# ROS-Industrial EU Fall'19 Workshop

## ROSPenTo & SROS2

Sebastian Taurer

ROBOTICS – Institute for Robotics and Mechatronics
JOANNEUM RESEARCH
Klagenfurt am Wörthersee, Austria

October 10, 2019

JOANNEUM RESEARCH ROBOTICS

# Outline

- Part 1: ROSPenTo
  - Introduction
  - User menu options
  - ROS publish/subscribe
  - ROSPenTo attacks
  - Workshop about ROSPenTo
  - Video: Hacking a simulated robot using ROSPenTo
- Part 2: SROS2
  - SROS2 introduction
  - ROS2 built on DDS
  - SROS2 tools
  - Workshop about SROS2

# Part 1:

## ROSPenTo

JOANNEUM RESEARCH ROBOTICS

# Outline

- Part 1: ROSPenTo
  - Introduction
  - User menu options
  - ROS publish/subscribe
  - ROSPenTo attacks
  - Workshop about ROSPenTo
  - Video: Hacking a simulated robot using ROSPenTo
- Part 2: SROS2
  - SROS2 introduction
  - ROS2 built on DDS
  - SROS2 tools
  - Workshop about SROS2

JOANNEUM RESEARCH ROBOTICS

# ROSPenTo introduction

Robot Operating System (ROS) penetration testing tool:

- Uses the ROS XMLRPC Master/Slave API to:
  - Analyse running ROS systems
  - Modify ROS topic communication flow
  - Isolate ROS services
  - Manipulate ROS parameters
  - Inject (malicious) data in ROS topic communication
- Is **not** build on top of ROS (source code of ROSPenTo is ROS independent)
- Implemented in C#
- GitHub: `https://github.com/jr-robotics/ROSPenTo`

# ROSPenTo user menu options

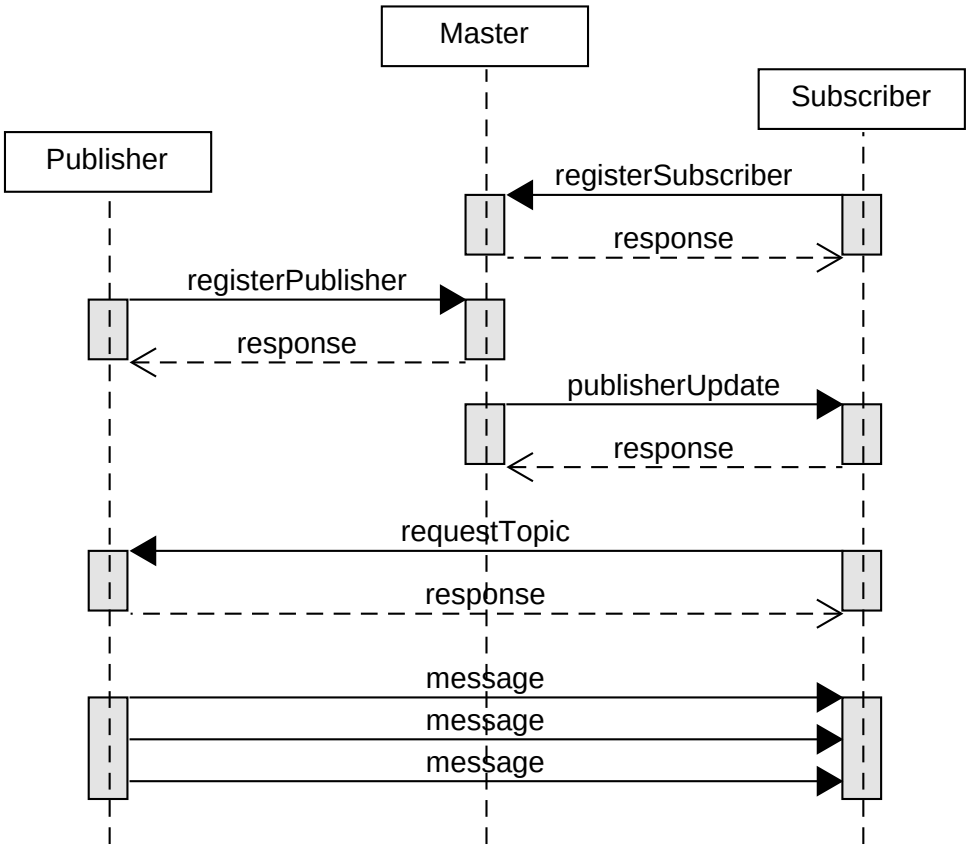
```
$ rospento

What do you want to do?
0: Exit
1: Analyse system...
2: Print all analyzed systems
3: Print information about analyzed system...
4: Print nodes of analyzed system...
5: Print node types of analyzed system (py or cpp)...
6: Print topics of analyzed system...
7: Print services of analyzed system...
8: Print communications of analyzed system...
9: Print communications of topic...
10: Print parameters...
11: Update publishers list of subscriber (add)...
12: Update publishers list of subscriber (set)...
13: Update publishers list of subscriber (remove)...
14: Isolate service...
15: Unsubscribe node from parameter (only C++)...
16: Update subscribed parameter at Node (only C++)...
```

ROSPenTo

- Console application
- Analyse system(s)
- Print system information
- Update publisher list
- Isolate service(s)
- Update parameters

# ROS publish/subscribe

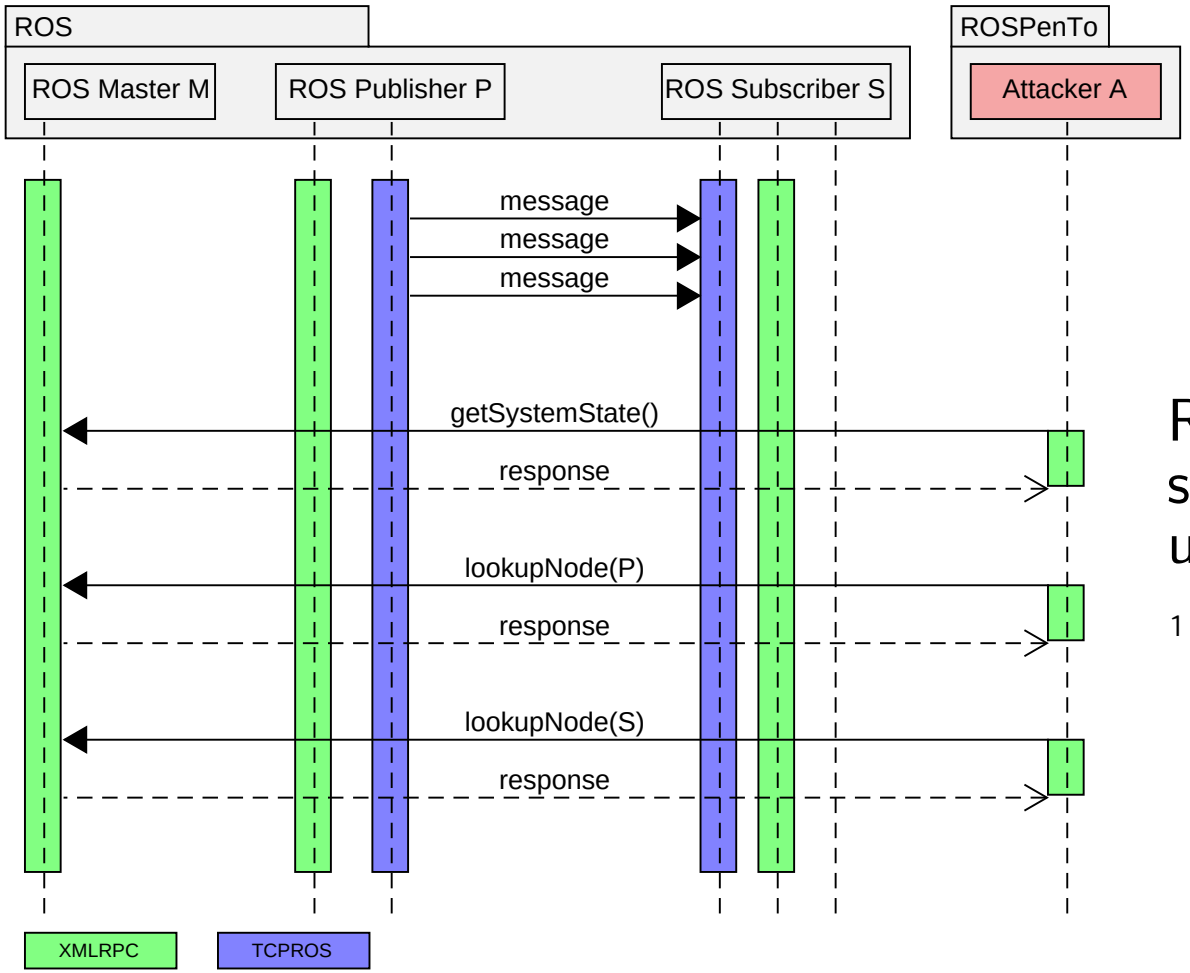



## ROS XMLRPC API [1]:

- *registerSubscriber*
  Subscribes the caller to the specified topic.
- *registerPublisher*
  Registers the caller as a publisher.
- *publisherUpdate*
  Updates current publisher list for topic.
- *requestTopic*
  Requests topic communication.
- etc.

[1] http://wiki.ros.org/ROS/Master_Slave_APIs

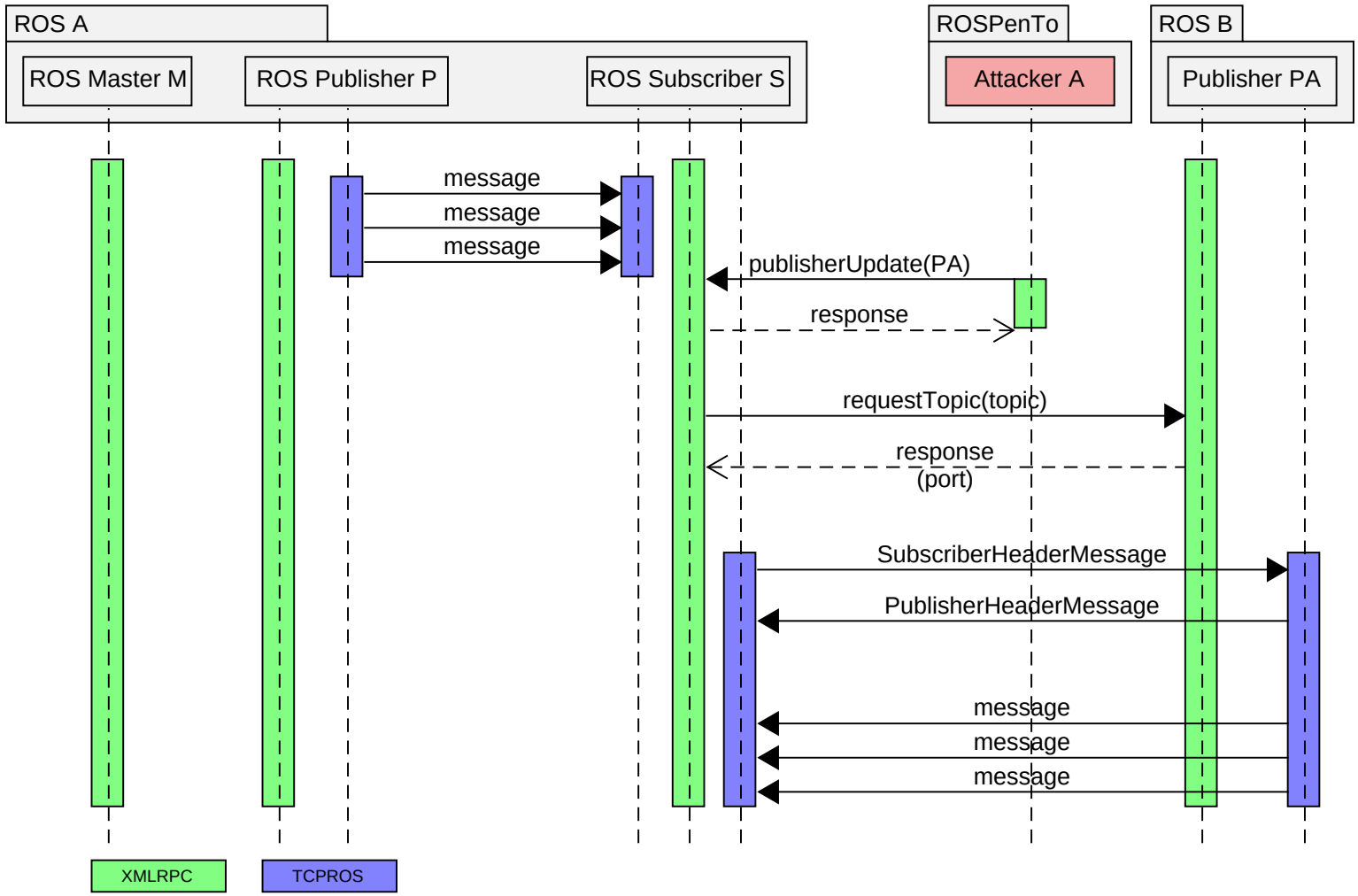
# ROSPenTo attack prerequisites



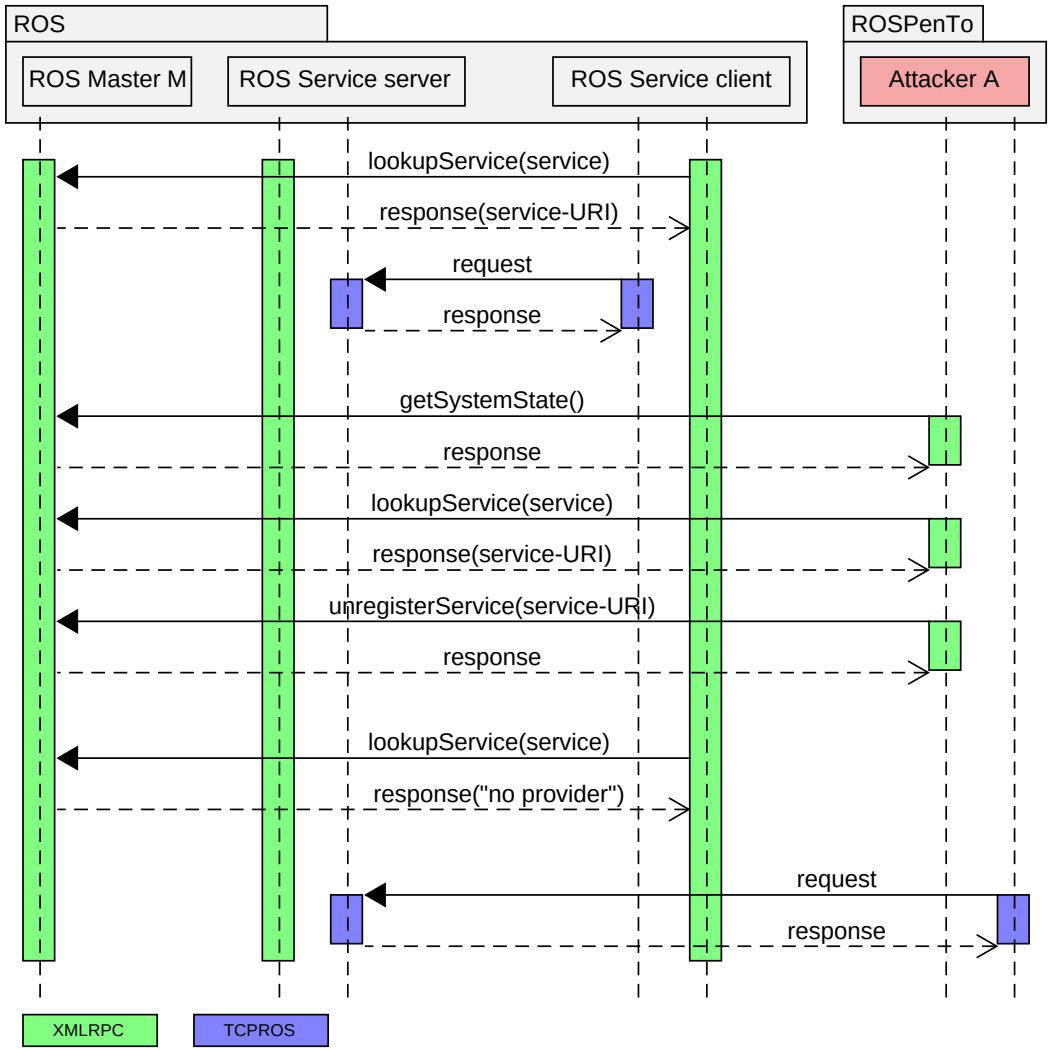

ROSPenTo performs this step (and others) in the user menu option 1:

```
1: Analyse system...
```

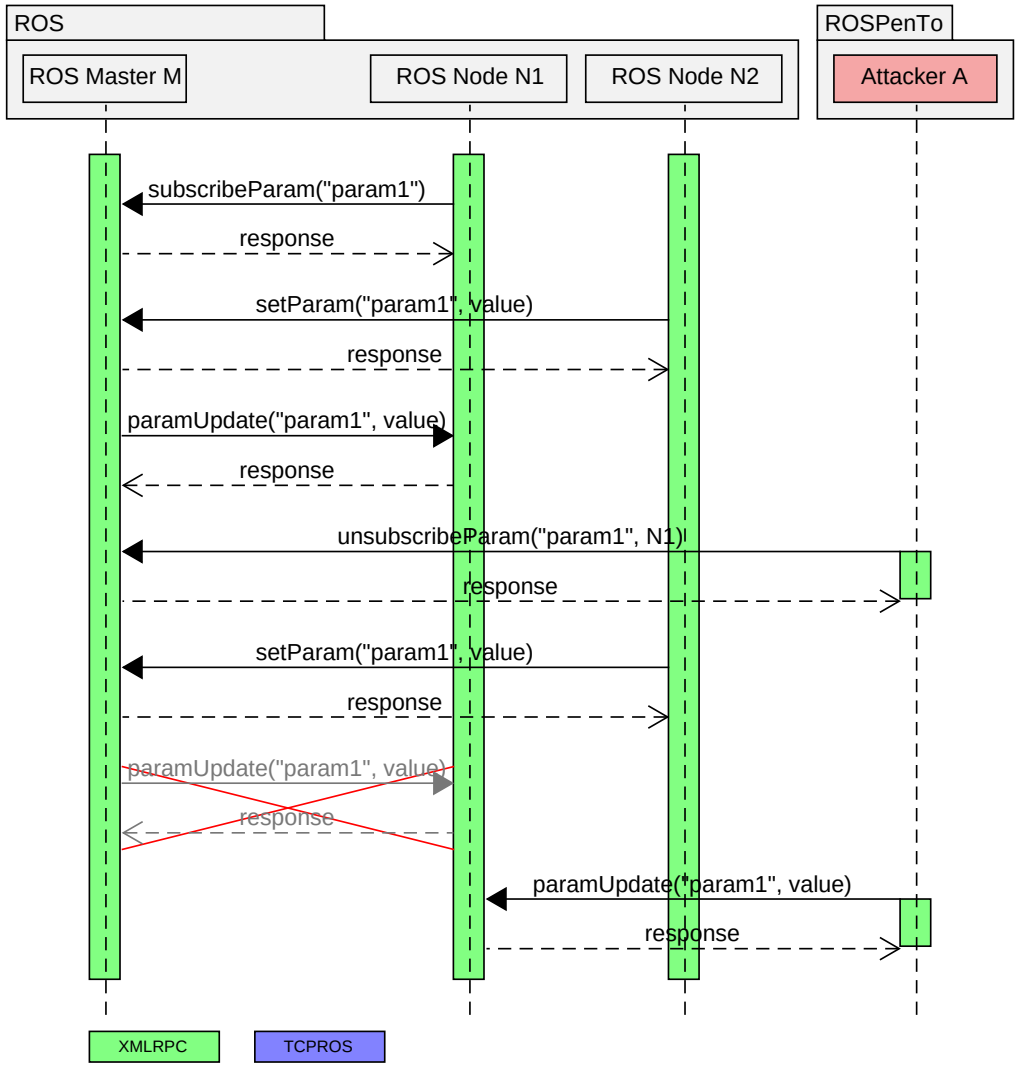
# ROSPenTo Stealth Publisher Attack



# ROSPenTo Service Isolation Attack



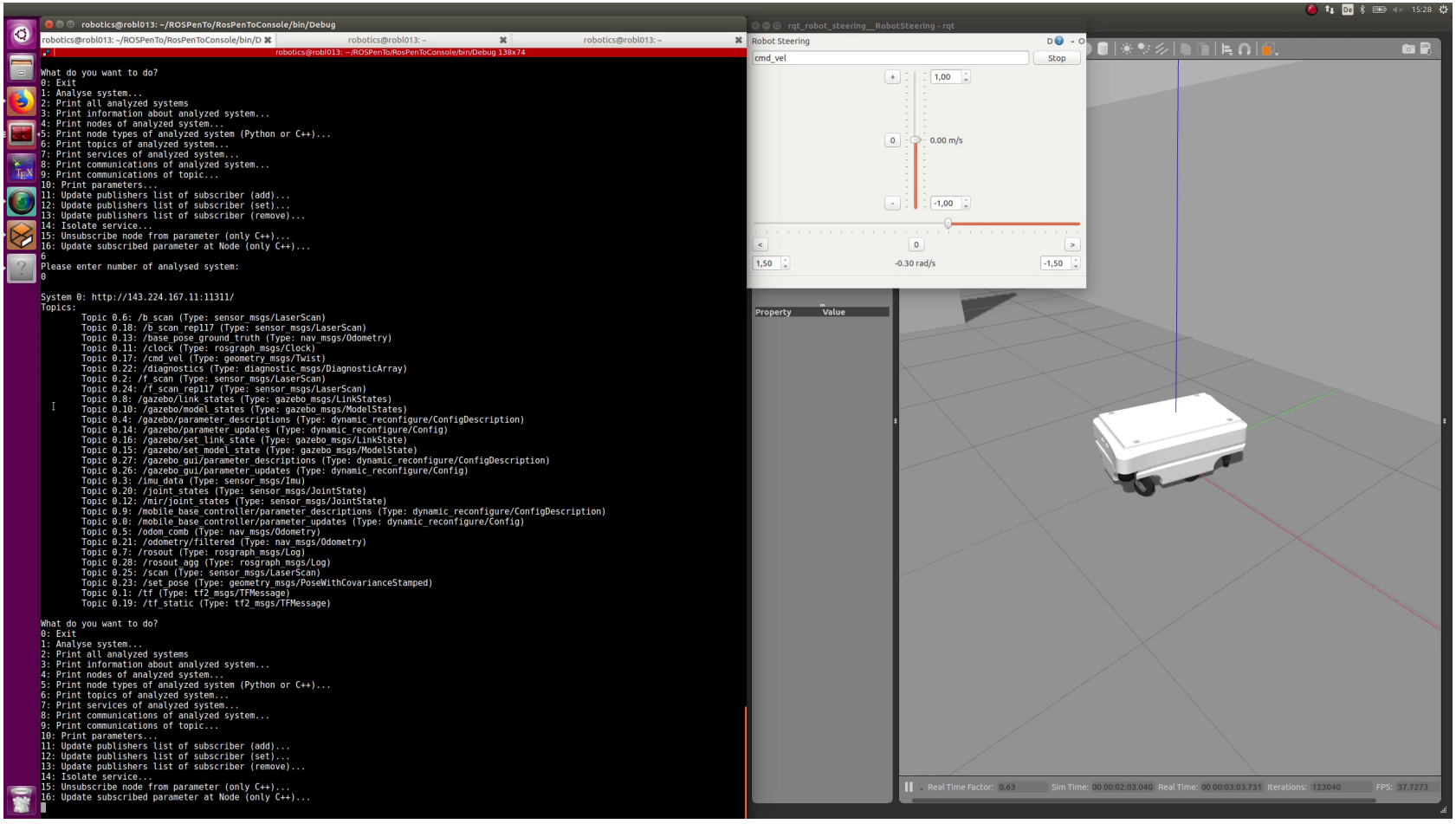
# ROSPenTo Parameter Update Attack



# ROSPenTo Workshop


https://github.com/jr-robotics/ROS-Industrial_EU_Fall19_Workshop

# Video: Hacking a simulated robot using ROSPenTo




https://vimeo.com/295958598

# Part 2:

## SROS2

JOANNEUM RESEARCH ROBOTICS

# Outline

- Part 1: ROSPenTo
  - Introduction
  - User menu options
  - ROS publish/subscribe
  - ROSPenTo attacks
  - Workshop about ROSPenTo
  - Video: Hacking a simulated robot using ROSPenTo
- Part 2: SROS2
  - SROS2 introduction
  - ROS2 built on DDS
  - SROS2 tools
  - Workshop about SROS2

## SROS2

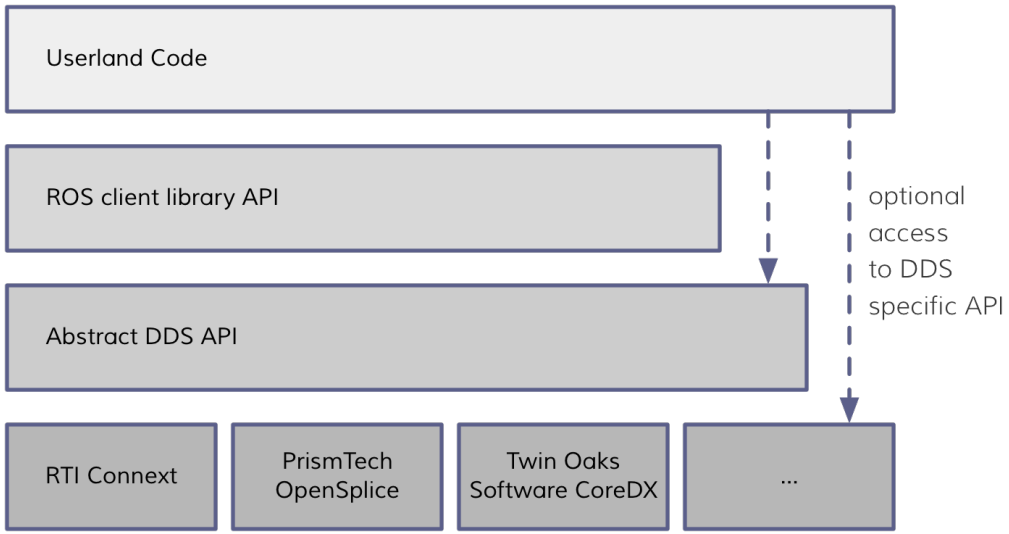
- provides tools to setup and configure a security infrastructure
- describes instructions on how to use SROS2 on top of DDS

```
$ ros2 --help

ros2 is an extensible command-line tool for ROS 2.

Commands:
action     Various action related sub-commands
component  Various component related sub-commands
daemon     Various daemon related sub-commands
launch     Run a launch file
lifecycle  Various lifecycle related sub-commands
msg        Various msg related sub-commands
multicast  Various multicast related sub-commands
node       Various node related sub-commands
param      Various param related sub-commands
pkg        Various package related sub-commands
run        Run a package specific executable
security   Various security related sub-commands
service    Various service related sub-commands
srv        Various srv related sub-commands
topic      Various topic related sub-commands
```

# ROS2 built on DDS



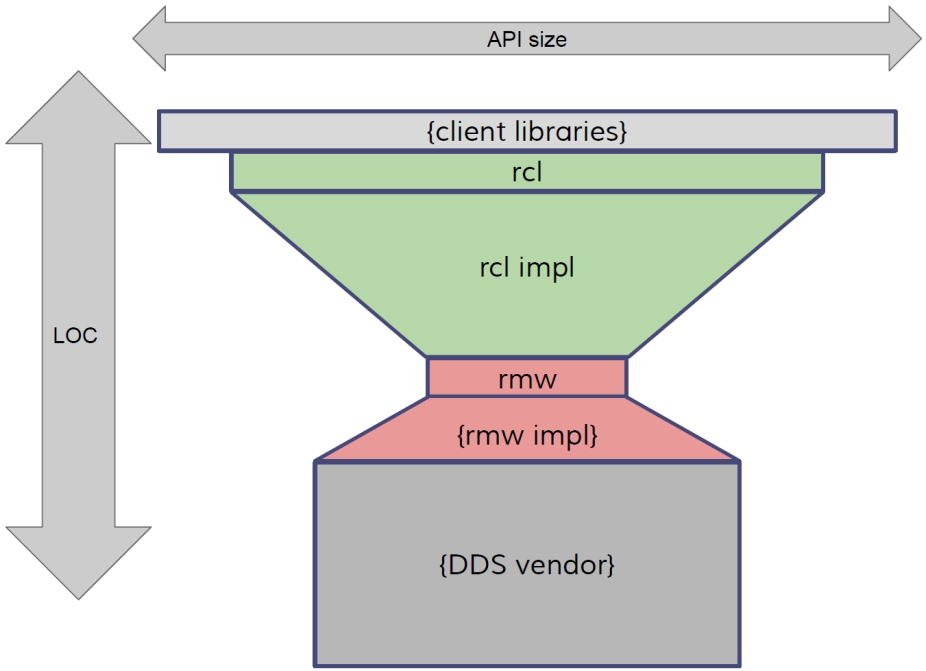

ROS2:

- Data Distribution Service (DDS)
- Replace ROS(1)'s TCPROS and UDPROS
- ROS2 hides DDS complexity

Source: Open Source Robotics Foundation (OSRF): ROS 2 Design

By William Woodall

# ROS2 API levels




ROS2 API levels:

- ROS Client Librarys:
  - rclcpp, rclpy, etc.
- Supported RMWs:
  - eProsima Fast RTPS
  - RTI Connext
  - ADLINK Opensplice
- Vendors:
  - eProsima
  - RTI
  - ADLINK Technologies

Source: Open Source Robotics Foundation (OSRF): ROSCon 2016 - ROS2 Update By Deanna Hood, William Woodall

# SROS2

## SROS2 tools

- Create keystore
- Create keys/certificates for each node
- Activate Access Control
- Enable secure communication

```
$ ros2 security --help

    Various security related sub-commands

    Commands:
    create_key           Create key
    create_keystore      Create keystore
    create_permission    Create permission
    distribute_key       Distribute key
    generate_artifacts   Generate keys and permission files
                         from a list of identities and policy files
    generate_policy      Generate XML policy file from ROS graph data
    list_keys            List keys

$ export ROS_SECURITY_ROOT_DIRECTORY=keystore
$ export ROS_SECURITY_ENABLE=true
$ export ROS_SECURITY_STRATEGY=Enforce
```

# SROS2 Workshop


https://github.com/jr-robotics/ROS-Industrial_EU_Fall19_Workshop

# The end

# Thank you for your attention!

Questions?

Sebastian Taurer

phone: +43 316 876 - 2011
fax: +43 316 8769 - 2011
mail: sebastian.taurer@joanneum.at