Toward Automatic Detection of Cloud Server Security Vulnerabilities

Olufogorehan Tunde-Onadele[1], Yuhang Lin[1], Xiaohui Gu[1], Jingzhu He[2]

[1] North Carolina State University; [2] ShanghaiTech University

Motivation

Cloud server systems are popular for deploying web applications

- However, cloud systems are constantly under attacks
- A single security exposure can have tremendous cost, especially for large-scale cloud services
- Attack detection systems based on system activity do not help developers understand the bugs in code

Research Questions

1. What are the causes of security bugs in the code?
2. What threat impact do those vulnerable code have?
3. How do developers patch those vulnerable code?

Contribution

- We manually investigated **109** real-world security vulnerabilities in **13** popular server applications:
  - Apache ActiveMQ, Apache Commons FileUpload, Apache Solr, Apache Struts, Apache Tomcat, Apache Unomi, Elasticsearch, GlassFish, JBoss, Jenkins, Jetty, Undertow, and WildFly/Jboss

- We identify **five** common root cause categories with similar code patterns that can guide automatic detection and patching

Future Work

- Build automatic detection checkers based on the root cause code patterns

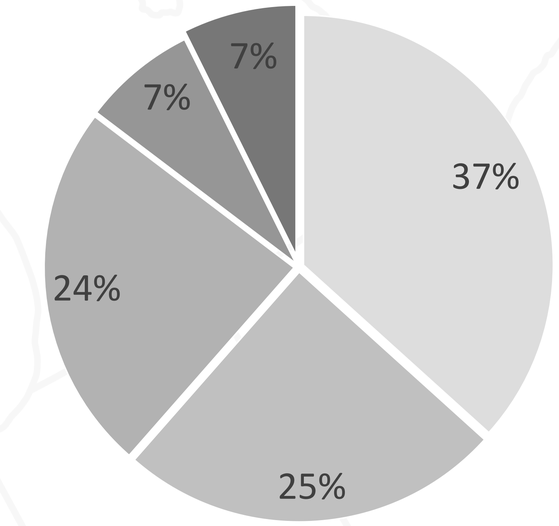

Fig 1: Distribution of Security Bugs by Root Cause Code Category

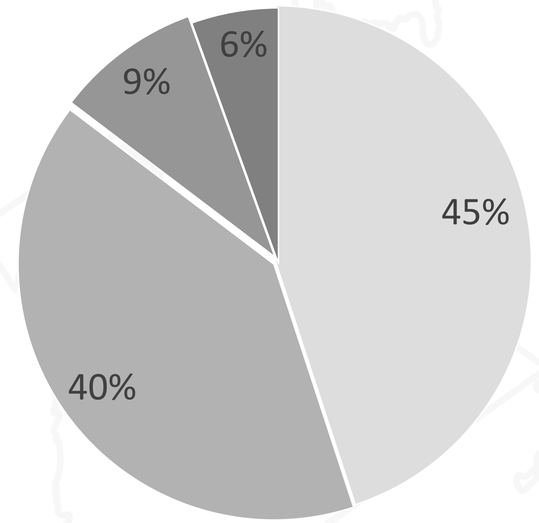

Fig 2: Distribution of Security Bugs by Threat Impact

Root Cause Category	Description
1. Improper execution restrictions	Incomplete or missing restrictions to functions that can execute commands
2. Improper permissions checks	Incomplete or missing checks for security-sensitive parameters used in privileged functions
3. Improper resource path-name checks	Incomplete or missing checks to filter requested resource paths and filenames
4. Improper sensitive data handling	Improper protection of sensitive data that become exposed in program output
5. Improper synchronization handling	Improper handling of concurrent requests

9TH ANNUAL
HOT TOPICS *in the* SCIENCE OF SECURITY
April 5-7, 2022 | Virtually Hostedby UNIVERSITY OF ILLINOIS, URBANA-CHAMPAIGN
http://hot-sos.com