de uma placa de rede. Após excedida esta tolerância, considera-se que o sistema não é mais válido.

A informação relativa à identificação do utilizador é útil na medida que torna o Cartão de Cidadão num dispositivo de segurança, condicionando a execução da aplicação à presença de um utilizador específico (cartão específico, com uma chave privada específica). A biblioteca, fazendo uso da chave pública do utilizador registada na licença poderá autenticar o utilizador. Visto que esta operação é mais demorada que as anteriores, deixa-se ao critério dos alunos decidirem quando é que o cartão é validado. Depois de corretamente validado, pode-se considerar que testar a presença do cartão, sem realizar assinaturas é suficiente para continuar a execução.

A informação relativa à identificação da aplicação serve para validar a integridade do sistema. Garante-se desta forma que a aplicação não foi manipulada (de forma simples), numa tentativa de ignorar o sistema de validação de licença.

1.4 Registo

O processo de registo implica a biblioteca recolher toda a informação necessária (utilizador, sistema e aplicação), o que é expresso num documento, o pedido de registo (e.x., codificado em base64, XML ou JSON). Este documento deve ser assinado pela chave presente no Cartão de Cidadão do utilizador em causa, sendo depois cifrado de forma a que forme um pedido de registo seguro. O documento de pedido de registo deve ser guardado num ficheiro para ser enviado para o autor da aplicação, podendo também ser apresentado no ecrã. É da responsabilidade do utilizador a cópia e envio do pedido de registo para o autor da aplicação.

Após receber o pedido de registo, o autor, utilizando um conjunto de ferramentas criadas para o efeito de processar o pedido de registo, emite um ficheiro de licença assinado. Considere que o autor possui um par de chaves assimétricas e considere a utilização de cifras híbridas.

A duração de cada licença é definida pelo autor.

É obrigatório que estas ferramentas mantenham informação organizada relativa às aplicações distribuídas, licenças existentes e utilizadores. Embora não seja necessária a utilização de bases de dados relacionais, pois uma estrutura de diretórios adequada é suficiente, o seu uso não é desencorajado.

Não se considera necessário implementar qualquer mecanismo de comunicação entre sistemas. Desta forma, e considerando um cenário "real" os ficheiros de pedido de registo e de licença podem ser transferidos por meios alternativos (e.x., email, ftp, dropbox, etc..).

Atenção: Todas as chaves privadas devem ser armazenadas de forma segura e não em claro!

2. Avaliação

Os projetos devem ser realizados preferencialmente em grupos com o máximo de 2 elementos. Fazer o trabalho de forma individual não implica qualquer tipo de atenuante na avaliação. A nota final dependerá de 3 aspetos:

1. O grau de satisfação dos requisitos expostos neste enunciado. Isto é, quantas das funcionalidades pedidas foram implementadas.
2. O grau de complexidade da solução apresentada. São mais valorizadas soluções simples que conseguem o maior grau de integração de funcionalidades e que melhor satisfazem a experiência dos utentes. É também valorizada a identificação, discussão e proposta de solução de alguma eventual vulnerabilidade na aplicação proposta.
3. A participação individual de cada elemento do grupo será aferida em discussão oral e em casos extremos pela análise do código do grupo. O desconhecimento de quaisquer partes relevantes do projeto apresentado será interpretado como não tendo participado na sua realização, ou contribuído de forma irrelevante para a mesma.

A seguinte lista resume as funcionalidades a implementar:

- Criação de um ficheiro com um pedido de licença que inclua a identificação do utilizador, dados sobre a plataforma para a execução da aplicação e dados sobre a aplicação (1,5 valores)
- Proteção (integridade, confidencialidade, autenticação, não repudiação) do pedido de licença (1,5 valores)
- Validação do pedido de licença (1,5 valores)
- Emissão da licença, com todos os dados que garantam que apenas uma aplicação legitima pode ser executada no sistema autorizado e pelo utilizador autorizado (1,5 valores)
- Proteção (integridade, confidencialidade, autenticação, não repudiação) da licença emitida (1,5 valores)
- Validação do documento da licença (1,5 valores)
- Proteção contra execução da aplicação noutro sistema (2 valores)

- Proteção contra a execução da aplicação por outro utilizador (2 valores)
- Proteção contra a alteração da aplicação (2 valores)

Para simplificar a implementação, pode assumir a utilização de algoritmos criptográficos fixos, i.e. pré-definidos, sem necessidade da sua descrição. Além disso, assuma que o autor possui um par de chaves assimétricas cuja componente pública é bem conhecida.

Para soluções que implementem corretamente características de segurança interessantes e não referidas na descrição do problema, serão atribuídos 2 valores de bónus.

No final do semestre, os alunos deverão entregar um relatório sobre o trabalho realizado (4 valores) e fazer uma demonstração final do trabalho, o que inclui uma discussão individualizada onde o grupo fará a defesa do seu trabalho. O relatório deverá referir:

- Todos os estudos/análises realizadas, as alternativas consideradas e as decisões tomadas
- Todas as funcionalidades implementadas
- Todos os problemas e deficiências conhecidos da solução implementada.

O relatório deverá ainda conter imagens devidamente comentadas que evidenciem a correção da solução implementada.

Nota, a inclusão no trabalho de código alheio (de colegas de sítios na Web, ou de outras fontes) sem estar devidamente referenciado, é interpretado como plágio, aplicando-se os regulamentos da Universidade para esses casos.

A data limite para a entrega do relatório é o dia 2 de Janeiro de 2020 e a apresentação e discussão do trabalho será realizada na última semana de aulas, preferencialmente no dia da aula (9 de Janeiro de 2020).