



Enterprise Scale Separation VMM Systems

Myong Kang

Computer Security Section
Naval Research Laboratory
Washington, DC 20375

myong.kang@nrl.navy.mil

Issues of Some Secure Systems

- Poorly constructed secure systems
 - Error prone
 - Difficult to understand and maintain
- Security mechanisms/features are too complex or not matching with underlying systems to protect
 - Too difficult to specify security policies
 - Too difficult to understand security policy and enforcement mechanism
- Not enough qualified sys admins / security officers to manage the system in the organization
 - Full power of security mechanisms of the system is not being utilized
 - Security or performance may be sacrificed
 - Complex security policy and mechanism compound the problem

- Replaced Xen's FLASK security architecture with a simpler, more intuitive Xenon security architecture
 - Separation of security policy and enforcement mechanism
 - Intuitive and expressive policy language and interface that are tailored to the hypervisor
 - Easy to validate security mechanisms
 - Easy to understand security policies
- Reduced in size and refactored the source code to significantly reduce its cyclomatic complexity
- Reduced attack surface of control domain (Domain-0)
- Provided a visual management interface for easy and intuitive security policy authoring, VM management and VM monitoring
- Added a network access policy that is easily configurable through the management interface
 - Enforced by Open vSwitch to restrict VM network access

Xenon Security Features

- Security Tags – e.g., Red, Yellow, Admin, Operational, Entertainment
- Enclave – Container for resources (e.g., VMs, hardware) that inherit the same Tag
- Relationship among Tags
 - A “conflict” between two or more tags can be defined, which will be translated into virtualization connectivity rules enforced by Xenon and network connectivity rules enforced by Open vSwitch
 - Hypervisor does not allow any communication between VMs with different tags
 - Open vSwitch does not allow any network communication between VMs with different tags
 - Option for VMs with two different tags cannot run at the same time on an Xenon host

Xenon Security Features (cont'd)

The image displays three windows from the Xenon Enterprise Demo:

- Policy Editor (Left):** Shows the configuration for the 'security' tag. The 'Tags' menu is circled in red. The tag is assigned the colors Red, Green, and Blue. The 'Name' is 'security' and the 'ID' is 4.
- Policy Editor (Right):** Shows the configuration for the 'tag_separation' conflict. The 'Conflicts' menu is circled in red. The conflict is assigned the colors Blue, Green, and Red. The 'Name' is 'tag_separation' and the 'ID' is 2. The 'Mode' is set to 'Allow to run simultaneously?'.
- Live Mode (Bottom):** Shows the system's state. The 'Enclaves' menu is circled in red. It displays three enclaves: 'human_resources' (blue), 'entertainment' (green), and 'security' (red). Each enclave shows its assigned hardware and domains.

Unassigned Hardware:

- Network controllers: Network controller (wlp6s0, 60:57:18:d7:62:20) on Ethernet controller (enp7s0f1, 74:e6:e2:53:45:ab)
- Storage controllers: SATA controller on 00:1f:2

Domains, SecLabels, & Enclaves:

- Domain-0 (required)
- human_resources: personnel_mgr (stopped)
- entertainment: user_vm_1 (stopped), user_vm_2 (stopped), user_vm_3 (stopped)
- security: firewall (stopped), nids (stopped)

Enclaves:

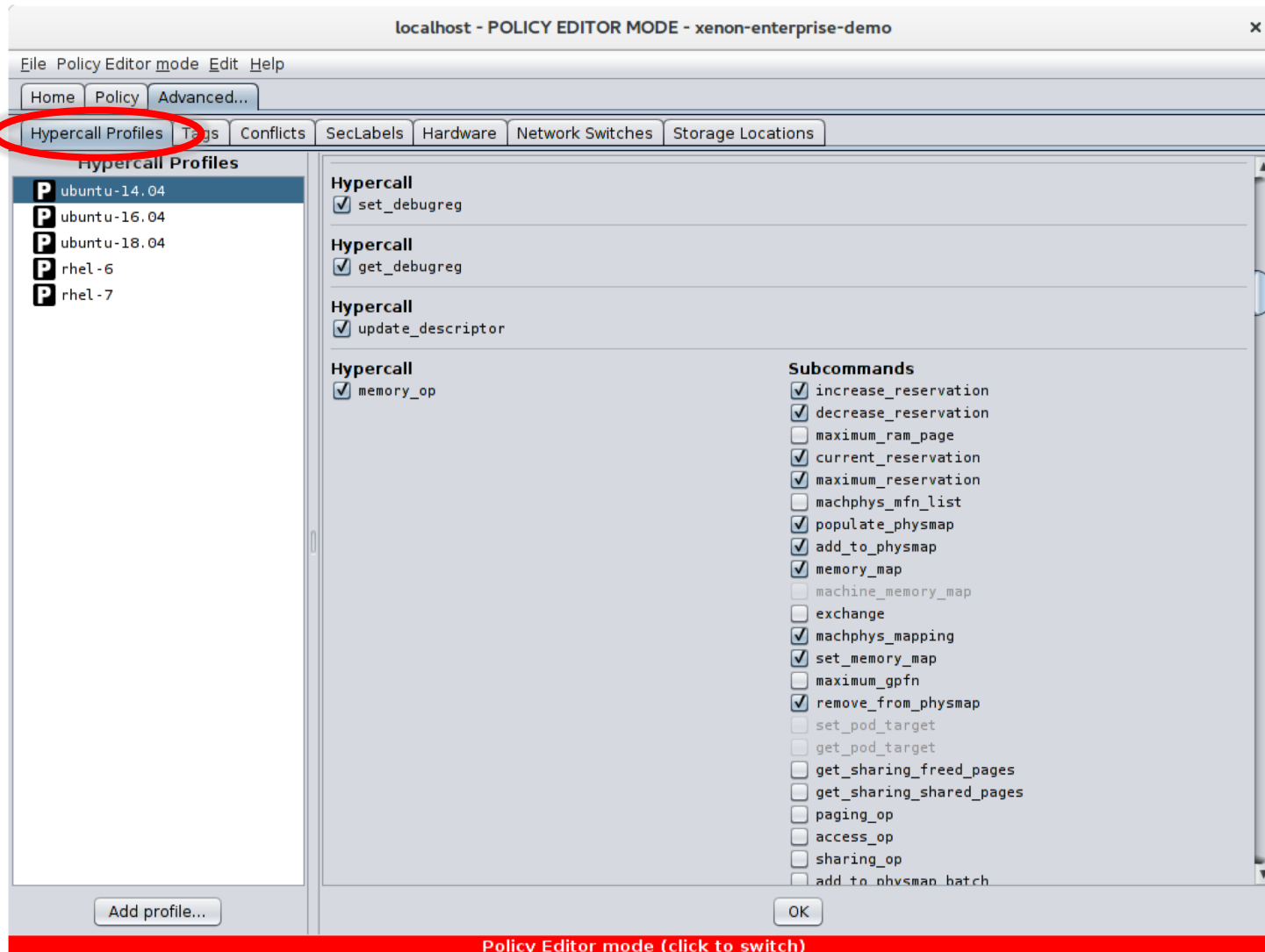
- human_resources: hr_vms, personnel_mgr (stopped)
- entertainment: user_vms, user_vm_1 (stopped), user_vm_2 (stopped), user_vm_3 (stopped)
- security: sec_vms, firewall (stopped), nids (stopped)

Buttons: 'Add tag', 'Add root domain...', 'Add enclave...', 'Live mode (click to switch)'.

Xenon Security Features (cont'd)

- Xenon security policy restricts each VM's interface to the hypervisor via *hypercall privileges and profiles*
 - A VM interacts with the hypervisor through hypercalls
 - Hypercall privilege levels
 - Management privileged hypercalls – mainly Dom0
 - Security privileged hypercalls – VM introspection, etc.
 - Regular hypercalls
 - Every VM is required to have an associated hypercall profile
 - VM introspection domain profile, Ubuntu 14.04 profile, etc.

Xenon Security Features (cont'd)



Policy Editor mode (click to switch)

- Persistent audit logging of all policy violations
 - Logs are stored outside the VM, physically separated from and inaccessible by the violating VM
 - Security policy can be configured to permit a maximum number of violations per VM
- Xenon security policies can be set dynamically (i.e., modified at runtime without rebooting)
 - Supports scalability and significantly reduces the need for downtime
 - Tags and VMs can be added but not removed

Xenon Security Features (cont'd)

localhost - LIVE MODE - xenon-enterprise-demo

File Live mode View Help

Home Policy **Policy Violations Log** Current Performance Performance History Advanced...

	Domain	When	Reason	Module	Info
ⓘ ⚠	user_vm_1	2018-05-21 10:06:35	hypercall rate exceeded	hypercall guard	hmax=10, hrate=16
✓	user_vm_1	2018-05-10 13:45:29	hypercall violation	hypercall guard	hcall=17(xen_version), cmd=1(extraversion)
✓	user_vm_1	2018-05-10 13:45:29	hypercall violation	hypercall guard	hcall=12(memory_op), cmd=9(memory_map)
✓	user_vm_1	2018-05-10 13:45:29	hypercall violation	hypercall guard	hcall=29(sched_op), cmd=2(shut down)

Get new policy violations

Mark violations as viewed

Clear policy violations

Filter by tag or domain

Live mode (click to switch)

Xenon is More Than A Secure Hypervisor

- Out of the box, customers gain security and performance best practices
 - Preconfigured service VMs (e.g., network service VM)
 - Distribution of security policy through a signed XML policy document
 - Role-based access control for different administrative tasks
 - System admin role (e.g., starting, migrating VMs)
 - Security policy admin role (e.g., setting up security policies)
 - System monitoring role
- Guide users to configure virtual computing environment securely through intuitive visual management tool
 - Provide hardware-independent secure configuration mechanism
 - Export & import policy “templates”
 - Visual management interface provides
 - An easy and intuitive way to author and understand security policy
 - An easy way to manage and monitor user domains

Hardware overview at-a-glance

Simple configuration of resources

Xenon is More Than A Secure Hypervisor (cont'd)

Create pre-configured Service VMs

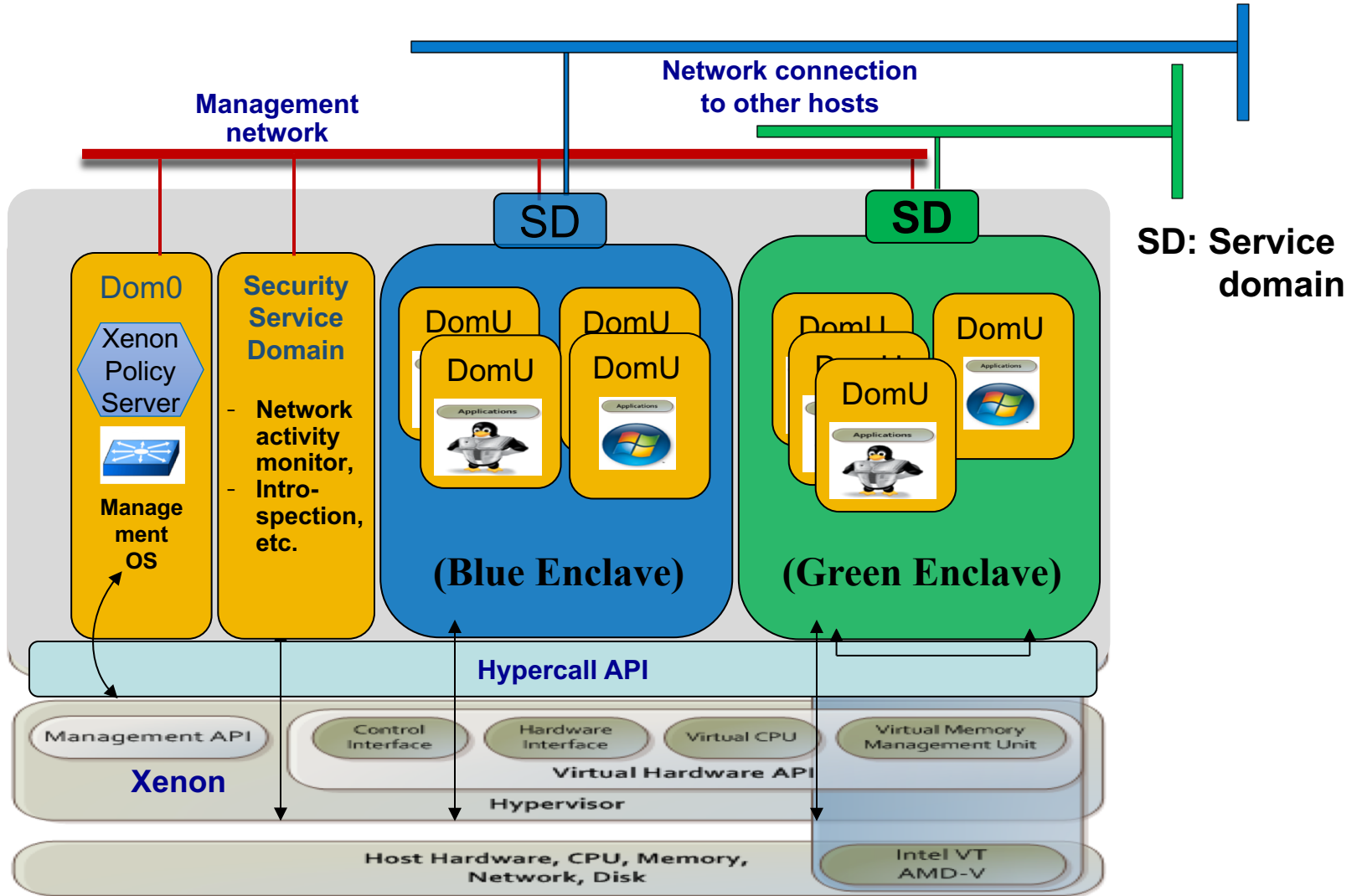
Assign resources to unprivileged VMs

The screenshot displays the Xenon Policy Editor in '10.0.2.107 - POLICY EDITOR MODE - a simple policy'. The interface is divided into several panes:

- Unassigned Hardware:** Lists network controllers (eth1, eth2, eth3) and storage controllers (SATA).
- Enclave B Assigned Hardware:** Shows assigned network controllers (eth4, eth0) and storage controllers.
- Domains, SecLabels, & Enclaves:** A tree view showing the hierarchy: Domain-0, Enclave B (Service Domains: EBNetDom1, User Domains: EB-domu-1 to EB-domu-4), and Enclave A (Service Domains, User Domains: MigrateVM1-pv).
- Edit EBbr2:** A configuration window for the network switch EBbr2, showing three VIFs (Virtual Interface Functions) with their respective settings:
 - VIF 1:** Driver domain EBNetDom1, Domain EB-domu-1, Enable VIF checked, MAC address 00:16:3e:a4:22:9b, Switch address/mask 192.168.5.1/255.255.255.0, IP address 192.168.5.101.
 - VIF 2:** Driver domain EBNetDom1, Domain EB-domu-2, Enable VIF checked, MAC address 00:16:3e:35:56:bc, Switch address/mask 192.168.5.1/255.255.255.0, IP address 192.168.5.102.
 - VIF 3:** Driver domain EBNetDom1, Domain EB-domu-3, Enable VIF checked, MAC address 00:16:3e:42:24:7f.

Buttons for 'Add root domain...', 'Add enclave...', 'Add VIF...', 'Cancel', and 'OK' are visible at the bottom of the interface.

A Typical Xenon Host Configuration



Xenon Enterprise

Manage multiple Xenon hosts



...

Situation Awareness
Moving Target Defense
Continuity of Operations
Provide scalable upgrade paths

Xenon Enterprise

Services:

Compute
Network
Image
Storage
User
Policy

...

Xenon Host 1



Xenon Host 2



Xenon Host n



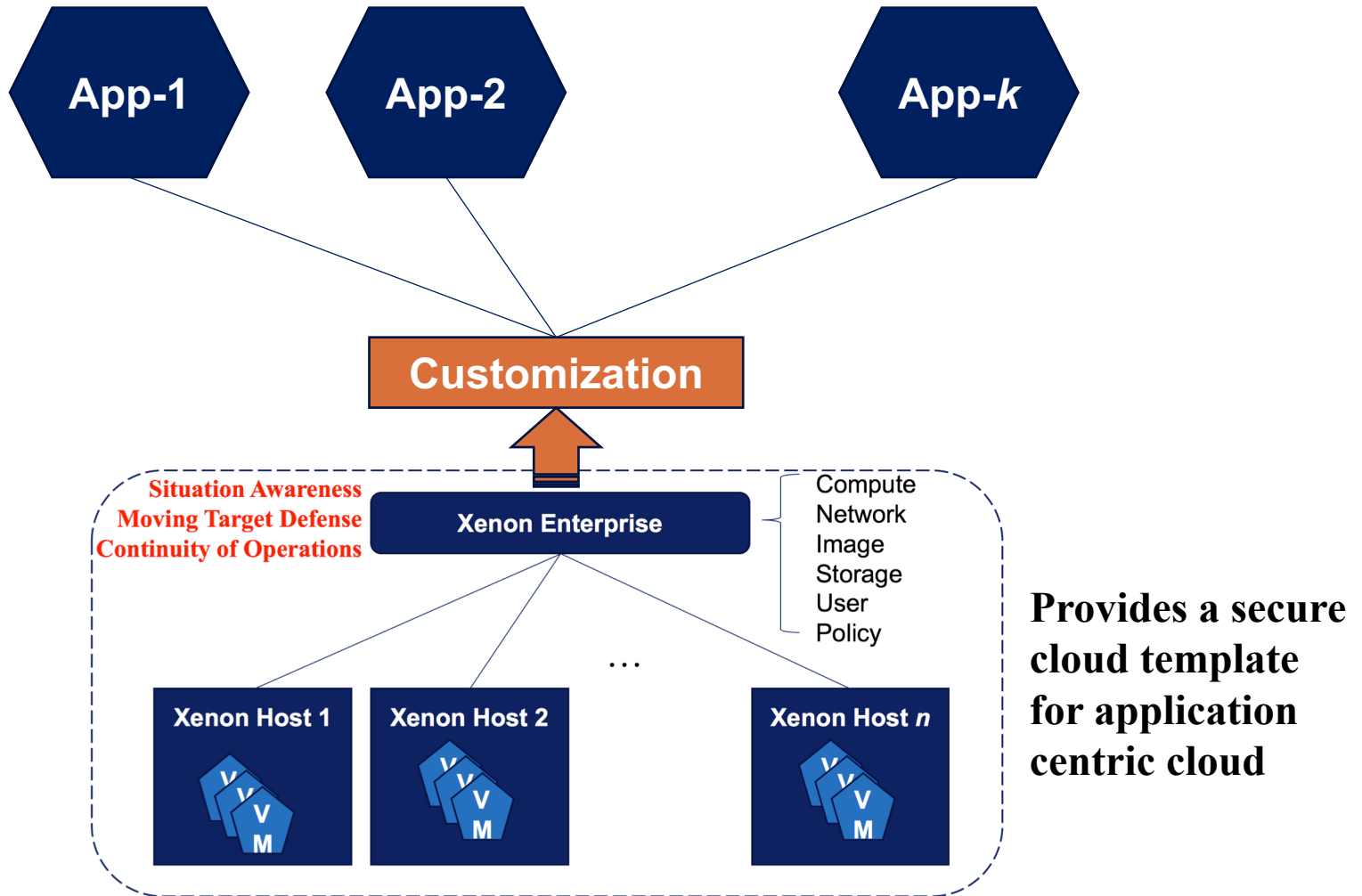
Hosts & VMs

Enclaves, security labels, and VMs

The screenshot displays the Xenon Enterprise management interface. On the left, a tree view under 'Hosts' shows three hosts: heisenberg.fw5540.net (10.0.0.1), ntc.fw5540.net (10.0.2.66), and moriarty.fw5540.net (10.0.2.1). Each host has a set of Enclaves (A, B, C, D) and associated VMs. The main area shows a detailed view of these Enclaves and VMs, organized into four columns: Enclave A, Enclave B, Enclave C, and Enclave D. Each column has a header with 'Enclave', 'SecLabels', and 'Domains'. Below the headers, the VMs are listed with their names and status icons (e.g., EA-domu-1 to EA-domu-4 for Enclave A). The bottom of the main area features a color-coded bar for each Enclave: Enclave A (red), Enclave B (blue), Enclave C (yellow), and Enclave D (purple).

Host	Enclave	VM	Status	
heisenberg.fw5540.net (10.0.0.1)	Enclave A	EA-domu-4	Red	
		Enclave B	EB-domu-2	Blue
			EB-domu-3	Blue
			EB-domu-5	Blue
	Enclave C	EC-domu-1	Yellow	
		EC-domu-2	Yellow	
	ntc.fw5540.net (10.0.2.66)	Enclave A	EA-domu-1	Red
			Enclave B	EB-domu-1
		Enclave C		EC-domu-1
			Enclave D	ED-domu-1
	moriarty.fw5540.net (10.0.2.1)	Enclave A		EA-domu-2
			EA-domu-3	Red
Enclave B		EB-domu-1	Blue	

Xenon Enterprise Provides Templates for Application-centric Cloud

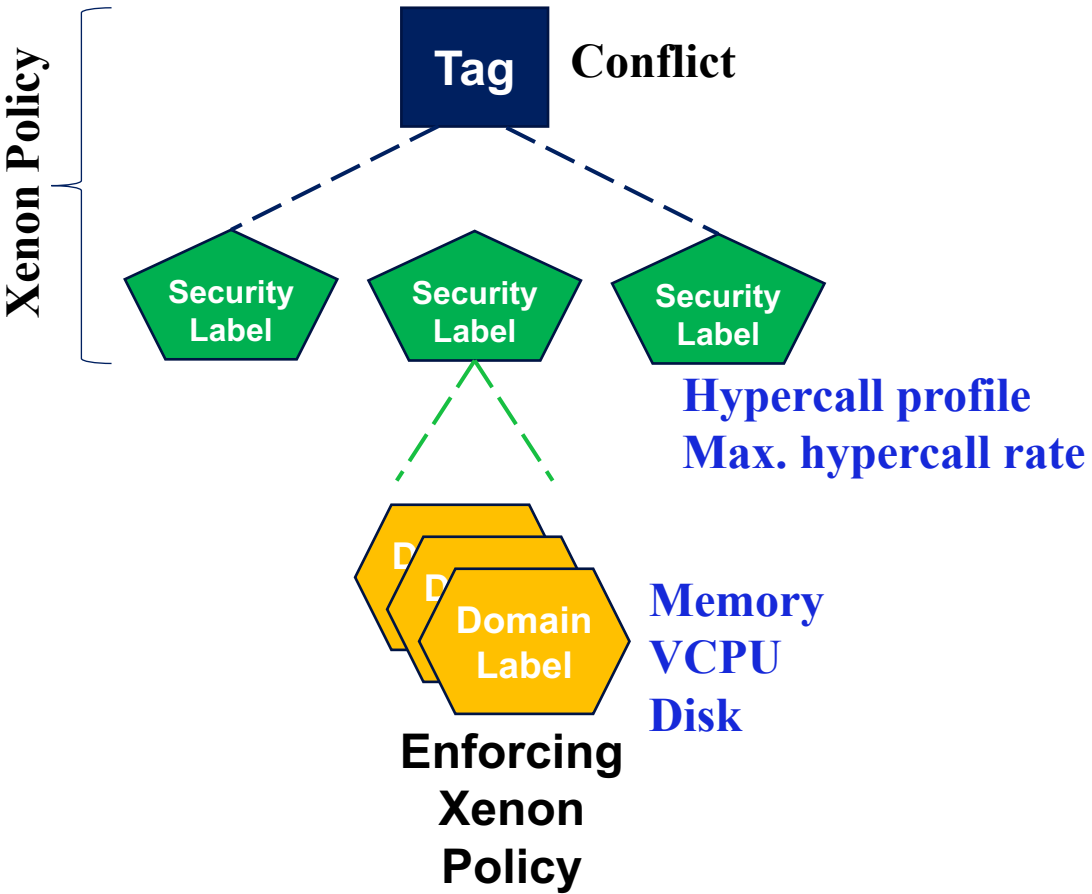


Xenon Enterprise with Xenon's Enclaves Provides Secure Cloud Computing Platform for Multiple Applications

Situation Awareness
Moving Target Defense
Continuity of Operations
Scalable upgrade paths



Security Implementation Details



Xenon Policy

Xenon Enterprise part

Xenon Host part

Enterprise-wide policy

Per-host configuration (including policy)

Policy + configuration distributed as signed XML document

The screenshot displays a hierarchical tree view of a policy configuration. The root is 'a simple policy', which contains several sub-sections:

- Profiles:** A list of profiles including 'AnyDomU-AllowAll', 'PV-Combined', 'PVHVM-Combined', 'PVH-Combined', 'PV-LinuxGeneric', 'PVHVM-LinuxGeneric', 'PVH-Ubuntu14', 'PV-Ubuntu14-Security', 'PV-Ubuntu14-Storage', and 'PVHVM-Ubuntu14-Network'.
- Tags:** A list of tags for 'Enclave A' (red), 'Enclave B' (blue), 'Enclave C' (yellow), and 'Enclave D' (purple).
- Conflicts:** A section for 'EnclavesConflict' with four colored indicators.
- SecLabels:** A list of security labels: 'ED-pvLabel1' (blue), 'EB-pvLabel1' (blue), 'EA-pvLabel1' (red), and 'EC-pvLabel1' (yellow).
- Domains:** A list of domains including 'Domain-0', 'EB-domu-2' through 'EB-domu-5', 'EA-domu-4', 'EC-domu-1', and 'ED-domu-5' through 'ED-domu-6'. Each domain entry includes details like UUID, security labels, guest type, VIFs, and disks.

```

<ns1:extraXlConfigKeyValPairs/>
</ns1:domain>
<ns1:domain ns1:uuid="b74f6840-69f3-42e7-90fe-845d299ef334" ns1:name="EB-domu-3" ns1:
<ns1:pvBootOptKernel>/usr/local/lib/xen/boot/pv-grub-x86_64.gz</ns1:pvBootOptKern
<ns1:pvBootOptCmdline>(hdo,0)/boot/grub/menu.lst</ns1:pvBootOptCmdline>
<ns1:vifs/>
<ns1:disks/>
<ns1:netAccessRestrictions ns1:whiteList="false"/>
<ns1:extraXlConfigKeyValPairs/>
</ns1:domain>
<ns1:domain ns1:uuid="2e5ef327-b88f-4c99-81ea-606a1f26ab06" ns1:name="EB-domu-4" ns1:
<ns1:pvBootOptKernel>/usr/local/lib/xen/boot/pv-grub-x86_64.gz</ns1:pvBootOptKern
<ns1:pvBootOptCmdline>(hdo,0)/boot/grub/menu.lst</ns1:pvBootOptCmdline>
<ns1:vifs/>
<ns1:disks/>
<ns1:netAccessRestrictions ns1:whiteList="false"/>
<ns1:extraXlConfigKeyValPairs/>
</ns1:domain>
</ns1:domains>
</ns1:enclave>
<ns1:enclave ns1:tagUuidRef="5e328575-c43f-489c-a640-b109b557e85e">
<ns1:domains>
<ns1:domain ns1:uuid="7c045bb3-2edc-4785-9b4e-38f8374394fa" ns1:name="MigrateVM1-pv"
<ns1:pvBootOptKernel>/usr/local/lib/xen/boot/pv-grub-x86_64.gz</ns1:pvBootOptKern
<ns1:pvBootOptCmdline>(hdo,0)/boot/grub/menu.lst</ns1:pvBootOptCmdline>
<ns1:vifs/>
<ns1:disks/>
<ns1:netAccessRestrictions ns1:whiteList="false"/>
<ns1:extraXlConfigKeyValPairs>
<ns1:xlConfigKeyValPair># PV configuration template</ns1:xlConfigKeyValPair>
<ns1:xlConfigKeyValPair>builder = "generic"</ns1:xlConfigKeyValPair>
<ns1:xlConfigKeyValPair>vif = [ "mac=00:16:3e:f0:75:6d,bridge=EABr,script=vif
<ns1:xlConfigKeyValPair>disk = [ "script=block-iscsd,vdev=xvda,target=iqn=iqn
</ns1:xlConfigKeyValPairs>
</ns1:domain>
</ns1:domains>
</ns1:enclave>
</ns1:enclaves>
<ns1:netSwitches/>
<ns1:storageLocations/>
</ns1:hostConfig>

```

Questions?