FACULDADE ENGENHARIA
Departamento de Informática

Ferramenta para Fluxo de Análise e Identificação de Requisitos de Software de Segurança

Proposta de Projeto

Orientador: Pedro R. M. Inácio(inacio@di.ubi.pt)

Objetivos

Desenhar sistemas e software seguro por construção (ou por desenho) tem-se revelado uma tarefa difícil. Infelizmente, repetem-se exemplos de software que é projetado, desenvolvido, testado e colocado em produção sem quaisquer preocupações de segurança, a não ser no período de suporte pós produção, onde endereçar segurança é muito mais custoso e complexo. Se por um lado seria de pensar que este problema estava já em atenuação, por outro, novas tecnologias e paradigmas de computação e comunicação (como computação na nuvem, computação móvel e Internet das Coisas (IdC)) voltam a introduzir atrito na engrenagem, demonstrando que é necessário redobrado esforço a montante do processo de desenvolvimento de software nesta área. Por exemplo, há uma clara necessidade de tornar o processo de identificação e análise de requisitos de segurança para sistemas ou software mais simples de (con)seguir por arquitetos de sistema, mesmo que não tenham conhecimentos aprofundados de segurança informática.

No contexto dado pelo parágrafo anterior, este projeto tem os seguintes objetivos principais: (i) estudar o estado da arte em termos de análise de requisitos de segurança para sistemas de software, com foco sobretudo na IdC, mas também em computação móvel e Cloud; (ii) enumerar exaustivamente requisitos de segurança através de casos de estudo ou literatura especializada; (iii) desenvolver uma ferramenta que ajude a identificar e analisar os requisitos de segurança para um sistema de software, a partir da ideia que o arquiteto tem para esse sistema (e.g., características, dados recolhidos, processados e/ou enviados, tipo de comunicação, dispositivos envolvidos), e produzindo documentação de uma forma estruturada e adequada; (iv) testar a ferramenta com alguns casos de estudo (fictícios ou reais); e (v) desenhar o formato do *output* da ferramenta no contexto do conjunto de outras ferramentas em que se vai inserir. O formato para entrada e saída de informação nas diferentes ferramentas do projeto deve ser desenhado em XML. O objetivo será que a saída de uma ferramenta possa ser entrada de outra sem necessidade de intervenção por parte do utilizador. O formato deverá também ser estruturado de forma a auxiliar a geração automática de documentação. Para referência, verificar o formato XACML (https://en.wikipedia.org/wiki/XACML) para ter uma ideia base daquilo que é pretendido. A ferramenta deve ser orientada para ambiente de linha de comandos e ter opcionalmente um ambiente gráfico. Deve ser definida a forma uniforme da ferramenta (e outras que façam parte do conjunto) suportar esse ambiente gráfico. A documentação do código desenvolvido deve ser rica e uniforme e devem ser usados repositórios de código para manutenção e gestão de versões (e.g., github).

Dada a sua natureza, este projeto requer conhecimentos sólidos em Segurança

Informática, Sistemas Operativos e Redes de Computador, bem como em Engenharia de Software e Programação. O(a) aluno(a) terá uma oportunidade de solidificar o seu conhecimento nas várias áreas abrangidas por este projeto, e também trabalhar em ambiente laboratorial com elementos do grupo *Multimedia Signal Processing*-Covilhã, do Instituto de Telecomunicações. Este (sub)projeto será desenvolvido no âmbito do projeto *Towards the assurance of SECURity by dESIGN of the Internet of Things* (SECUR IoT ESIGN) [1].

Tarefas a Realizar e Cronologia

T1 Contextualização com as tecnologias envolvidas e trabalho desenvolvido. Estudo do estado da arte em Análise de Requisitos de Segurança (0,5 meses).

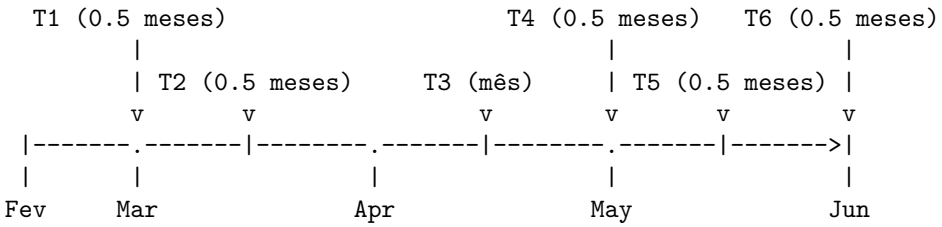
T2 Planeamento da ferramenta a desenvolver; definição da ferramenta em termos de entradas e saída de dados, nomeadamente do formato dos dados de saída (0,5 meses).

T3 Preparação do ambiente de desenvolvimento e infraestrutura de suporte e implementação preliminar da ferramenta (1 mês).

T4 Estudo de casos de uso para teste de conceito (0,5 meses).

T5 Aprimoramento da ferramenta e documentação (0,5 meses).

T6 Escrita do relatório de projeto (0,5 meses).



Requisitos Técnicos / Académicos

Ter boas classificações e conhecimentos em programação, sistemas operativos, engenharia de software e segurança informática.

Elementos de Avaliação a Entregar

Para além do relatório, o(a) aluno(a) deverá entregar o código fonte desenvolvido e a documentação associada.

Resultados Esperados

* A enumeração de requisitos de segurança a suportar pela ferramenta;
* Uma ferramenta informática que guie um arquiteto de sistema na identificação de requisitos de segurança de software, produzindo documentação adequada;
* Análise de vários casos de estudo com a ferramenta;
* 1 relatório de projeto [2].

Referências Bibliográficas (caso existam)

[1] SECURIoTESIGN Team, Towards the assurance of SECURity by dESIGN of the Internet of Things, Disponível online em `https://lx.it.pt/securIoTesign/`, 2019 [último acesso: 4 de fevereiro de 2019].
[2] C. Collberg and S. Kobourov, Self-plagiarism in Computer Science, Communications of the ACM, 48(4): 88 - 94, 2005.