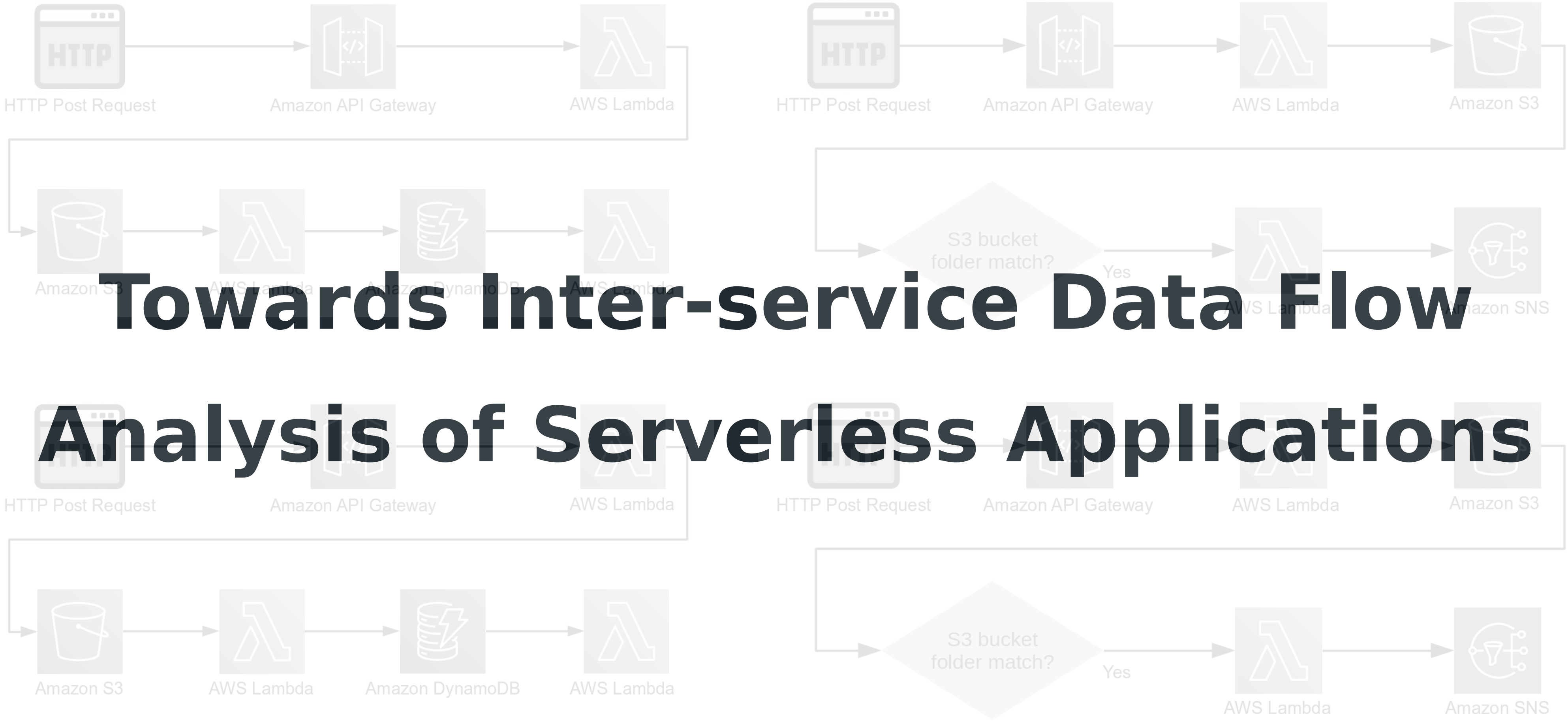


Towards Inter-service Data Flow Analysis of Serverless Applications

Giuseppe Raffa, J. Blasco, D. O’Keeffe, S. K. Dash

SANER 2024 Conference, ERA Track, 15th March 2024

Contact email: giuseppe.raffa.2018@live.rhul.ac.uk

ROYAL
HOLLOWAY
UNIVERSITY
Of LONDON

Motivation & Challenges

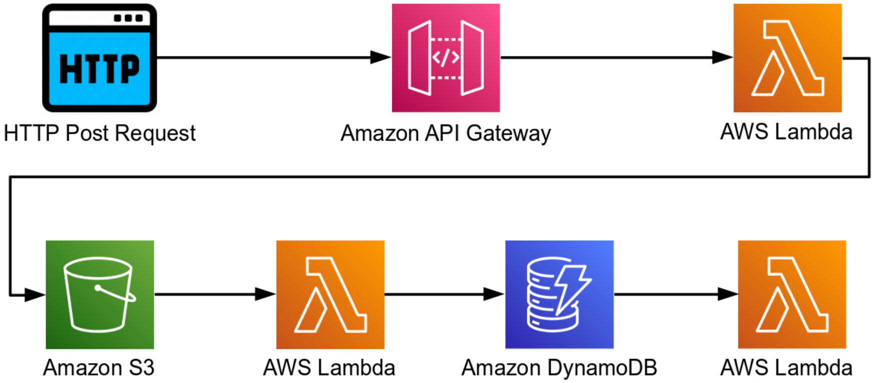
- **Why static data flow analysis?**
  - Most of serverless security tools rely on dynamic analysis
  - Static analysis is an effective supplement
- **What are the challenges?**
  - Information from infrastructure and application code
  - Variety of sources and events
  - Black-box nature of platform services
- **Our work**

Suite of security-oriented microbenchmarks

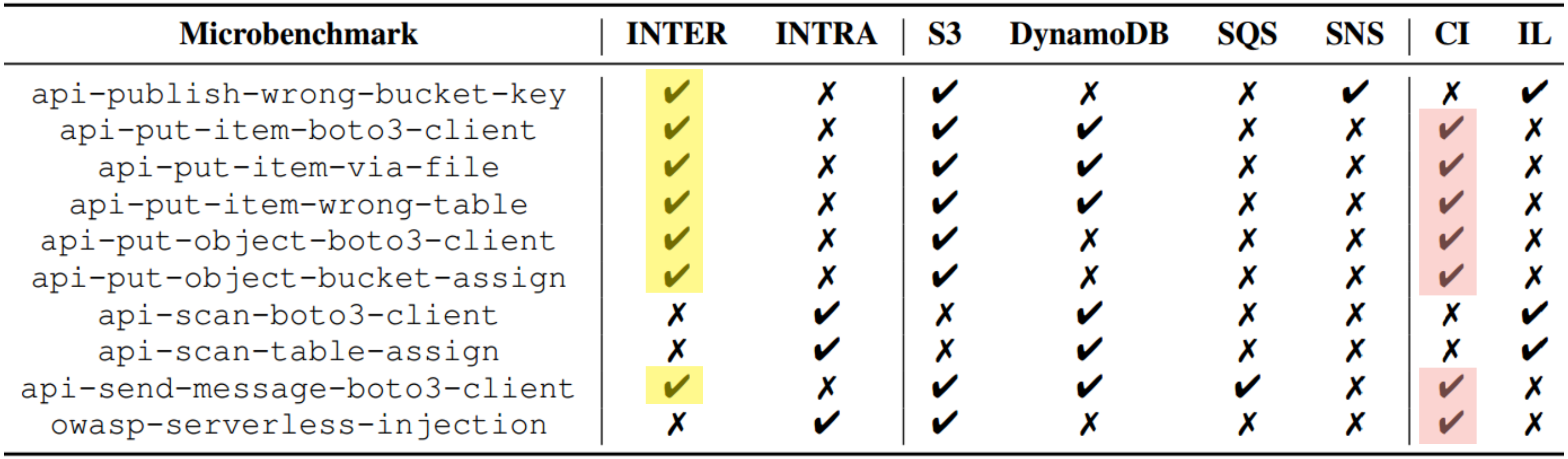
Approach to detecting security-sensitive data flows

Microbenchmarks Suite

- **Design approach**
  - Code injection and information leakage vulnerabilities
  - AWSomePy dataset characterization



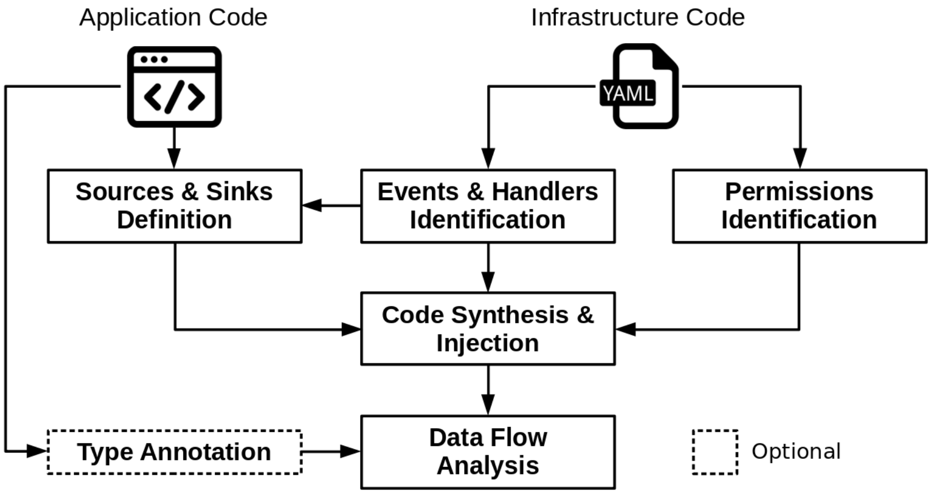
- **Summary**



	Flow		Services				Vuln.	
Microbenchmark	INTER	INTRA	S3	DynamoDB	SQS	SNS	CI	IL
api-publish-wrong-bucket-key	✔	✗	✔	✗	✗	✔	✗	✔
api-put-item-boto3-client	✔	✗	✔	✔	✗	✗	✔	✗
api-put-item-via-file	✔	✗	✔	✔	✗	✗	✔	✗
api-put-item-wrong-table	✔	✗	✔	✔	✗	✗	✔	✗
api-put-object-boto3-client	✔	✗	✔	✗	✗	✗	✔	✗
api-put-object-bucket-assign	✔	✗	✔	✗	✗	✗	✔	✗
api-scan-boto3-client	✗	✔	✗	✔	✗	✗	✗	✔
api-scan-table-assign	✗	✔	✗	✔	✗	✗	✗	✔
api-send-message-boto3-client	✔	✗	✔	✔	✔	✗	✔	✗
owasp-serverless-injection	✗	✔	✔	✗	✗	✗	✔	✗

Prototype Analysis Framework

- **Analysis approach**
  - Infrastructure and application code processed
  - Code instrumented to obtain synchronous equivalent
- **Implementation**
  - Code modified semi-automatically
  - Data flow analysis with Pysa
- **Evaluation**


Application Code
Infrastructure Code
YAML
Sources & Sinks Definition
Events & Handlers Identification
Permissions Identification
Code Synthesis & Injection
Type Annotation
Data Flow Analysis
Optional

7 true positives

2 false positives

1 false negative

ROYAL HOLLOWAY UNIVERSITY Of LONDON

Conclusion & Future Work

- **Key takeaways**

Security-sensitive data flows

New suite of microbenchmarks

Studied approach is feasible

- **Future work**
  - Fully automated analysis pipeline
  - Improvement of infrastructure code processing
  - Support for higher number of cloud services and APIs

https://github.com/giusepperaffa/serverless-security-microbenchmarks