UNIVERSITY OF GOTHENBURG

CHALMERS UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

CHALMERS

UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

CHALMERS UNIVERSITY OF TECHNOLOGY

Developers’ Needs for Software Supply Chain Tooling: Insights from an Interview Study

Raffaela Groner

Postdoctoral researcher

Modeling and Analyzing Non-Functional Properties:

- Safety
- Security
- Performance

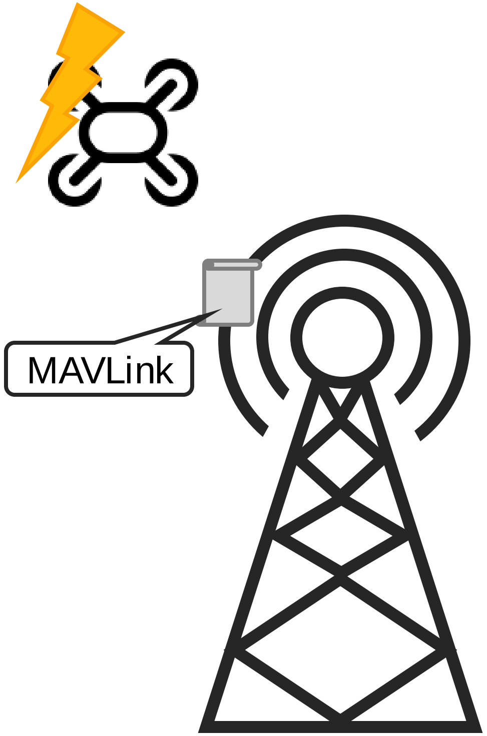
Research Areas:

- Self-Adaptive Systems
- Model Transformations

Safety & Security of Self-Adaptive Systems

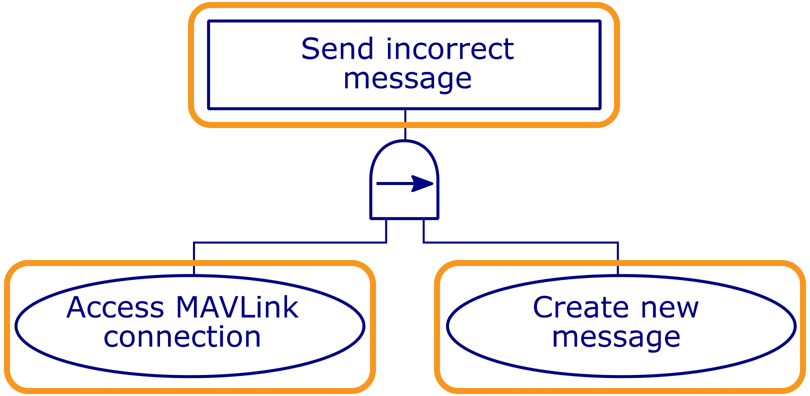
Joint work with Thomas Witte, Alexander Raschke, Irdin Pekaric, Jubril Adigun, Michael

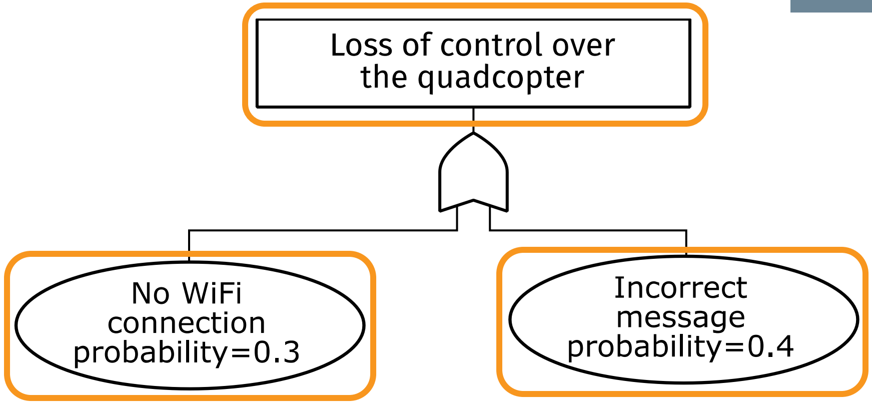
- I. Pekaric, M. Frick, J. G. Adigun, **R. Groner**, T. Witte, A. Raschke, M. Felderer, and M. Tichy, “Streamlining attack tree generation: A fragment-based approach,” in *Proceedings of the 57th Hawaii International Conference on Social Systems*, ser. HICSS-57, 2024.
- **R. Groner**, T. Witte, A. Raschke, S. Hirn, I. Pekaric, M. Frick, M. Tichy, and M. Felderer, “Model-based generation of attack-fault trees,” in *Computer Safety, Reliability, and Security*, 2023.
- I. Pekaric, **R. Groner**, T. Witte, J. G. Adigun, A. Raschke, M. Felderer, and M. Tichy, “A systematic review on security and safety of self-adaptive systems,” *Journal of Systems and Software*, vol. 203, 2023.
- T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022.



MAVLink

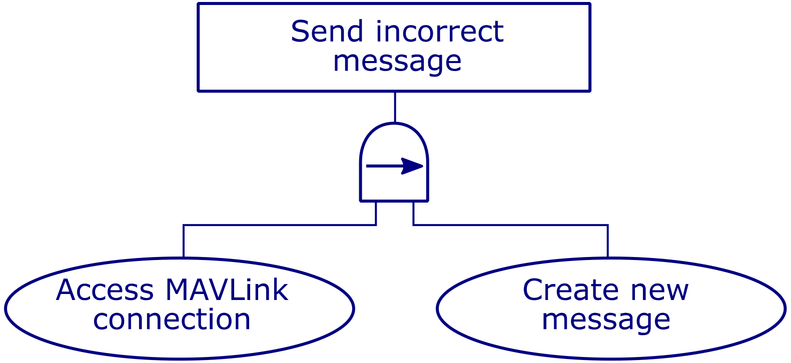
Ground Control Station (GCS)




Loss of control over the quadcopter
No WiFi connection probability=0.3
Incorrect message probability=0.4

[1]

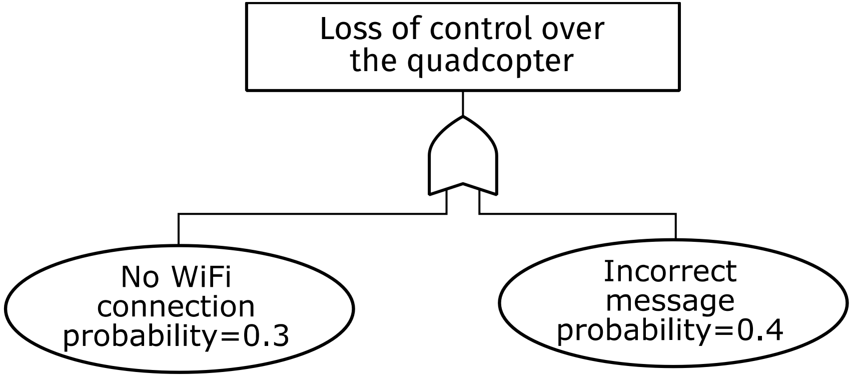
[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)



Send incorrect message

Access MAVLink connection

Create new message



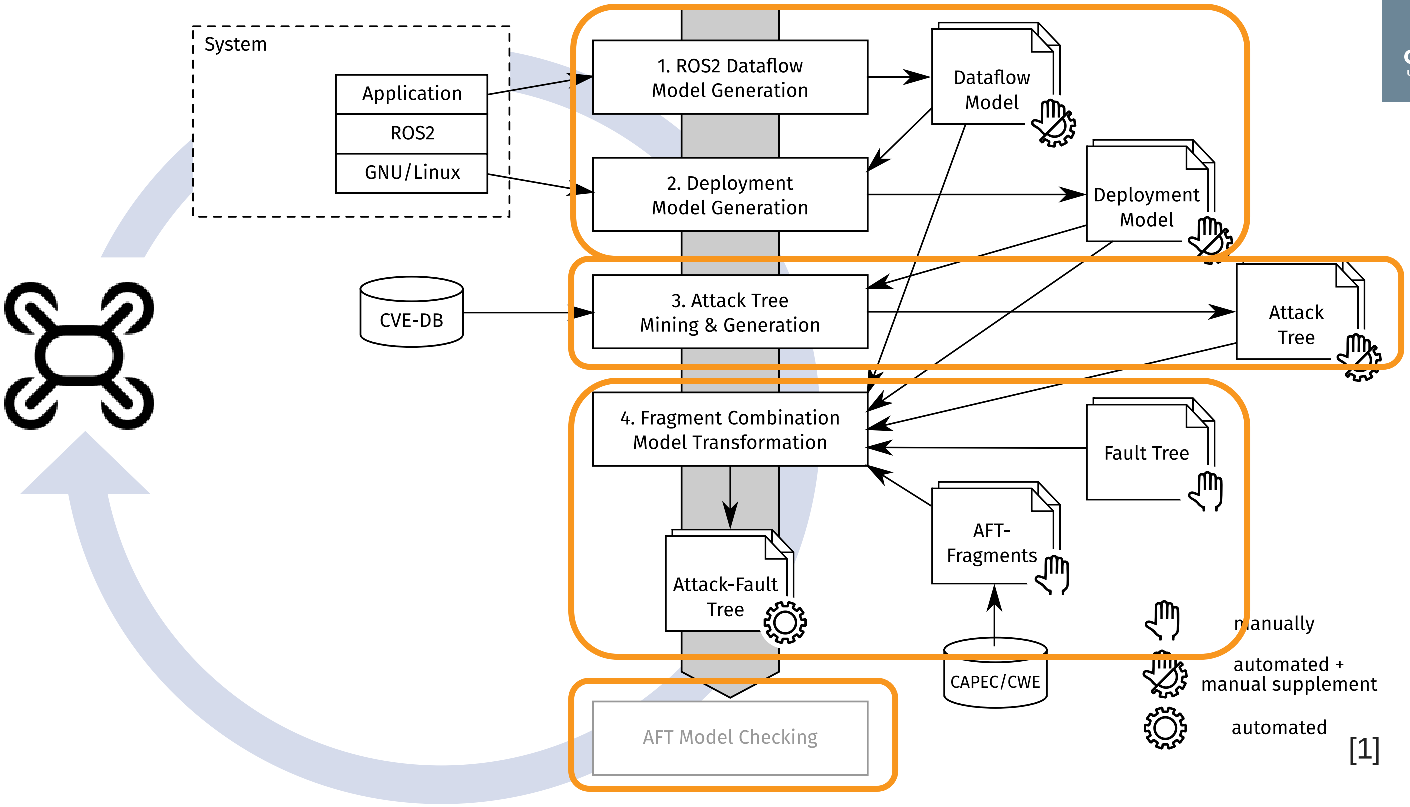
Loss of control over the quadcopter

No WiFi connection probability=0.3

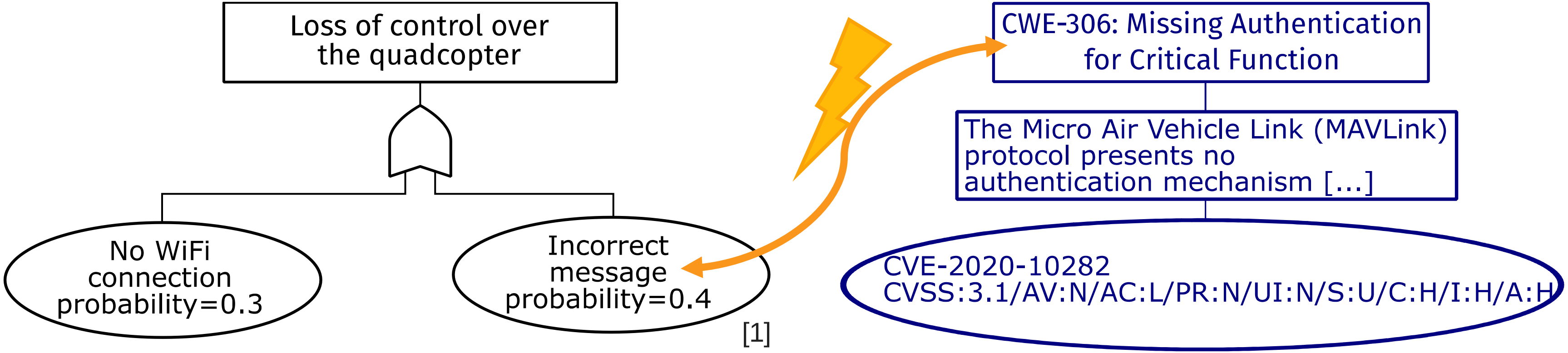
Incorrect message probability=0.4

[1]

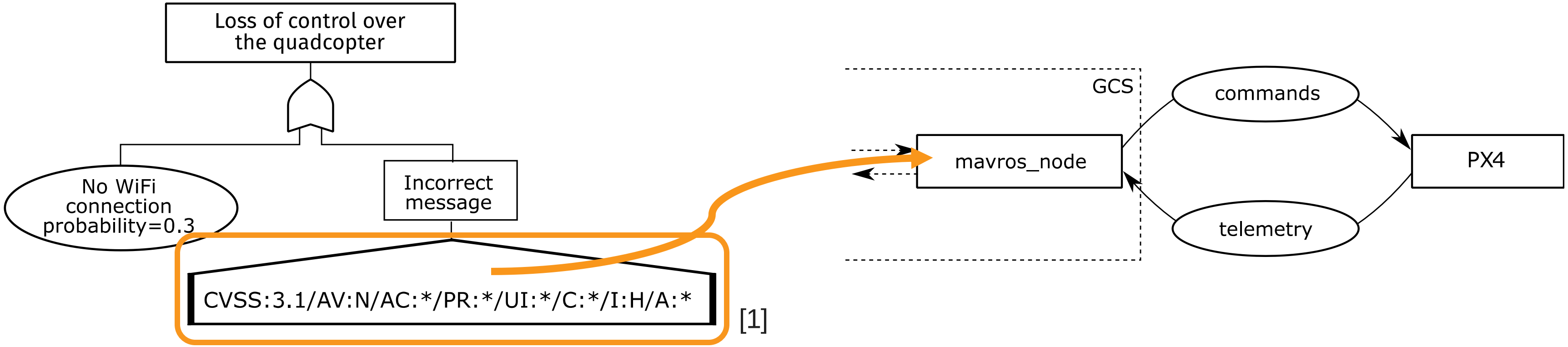
[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)


System
Application
ROS2
GNU/Linux
CVE-DB
1. ROS2 Dataflow Model Generation
2. Deployment Model Generation
3. Attack Tree Mining & Generation
4. Fragment Combination Model Transformation
AFT Model Checking
Dataflow Model
Deployment Model
Attack Tree
Fault Tree
AFT-Fragments
Attack-Fault Tree
CAPEC/CWE
manually
automated + manual supplement
automated
[1]

[1] R. Groner, T. Witte, A. Raschke, S. Hirn, I. Pekaric, M. Frick, M. Tichy, and M. Felderer, “Model-based generation of attack-fault trees,” in *Computer Safety, Reliability, and Security*, 2023.


Loss of control over the quadcopter
No WiFi connection probability=0.3
Incorrect message probability=0.4
[1]
CWE-306: Missing Authentication for Critical Function
The Micro Air Vehicle Link (MAVLink) protocol presents no authentication mechanism [...]
CVE-2020-10282
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

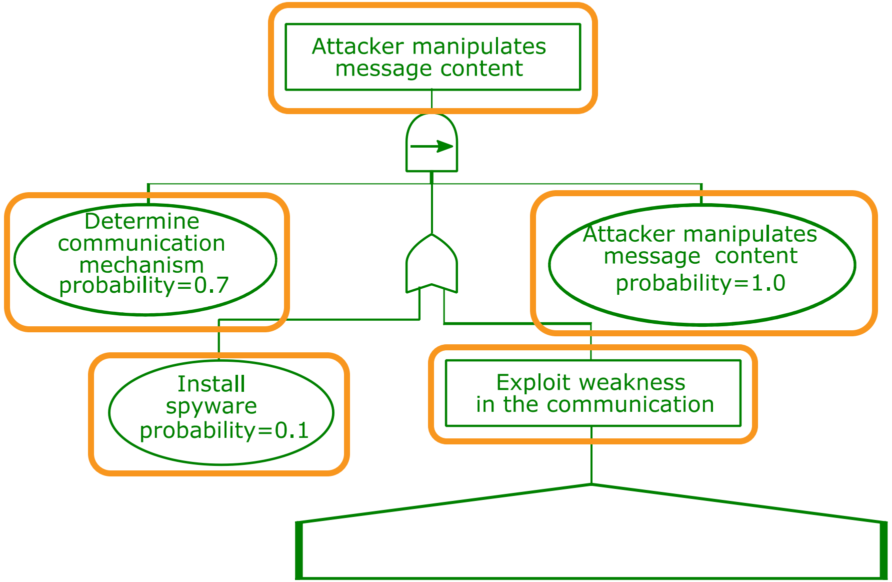
[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)

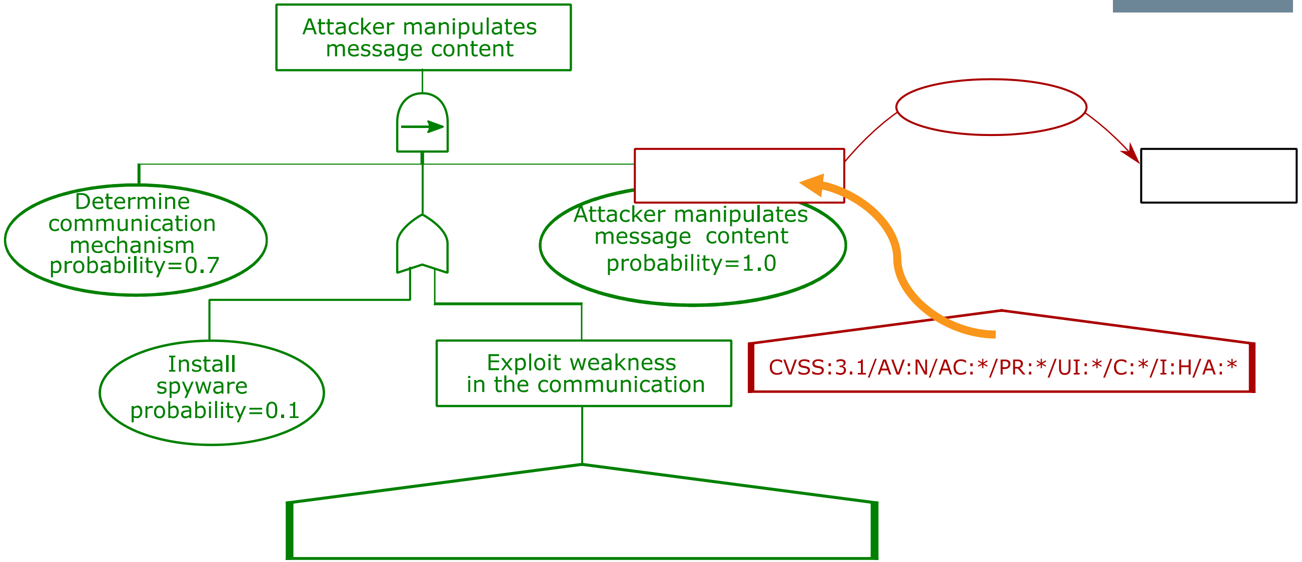

Loss of control over the quadcopter
No WiFi connection probability=0.3
Incorrect message
CVSS:3.1/AV:N/AC:*/PR:*/UI:*/C:*/I:H/A:*
GCS
mavros_node
commands
telemetry
PX4

[1]

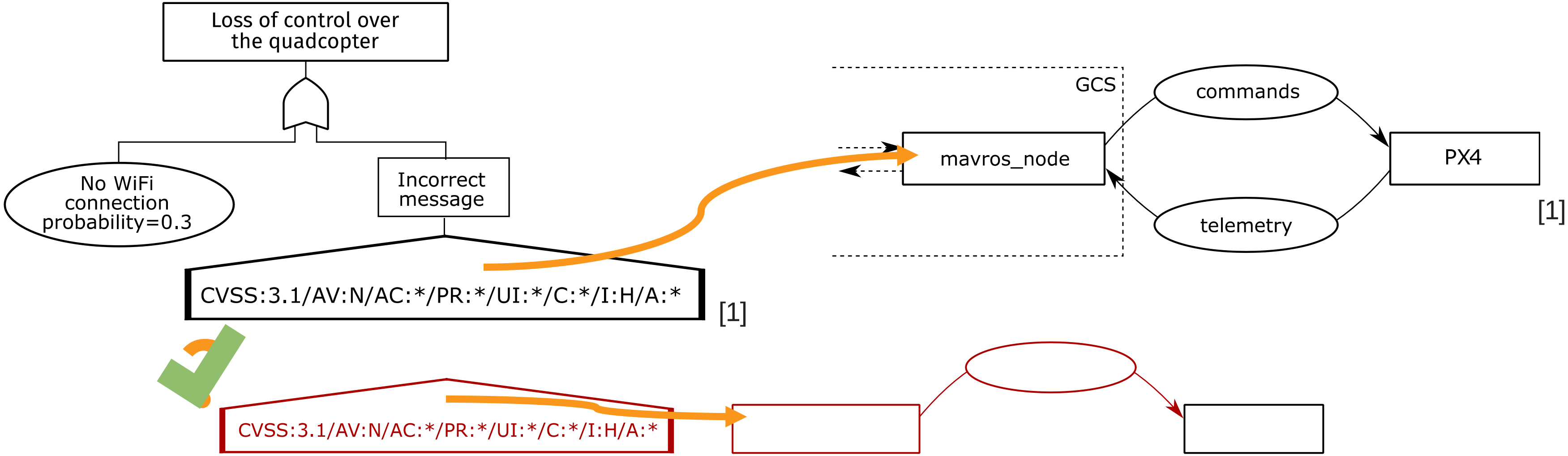
[1]

[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)

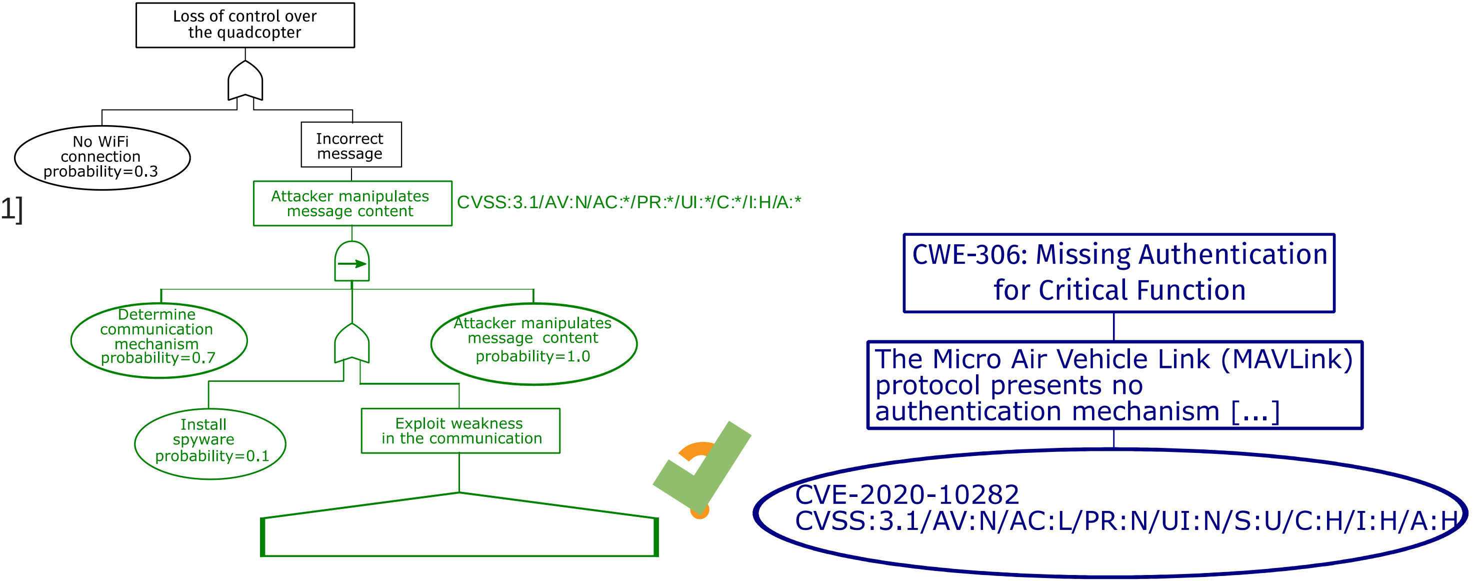

Attacker manipulates message content
Determine communication mechanism probability=0.7
Attacker manipulates message content probability=1.0
Install spyware probability=0.1
Exploit weakness in the communication



Attacker manipulates message content
Determine communication mechanism probability=0.7
Attacker manipulates message content probability=1.0
Install spyware probability=0.1
Exploit weakness in the communication
CVSS:3.1/AV:N/AC:*/PR:*/UI:*/C:*/I:H/A:*


Loss of control over the quadcopter
No WiFi connection probability=0.3
Incorrect message
CVSS:3.1/AV:N/AC:*/PR:*/UI:*/C:*/I:H/A:*
[1]
GCS
commands
mavros_node
PX4
telemetry
[1]
CVSS:3.1/AV:N/AC:*/PR:*/UI:*/C:*/I:H/A:*

[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)



[1]

Loss of control over the quadcopter

No WiFi connection probability=0.3

Incorrect message

Attacker manipulates message content

CVSS:3.1/AV:N/AC:*/PR:*/UI:*/C:*/I:H/A:*

Determine communication mechanism probability=0.7

Attacker manipulates message content probability=1.0

Install spyware probability=0.1

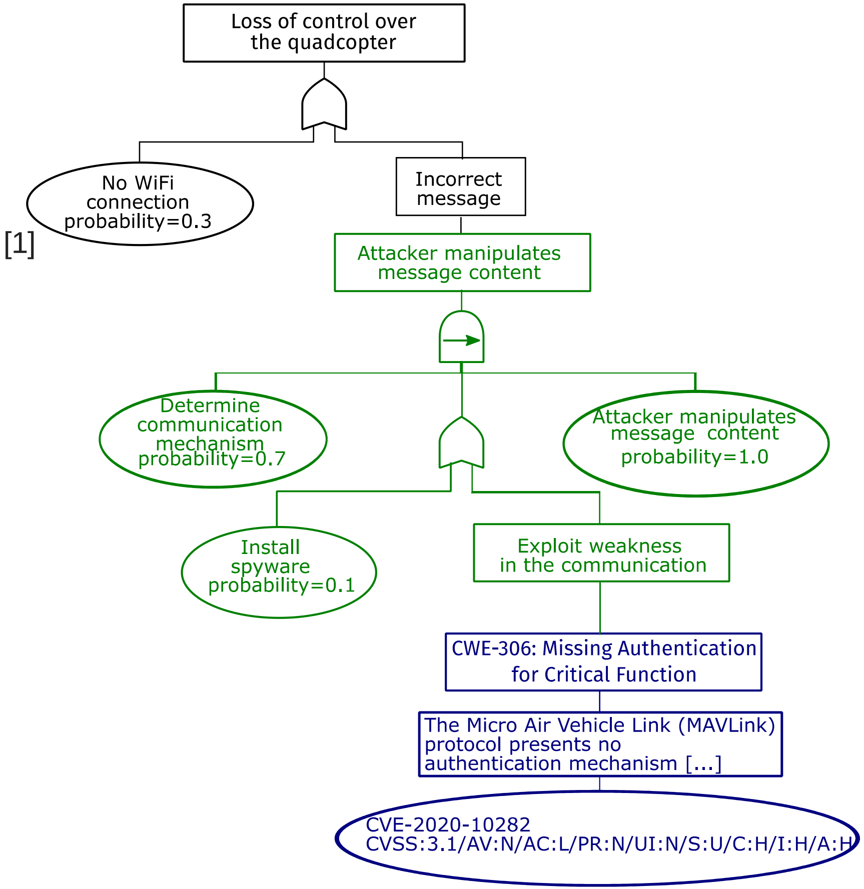
Exploit weakness in the communication

CWE-306: Missing Authentication for Critical Function

The Micro Air Vehicle Link (MAVLink) protocol presents no authentication mechanism [...]

CVE-2020-10282
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)


Loss of control over the quadcopter
No WiFi connection probability=0.3
[1]
Incorrect message
Attacker manipulates message content
Determine communication mechanism probability=0.7
Attacker manipulates message content probability=1.0
Install spyware probability=0.1
Exploit weakness in the communication
CWE-306: Missing Authentication for Critical Function
The Micro Air Vehicle Link (MAVLink) protocol presents no authentication mechanism [...]
CVE-2020-10282
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

[1] T. Witte, **R. Groner**, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, “Towards model co-evolution across self-adaptation steps for combined safety and security analysis,” in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*, ser. SEAMS ’22, 2022. (CC BY 4.0, https://creativecommons.org/licenses/by/4.0/)

Safety & Security of Self-Adaptive Systems

Joint work with Thomas Witte, Alexander Raschke, Irdin Pekaric, Jubril Adigun, Michael Felderer & Matthias Tichy

Developers’ Needs for Software Supply Chain Tooling

What do developers actually do to develop secure applications?

- “Security tools generally see poor adoption by developers” [1]
  - having poor warning messages
  - interrupting workflow
  - having too many false positives
  - not providing enough support for teamwork
  - ….

[1] Tahaei, Mohammad, and Kami Vaniea. "A survey on developer-centred security." *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019.

What do developers actually do to develop secure applications?

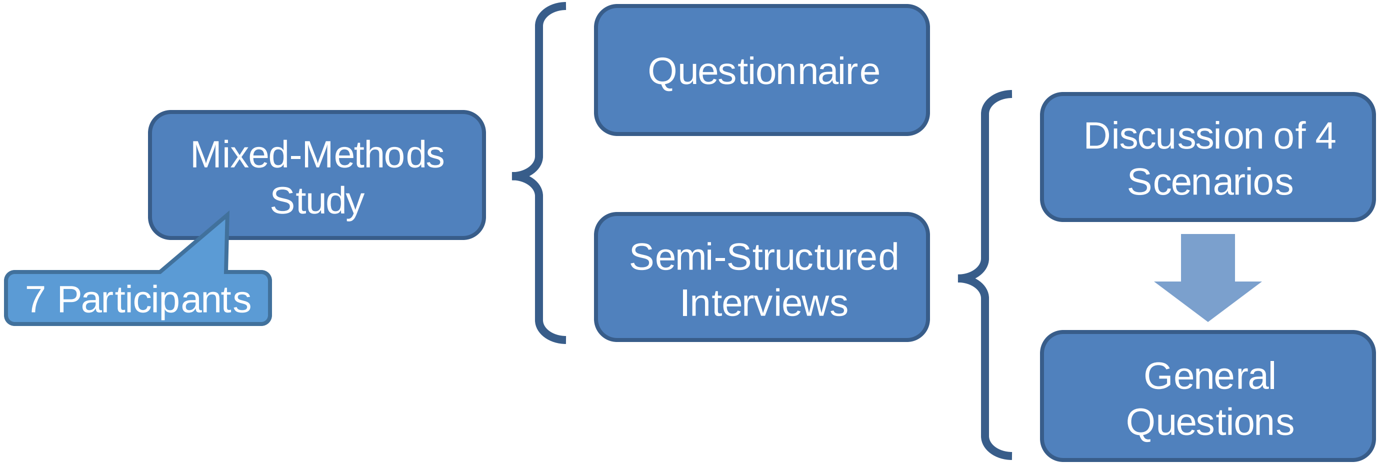
- “Security tools generally see poor adoption by developers” [1]

⇨ How can we enhance what developers currently do?

- Lack of common terminology

⇨ What terms do developers use?

[1] Tahaei, Mohammad, and Kami Vaniea. "A survey on developer-centred security." *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019.



Mixed-Methods Study

7 Participants

Questionnaire

Semi-Structured Interviews

Discussion of 4 Scenarios

General Questions

What security considerations do developers make when they …

1. Scenario

… reuse third-party components?

2. Scenario

… want to establish an automatic build and publishing process?

3. Scenario

… realize that there is a new version of a third-party component available?

4. Scenario

… rely heavily on a third-party component for which a vulnerability is reported and no patch is available?

		I1	I2	I3	I4	I5	I6	I7
Practical Experience in Software Development/Engineering		40	30	4	15	7	25	14
Familiarity with Security		4	3	3	4	3	5	4
Domain	**Academia**			X				X
	Industry	X	X		X	X	X	X
	Open Source	X	X	X	X	X	X	X
Role	**Contributor**	X	X		X	X		X
	Maintainer	X	X	X	X			X
	SW Architect		X		X	X	X	X
	SW Developer	X	X	X	X	X	X	X
	Tester		X					

		I1	I2	I3	I4	I5	I6	I7
Team Size		<10	<10	<10	<10	<10	<50	<10
Software Types	Analysis Tools		X	X	X			X
	Data Management / Database	X	X		X	X	X	X
	Game						X	X
	Library	X	X	X	X			X
	Machine Learning / AI		X				X	
	Web Application	X	X		X	X	X	X
	Other	X	X		X			

General results for the scenarios

- Ad-hoc decisions based on the current context
- Usually, there are no predefined processes/rules/guidelines on how to handle security-related tasks
- Enterprise environment:
  - Documents with security specifications (password policies)
  - Code audits by security specialists
- Limited use of tools
  - Too noisy/lack of prioritization
  - Lack of trust

What security considerations do developers make when they …

1. Scenario

… reuse third-party components?

- Proxy metrics to assess the trustworthiness
  - How active is the community?
    - Maintenance, frequency of new releases, response time
  - How many other projects use the component?
  - How many dependencies does a component have?
  - Who are the developers?
  - What tools do the developers use?
    - Dependapot, automatic build process
  - …

What security considerations do developers make when they …

1. Scenario

… reuse third-party components?

- Proxy metrics to assess the trustworthiness
- Considerations depend on the current context
  - Should I implement a functionality or use a third-party component/library?
  - Is sensitive data involved?
  - To what extent are the users of my software affected by possible vulnerabilities?

What security considerations do developers make when they …

2. Scenario

… want to establish an automatic build and publishing process?

- Trust CI/CD pipeline
- Build locally and publish the artifact
- Build his own snapshot of third-party components

What security considerations do developers make when they …

3. Scenario

… realize that there is a new version of a third-party component available?

- Always update immediately
- Avoiding updates unless there are security issues or a bug that affects own code
- Depending on the trustworthiness of the maintainer and correct semantic versioning
  - Immediate update of bugfixes
  - Bigger updates as part of their own release cycle
- Check changelog
- Check commits to assess changes
- More concerned with breaking changes than security aspects

What security considerations do developers make when they …

4. Scenario

… rely heavily on a third-party component for which a vulnerability is reported and no patch is available?

- Actions depend on the exploitability of the vulnerability
- Vulnerabilities that affect users are prioritized
  - Developer dependency vs runtime dependency
- Situation-dependent assessment of potential solutions
  - Look for an alternative component/library
  - Look for workaround
  - Look for a version that is not affected
  - Try to fix the vulnerability
  - Contact authors and ask about their timeline to fix the vulnerability

Security Policies

- ”My definition of the term is just an in-place document that describes how we respond to security incidents and vulnerabilities.”
- ”Password combination rules or other guidelines related to security you need to enforce in your work […] access to VPN, […] who could actually change, e.g., information on GitHub.”
- ”Security policy is a checkable set of rules that can be enforced to ensure a security posture is maintained.”
- ”A checklist you use to verify a decision about, for instance, pulling in dependencies.”
- ”I think it's a set of rules, and if I adhere to the rules, then the software I build and deploy meets a certain security standard.”

All statements were adjusted to improve readability

What did we learn?

- Developers use proxy metrics to assess trustworthiness.
  - How can we automatically provide these metrics?
- There are different definitions for security policies, but they all represent a nuance of security guidelines.
  - How can we classify security policies?
- The majority of the interviewees were very experienced developers who had established their own best practices for our study scenarios.
  - How can we assist inexperienced developers to follow these practices?

UNIVERSITY OF GOTHENBURG

CHALMERS

UNIVERSITY OF TECHNOLOGY