Software Reliability and Security
The Formal Methods perspective

Simão Melo de Sousa
Departamento de Informática
Universidade da Beira Interior

This document in pdf (link).

Abstract

Num mundo em que o software é "de facto"ubíquo e omnipresente em cada actividade que um cidadão tenha, em cada dispositivo da internet das coisas, em cada máquina desde a de café ao sistema de apoio ao piloto de um avião, passando pelos sistemas de controlo de satélites, pelos sistemas de transação bolsistas, e até mesmo em cada funcionalidade, outrora mecânica, de um automóvel.

É assim natural e espectável que o software deva então ser concebido como são os aviões, edifícios em zona de terramotos, etc... isto é, projectos de software com garantias objetivamente comprováveis de que cumprirá a sua missão. Infelizmente esse não é caso frequente e as razões não são desconhecidas.

Falhas no software causam danos: vidas, perdas financeiras, prejuízo no negócio... Até potenciam o ciber-crime.

O ciber-crime tira proveito essencialmente de dois aspetos: os utilizadores, pela engenharia social, e as falhas de software que expõem indevidamente todo ou parte do sistema. É assim de primeira importância de que este esteja concebido com padrões de qualidade cada vez mais altos, sem no entanto impor custos proibitivos.

O desenvolvimento formal de software, e em particular a verificação formal de software, introduzem técnicas, ferramentas e práticas que visam col-

matar parte dessas falhas na actividade de concepção de software. Esta intervenção visará mostrar a investigação realizada, a experiência e a prática do LISP nesta área de saber, as aplicações industriais que atestam do impacto desta ciência e desta engenharia de software, do seu sucesso e dos seus custos.

Slides

Slides for the talk "Software Reliability and Security - The Formal Methods perspective"(link)

any comments are welcomed and appreciated: (please make the obvious changes to the email address) : desousa_ @ _di.ubi.pt