Serverless need not be Security-less

Praveen Gupta, Arshia Moghimi, Aastha Mehta, Mohammad Shahrad

Yayu Wang, Aastha Mehta

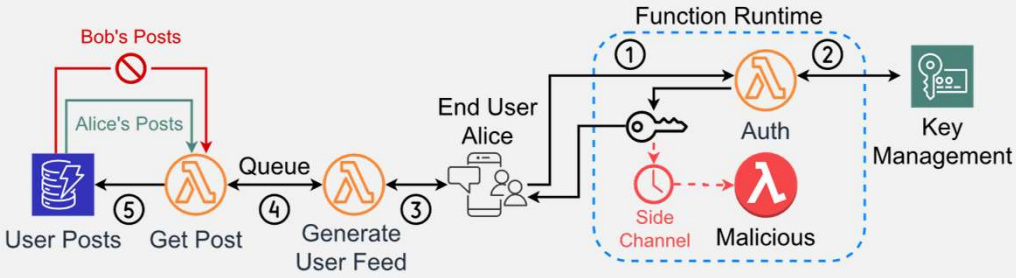
THE UNIVERSITY OF BRITISH COLUMBIA

SYSTOPIA

1 – State of Serverless Computing in Cloud

Short Invocation Time (Median – 60ms)	Language Heterogeneity (Python, JS, Java, Go)
Several invocation triggers (API Gateway, DB Triggers, Events)	Multi-tenancy & Container Reuse

2 – Social Media Application Functions



3a – Problems in Data Privacy

- Large number of cloud components & 3rd party dependencies
- Complex data flows between components over network
- Rapidly evolving code, data & privacy policies

Bugs & Misconfigurations can lead to **unauthorized data access & privacy violations**

3b – Solution: Dev Tools for Privacy Compliance

Policy discovery: Automated workflow-level data provenance tracking

Policy specification: Declarative & decoupled from application code

Policy enforcement: Per-function static analysis + runtime reference monitor in function container

4a – Side-Channel Attacks on Serverless

- Multi-tenancy introduces resource sharing on Serverless
- Adversary can achieve colocation with the victim's function and learn victim's activity via resources usage (e.g., cache miss)
- Adversary can infer fine-grained application **secrets** (e.g., encryption key) via side-channel

4b – Proposed Solution Approaches & Challenges

Key Property: Secret-independent code execution & data accesses

Challenges

- ✓ Complex data types (maps, lists)
- ✓ Dynamic language features (dynamic types, async programming)
- ✓ Vulnerable dynamic optimizations

Source Code

CodeGen

Runtime

Solution

- ✓ Constant-time transformations
- ✓ Compositional reasoning