A Survey on Microservices Security

Davide Berardi*; Saverio Giallorenzo°; Jacopo Mauro°; Andrea Melis*;
Fabrizio Montesi°
* University of Bologna
° University of Southern Denmark

A systematic literature review

- A survey review with a systematic method
- Research
- Select
- Reject

Main goal is to provide a complete, exhaustive summary of current evidence, published and unpublished, that is "methodical, comprehensive, transparent, and replicable.

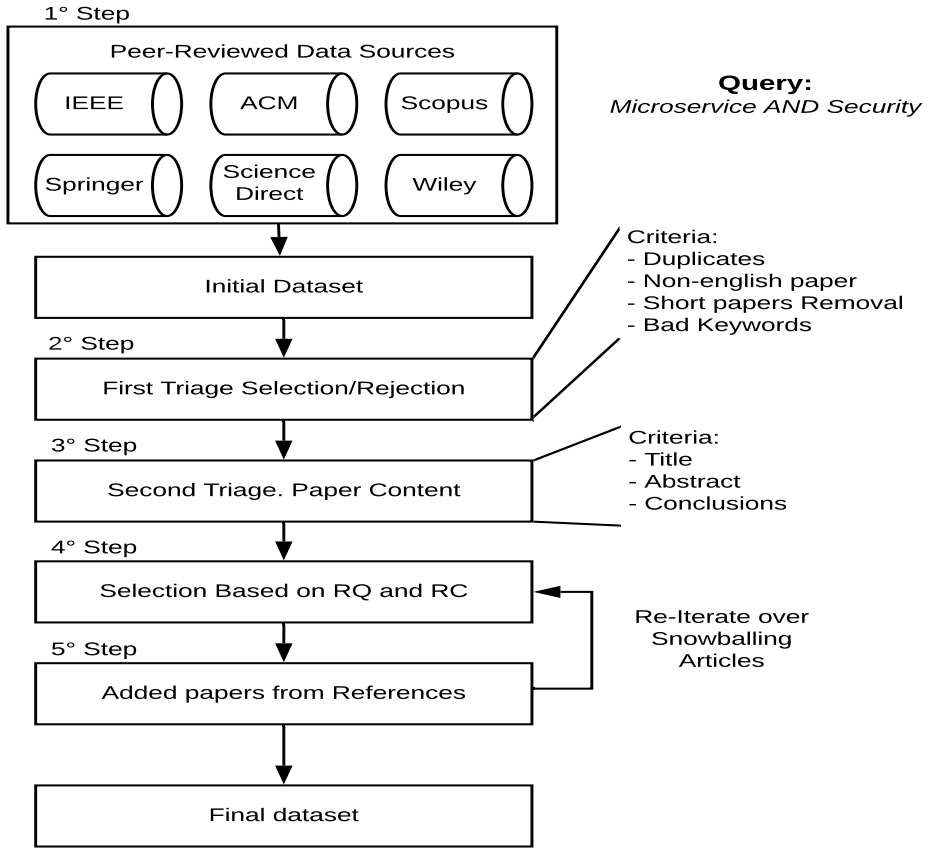
Topic: Microservice and Security

- Microservice is nowdays trending topic
- It introduced several improvements in terms of
  - Scalability
  - Flexibility
  - Modularity
  - ..

- These improvements have a price in terms of security

So the question, what the community is doing/have done about microservice and security?

Methodology



- Definition of the query
- First paper triage
- Second Triage based on Research Questions
- Re-Iteration over Referenced Articles: Snowballing process

Research Questions

- **Threat Model**
  We aimed to understand whether a paper followed some known model, strategy, or guidelines. Alternatively, we wanted to know if some new security model was proposed.

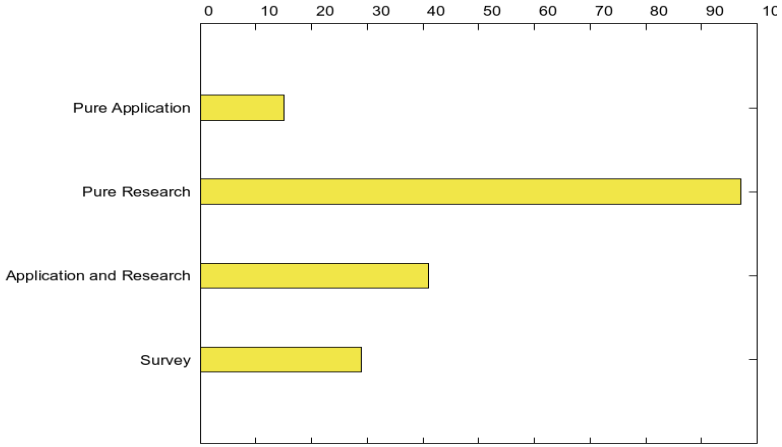
- **Infrastructure**
  With this set of questions we looked into the details of the proposed infrastructure.

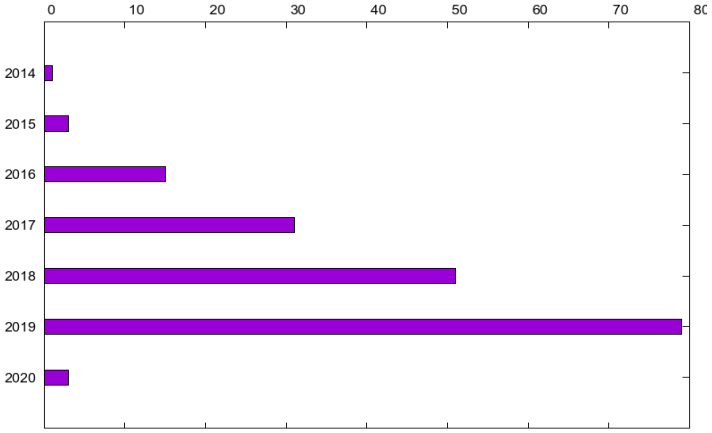
- **Security Approach**
  Deeper into the security aspects of the paper, consider the specific security approaches and solutions, and also the role that microservice play.

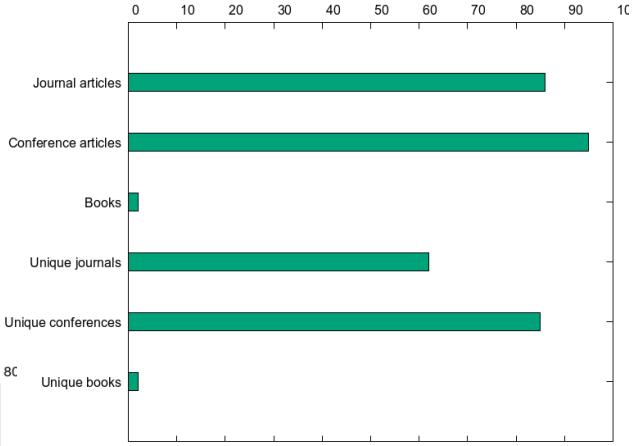
- **Development**
  Check if practices such as DevOps ones are used also in the context of security, for example by verifying whether specific development processes and security standards are considered.

Results. Some Numbers

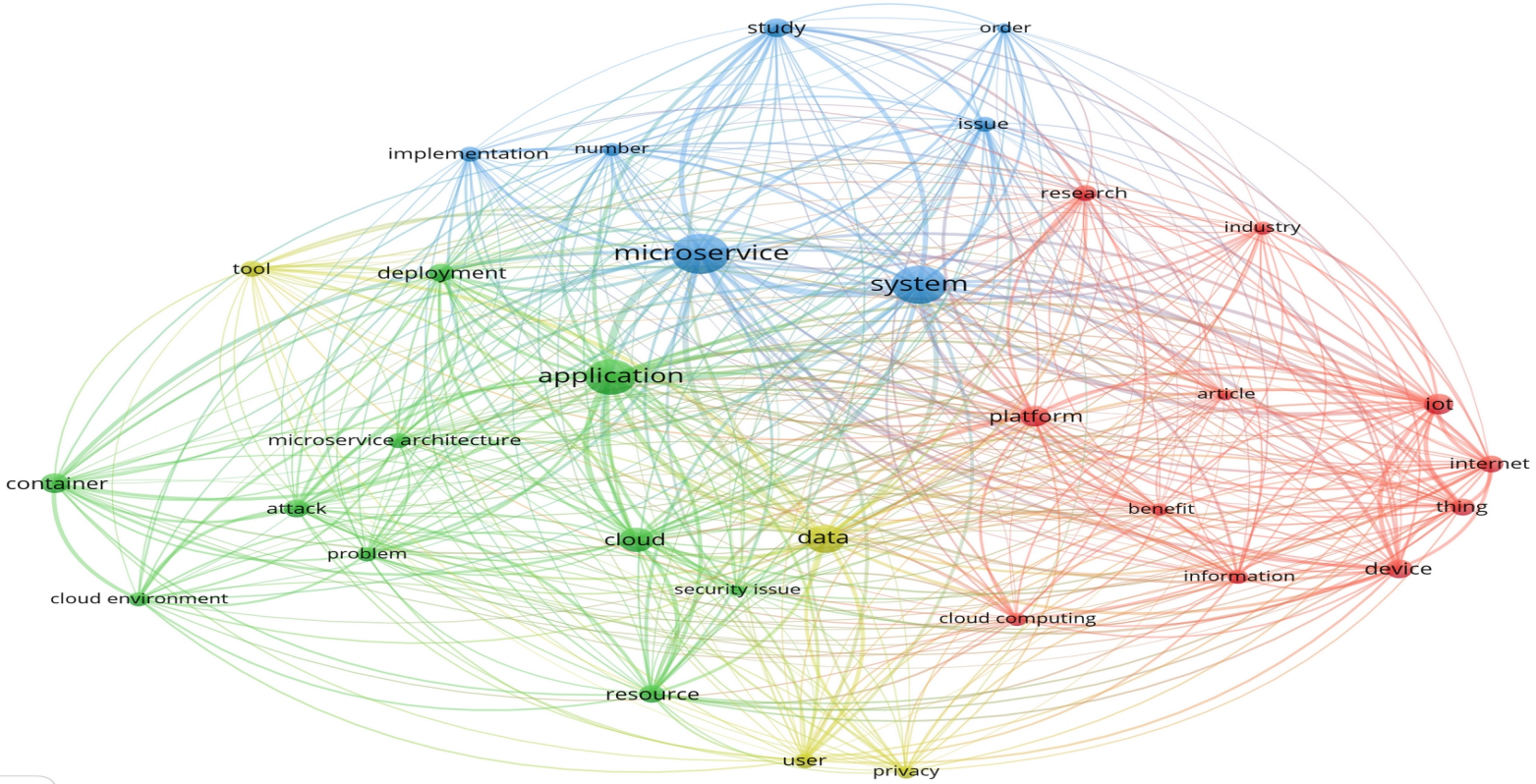
Final dataset composed of 183 papers







Word Cloud



VOSviewer

Qualitative Results: Threat Model

- 38 papers mention the use of at least a threat model to classify and analyze the threats.
- Less than 20% of them mention/use known threat model e.g. STRIDE PASTA
- Many custom model scenario-related.

- **So... There is a Lack of a generic threat model?**
  - Deal with Fog, Edge, Cloud paradigms

Qualitative Results: Infrastructure

- 57 Papers used a centralized approach;
- 34 Papers used a decentralized approach;
- 20 Papers used an hybrid approach.

- There is a trend switching from centralized approaches to decentralized/hybrid approaches.

- New Technologies such blockchain will help this transiction.

Qualitative Results: DevOps

- DevOps is a recurring topic, the reasons are known
  - The Microservices paradigm seems to be the perfect match for DevOps development model.
  - The ability to independently isolate services into small components that can be managed by small teams helps the Continuous Integration process.

- From a security point-of-view several challenges seems to affect the community:
  - From DevOps to DevSecOps
  - Migration from different domain
  - Coordination between development teams

Future Trends: A Roadmap

- The image that emerges is that this subject is lacking both a complete coverage of the relevant sub-topics and a comprehensive framework to treat them.

- **Design**
  - Formal methods for secure distributed systems design
- **Development**
  - Best practices, Security-oriented languages and development processes
  - Toolchain security, automated compliance check
- **Deployment**
  - Compliance checking before admission / static analysis, Integrated IDS/IPS features in gateways
- **Runtime**
  - Data provenance tracking, authentication and monitoring frameworks

Conclusions

- A systematic literature review for Microservices and Security papers.
- 183 papers analyzed and cathegorized among several research-questions and patterns.
- Identified the main strength and weaknesses.
- Proposed Research Directions.

Questions?