Robot Security – Challenges and Opportunities

Joanneum Zukunftskonferenz

09.03.2016

Stefan Rass
Associate Professor @ Universität Klagenfurt
Institute of Applied Informatics – System Security
stefan.rass@aau.at

Agenda

- Why bother with security?
- Security in the Robot Operating System (ROS)
- How (easy) security enhancements can/could be implemented
- Where security can(not) be added „on top“

Security – Why Bother?

- Newly evolving vulnerabilities in industrial control networks
  - Internet of Things
  - Teleworking / remote access
  - Cloud computing
  - Bring your own device
  - …
- Several successful attacks have been reported (not always officially)
  - Stuxnet
  - Jeep hack
  - Robots manipulated to put less welding points
  - …

Security in ROS

- Actually: not part of the design so far – many vulnerabilities*
- Message transmission between talker and listener on different topics (publish/subscribe model)
  - Logging ✓
  - no authentication → malicious talkers can fiddle with the system
    injection of messages (person-in-the-middle)
    → „replacements“ of existing talkers/listeners is most trivial
  - no encryption → unauthorized listeners can gather information

* D.D. Mascarenas, J. McClean, C.J. Stull, C.R. Farrar: *Preliminary Cyber-Physical Security Assessment of the Robot Operating System (ROS)*, Los Alamos National Laboratory, Report LA-UR-13-23117, 2013.

Security Enhancements

- Authentication of talkers/listeners
  - Registration: challenge-response authentication of legitimate components (use certificates)
  - Sending messages: mandatory digital signature
  - Receiving messages: reject if not signed or signature invalid
- Confidentiality
  - use topic-key shared between all talkers/listeners
  - illegitimate talkers cannot produce „understandable“ messages
  - illegitimate listeners won‘t understand what others talk about
- Accountability: investigate log files → find cause of malfunctions

Security – Inherently or „on top“?

- Several things can be done on the application layer (→ „on top“)
  - Authentication
  - Encryption
- Other things, like
  - preventing to sublet identities (keys)
  - impersonation / replacement of legitimate components
  - denial-of-service attacks
  - …

cannot be prevented without either

- applying changes to ROS
- using hardware security

} → „inherently“

Outlook

- ROS has serious design issues related to security
- Some issues can be settled on the application level
- Comprehensive security requires changes to the operating system
  $\rightarrow$ ongoing and future work

- Join forces and expertises!
  (robot experts + security people $\Rightarrow$ safe & secure industrial control applications)

Discussion is open…

Robot Security – Challenges and Opportunities

Joanneum Zukunftskonferenz

09.03.2016

Stefan Rass
Associate Professor @ Universität Klagenfurt
Institute of Applied Informatics – System Security
stefan.rass@aau.at