ROS Security Project

CJ, Simon Chu

March 9, 2021

17803 - Empirical Methods

ROS in a Nutshell

What is ROS?

- **R**obot **O**perating **S**ystem
- Open-source meta OS
- Hardware abstraction
- Low-level device control
- Message passing
- Package management

...

Motivation

- Widely used in **research** communities.
- Recently drew attention from **industry/gov't** for **safety-critical systems**.
- Not designed for security-critical applications.
- ROS community is aware of such needs, and there are some ongoing security-focus projects, (e.g., SROS, ROS 2)

Goals

- ROS application developers: provide guidelines on how to secure their systems from an architecture level.
- ROS platform developers & security researchers: provide advice on how to build security infrastructures.

Research Questions

- RQ1: By domains, what are the architectural characteristics of the open-source ROS-based projects?
  - What are the typical architectural pattern for a domain?
  - What are the frequently used libraries for a particular domain? What are their functionalities?
- RQ2: How to guide roboticists to build secure ROS-based systems?
- RQ3: How to guide platform-developers and researchers to develop future security framework?

Method Overview

Three phases:

1. Collect architectural related data from representative open-source ROS projects from different domains from GitHub.
2. Collect guidelines from security experts based on the data extracted.
3. Evaluate and elicit the guidelines via surveys.

Phase 1: Architectural Data Collection

- Select ROS-based open source projects representative of different domains (security-critical).
- Extract architecture-related information, including application domain, documentation, actual architecture, library used, functionalities of specific components.

Phase 2: Guideline Elicitation from Experts

- Collect security guidelines from some security experts by providing the data from Phase 1.
- E.g., threat modeling for guideline elicitation

Phase 3: Guideline Evaluation & Elicitation

- Evaluate the usefulness of these guidelines with a survey (classify by participants background, e.g., app developers, ROS platform developers, researchers)
- In the same survey, collect additional guidelines from participants.

References

- https://www.theconstructsim.com/history-ros/
- https://www.ros.org/history/
- http://wiki.ros.org/ROS/Introduction
- http://wiki.ros.org/SROS
- Malavolta, Lewis, et al. How do you Architect your Robots? State of the Practice and Guidelines for ROS-based Systems *ICSE: Software Engineering in Practice*, 23-29 May 2020