Security fundamentals and ROS security

Bernhard Dieber, Sebastian Taurer

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

01.10.2018
Table of contents

ROBOTICS

Security basics

ROS (in)security
  Attacks on ROS
  Videos

ROSPenTo Demonstration
Institute for Robotics and Mechatronics

- Founded 2015
- Focus on industrial robotics and mechatronics
- https://www.joanneum.at/robotics

- 45 researchers in 2021 in 3 groups
  - Mechatronic Systems
  - Robot Systems
  - Cognitive Robotics

[Taurer et al., 2018]
Cyber threats in robotics

- Classically, robots have worked in isolation
- Modern robots work in highly interconnected environments
- Industry-grade robots are not harmless machines
- Robots pose risks to property and life
- Insecure robots may be manipulated remotely
- Industrial security is breached frequently [Byres et al., 2004, Cheminod et al., 2013, Stouffer et al., 2015, Karnouskos, 2011, Nelson, 2016, Fairley, 2016]
CIA+: The security objectives

- **Confidentiality**
  - Only the intended recipients can read data
  - Hide the contents of messages from third-party observers
  - Enabled by: **Encryption**

- **Integrity**
  - Prevent data from being tampered/modified by a third party
  - Prevent spoofing/masquerading and the so called ”man in the middle” attacks
  - Enabled by: **Integrity checks, hashes**

- **Authenticity**
  - A given entity’s claimed identity can be proven
  - Enabled by: **Certificates, digital signatures**

- **Availability**
  - Ensure that the system is working within defined boundaries
CIA priorities

In production, the priorities are reversed compared to the classical office environment. Availability is key!

<table>
<thead>
<tr>
<th>Prio</th>
<th>Office environment</th>
<th>Production environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Confidentiality</td>
<td>Availability</td>
</tr>
<tr>
<td>2</td>
<td>Integrity</td>
<td>Integrity</td>
</tr>
<tr>
<td>3</td>
<td>Availability</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>
ROS1 security issues

- ROS has no built-in security [McClean et al., 2013]
- Missing authentication, authorization and confidentiality functions
- ROS is an easy target
  - Exploit XMLRPC-API
  - Use stealth publisher attack to inject data or isolate subscribers
  - Use service isolation for DoS
  - Use malicious parameter attack to manipulate parametrization for individual nodes
Master API

- XMLRPC API to interact with ROS master
- Enables discovering publishers and services
- `getSystemState` → get overview of whole network
- `lookupNode` → get URI of specific node
- `lookupService` → get URI of specific service
- `register{Subscriber,Publisher}` → subscribe, advertise
- `unregister{Subscriber,Publisher}` → unsubscribe, unadvertise
- **No authentication/authorization**
Node API

- Communication mainly node2node (some Master→Node calls)
- `publisherUpdate` → send update on available publishers
- `requestTopic` → perform subscription
- `paramUpdate` → send new parameter server values
- `shutdown` → kill node
- **No authentication/authorization**
- After XMLRPC-handshake, topic communication is done using a binary wire protocol (unencrypted)
Communication structure in ROS

1. registerPublisher
2. registerSubscriber
3. requestTopic
4. Exchange TCPROS-Header
5. Topic-Messages
Phase 1 Prepare attack

getSystemState, caller_id

[1, statusMessage, [ [topic, [P]] [topic, [S]] [] ]]

lookupNode, caller_id, S

[1, statusMessage, sURI]

lookupNode, caller_id, P

[1, statusMessage, pURI]

Figure: Sequence diagram of a Stealth Publisher Attack
Phase 2 Run attack

`publisherUpdate, "/master", topic, [aURI]`

`requestTopic, S, topic, "TCPROS"

`requestTopic, S, topic, "TCPROS"

`[1, statusMessage, 0]`

`[1, statusMessage, ["TCPROS", pHost, pPort]]`

`[1, statusMessage, ["TCPROS", aHost, aPort]]`

TCPROS header hS

TCPROS header hS

TCPROS header hP

TCPROS header hP

Topic message
getSystemState, "caller"

lookupService, "caller", service

unregisterService, S, service, service-URI

lookupService, C, service

TCPROS-Header

TCPROS-Header

Service-Request

Service-Response

Figure: Sequence diagram of a Service Isolation Attack
subscribeParam, caller_id, nURI, "param1"

getParam, caller_id, paramKey

lookupNode, caller_id, N

unsubscribeParam, N, nURI, paramKey

paramUpdate, "/master", paramKey, newValue

Figure: Sequence diagram of a malicious parameter update attack
Some Videos

- Disabling safety functions
- Disturbing a MiR robot
ROSPenTo

- Penetration testing tool for ROS
- https://github.com/jr-robotics/ROSPenTo
- Analyze multiple ROS networks
- Reroute communication
- Isolate services
- Manipulate parameters
- Alternative: roschaos
- Countermeasures: [Dieber et al., 2017, White et al., 2016], http://secure-ros.csl.sri.com/
- Video
The myths and facts behind cyber security risks for industrial control systems.
In In Proc. of VDE Kongress.

Review of security issues in industrial networks.
*Industrial Informatics, IEEE Transactions on*, 9(1), 277–293.

Security for the robot operating system.

Cybersecurity at u.s. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [news].

Stuxnet worm impact on industrial cyber-physical system security.
In 37th Annual Conference of the IEEE Industrial Electronics Society *(IECON 2011)* (pp. 4490–4494).

A preliminary cyber-physical security assessment of the robot operating system (ros).
In *Proc. SPIE*, volume 8741 (pp. 874110–874110–8).

