When dynamic VM migration falls under the control of VM user…

Kahina LAZRI, Sylvie LANIEPCE, Haiming ZHENG
IMT/OLPS/ASE/SEC/NPS
Orange Labs, Caen

Jalel Ben-Othman
L2TI laboratory
Paris13

Symposium sur la sécurité des technologies de l'information et des communications.
SSTIC'14. Friday 6th June, 2014. Rennes.

Outline

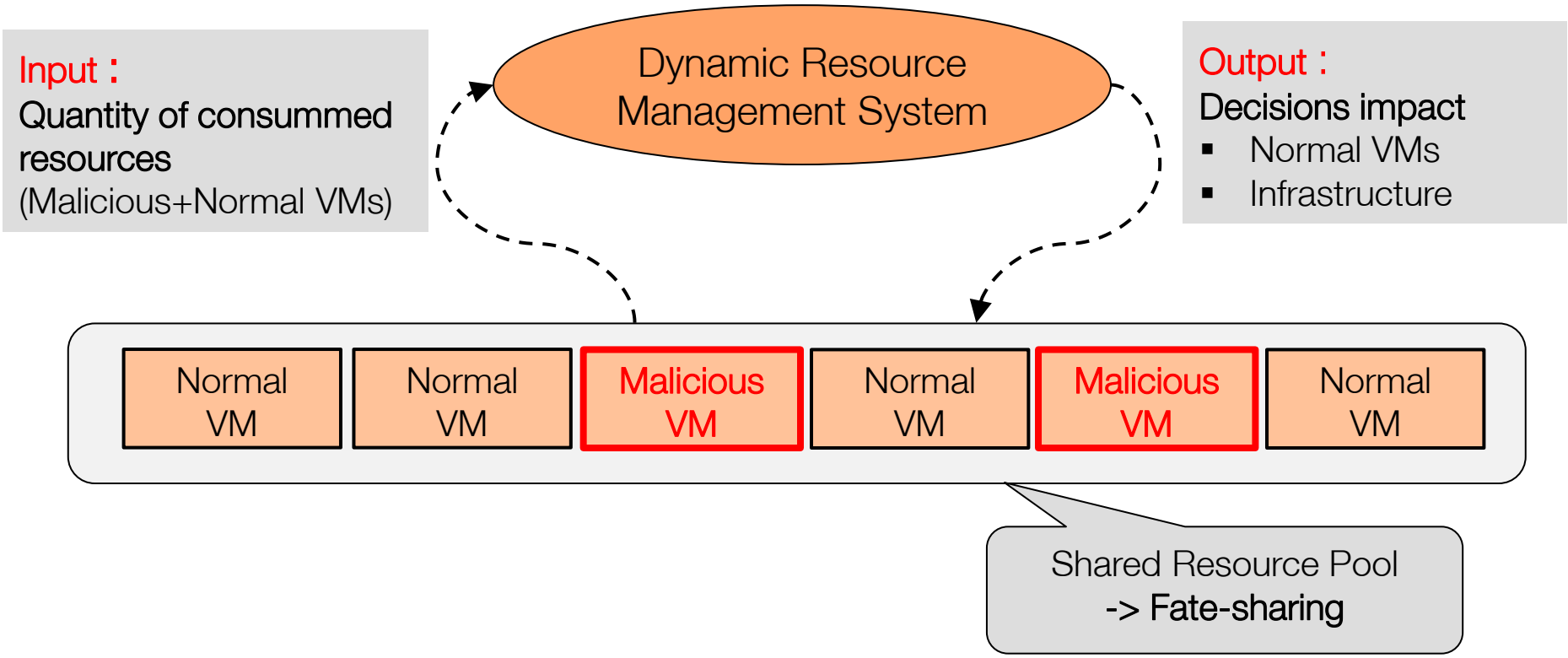
- Problem Definition
- Dynamic Resource Management Vulnerability
  - VMware Distributed Resource Scheduler (DRS) algorithm analysis
  - Attack scheme
  - Cluster vulnerability assessment
- Demonstration
- Conclusion

Scope

- Domain of new vulnerabilities appeared with cloud (virtualization)
  - ➢ Resource Sharing & Multi-tenancy: cross-Virtual Machine attacks (cross-VM)
    - ➢ Dynamic resource management

- Elasticity <-> Dynamicity (today)
  - – Resource Overcommitment
  - – VM Migration

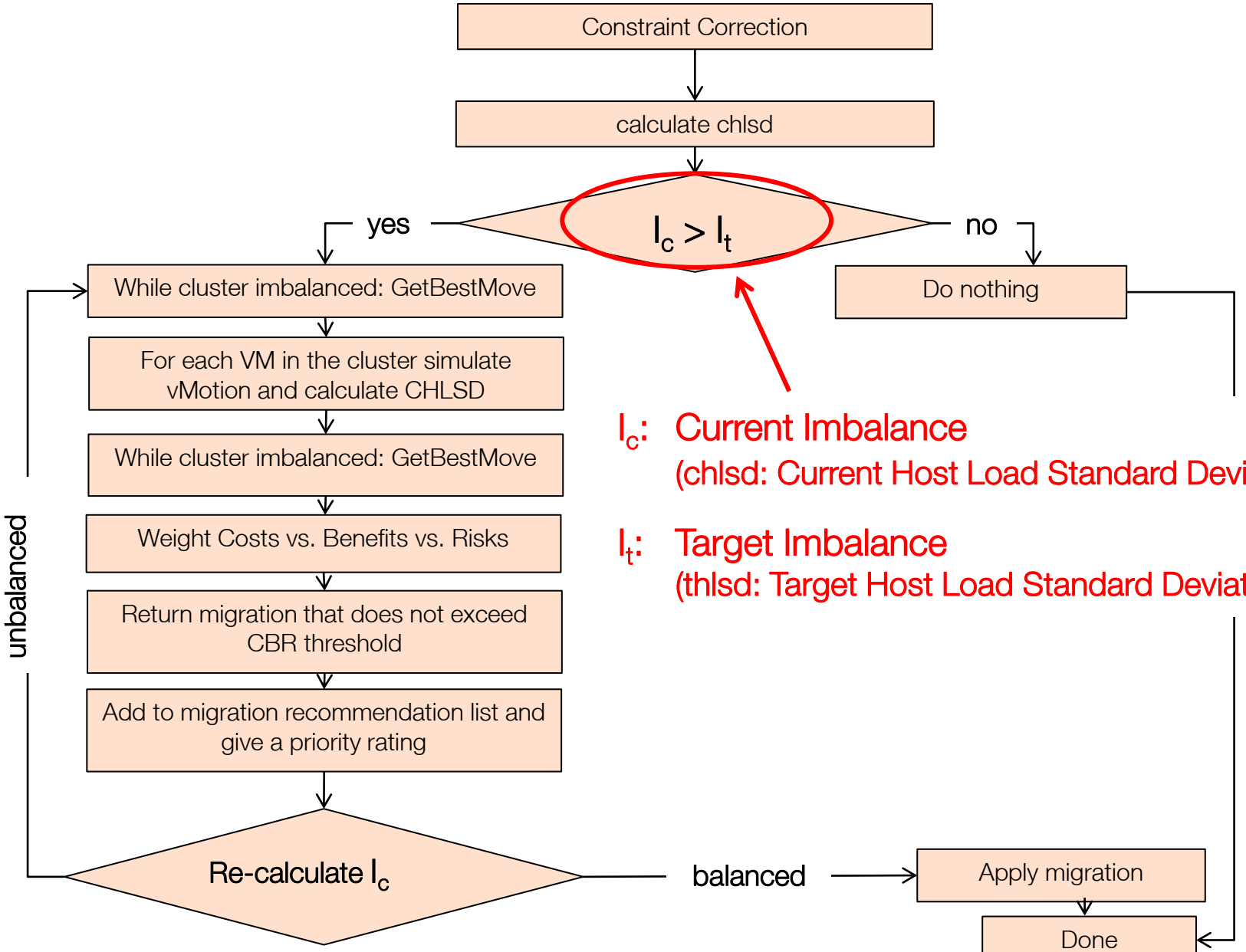
Resource sharing and dynamic resource allocation



- Demonstrate that dynamic resource management systems might be vulnerable to malicious manipulation of VM resource consumption

- Abuse: cause the resource management system to trigger VM migrations
  Cost for both the infrastructure and migrated VMs

Distributed Resource Scheduler Algorithm (DRS, VMware)



I_c: Current Imbalance
(chlsd: Current Host Load Standard Deviation)

I_t: Target Imbalance
(thlsd: Target Host Load Standard Deviation)

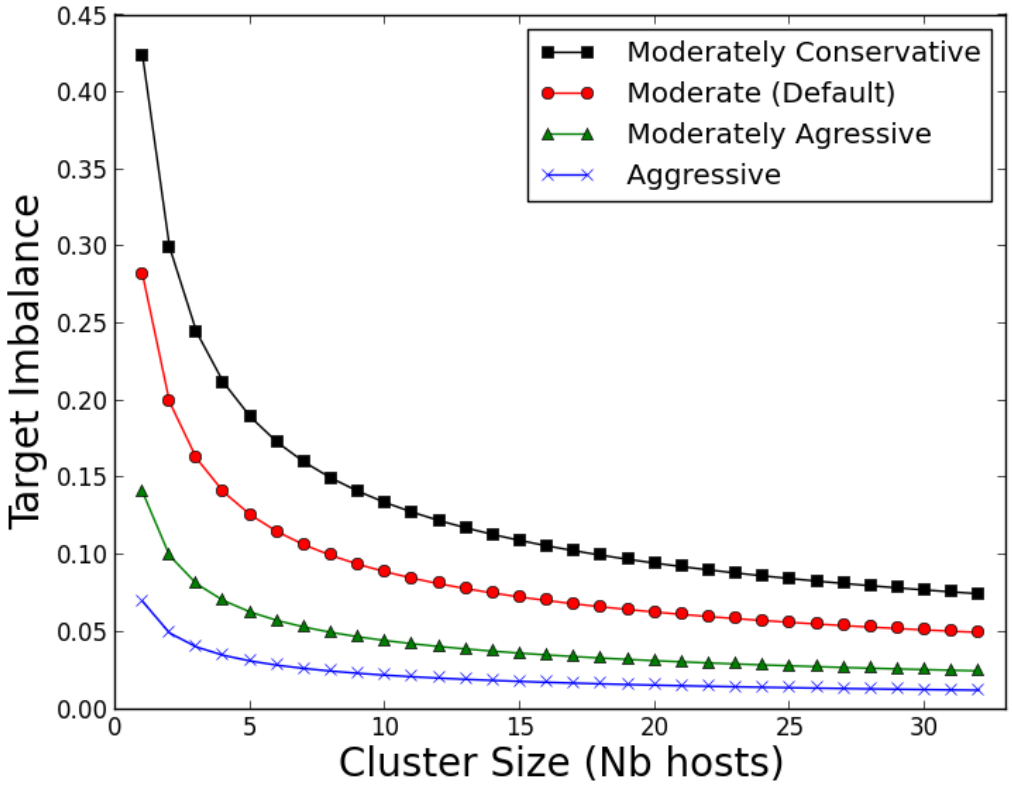
source: VMware vSphere 4.1 HA and DRS. technical Deepdive. D.Epping et F. Denneman

DRS: Target Imbalance (I_t) analysis

$$I_t = \frac{Constant_{Aggressiveness}}{\sqrt{Cluster\ Size}}$$

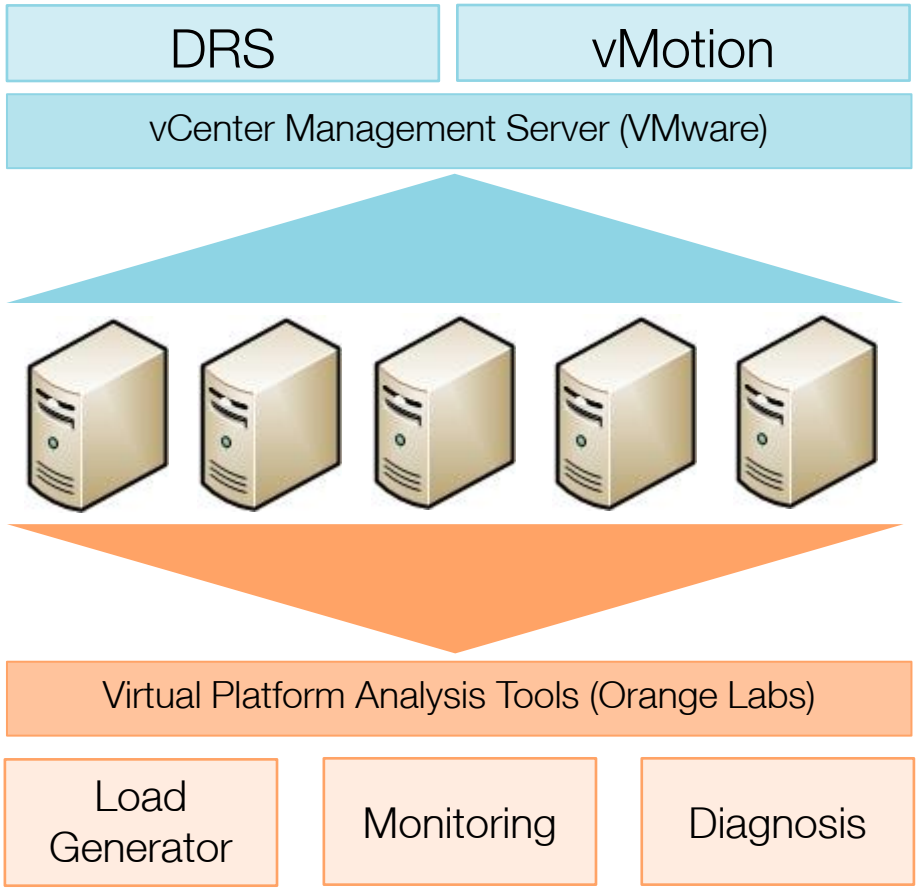
Four Aggressiveness Levels enabling dynamic migrations:

- Moderately Conservative
- Moderate (Default)
- Moderately Aggressive
- Aggressive



Abusive VM Migration Attack:
deliberately manipulate the quantity of resources consumed by VMs to enforce DRS to trigger VM migrations : $I_c > I_t$

Experimentation Setup



Context

5 Hosts
- 16 GB of RAM each
- 8 CPU x 2.133 GHz each
- VMs / Host = 10

% Overcommitment
- Mem = 13.18% (17.5 GB)
- CPU = 25% (10 vCPU)

Resource Usage in normal VMs
- Real private IaaS cloud traces

Abusive VM Migration Attack: one shot

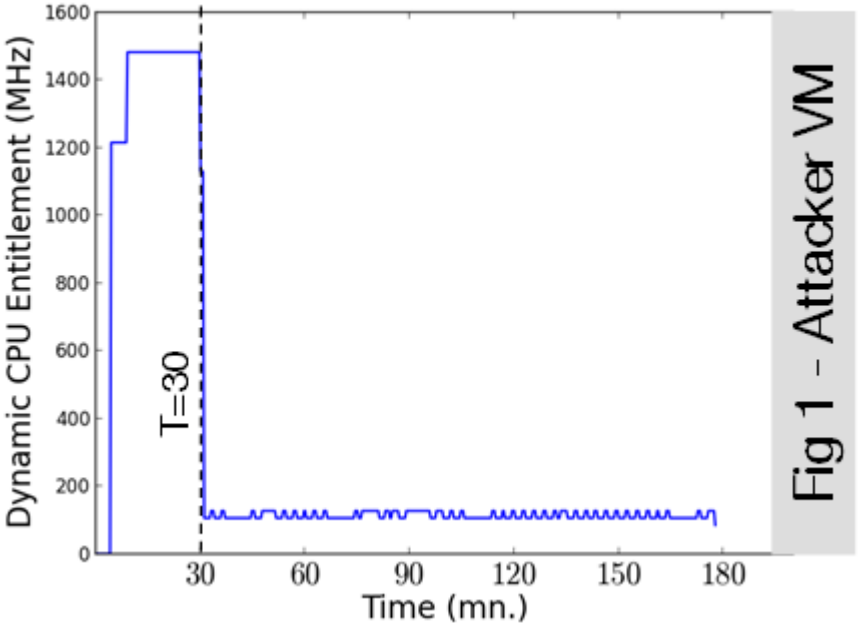


Fig 1 - Attacker VM

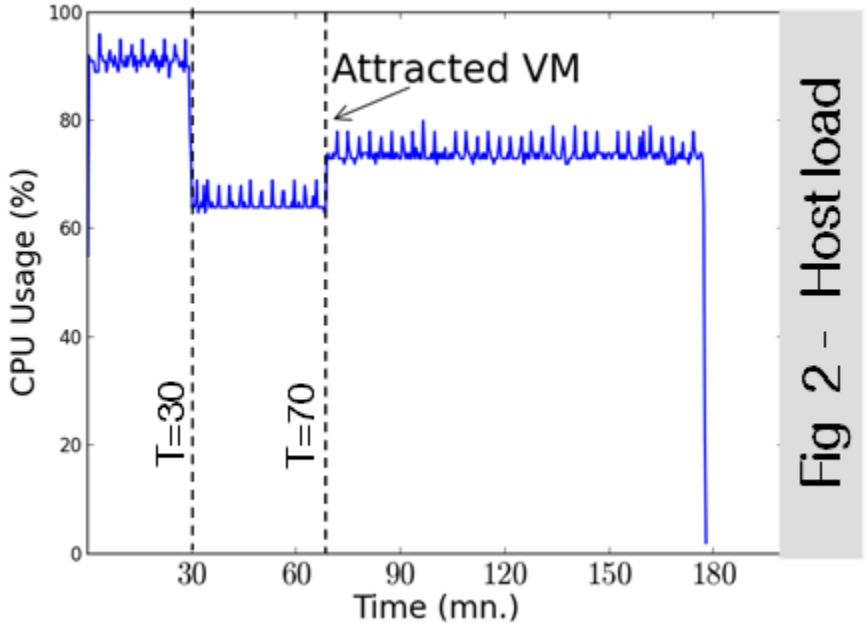


Fig 2 - Host load

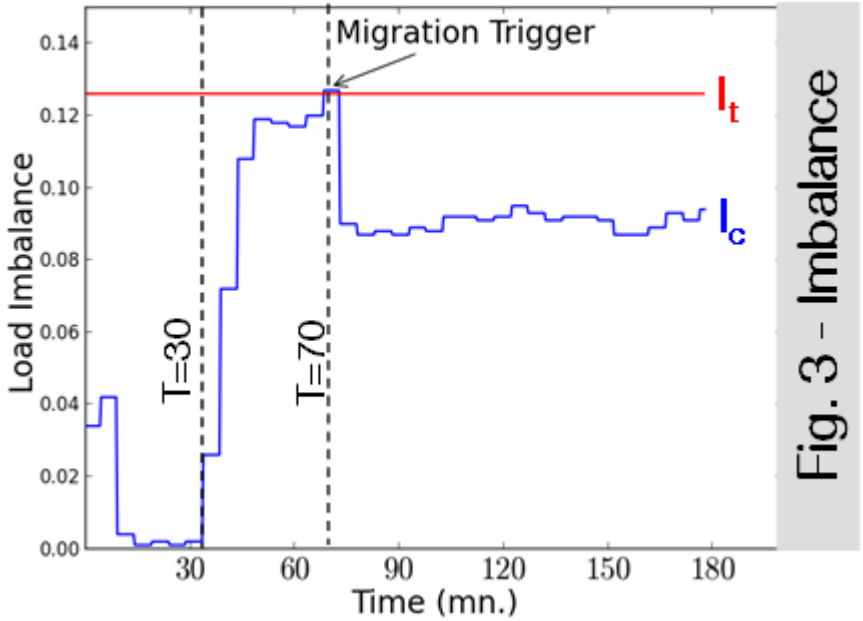


Fig. 3 - Imbalance

Coordinated Abusive VM Migration Attack: Serial Migration

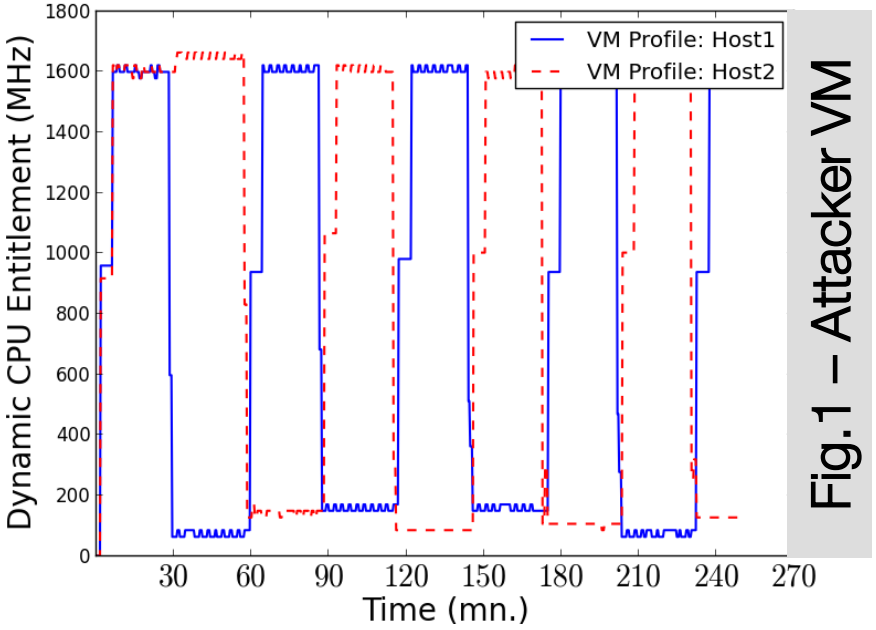


Fig.1 – Attacker VM

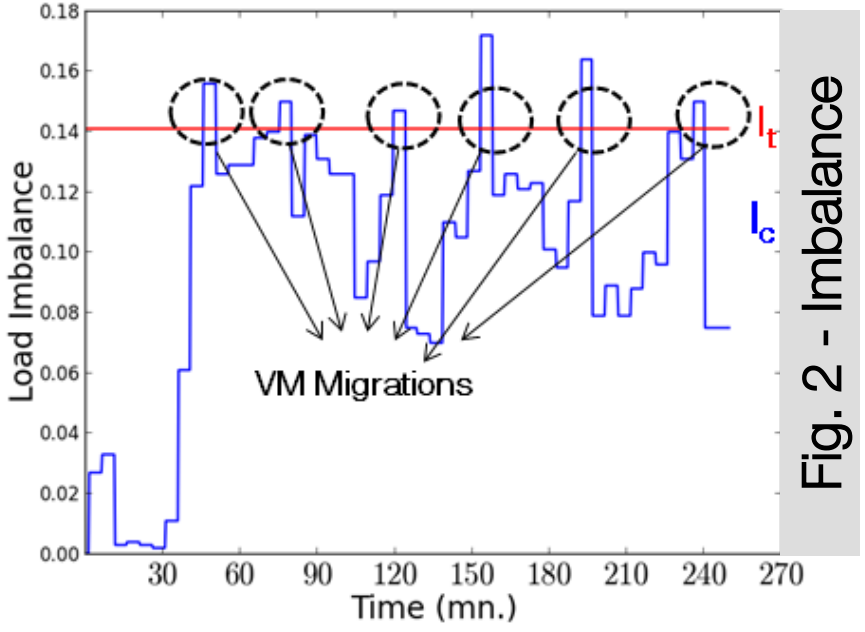


Fig. 2 - Imbalance

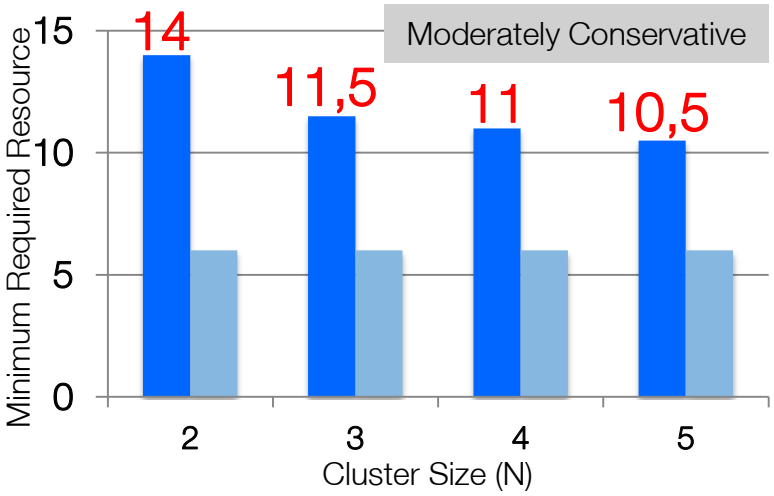
Attack conditions:

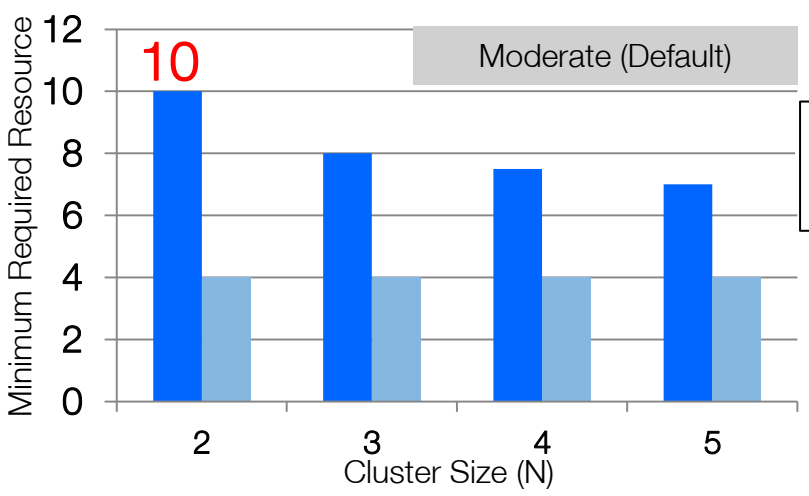
- Attacker coordinates VMs on two different hosts
- VMs fluctuate their resource consumption in phase opposition between the two hosts

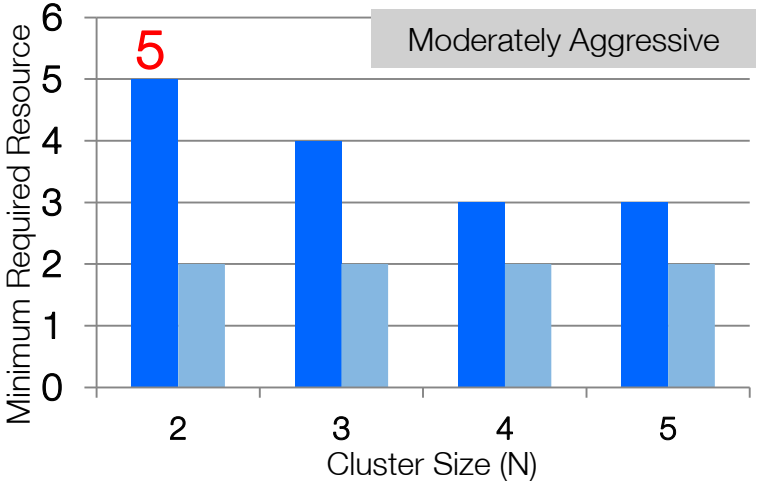
Vulnerability Measurement (small cluster)

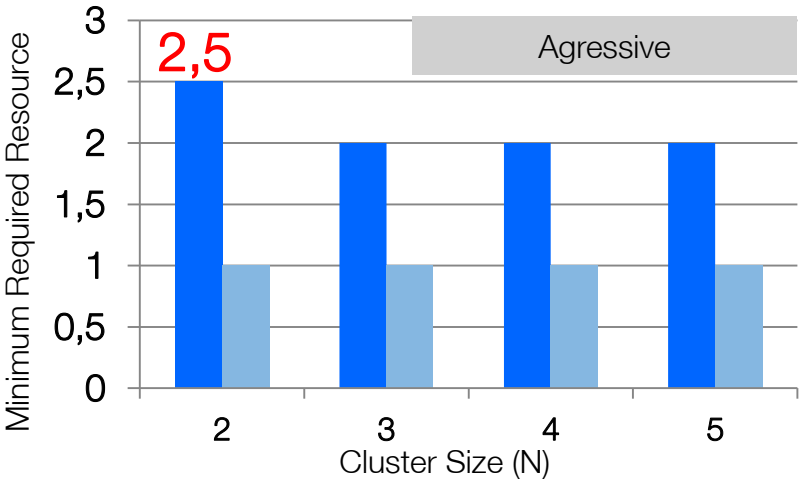
Vulnerability increases when cluster size increases

Vulnerability increases when DRS Aggressiveness increases



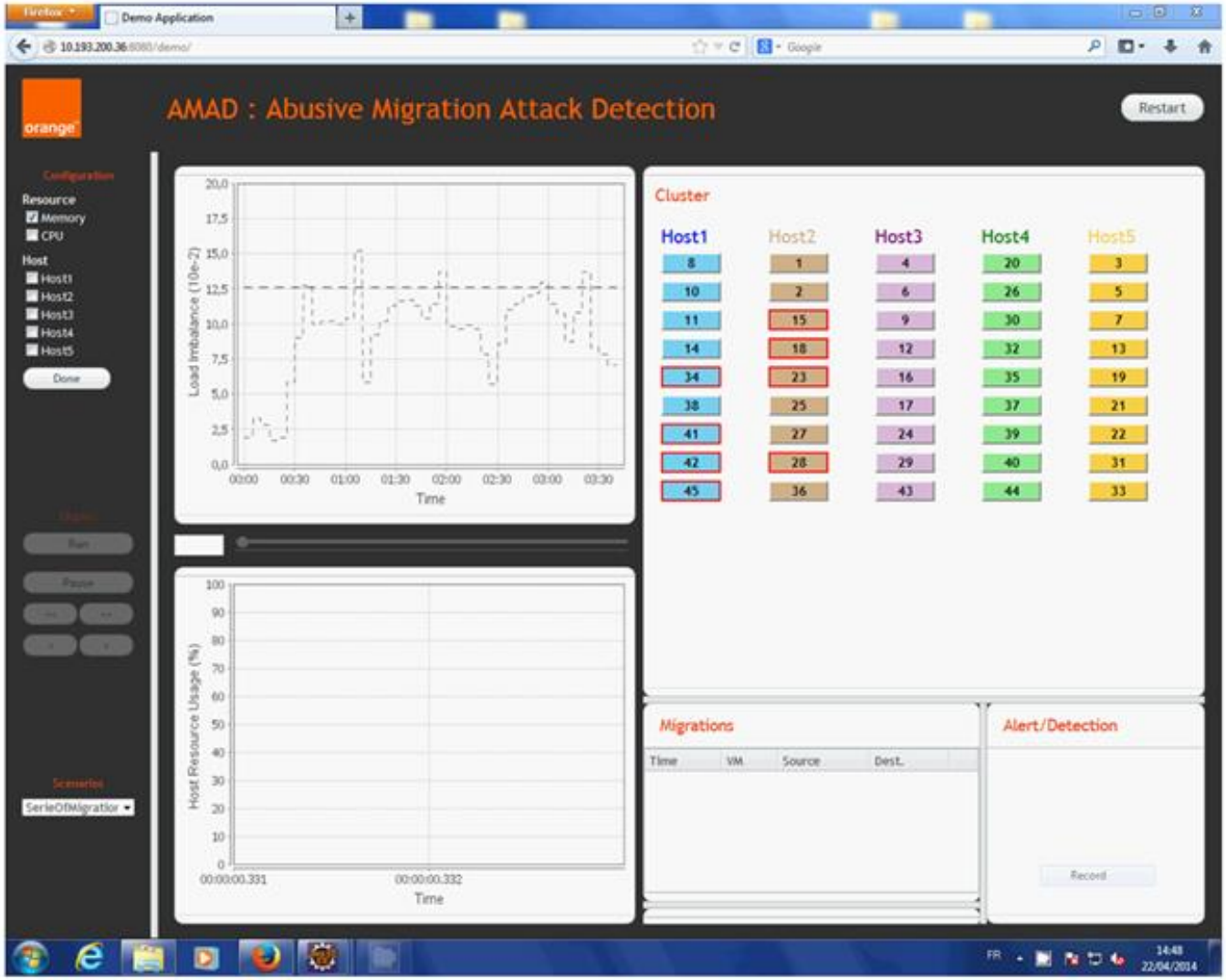






Context:'one shot' Abusive VM Migration attack, execution context described in slide 8

Demonstration



Conclusion

- How to autonomously mitigate such threats ?
  - Proactive

    Integrating security considerations in dynamic resource management systems design?

  - Reactive

    Autonomic Monitoring and detection of malicious resource consumption profiles
    - How to characterize such profiles?
    - How to deal with these profiles?

Thank you
Questions?