A Formal Model for Isolation Management in Cloud Infrastructure-as-a-Service

Khalid Zaman Bijon, Ram Krishnan and Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio

October 15-17, 2014
NSS 2014: The 8th International Conference on Network and System Security

Intro. & Motivation

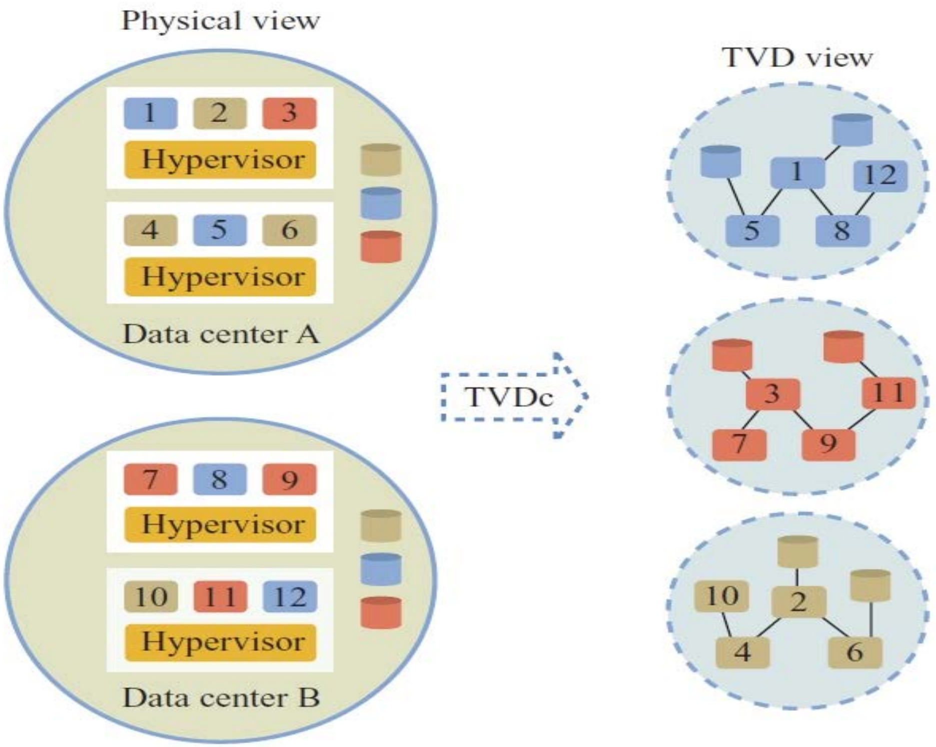
- A IaaS cloud service provider offers
  - A number of heterogeneous virtual resources, e.g., virtual machines, virtual networks, etc.
  - To a large number of clients, also referred as tenants.

- Management of these virtual resources is very complex
  - Cloud datacenter may contain thousands of virtual resources from hundreds of tenants.
  - Different configurations requirements from different tenants.
  - Management proper sharing of physical resources among different virtual resources across tenants (multi-tenancy).

- The challenge is to develop proper mechanism to manage isolation of the virtual resources across tenants.

Background

- Recently, trusted virtual datacenter (TVDc)[1] is proposed to manage isolation in cloud IaaS
  - By defining trusted virtual domains (TVDs) where each TVD is assigned to virtual machines and its associated virtual resources such as virtual networks, virtual storages, etc. that serve a common purpose.
  - A TVD identifier is represented as a security clearance (also referred as a color).
  - Here, for example, a color can represent the virtual resources of a particular tenant.
  - Therefore, in TVDc, virtual resources with same color are viewed as single and disjoint computing resources.



[1] S. Berger et al. Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal of R&D, 53(4):6{1, 2009.

Background (cont.)

- TVDc provide mechanism for isolating administrative user privileges
  - Proposed three different administrative roles for performing three different jobs in cloud: IT datacenter administrator, TVDc administrator, and tenant administrator.
- IT datacenter administrator
  - A user having this role is a superuser in the system.
  - Discover virtual resources and grouped as different trusted virtual datacenters (TVDc) groups.
  - Assign a TVDc group to each user having TVDc or tenant administrator role.
  - Create colors and assign colors to each user having TVDc administrator role.
- TVDc administrator
  - Assign colors to virtual resources in their TVDc groups.
  - Assign colors to users having tenant administrator role and belongs to same TVDc groups.
- Tenant administrator
  - perform basic cloud administrative operations, such as connect vm to a virtual network, if the resources have same color.

Isolations

- TVDc supports following four types of isolations:

- Data Sharing
  - A VM Only can share data with another VM with same color.
  - VMs are allowed to connect to a VLAN only if both VMs and the VLAN have common colors.

- Hypervisor (host) Authorization
  - A host is assigned a set of colors.
  - Only allowed to run vms having a color belong to that set.

- Co-location Management
  - Certain colors can be declared as conflicting with each other.
  - Constraints VMs to run in same host that are assigned conflicting colors.

- Management Constraints
  - Tenant Administrator role.
  - Each user having this role only perform operation within his assigned color.

Proposed Model

- Develop a formal model for TVDc which we call Formalized-TVDc (also referred as F-TVDc)

- Leverage an Attribute based system to represent different properties of the virtual resources, such as color and TVDc groups

- Consists authorization model for three type of administrative users

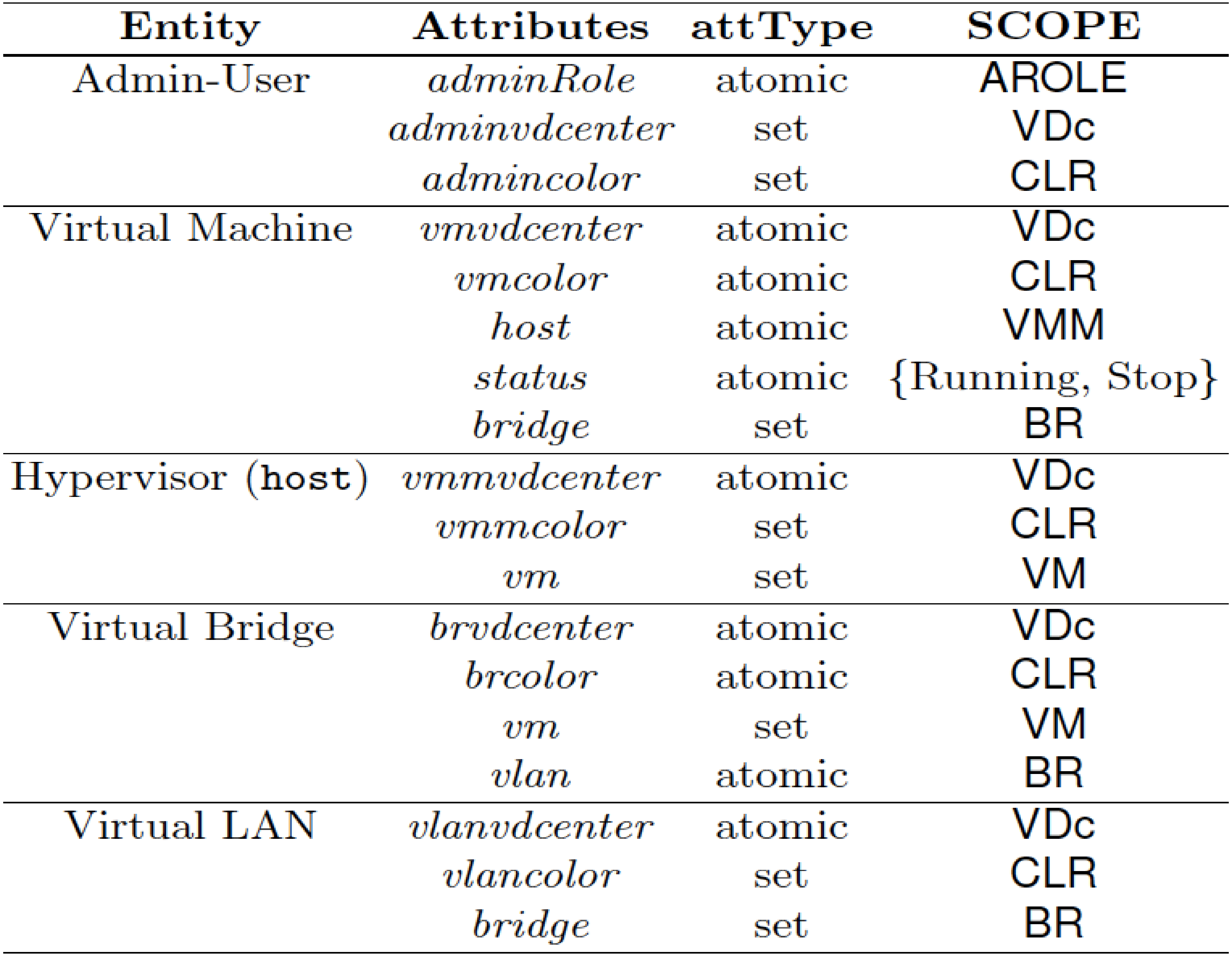
- Enforcement mechanism for the co-location constraints

Formalized-TVDc

- F-TVDc contains following sets of the basic components:
  - CLR = Finite set of existing colors
  - VDc = Finite set of existing virtual data centers
  - AROLE = {itAdmin, tvdcAdmin, tntAdmin}
  - AU = Finite set of existing admin-users
  - VM = Finite set of existing virtual machines
  - VMM = Finite set of existing hypervisors
  - BR = Finite set of existing virtual bridges
  - VLAN = Finite set of existing virtual LANs

- Admin-users and virtual resources have different attributes:
  - Attributes are name:value pairs
  - Can be set valued or atomic valued
  - Characterize different properties of the element

Attributes



Entity	Attributes	attType	SCOPE
Admin-User	*adminRole*	atomic	AROLE
	adminvdcenter	set	VDc
	admincolor	set	CLR
Virtual Machine	*vmvdcenter*	atomic	VDc
	vmcolor	atomic	CLR
	host	atomic	VMM
	status	atomic	{Running, Stop}
	bridge	set	BR
Hypervisor (**host**)	*vmmvdcenter*	atomic	VDc
	vmmcolor	set	CLR
	vm	set	VM
Virtual Bridge	*brvdcenter*	atomic	VDc
	brcolor	atomic	CLR
	vm	set	VM
	vlan	atomic	BR
Virtual LAN	*vlanvdcenter*	atomic	VDc
	vlancolor	set	CLR
	bridge	set	BR

Administrative Models

- F-TVDc formally specifies operations for the admin-users with three different roles

- Operations for admin-users with **itAdmin** role
  - **CreateVDC:** This operation creates a virtual datacenter,
  - **CreateCl** and **RemoveCl:** Using these two operations, an admin-user with itAdmin role create a new color cl and remove an existing color cl.
  - **Add_Cl$_{\mathbf{TVDcAdmin}}$:** This operation adds a clearance to an admin-user having tvdcAdmin role.
  - **Rem_Cl$_{\mathbf{TVDcAdmin}}$:** Using this operation, an itAdmin removes a color cl from an admin-user having role tvdcAdmin.
  - **Assign_VDC$_{\mathbf{Admin}}$:**This operation assign a virtual datacenter identifier to an admin-user having tvdcAdmin or tenantAdmin role.
  - Similarly, **Assign_VDC$_{VM}$**, **Assign_VDC$_{VMM}$**, **Assign_VDC$_{VLAN}$**, and **Assign_VDC$_{BR}$** assign a virtual datacenter identifier to respective virtual resource.

- All these operations are only authorized for admin-users who have **itAdmin** assigned to their *adminRole* attribute

Administrative Models (cont.)

Operations for admin-users with **tvdcAdmin** role:

- **Assign_Cl$_{\textbf{TAdmin}}$:** This operation adds a clearance to an admin-user having tenantAdmin role. The tvdcAdmin can only add a clearance to a tenantAdmin if they are in same virtual datacenter which is assigned to their **adminvdcenter** attribute.

- **RM_Cl$_{\textbf{TAdmin}}$:** This operation removes a clearance from an admin-user having tenantAdmin role. The tvdcAdmin can only remove a clearance to a tenantAdmin if they are in same virtual datacenter which is assigned to their **adminvdcenter** attribute.

- Similarly, **Assign_Cl$_{\textbf{VM}}$**, **Assign_Cl$_{\textbf{VMM}}$**, **Assign_Cl$_{\textbf{VLAN}}$**, and **Assign_Cl$_{\textbf{BR}}$** assign a virtual datacenter identifier to respective virtual resource by a admin-user having tvdcAdmin role and they are in same virtual datacenter.

Administrative Models (cont.)

Operations for admin-users with **tenantAdmin** role:

- **Boot:** Using this operation a tenant admin-user u boots a VM vm in a Host vmm.

  1. The precondition of this operation veries if the u has same color of the vm. This ensures management isolation constraint.

  2. It also varifies if both VM (vm) and Host (vmm) has same color which ensures host authorization isolation.

- **ConVmToBr** and **ConBrToVLAN:** These operations connect a vm to a virtual bridge br and a bridge to a virtual LAN respectively.

  1. A vm can be connected to a virtual bridge if they have same color.

  2. A virtual bridge can be connected to a VLAN if they have same color.

  3. This approach ensures data isolation constraint.

Administrative Models (cont.)

- Co-location Constraints Verification
  - Verified during each boot operation
  - **Evaluate_CLocConst** method is called
  - Some colors are specified as conflicted in a set called **ConflictColor**
  - VMs with conflicted color in same Host
  - Ensures co-location isolation of VMs

Conclusion

- Formally represents an isolation management process of virtual resources in cloud IaaS.
  - Develop an attribute based system
  - Identified administrative operations in cloud IaaS
  - Develop a mechanism to handle co-location issues in multi-tenant scenarios

- Future Work
  - Identify conflicts among various attributes, e.g., tenant, performance, of virtual machines
  - Suitable virtual machine scheduler when there are conflicts