Serverless Computing: Security Risks, Tools and Ongoing Research

Presenter: G. Raffa

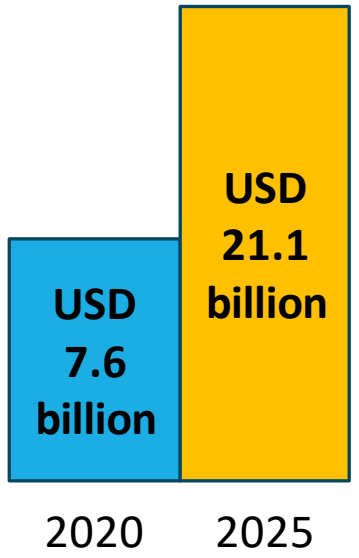
Co-authors: J. Blasco, D. O'Keeffe, S. Dash

i-4 Hybrid Roundtable, London, February 2024

Why Does Serverless Computing Matter?

Recent market research [1]

- Serverless market size expected to grow to USD 21.1 billion by 2025 at a CAGR of 22.7% during the forecast period 2020-2025
- A growing number of companies are using serverless platforms to reduce infrastructure cost



Why Does Serverless Security Matter?

Insecure Amazon S3 bucket exposed personal data on 500,000 Ghanaian graduates

John Leyden 06 January 2022 at 10:58 UTC
Updated: 10 January 2022 at 09:40 UTC

Misconfigured AWS bucket results in mass clinical data exposure

James Walker 10 October 2017 at 12:00 UTC
Updated: 09 September 2019 at 13:38 UTC

Major jobs website left sensitive client data exposed for months

Catherine Chapman 24 July 2018 at 13:59 UTC
Updated: 18 June 2021 at 09:34 UTC

Turkish flight operator Pegasus Airlines suffers data breach

Jessica Haworth 09 June 2022 at 12:29 UTC
Updated: 09 June 2022 at 14:52 UTC

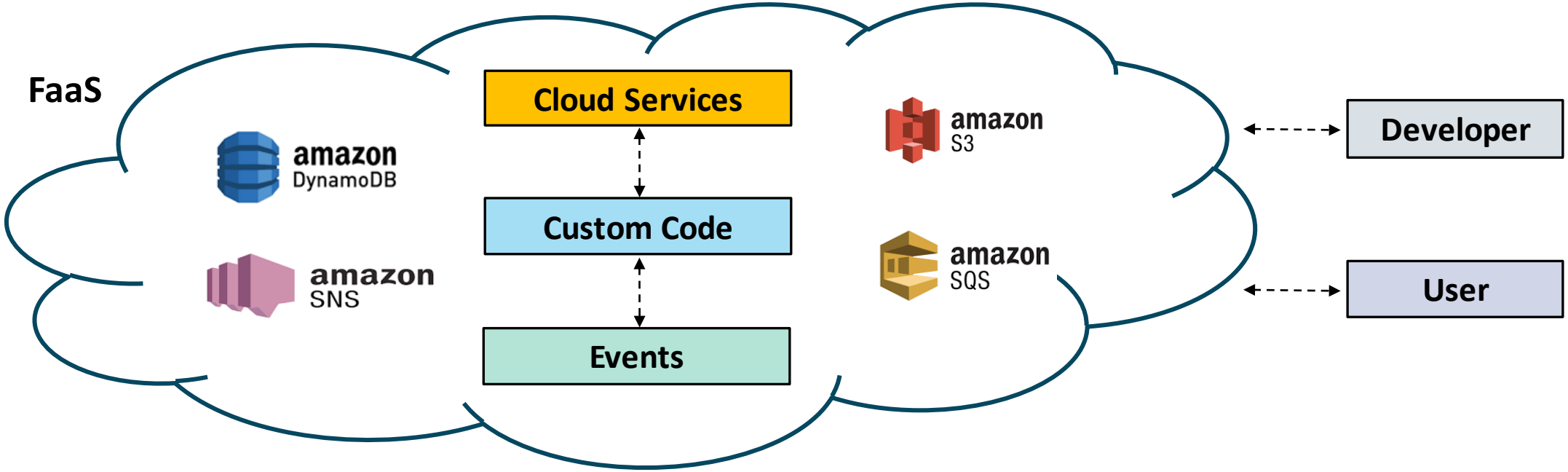
Internal AWS credentials swiped by researcher via SQL payload

Adam Bannister 12 April 2022 at 15:47 UTC
Updated: 12 April 2022 at 16:02 UTC

Vulnerability in AWS IAM Authenticator for Kubernetes could allow user impersonation, privilege escalation attacks

Jessica Haworth 13 July 2022 at 14:29 UTC
Updated: 05 September 2022 at 09:53 UTC

Serverless Computing Model



Advantages

- Cost-effectiveness
- No infrastructure management

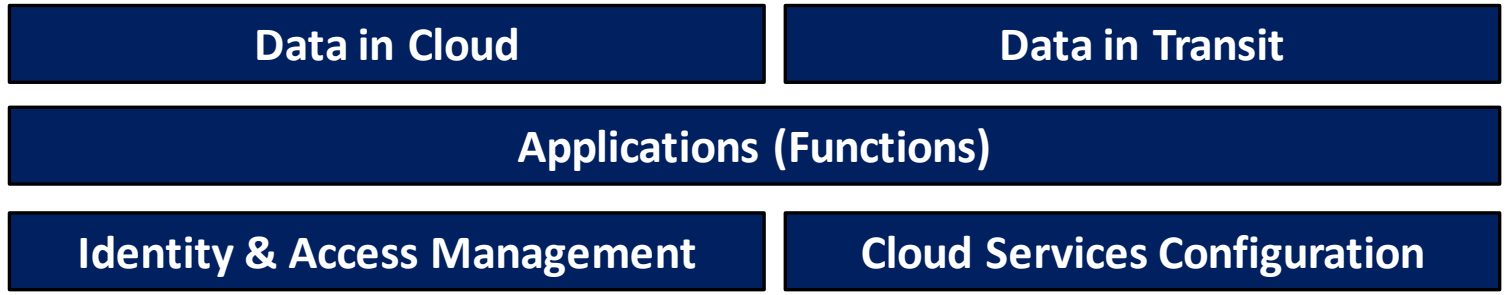
Disadvantages

- Debugging
- Execution-related limits

Shared Responsibility Model

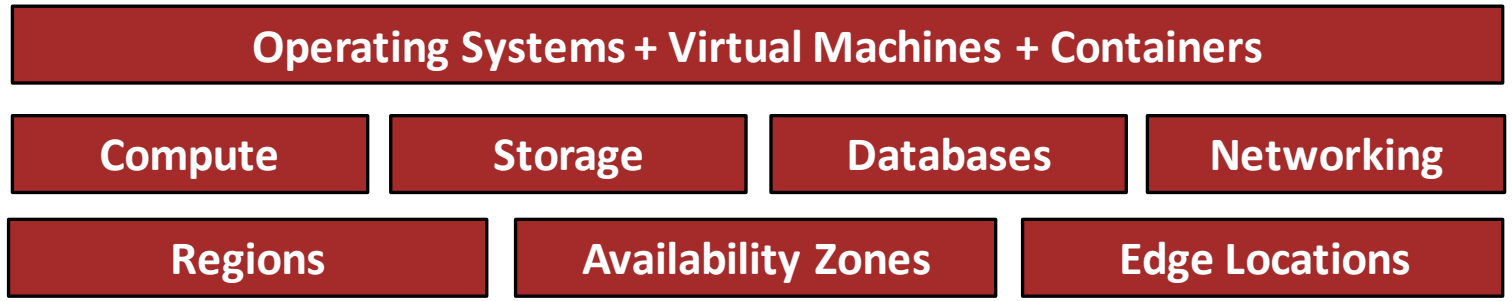
Application Owner

Responsible for security "in" the cloud



FaaS Provider

Responsible for security "of" the cloud



Key concept

- Serverless application developers must take care of security

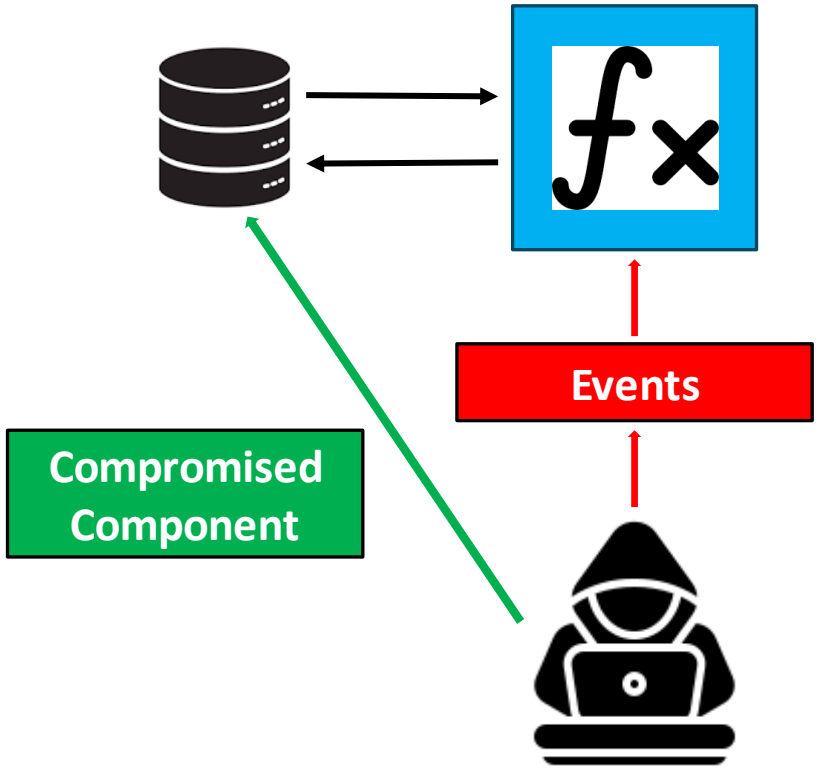
Serverless Security Issues

Many different attacks possible [2]

- External attacks
- Malicious insider attacks
- Horizontal attacks between tenants
- Vertical attacks

Serverless-specific issues

- Large attack surface
- Many types of event triggers
- Tools are still evolving



Critical Risks for Serverless Applications

Risks identified by the Cloud Security Alliance [3]

Function Event Data Injection	Broken Authentication	Insecure Serverless Deployment Configuration	Over-Privileged Function Permissions & Roles
Inadequate Function Monitoring and Logging	Insecure Third-Party Dependencies	Insecure Application Secrets Storage	DOS & Financial Resource Exhaustion
Serverless Business Logic Manipulation	Improper Exception Handling and Verbose Error Messages	Obsolete Functions, Cloud Resources and Event Triggers	Cross-Execution Data Persistency

Injection Flaws

Well understood attacks

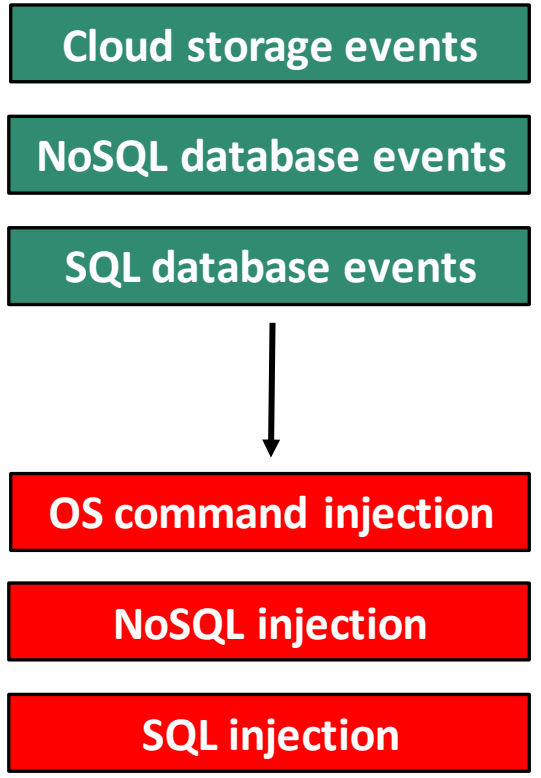
- Execution of code based on untrusted inputs

Serverless context

- Multiple event sources can trigger code execution
- Different events include different message formats

Mitigation strategy

- Traditional strategies applicable, but not enough
- All possible event types and entry points should be considered



Amazon Web Services Security Tools

Inspector

- Automated vulnerability management service
- Scans both cloud infrastructure components and serverless functions
- Central management and integration into CI/CD tools

X-Ray

- Tracing tool to debug and analyze applications
- Provides end-to-end views of requests as they travel through the application
- Service maps can be used to identify data flows

GuardDuty

- Threat detection service for continuous monitoring
- Detects unauthorized behavior and malicious activity
- Relies on machine learning and malware scanning

All these tools require the deployment of resources in the cloud

Microsoft Azure Security Tools

Defender for Cloud

- Continuous assessment of configuration of cloud resources
- Monitoring tool to detect suspicious activities
- Scanning of application and infrastructure code **prior** to deployment

Multicloud, as some features are usable in AWS and Google Cloud Platform

Sentinel

- Security Information and Event Manager (SIEM) built into Azure
- Collects security events and contextual data from various data sources
- Supports threat detection, investigation and remediation

Relies on logging and monitoring of deployed resources

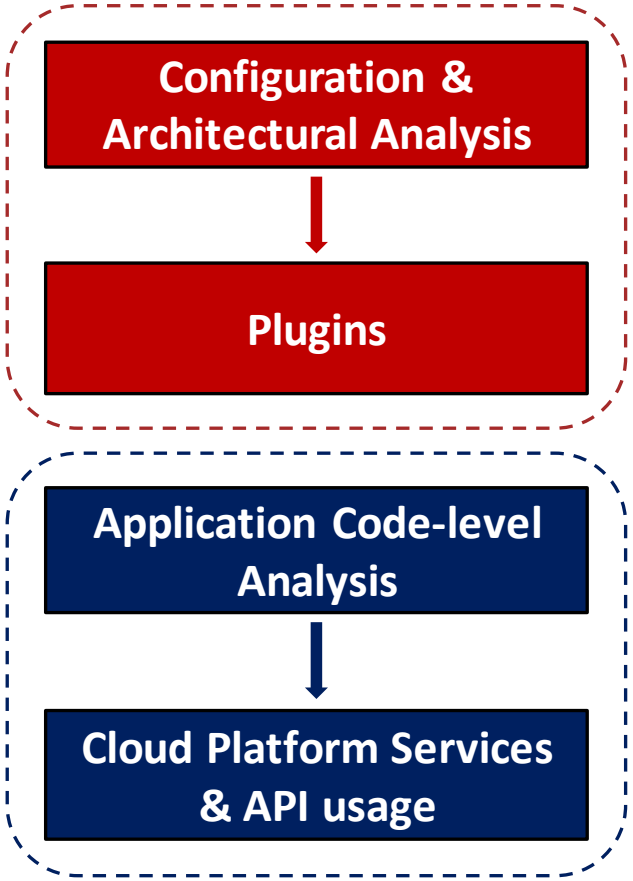
Our Serverless Security Research

Static analysis of serverless applications

- Effective supplement to dynamic methods
- Variety of sources and events
- Black-box nature of cloud services
- Models and approximations needed

AWSomePy dataset [4]

- Focus on AWS and Python
- Focus on Serverless Framework deployment tool



Dataset Config & Architectural Analysis

Plugin analysis

- Specified in the infrastructure code file
- 44 plugins in total

Results

- 1st and 2nd => configuration
- 3rd and 4th => functionality

Plugins	Occurrences
serverless-python-requirements	95
serverless-pseudo-parameters	25
serverless-domain-manager	15
serverless-step-functions	14
serverless-offline	9
serverless-dotenv-plugin	8
serverless-prune-plugin	8
serverless-iam-roles-per-function	7

Developers are not configuring permissions in a granular fashion

Dataset Application Code Analysis

Cloud services

- 46 services in total
- Data storage and NoSQL services the most common
- Configuration-oriented services frequently used

Cloud APIs

- Programmatic creation of buckets and tables

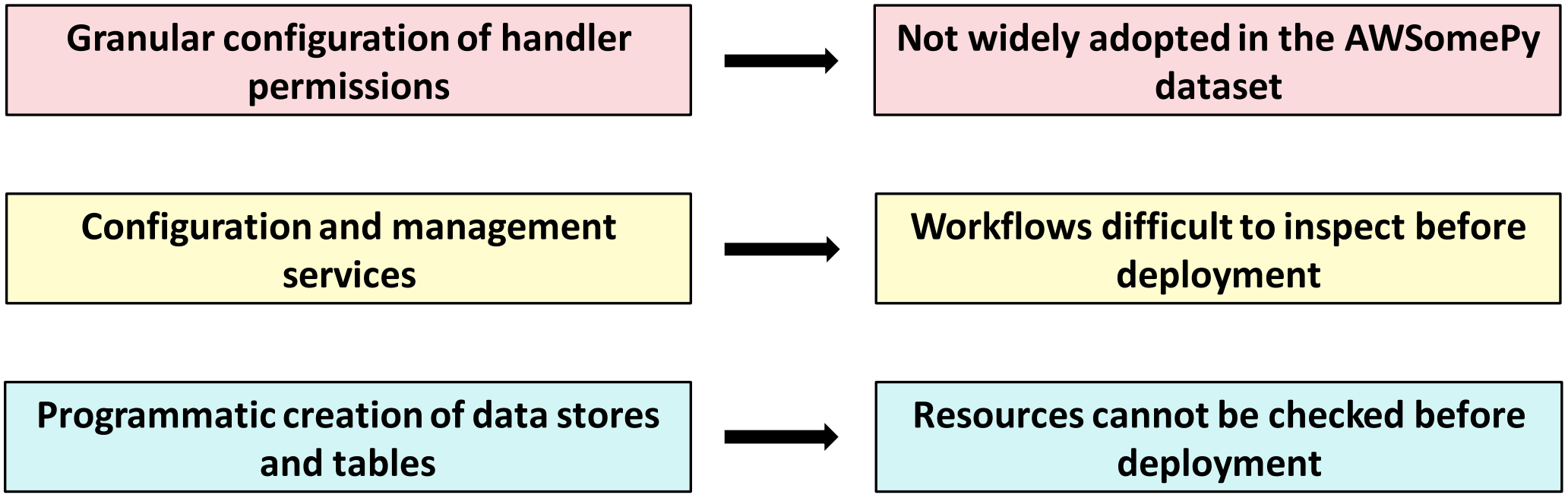
Resources created programmatically cannot be statically checked via infrastructure code analysis

Services	No. of Repositories	Occurrences
s3	59	217
dynamodb	47	201
lambda	24	47
ssm	14	46
sqs	21	41

s3		dynamodb	
API	#	API	#
put_object	61	put_item	143
get_object	52	scan	64
create_bucket	50	query	62
upload_file	48	get_item	58
download_file	24	update_item	57
list_objects_v2	22	create_table	41
other	111	*other*	93

Dataset Study Takeaways

All security-related



Static Analysis Pipeline for Serverless

Identification of data flows

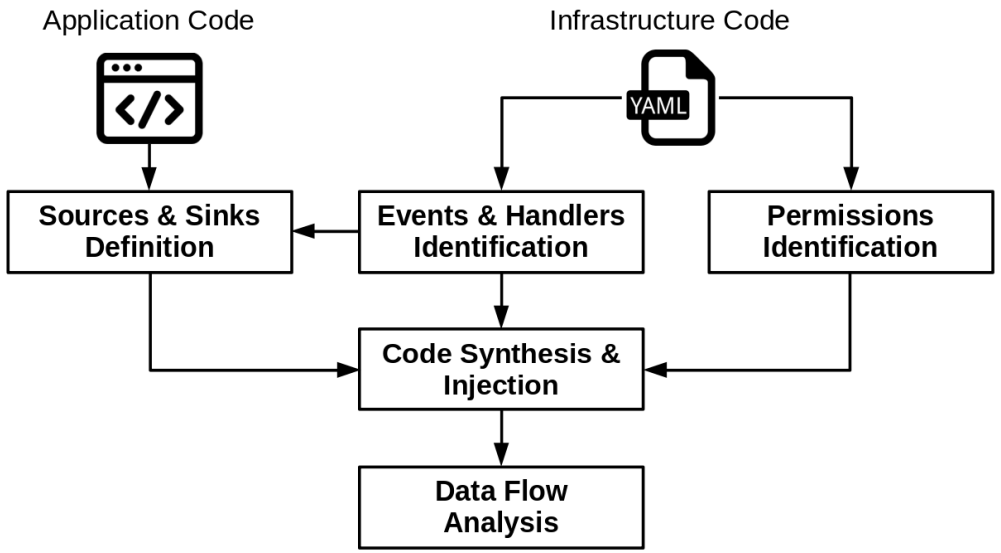
- Code injection
- Information leakage

Starting points

- Serverless-specific vulnerabilities
- AWSomePy dataset characterization

Two-pillar approach

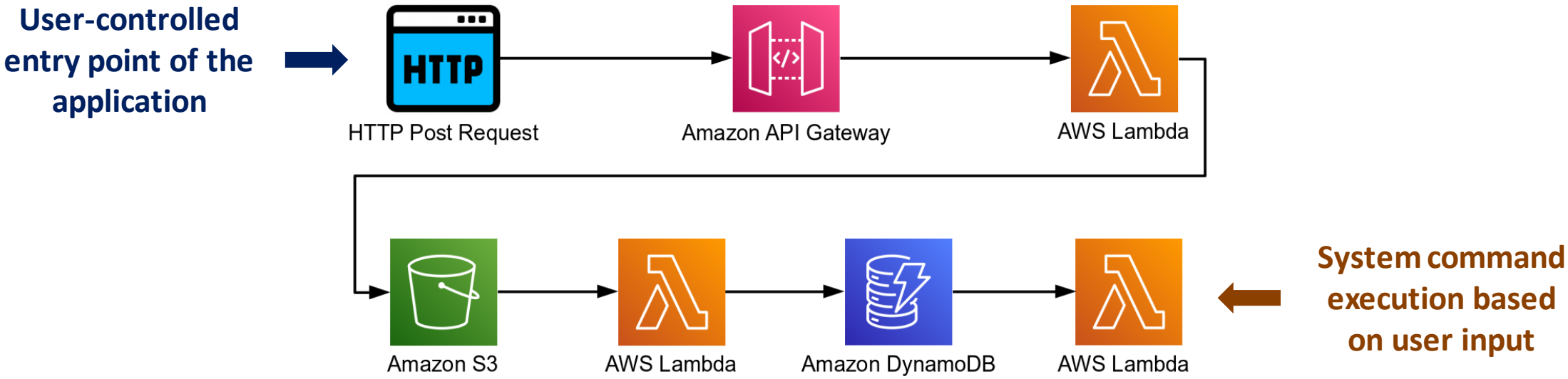
- Information extraction (infrastructure and application)
- Injection of synthesized code into the application



A general-purpose static analysis tool not effective without information included in the synthesized code

Microbenchmarks Suite

Example [5]



What Have We Learned?

Paradigm

- Users focus on business logic as well as security
- Large attack surface because of multiple events
- Injection attacks considered the most critical risk by CSA

Tools

- Many tools exist to monitor deployed applications
- Serverless-specific tools often have a narrow scope
- Some tools compatible with multiple platforms

Research

- Focus on static analysis of serverless applications
- Novel dataset characterized and publicly released
- Generic static analysis pipeline being developed

References

1. MarketandMarkets, Serverless Architecture Market Analysis, 2020, https://www.marketsandmarkets.com/Market-Reports/serverless-architecture-market-64917099.html
2. X. Li, X. Leng and Y. Chen, "Securing Serverless Computing: Challenges, Solutions, and Opportunities," in IEEE Network, vol. 37, no. 2, pp. 166-173, March/April 2023, DOI.
3. Cloud Security Alliance, The 12 Most Critical Risks for Serverless Applications, 2019, https://cloudsecurityalliance.org/blog/2019/02/11/critical-risks-serverless-applications
4. G. Raffa, J. Blasco Alis, D. O'Keeffe and S. K. Dash, "AWSomePy: A Dataset and Characterization of Serverless Applications," in Proceedings of the 1st Workshop on SErverless Systems, Applications and MEthodologies (SESAME '23), 2023, DOI.
5. G. Raffa, Serverless Microbenchmarks Suite, https://github.com/giusepperaffa/serverless-security-microbenchmarks

Thank you

Giuseppe Raffa

giuseppe.raffa.2018@live.rhul.ac.uk