Formalizing ROS2 security configuration with Alloy

Master Dissertation in Informatics Engineering

Luís Mário Macedo Ribeiro

Universidade do Minho
Escola de Engenharia
Departamento de Informática

Introduction

- Automation in the Industrial world
- Software development in Robotics
  - Complexity and Middlewares as solution
- The Robot Operating System

Problem and Opportunity

- Problem contextualization
  - Robots and security
  - Software Verification
- The purpose of this dissertation

The Alloy Framework

- Quality Assurance on Robotic Systems
  - Usage of formal methods and verification techniques
  - Automated analysis to avoid security-critical faults
- Model Checking
  - Software verification with temporal logic
  - Usage in testing
- The Alloy Framework
  - Modelling
  - Analysis

Software Development in ROS2

- Former Architecture approach
- ROS2 with DDS as communication middleware
- Security Analysis
  - Former problems
  - DDS-Security specification - Security Plugin Infrastructure
  - SROS2 - Enclaves and Access Control

Related Work

- Security in ROS
  - Exploiting techniques and potential solutions
  - DDS integration in ROS2 as solution
  - Evaluation works in ROS2
- Verification of Robotic Systems
  - Static Analysis
  - HAROS framework
  - Model Checking in ROS and in other robotics software

Future Work

TASKS	February	March	April	May	June	July
SROS Security Discussion						
Core Techniques Definition						
Evaluation						
Implementation						
Writing						