FAULT & INTRUSION TOLERANCE FOR CLOUD COMPUTING

WASIM BARI, VINICIUS V. COGO, ALYSSON BESSANI
MARCELO PASIN, HANS P. REISER

MOTIVATION
Cloud computing has been evolved into a major model for architcetuing large-scale distributed systems. Given today’s situation of countless vulnerabilities in production software and scores of malicious attackers exploiting these vulnerabilities, combined with ever-growing complexity of software as well as of systems, it is unlikely that clouds will not be a major target for malicious attacks and intrusions.

- Vulnerabilities exposed in cloud enabling virtualization software: Xen, VMware, Microsoft Virtual PC etc.
- Popularity brings attacks: “60% of virtual servers will be less secure than the physical servers they replace through 2012” by Gartner Inc.
- Cloud architectures make it difficult to apply traditional security approaches like cross administrative domains, lack of physical control etc.

WHAT IS CLOUDFIT ?
CloudFIT is a project aimed at defining an infrastructure for deploying intrusion & fault tolerant (IFT) services in a cloud environment. It’s based on intrusion-tolerant replication, which allows tolerating intrusions in a subset of the replicas.

KEY DEPENDENCIES
- Virtualization Technologies
- Software based Trusted Computing Base (TCB)
- Byzantine Fault-Tolerant Replication (BFT)

CHALLENGES
- Secure Hypervisor (Virtualization Layer)
- Design of Fault & Intrusion Aware Policies for Replication
- Reduce Replicas Inter-Communication Overhead
- Dynamicy of Available Resources

OUTPUT
- Prototype implementation of virtualization hardplan for cloud computing capable of hosting Intrusion tolerant services

FITC
A software architecture that incorporates a number of infrastructure components for BFT services that is globally called FITC, Fault and Intrusion Tolerant Cloud Computing Hardplan:

- VM based components
- Dynamic grouping of service replicas
- Proactive recovery with Replica Replacement Service (RRS)

PLAN & STEPS
Virtualization is now general state-of-the-art technology for managing resources in computational clouds and for executing cloud applications in isolation from one another. Intrusion-tolerant replication (ITR) with proactive recovery requires a timely and trusted component in order to ensure the execution of recovery. Our project can be breakdown into development of following individual components and their integration:

- Defining of virtualization architecture with minimal TCB, capable for intrusion tolerant replication
- Specification of an ITR infrastructure based on TCB & BFT
- BFT library with software based TCB
- Algorithm development for replica proactive & active replacement for safety by taking profit of virtualization features and incorporating IFT Policies
- Prototype development of cloud resource allocator with IFT algorithm

Contact Information:
Wasim Bari bari@lasige.di.fc.ul.pt
Vinicius Vielmo Cogo vielmo@lasige.di.fc.ul.pt
Prof. Alysson Bessani bessani@di.fc.ul.pt
Prof. Marcelo Pasin pasin@di.fc.ul.pt
Prof. Hans P. Reiser hans@di.fc.ul.pt

CLOUDFIT