Multi-Layer Threat Analysis of the Cloud

Salman Manzoor, Antonios Gouglidis, Matthew Bradbury and Neeraj Suri
Lancaster University, UK
{s.manzoor1, a.gouglidis, m.s.bradbury, neeraj.suri}@lancaster.ac.uk

Cloud's Benefits

- Access to geo-distributed resources.
- Flexible on-demand binding of resources to services.

Cloud's Security Concerns

- Multi-layer, multi-technology attack surfaces.
- Complex and dynamic threat propagation pathways.

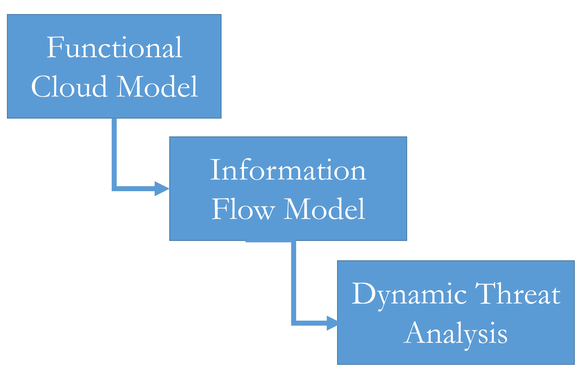
State of the Art

Threat Analysis (TA) as a process of ascertaining a system's exposure to threats focuses on analysing threats to targeted assets and considers static interconnections amongst the assets.

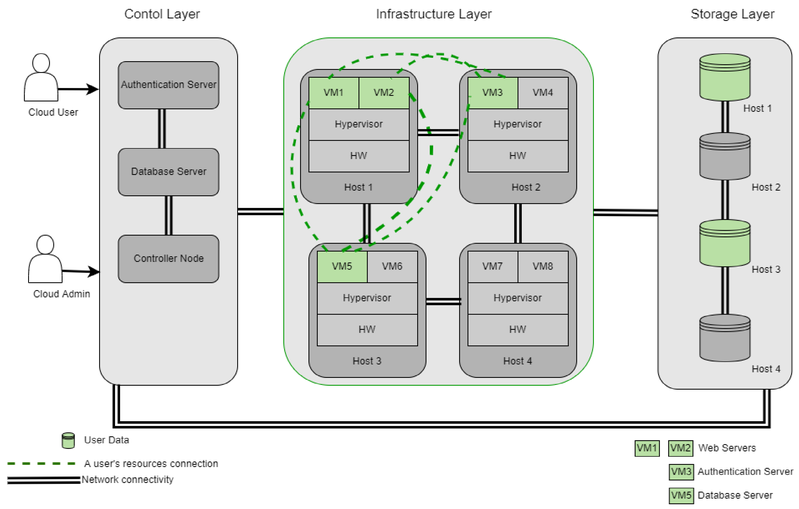
Our Contributions

- Development of a Functional Cloud Model.
- Development of a technology-agnostic Information Flow Model.
- Development of a Dynamic Threat Analysis approach for the Cloud.

Methodology: The Building Blocks

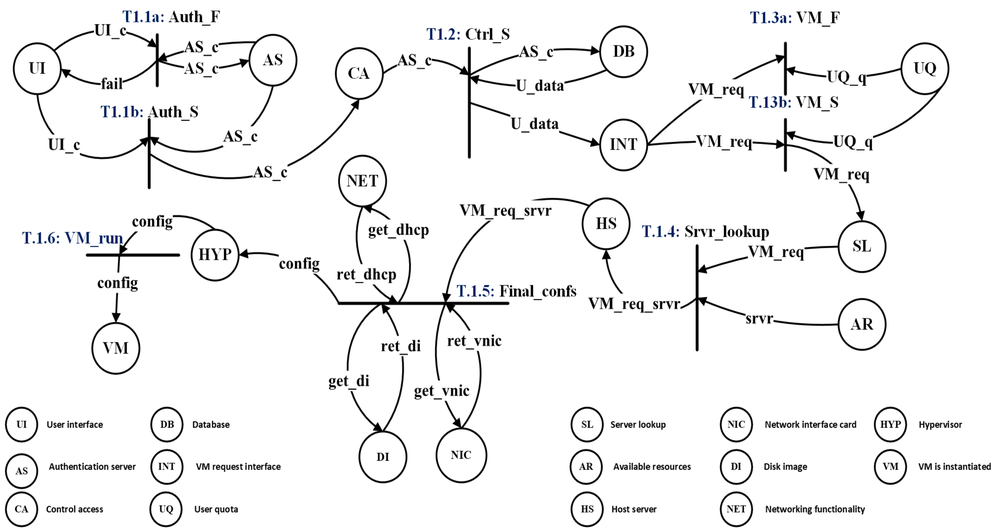


Functional Cloud Model



Control Layer: Authenticates users, manages and schedules resources.
Infrastructure Layer: Binds VMs to physical hosts.
Storage Layer: Provides consistent data to users.

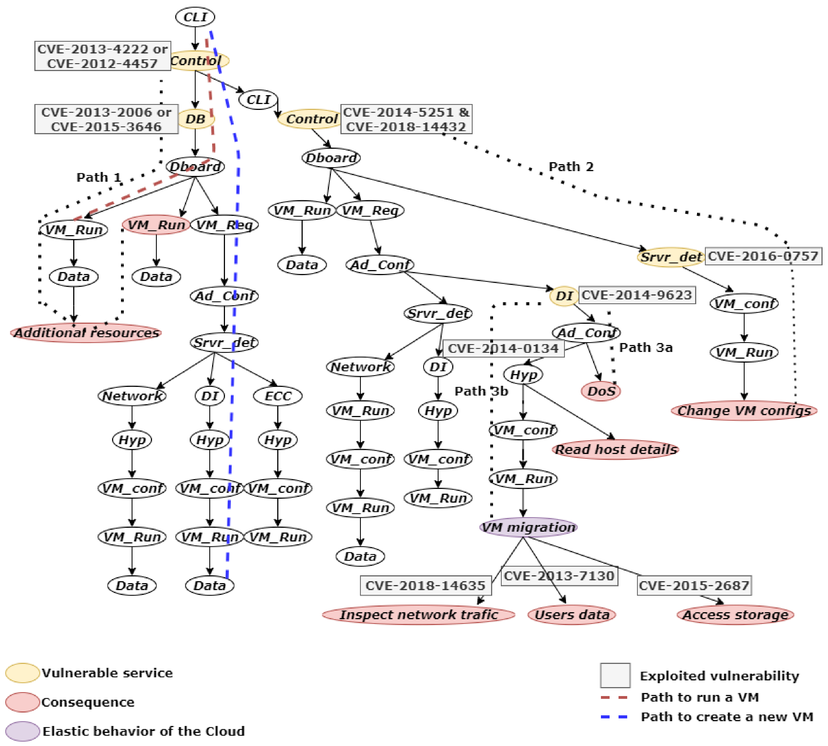
Information Flow Model



- Technology-agnostic information flow model using Petri nets.
- Ability to capture dynamic interconnections over the VM migration.
- Scalable to additional constraints, e.g., addition of new threats.

Threat Analysis

- Create a baseline of the Cloud's functional behaviour.
- Ability to explore propagation of threats in considering new interactions created at run-time.



- Capability to trace specific threats in a technology-agnostic manner (Path 1).
- Capability to analyse the impact of threats on services belonging to different layers in the Cloud (Path 2).
- Capability to explore the potential of threats to propagate across the Cloud considering the elasticity of the Cloud (Path 3(b)).

Acknowledgments

This work is conducted, in part, under the auspices of the EU Horizon 2020 Research and Innovation program under Grant Agreement No. 830927 (CONCORDIA) and by Security Lancaster under the EPSRC grant EP/V026763/1.