Security fundamentals and ROS security

Bernhard Dieber, Sebastian Taurer

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

01.10.2018

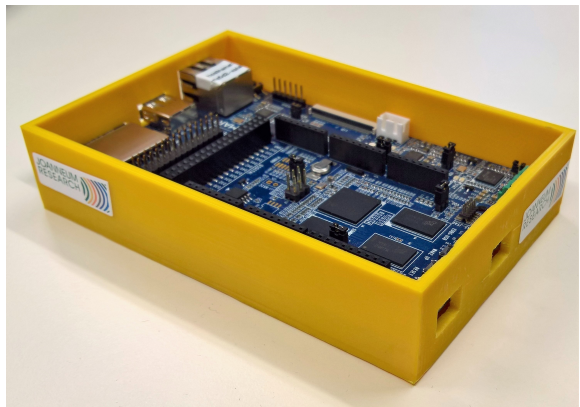
JOANNEUM RESEARCH ROBOTICS

Table of contents

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!

Prio	**Office environment**	**Production environment**
1	Confidentiality	Availability
2	Integrity	Integrity
3	Availability	Confidentiality

JOANNEUM RESEARCH ROBOTICS

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

JOANNEUM RESEARCH ROBOTICS

Master API[1]

- 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**

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

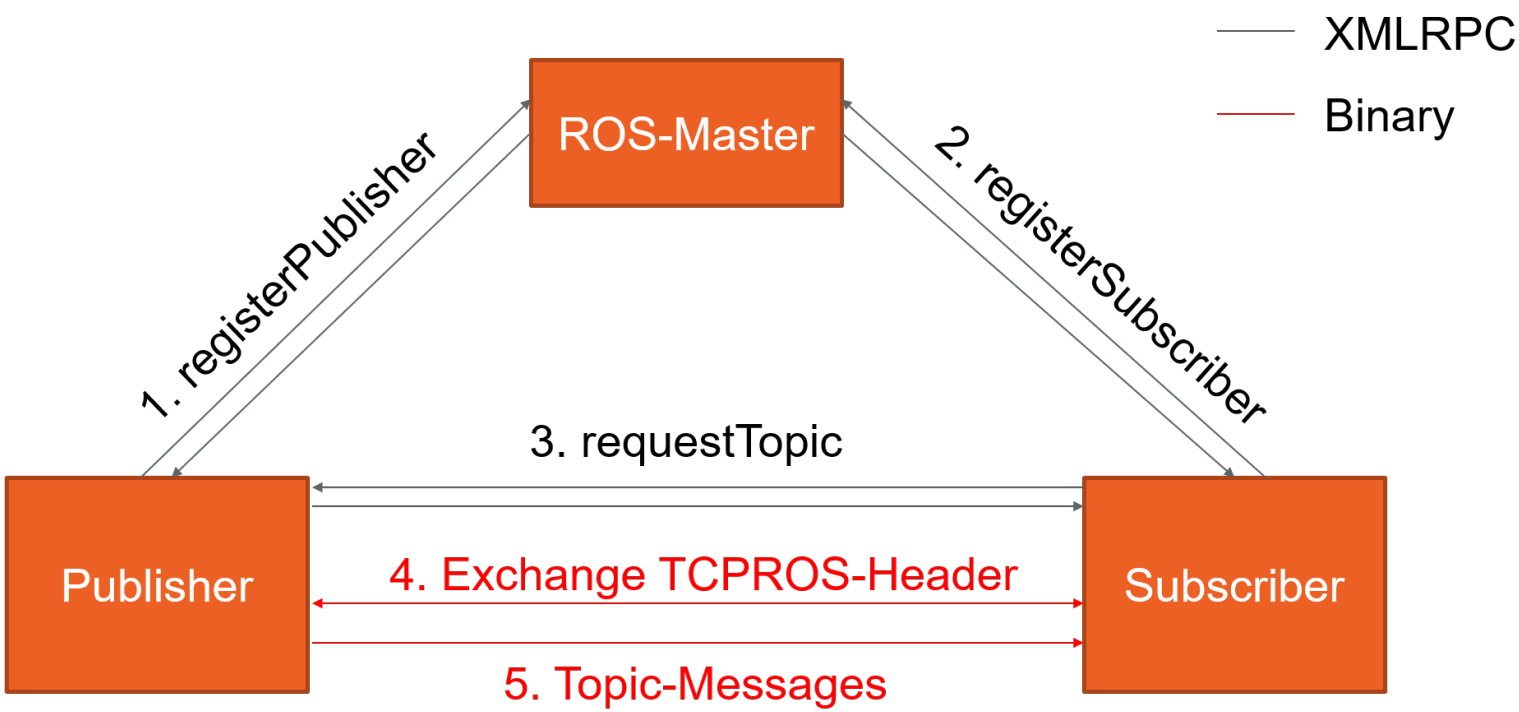
JOANNEUM RESEARCH ROBOTICS

Node API[2]

- Communication mainly node2node (some Master→Node calls)
- *publisherUpdate* → send update on available publisers
- *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)

[2] http://wiki.ros.org/ROS/Slave_API

Communication structure in ROS



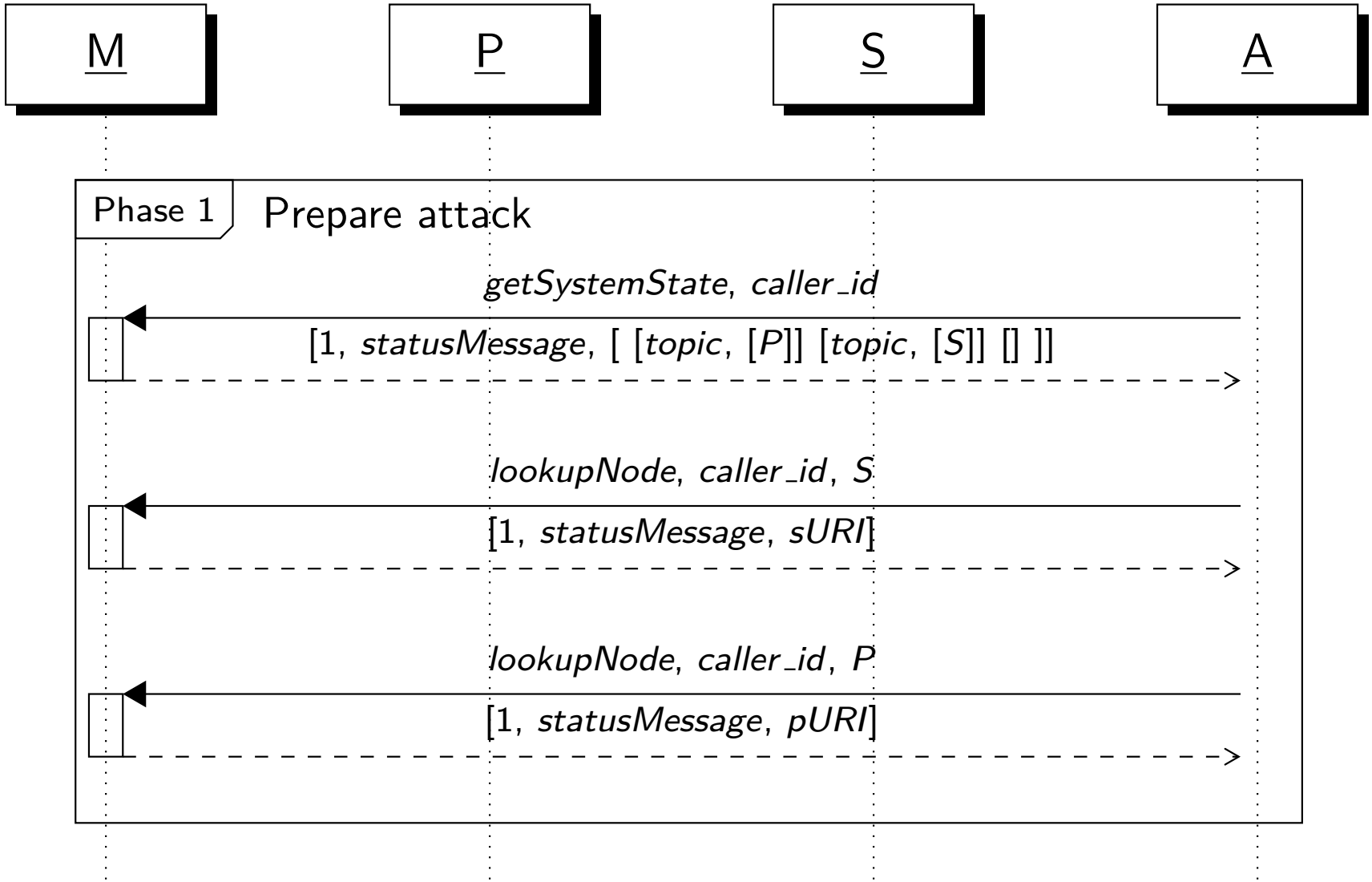
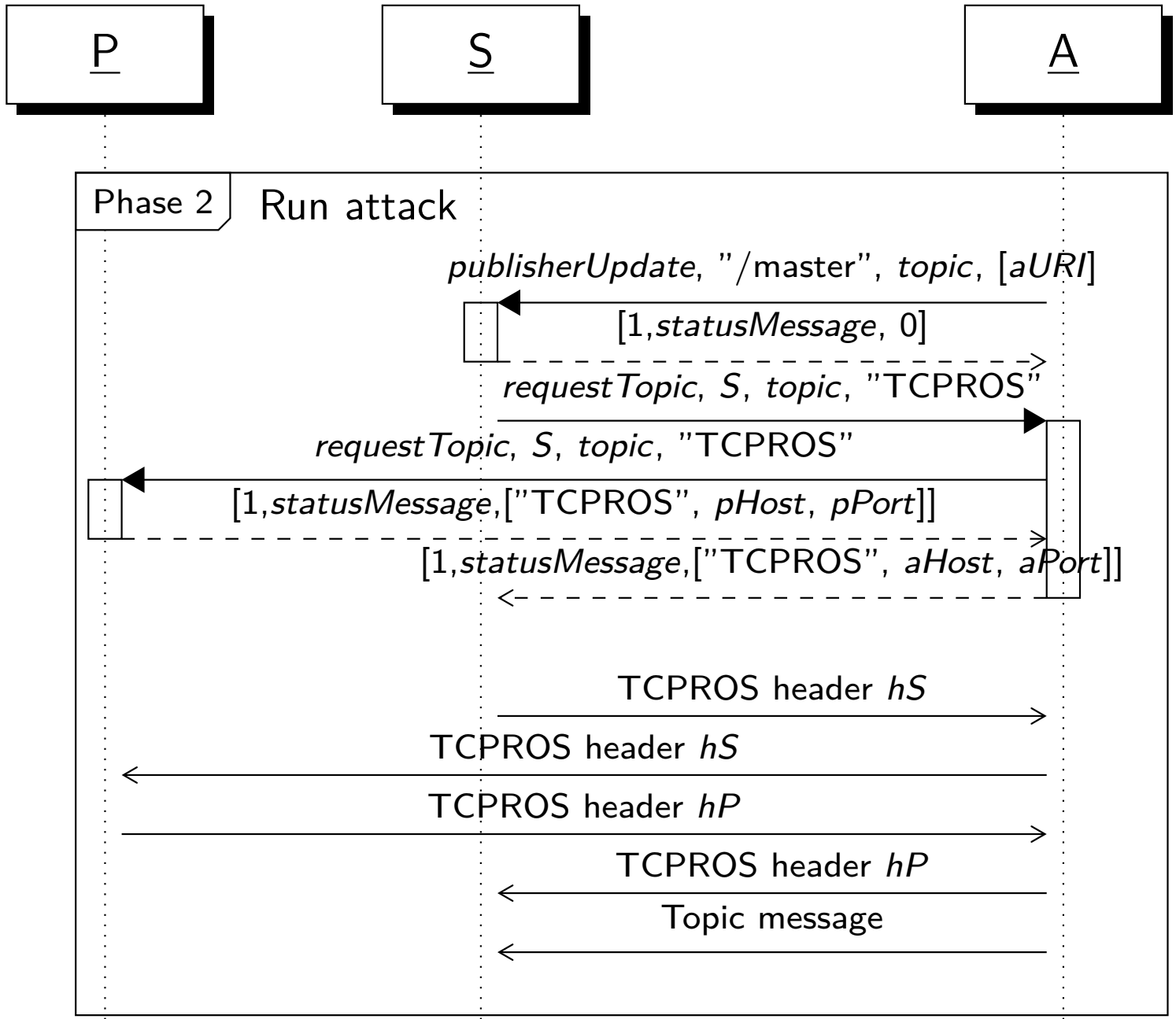


Figure: Sequence diagram of a Stealth Publisher Attack


P
S
A
Phase 2
Run attack
publisherUpdate, "/master", topic, [aURI]
[1,statusMessage, 0]
requestTopic, S, topic, "TCPROS"
requestTopic, S, topic, "TCPROS"
[1,statusMessage,["TCPROS", pHost, pPort]]
[1,statusMessage,["TCPROS", aHost, aPort]]
TCPROS header hS
TCPROS header hS
TCPROS header hP
TCPROS header hP
Topic message

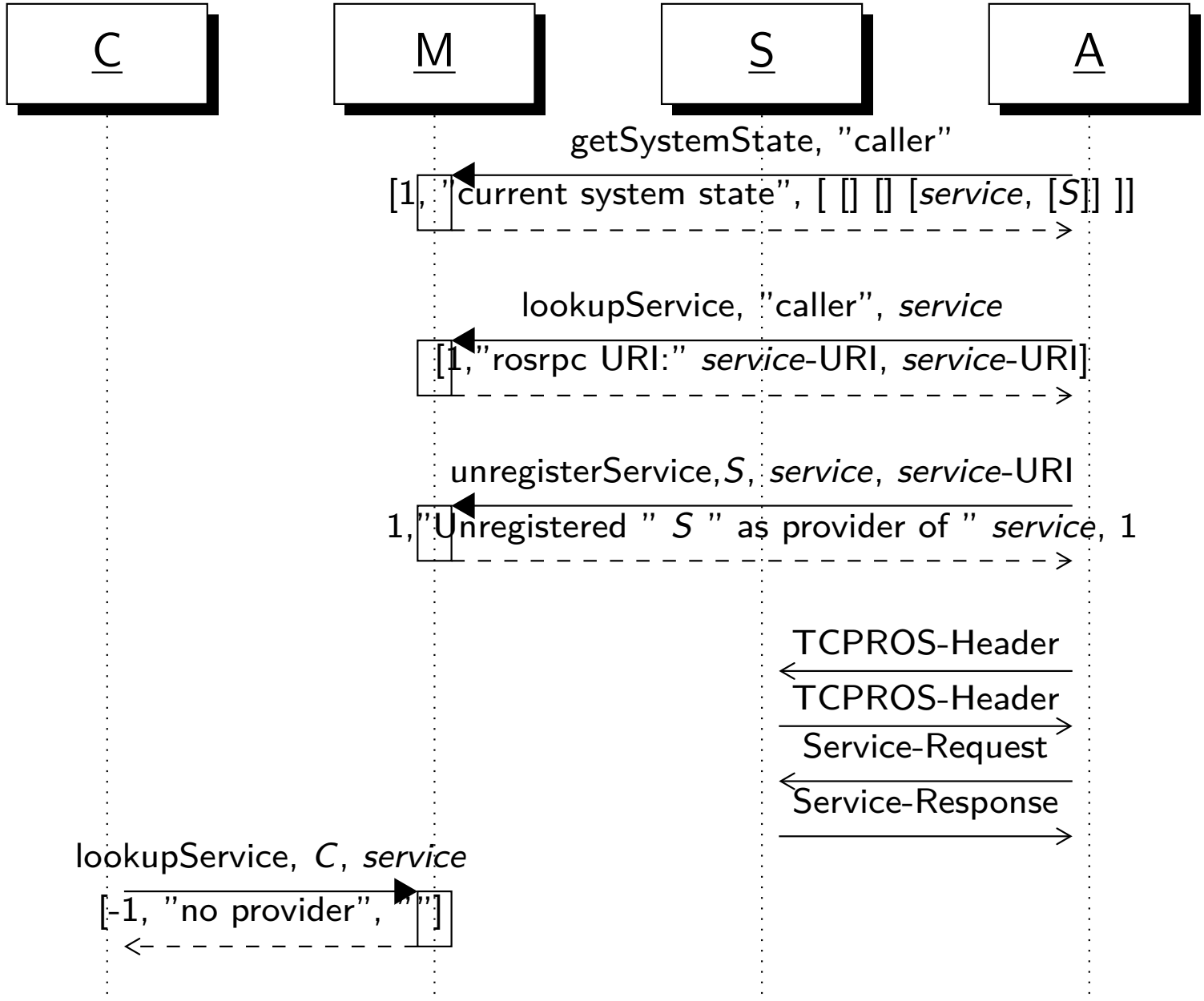


Figure: Sequence diagram of a Service Isolation Attack

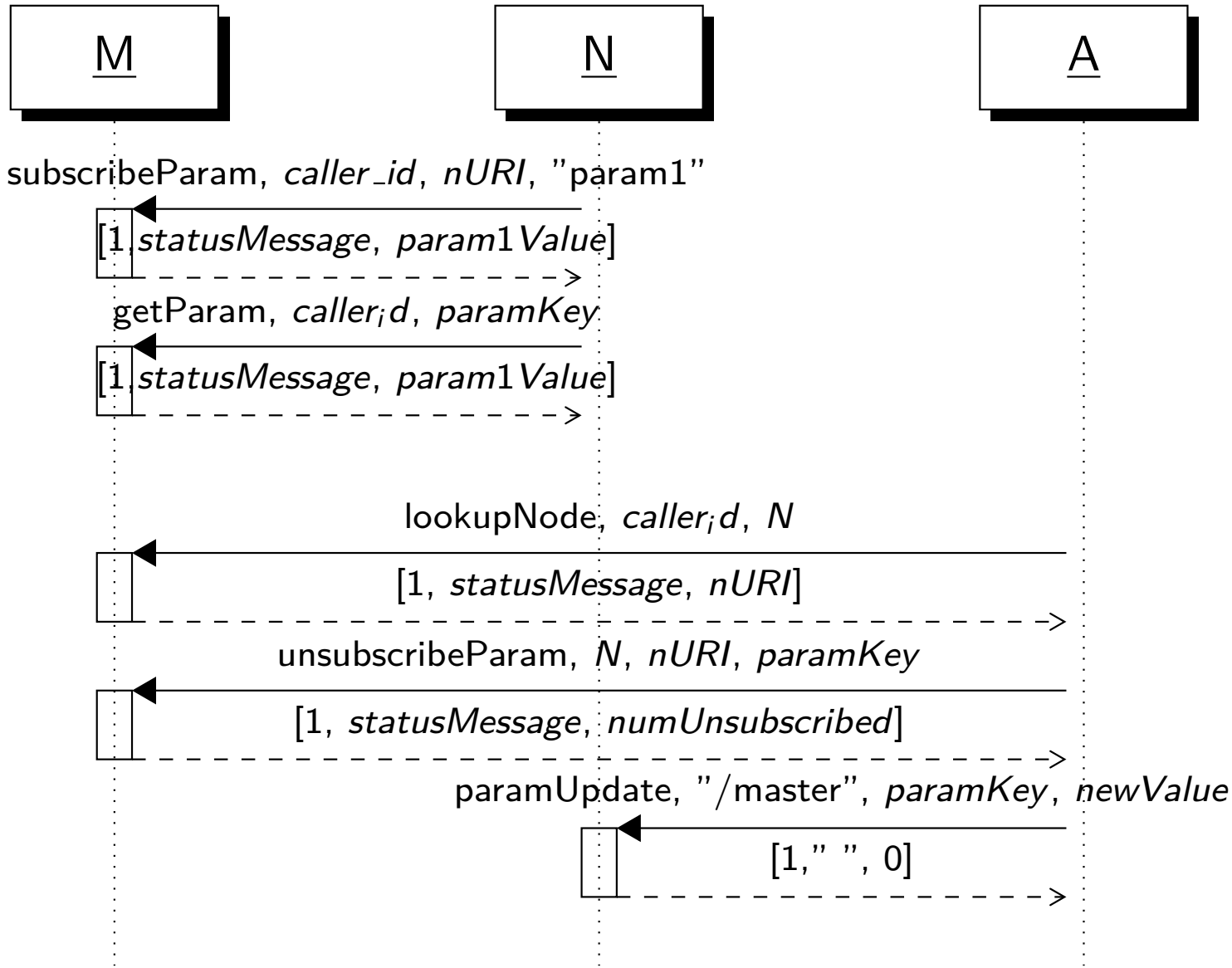


Figure: Sequence diagram of a malicious parameter update attack

JOANNEUM RESEARCH ROBOTICS

Some Videos

- Disabling safety functions
- Disturbing a MiR robot

JOANNEUM RESEARCH ROBOTICS

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

JOANNEUM RESEARCH ROBOTICS

References I

Byres, E., Dr, P. E., & Hoffman, D. (2004).
The myths and facts behind cyber security risks for industrial control systems.
In *In Proc. of VDE Kongress*.

Cheminod, M., Durante, L., & Valenzano, A. (2013).
Review of security issues in industrial networks.
Industrial Informatics, IEEE Transactions on, 9(1), 277–293.

Dieber, B., Breiling, B., Taurer, S., Kacianka, S., Rass, S., & Schartner, P. (2017).
Security for the robot operating system.
Robotics and Autonomous Systems, 98, 192–203.

Fairley, P. (2016).
Cybersecurity at u.s. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory [news].
IEEE Spectrum, 53(5), 11–13.

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

McClean, J., Stull, C., Farrar, C., & MascareÃśas, D. (2013).
A preliminary cyber-physical security assessment of the robot operating system (ros).
In *Proc. SPIE*, volume 8741 (pp. 874110–874110–8).

JOANNEUM RESEARCH ROBOTICS

References II

Nelson, N. (2016).

The Impact of Dragonfly Malware on Industrial Control Systems.
Technical report, SANS Institute.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015).

Guide to Industrial Control Systems (ICS) Security.
Technical report, National Institute of Standards and Technology.
NIST Special Publication 800-82, Revision 2.

Taurer, S., Dieber, B., & Schartner, P. (2018).

Secure data recording and bio-inspired functional integrity for intelligent robots.
In *Proceedings of the 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2018)*.

White, R., Christensen, H., & Quigley, M. (2016).

Sros: Securing ros over the wire, in the graph, and through the kernel.
In *Proceedings of the IEEE-RAS International Conference on Humanoid Robots (HUMANOIDS)*.