Proposal Defense

Doctor of Philosophy in Computer Science

“Simplifying Deployment of Intrusion-Tolerant Systems by Leveraging Cloud Resources” by

Maher Khan

Date: April 24, 2023
Time: 12:00PM – 2:00PM
Place: 6106 E. Lilly, Sennott Square, 3810 Forbes Ave, Pittsburgh PA 15213

Committee:

• Dr. Amy Babay, Assistant Professor, Department of Computer Science and Department of Informatics and Networked Systems, SCI
• Dr. Daniel Mosse, Professor and Interim Chair, Department of Computer Science, SCI
• Dr. Adam Lee, Professor and Associate Dean for Academic Programs, Department of Computer Science, SCI
• Dr. Balaji Palanisamy, Associate Professor, Department of Informatics and Networked Systems, SCI

Abstract:

The rise of cyberattacks on high-value systems has led to a growing interest in intrusion-tolerant systems as a means of ensuring resilience. An intrusion-tolerant system can guarantee that it can continue to operate correctly even when parts of the system are compromised. The research community has developed techniques for intrusion-tolerant systems based on Byzantine Fault-Tolerant (BFT) replication. However, these systems are still not widely used in industry. One of the main obstacles is the technical expertise and infrastructure investment required for deploying and managing these systems. Cloud resources can help with this but are currently not feasible for many system operators due to concerns about maintaining the confidentiality of sensitive information.

We propose to address this issue by allowing system operators to deploy intrusion-tolerant applications by partially or fully outsourcing the responsibility of the BFT replication protocol to a cloud service while maintaining the privacy of the application's state and algorithms. We also define a hybrid management model for joint management of intrusion-tolerant applications by system operators and cloud providers, separating responsibilities. Only the replicas managed by the system operator execute the application logic, and the replicas managed by the cloud service provider participate in the BFT replication protocol to provide the needed resilience and only have access to encrypted state.

Furthermore, we propose to make the deployment of our solution easier and cost-effective for cloud providers by designing a scalable system for running multiple replicas of different applications on the same physical machines. Overall, this approach has the potential to make intrusion-tolerant systems more accessible to system operators while maintaining the confidentiality of sensitive information.