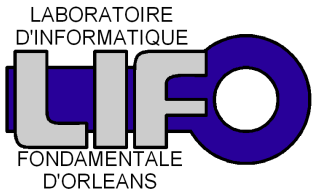
Spécification et analyse formelle des politiques de sécurité dans le cloud computing

Asma GUESMI, Patrice CLEMENTE, Frédéric LOULERGUE, Pascal BERTHOMÉ

Laboratoire d'Informatique Fondamentale d'Orléans (LIFO)
Université d'Orléans, INSA Centre-Val de Loire

SEC2 2015 - Premier atelier sur la Sécurité dans les clouds

June 30, 2015



Outline

1. Introduction
   - Context
2. Contribution
   - General Process
   - Requirements specification using Alloy
   - Alloy example
3. Conclusion

Problematic & Motivation

- Cloud brokers negotiate only service and resources requirements
- Cloud brokers do not consider security requirements

Contribution

1. The customer can specify the requirements for the resources to deploy in the cloud
2. Formal verification of the cloud systems and the security policies
3. Using the Alloy language for the requirements specification
4. Using Alloy analyzer to check the satisfiability of security and access control properties

General Process

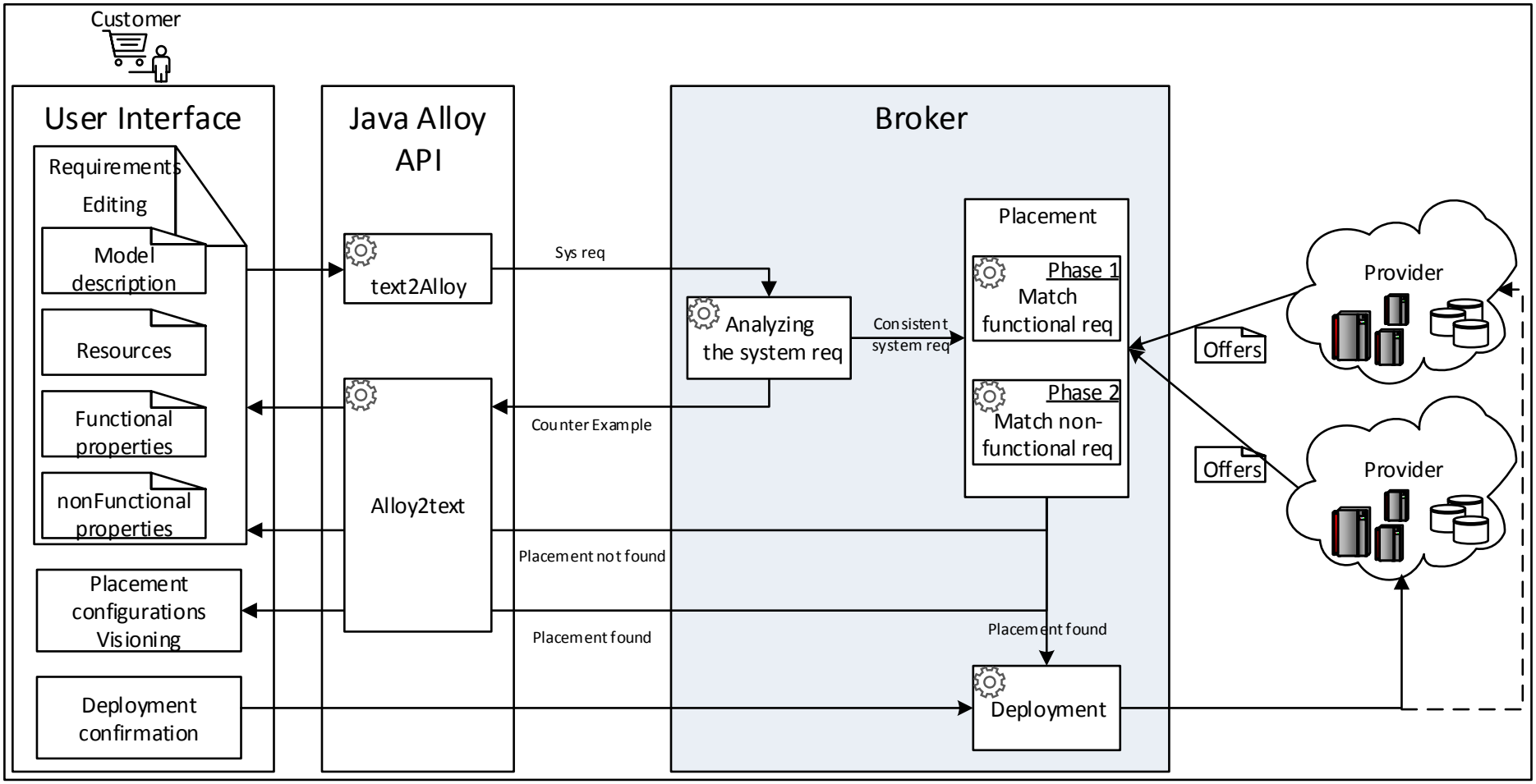


Figure: The workflow of the broker application

Requirements specification

- The model: virtual machines (vms), storage nodes
- Functional requirements (cpu, ram and storage)
- Non-functional requirements (security, usage and access control)

Non-fonctional requirements I

Usage properties

Collaboration, Concurrence, Isolation

- The customer specifies the type of relations between resources
- Collaborating vms should be related by information flows
- Concurrent vms should not be related by information flows

Security Properties

Confidentiality, Integrity, Privilege separation, Placement constraints

- Concurrent vms should be allocated on different clusters, and should not be related by information flows
- Collaborating vms should reside the same cluster, and should be related by information flows

Non-fonctional requirements II

Access Control

Specify rules to manage how final users can access to the client resources

- A user having the visitor status cannot write a comment on a document
- A user cannot access to two concurrent vms

Formal verification

- Using Alloy analyzer for the automatic syntactic and semantic verification
- Detection conflicts in the description
- Verification of the consistency of the customer's system
- Verification of the satisfiability of security properties
- Alloy returns a counter-example when a specification is not satisfied
- Alloy places the resources in cloud providers, in a way that fulfills all customer requirements

Alloy example I

Security property

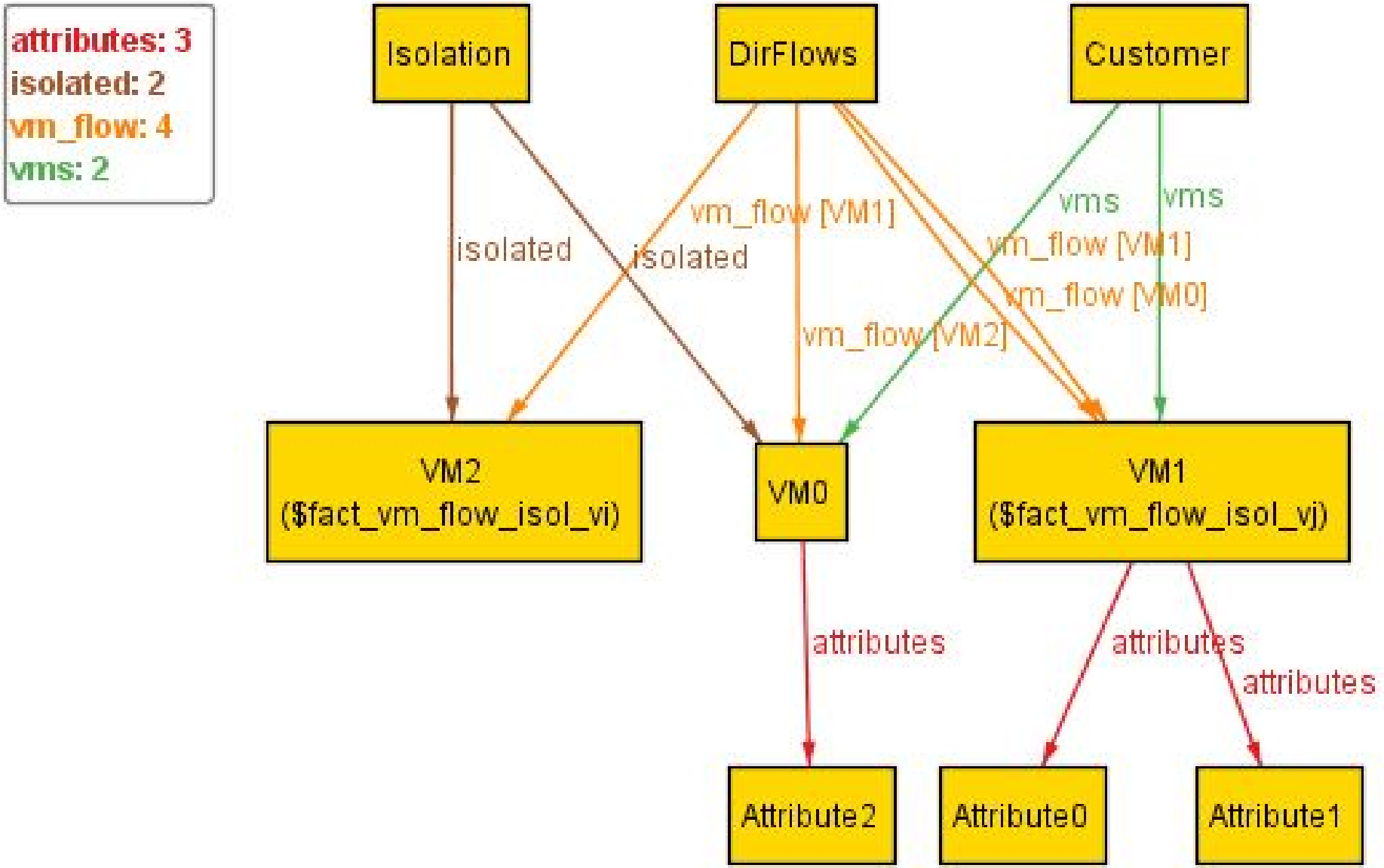
There is no information that flows into or outside all isolated vms

```
sig Customer{vms: some VM}
sig VM{attributes: set Attribute}
sig Attribute{}
abstract one sig DirFlows{vm_flow: set VM->VM }
abstract one sig Isolation{isolated: set VM}

pred fact_vm_flow_isol{ all vi:VM | no vj: VM |
vi in Isolation.isolated &&
(vi->vj in DirFlows.vm_flow || vj->vi in DirFlows.vm_flow)}

check {fact_vm_flow_isol}
```

Alloy example II



Conclusion

1. Describe a general process for cloud brokering considering security [1, 2]
2. Use formal language to describe complex cloud systems, and to express fine grained security requirements
3. Using formal methods to place resources in the cloud
4. Using formal methods to analyze complex cloud systems, to check their consistency and the satisfiability of security policies.

Asma Guesmi and Patrice Clemente.
Access control and security properties requirements specification for clouds' seclas.
In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, volume 1, pages 723–729. IEEE, 2013.

Asma Guesmi, Patrice Clemente, Frédéric Loulergue, and Pascal Berthomé.
Cloud resources placement based on functional and non-functional requirements.
In *SECRYPT 2015 - Proceedings of the 12th International Conference on Security and Cryptography, Colmar, France, 20-22 July*, 2015.