Paper Title

Detecting Missing-Permission-Check Vulnerabilities in Distributed Cloud Systems

Paper Link

https://dl.acm.org/doi/10.1145/3548606.3560589

1 Summary

1.1 Motivation

Distributed cloud system contains multiple remotely accessible API based components. These APIs builds communication between users or other components. Due to the lack of proper permission checks, easily exploitable MPC vulnerabilities can be emerged in the system. To mitigate them, the authors introduced permission check approach to restrict any outside attacker to prevent the cloud breaching.

1.2 Contribution

The authors conducted an in-depth study on 95 MPC vulnerabilities and proposed a new log-based analysis that automatically detects permission checks and privilege operations in distributed systems. Further, they developed a tool called MPChecker that reported 44 new critical bugs in 6 real-world distributed systems.

1.3 Methodology

MPChecker was build in 3 stages. Initially, this tool analyzed run time logs of java programs along with its byte-codes to infer automatically user and system related variables. Then, From the inferred variables,it identified permission checks and privileged operations. Lastly, the privileged operations which were not guarded with permission checks and accessible from public interfaces were reported as MPC vulnerabilities.

1.4 Conclusion

This tool was evaluated on 6 real-world distributed systems, and were able to report 44 new critical vulnerabilities successfully. Among them, 1 severe security flaws were found by MPChecker with details.

2 Limitations

2.1 First Limitation

Permission checking approach is sufficient to prevent unauthorized access. But it will not work on authorization vulnerabilities, making it ungeneralizable for token-based authorization systems.

2.2 Second Limitation

Assumption that inferred user and system related variables were privileged. In some systems, system related variables can be modified and user related variables may be exposed to public maintaining confidentiality, that may contradict this major assumption of this study.

3 Synthesis

Beside ensuring distributed cloud security, and maintaining access control, MPChecker can be used as compliance checker. Industries with strict compliance regarding data access and storage can use MPChecker to automate the compliance check by identifying permission gaps. This can also implemented to ensure data integrity for critical data by preventing unauthorized changes.Also, there is a scope to advance this tool by applying intelligent algorithms to implement corrective actions as the process of remediation.