Universidade do Minho
Escola de Engenharia

Plano de Trabalho de Dissertação

Ano Letivo 2021/2022

Nome Estudante	Luís Mário Macedo Ribeiro
N.º Estudante	85954
Curso	MIEI – Mestrado Integrado em Engenharia Informática
Título da Dissertação (em Português)	Formalização das configurações de segurança do ROS2 usando Alloy
Título da Dissertação (em Inglês)	Formalizing ROS2 security configuration with Alloy

Enquadramento e Motivação (150 - 200 palavras)

One of the most popular open-source software platforms for building robotic systems is the Robot Operating System (ROS) [1]. A major factor behind its popularity and widespread adoption is its flexibility and interoperability. One drawback of this flexibility, however, lies in the increased security risks that ROS applications face. The low barrier to entry and open nature of the ROS ecosystem means a malicious actor could potentially inject code or vulnerabilities into a library, which could then be reused by another unsuspecting developer.

The first version of ROS includes its own communication middleware, which does not scale well, and is unsuitable for safety-critical and real-time systems. This lead to the creation of ROS2, which continues to provide a simple, uniform message passing interface to allow components to communicate with each other, now implemented using the Data Distribution Service (DDS) [3] communication protocol. This means that it continues to be relatively straightforward for a developer to add and integrate a new component into an existing system.

ROS2 is deployed without security mechanisms by default, but DDS can provide security guarantees such as authentication and access control with a variant called DDS-Security. Using DDS-Security it is possible to configure ROS2 to run with security guarantees using the SROS2 toolset [4]. However, improper configuration can still lead security problems.

Alloy [7] is a formal specification language and analysis tool that has been successfully applied in the verification of safety and security properties in several domains. This thesis intends to explore the usage of Alloy in the analysis of the security configuration of ROS2 applications.

O plano de trabalho deve ser preenchido *offline* e realizado o *upload* do mesmo, depois de assinado, no formulário do requerimento de pedido de admissão à dissertação, disponível em http://dissertacao.eng.uminho.pt

Objetivos e Resultados Esperados (150 - 200 palavras)

The first goal of this thesis is to understand how ROS2 and SROS2 work. Likewise its predecessor, ROS2 has a distributed architecture, now using the DDS framework as communication middleware, which must be properly understood before considering the security aspects. To do so, simple examples will first be developed, before focusing on the domain of autonomous systems, where security is of extreme relevance, namely the Autoware [6] ROS2 platform for self-driving vehicles. To understand SROS2 we intend to configure and run a realistic case study related to Autoware with security guarantees.

The second goal is to extend a previously proposed [5] formalization of ROS applications in Alloy/Electrum [7,8] to also take into consideration the security configuration defined with SROS2. Using this extension, we intend to explore the viability of verifying simple information-flow security properties, for example, to ensure that no commands to the vehicle motor can be sent via the infotainment system.

The final goal is to automate the extraction of such formal Alloy models from the configuration files of a ROS2 application, in order to obtain a prototype tool that can be used by roboticists to easily detect security configuration issues.

Calendarização

The work for this Masters Dissertation will take place on a 9 month period between the 6th of October 2021 until the 30th of June 2022 and will follow the timings presented below:

- Literature Review (From the 6th of October 2021 until the 31st of January 2022):
  - Study of ROS2, DDS, and SROS2.
  - Study of the Autoware platform by running a realistic case study.
  - Study of Alloy.
  - Pre-Thesis writing.
- Core Techniques Definition (From the 1st of February 2022 until the 31th of March 2022):
  - Formalization of the architecture of ROS2 applications in Alloy.
  - Extend this formalization to cover the SROS2 security configuration.
  - Propose a technique to specify and verify information-flow security properties on top of the proposed Alloy formalization.
- Evaluation (From the 1st of April 2022 until the 30th of April 2022):
  - Selection of relevant case studies in the Autoware platform.
  - Identify and formalize relevant information-flow security properties for that case study.
  - Evaluate the effectiveness of the proposed formalization and verification technique on the identified case studies and security properties.
- Implementation (From the 1st of May 2022 until the 31th of May 2022):
  - Implement a prototype tool that can automatically infer an Alloy formalization of a ROS2 architecture and SROS2 security configuration
- Writing (From the 1st of June 2022 until the 30th of June 2022):
  - Thesis writing.

Referências Bibliográficas (5 - 10 referências)

[1] https://www.ros.org

[2] Nicholas DeMarinis, Stefanie Tellex, Vasileios P. Kemerlis, George Dimitri Konidaris, Rodrigo Fonseca: Scanning the Internet for ROS: A View of Security in Robotics Research. ICRA 2019: 8514-8521

[3] Object Management Group. Data Distribution Service (DDS). https://www.omg.org/omg-dds-portal/

[4] ROS 2 DDS-Security integration https://design.ros2.org/articles/ros2_dds_security.html

[5] Renato Carvalho, Alcino Cunha, Nuno Macedo, André Santos: Verification of system-wide safety properties of ROS applications. IROS 2020: 7249-7254
https://www.autoware.auto

[6] Shinpei Kato, Shota Tokunaga, Yuya Maruyama, Seiya Maeda, Manato Hirabayashi, Yuki Kitsukawa, Abraham Monrroy, Tomohito Ando, Yusuke Fujii, Takuya Azumi: Autoware on board: enabling autonomous vehicles with embedded systems. ICCPS 2018: 287-296
https://www.autoware.auto

[7] Daniel Jackson: Alloy: a language and tool for exploring software designs. Commun. ACM 62(9): 66-76 (2019), http://alloytools.org/

[8] Nuno Macedo, Julien Brunel, David Chemouil, Alcino Cunha, Denis Kuperberg: Lightweight specification and analysis of dynamic systems with rich configurations. SIGSOFT FSE 2016: 373-383, https://haslab.github.io/formal-software-design/

Justificação de Coorientação (se aplicável)

André Santos works at the Vortex Colab, where he researches on the topic of robotic software quality. He has a vast experience on reverse-engineering formal models from ROS applications and is the main developer of the well-known HAROS framework for static analysis of ROS applications, where we eventually intend to deploy the proposed security analysis technique.

Assinaturas

Estudante

Assinado por : **Luís Mário Macedo Ribeiro**
Num. de Identificação: 30040558
Data: 2021.10.25 14:23:04+01'00'

Orientador (tal como previsto no ponto 1 do Artigo 169.º do

Assinado por : **MANUEL ALCINO PEREIRA DA CUNHA**
Num. de Identificação: 10065313

Diretor do Ciclo de Estudos

Orientador (tal como previsto no ponto 3 do Artigo 169.º do RAUM. Neste caso, é obrigatório existir um Orientador pelo ponto 1 do Artigo 169.º do RAUM)

Assinado por : **André Filipe Faria dos Santos**
Num. de Identificação: 13736433
Data: 2021.10.22 08:42:00+01'00'

Assinatura digital qualificada com Cartão de Cidadão ou Chave Móvel Digital. Para os estudantes, nos casos em que tal não seja possível, os mesmos deverão imprimir este plano, assinar manualmente e, após digitalização, os restantes intervenientes usam a assinatura digital qualificada.

O plano de trabalho deve ser preenchido *offline* e realizado o *upload* do mesmo, depois de assinado, no formulário do requerimento de pedido de admissão à dissertação, disponível em http://dissertacao.eng.uminho.pt