Detailed Security Analysis of Serverless Functions with Interpreted Languages

Design Document

Team Number: 26
Client: Dr. Gulmezoglu
Advisers: Dr. Gulmezoglu
Team Members:
Michael Gohr
Dillon Hacker
Camera Hurt
Samuel Potter
Trent Walraven
Email: sdmay24-26@iastate.edu
Website: https://sdmay24-26.sd.ece.iastate.edu/

Revised: 09/10/2023

Executive Summary

Development Standards & Practices Used

List all standard circuit, hardware, software practices used in this project. List all the Engineering standards that apply to this project that were considered.

Summary of Requirements

- Determine limitations of APIs available for interpreted languages, and what is useable for potential knowledge of other code running
- Using the limitations, the data valuable and useable in the creation of machine learning models to analyze data from functions
- Attack code that collects data, then uses a machine learning model to classify the recorded data
- If possible, using this classified data, analyze potential leaked information from other serverless functions running at the same time
- If leakage is found, report through the proper channels to get the vulnerability fixed
- Created a formal detailed analysis of our findings, in a presentable manner

Applicable Courses from Iowa State University Curriculum

- Com S 227, 228, 309
- Cpr E 437x
- Cpr E 381
- Cyb E 230, 231, 331
- CpR E 308

New Skills/Knowledge acquired that was not taught in courses

- Knowledge about cloud computing, specifically relating to serverless functions.
- Understanding of different virtualization types, and how they interact

Table of Contents

1 Team 5

1.1 Team Members 5

1.2 Required Skill Sets for Your Project 5

(if feasible – tie them to the requirements) 5

1.3 Skill Sets covered by the Team 5

(for each skill, state which team member(s) cover it) 5

1.4 Project Management Style Adopted by the team 5

1.5 Initial Project Management Roles 5

2 Introduction 5

2.1 Problem Statement 5

2.2 Requirements & Constraints 5

2.3 Engineering Standards 5

2.4 Intended Users and Uses 6

3 Project Plan 6

3.1 Project Management/Tracking Procedures 6

3.2 Task Decomposition 6

3.3 Project Proposed Milestones, Metrics, and Evaluation Criteria 6

3.4 Project Timeline/Schedule 6

3.5 Risks And Risk Management/Mitigation 7

3.6 Personnel Effort Requirements 7

3.7 Other Resource Requirements 7

4 Design 8

4.1 Design Context 8

4.1.1 Broader Context 8

4.1.2 User Needs 8

4.1.3 Prior Work/Solutions 8

4.1.4 Technical Complexity 9

4.2 Design Exploration 9

4.2.1 Design Decisions 9

4.2.2 Ideation 9

4.2.3 Decision-Making and Trade-Off 9

4.3 Proposed Design 9
4.3.1 Design Visual and Description 10
4.3.2 Functionality 10
4.3.3 Areas of Concern and Development 10
4.4 Technology Considerations 10
4.5 Design Analysis 10
4.6 Design Plan 10
5 Testing 11
5.1 Unit Testing 11
5.2 Interface Testing 11
5.3 Integration Testing 11
5.4 System Testing 11
5.5 Regression Testing 11
5.6 Acceptance Testing 11
5.7 Security Testing (if applicable) 11
5.8 Results 11
6 Implementation 12
7 Professionalism 12
7.1 Areas of Responsibility 12
7.2 Project Specific Professional Responsibility Areas 12
7.3 Most Applicable Professional Responsibility Area 12
8 Closing Material 12
8.1 Discussion 12
8.2 Conclusion 12
8.3 References 13
8.4 Appendices 13
8.4.1 Team Contract 13

List of figures/tables/symbols/definitions (This should be the similar to the project plan)

1 Team

1.1 Team Members

Michael Gohr

Dillon Hacker

Cameron Hurt

Samuel Potter

Trent Walraven

1.2 Required Skill Sets for Your Project

- AWS Serverless Functions
- Virtualization
- Coding
- Data Analysis
- Communication
- Security Knowledge

1.3 Skill Sets covered by the Team

- Internal communication
- Task scheduling
- Coding
- Virtualization
- Security Knowledge

1.4 Project Management Style Adopted by the team

- Agile methodology (frequent meetings, achievable smaller tasks/deliverables between them)

1.5 Initial Project Management Roles

Micheal Gohr: Team organization and individual component design

Dillon Hacker - Client interaction, note taking/meeting minutes, and testing.

Cameron Hurt - Oversee testing, and ensure coverage

Trent Walraven - Meeting coordination and record keeping when needed

Samuel Potter - Component creation coordinator, documentation creation

2 Introduction

2.1 Problem Statement

2.2 Requirement & Constraints

2.3 Engineering Standards

2.4 Intended Users and Uses

3 Project Plan

3.1 Project Management/Tracking Procedures

3.2 Task Decomposition

3.3 Project Proposed Milestones, Metrics, and Evaluation Criteria

3.4 Project Timeline/Schedule

3.5 Risks and Risk Management/Mitigation

3.6 Personnel Effort Requirements

3.7 Other Resource Requirements

4 Design

4.1 Project Management/Tracking Procedures

4.1.1 Broader Context

4.1.2 User needs

4.1.3 Prior Work/Solutions

4.1.4 Technical Complexity

4.2 Project Management/Tracking Procedures

4.2.1 Design Decisions

4.2.2 Ideation

4.2.3 Decision-Making and Trade-Off

4.3 Project Management/Tracking Procedures

4.3.1 Design Visual and Description

4.3.2 Functionality

4.3.3 Areas of Concern and Development

4.4 Technology Considerations

4.5 Design Analysis

4.6 Design Plan

5 Testing

5.1 Unit Testing

5.2 Interface Testing

5.3 Integration Testing

5.4 System Testing

5.5 Regression Testing

5.6 Acceptance Testing

5.7 Security Testing

5.8 Results

6 Implementation

7 Professionalism

7.1 Areas Of Responsibility

7.2 Project Specific Professional Responsibility Area

7.3 Most Applicable Professional Responsibility Area

8 Closing Material

8.1 Discussion

8.2 Conclusion

8.3 References

8.4 Appendices

8.4.1 Team Contract