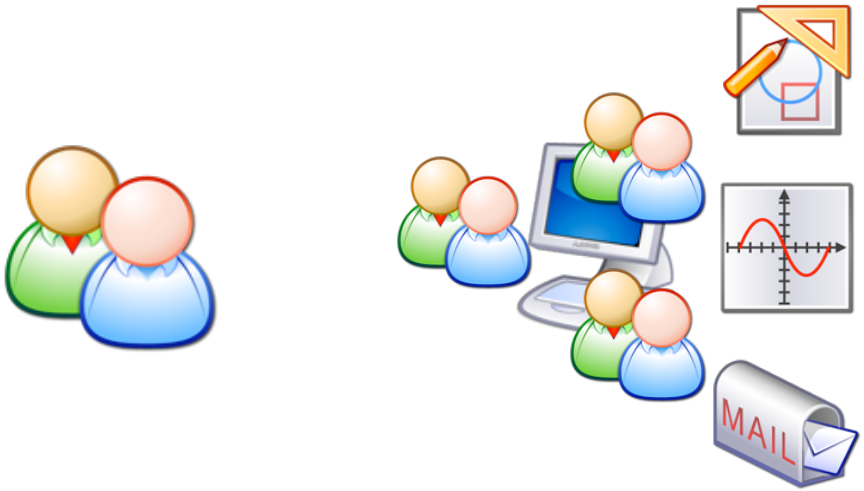
Systems and Internet Infrastructure Security

Network and Security Research Center
Department of Computer Science and Engineering
Pennsylvania State University, University Park PA

Advanced Systems Security: Cloud Computing Security

Trent Jaeger
Penn State University

Cloudy Foundations

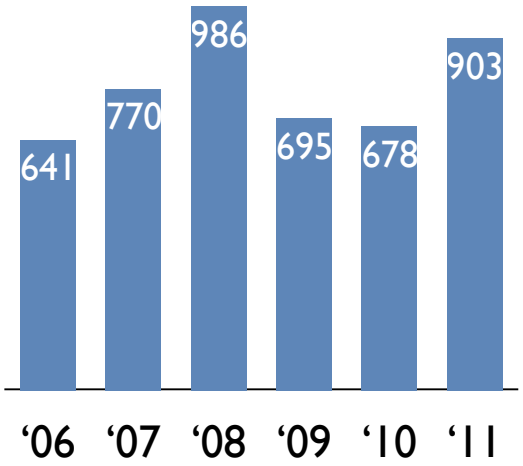


Can customers move their services and validate that they still protect data security?

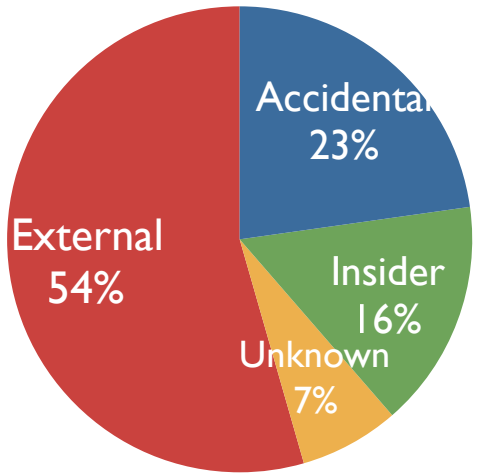
Reasons to Doubt

- History has shown they are vulnerable to attack
  - SLAs, audits, and armed guards offer few guarantees
  - Insiders can subvert even hardened systems

Data Loss Incidents



Incident Attack Vector



Credit: The Open Security Foundation datalossdb.org

Cloudy Future

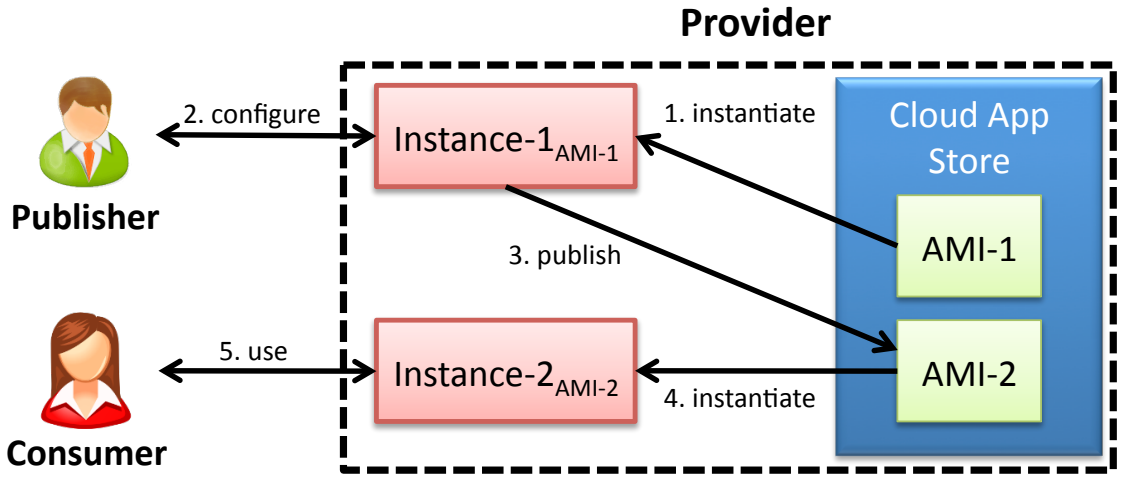
- New problem or new solution?
  - New challenges brought on by the cloud (plus old ones)
  - Utility could provide a foundation for solving such challenges

Cloudy Future

- Improve on data centers? On home computing?
  - Seems like a low bar

AmazonIA

Consumers use published instances *[CCS 2011]*



Instances may be flawed - have adversary-controlled public and private keys

Security Configuration

PENNSTATE 1855

- Zillions of security-relevant configurations for instances
  - Firewalls
  - Mandatory access control
    - SELinux, AppArmor, TrustedBSD, Trusted Solaris, MIC
  - Discretionary access control
  - Application policies (e.g., Database, Apache)
  - Pluggable Authentication Modules (PAM)
  - Application configuration files
  - Application code enforces security
- Plus new configuration tasks for the cloud - e.g., storage

Insiders

- Although the vendor may have a good reputation, not every employee may

Side Channels

PENNSTATE 1855

- Shared infrastructure leads to visibility for others
  - You can't monitor, but others can
- Get Off My Cloud - Ristenpart et al. *[CCS 2009]*
  - Caches (Memory)
  - Devices (I/O)
  - CPU
  - Scheduling
- Ari Juels -- "Many of the security implications of the cloud stem from tenants entrusting computing resources to a third party that they controlled in the past."
- Not really going to discuss this further

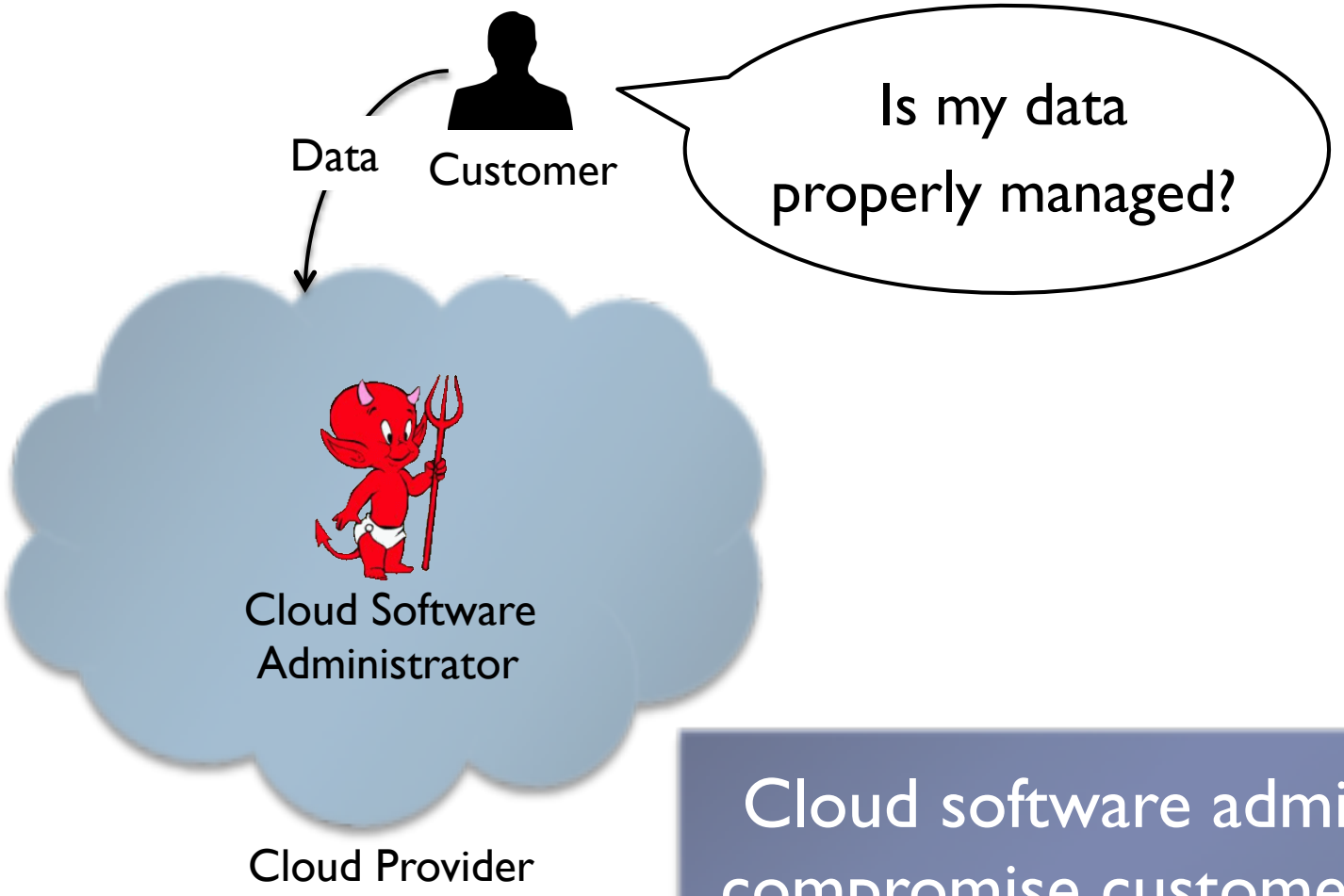
Max
Planck
Institute
for
Software Systems

Policy-Sealed Data:
A New Abstraction for Building Trusted Cloud Services

Nuno Santos[1], Rodrigo Rodrigues[2], Krishna P. Gummadi[1], Stefan Saroiu[3]

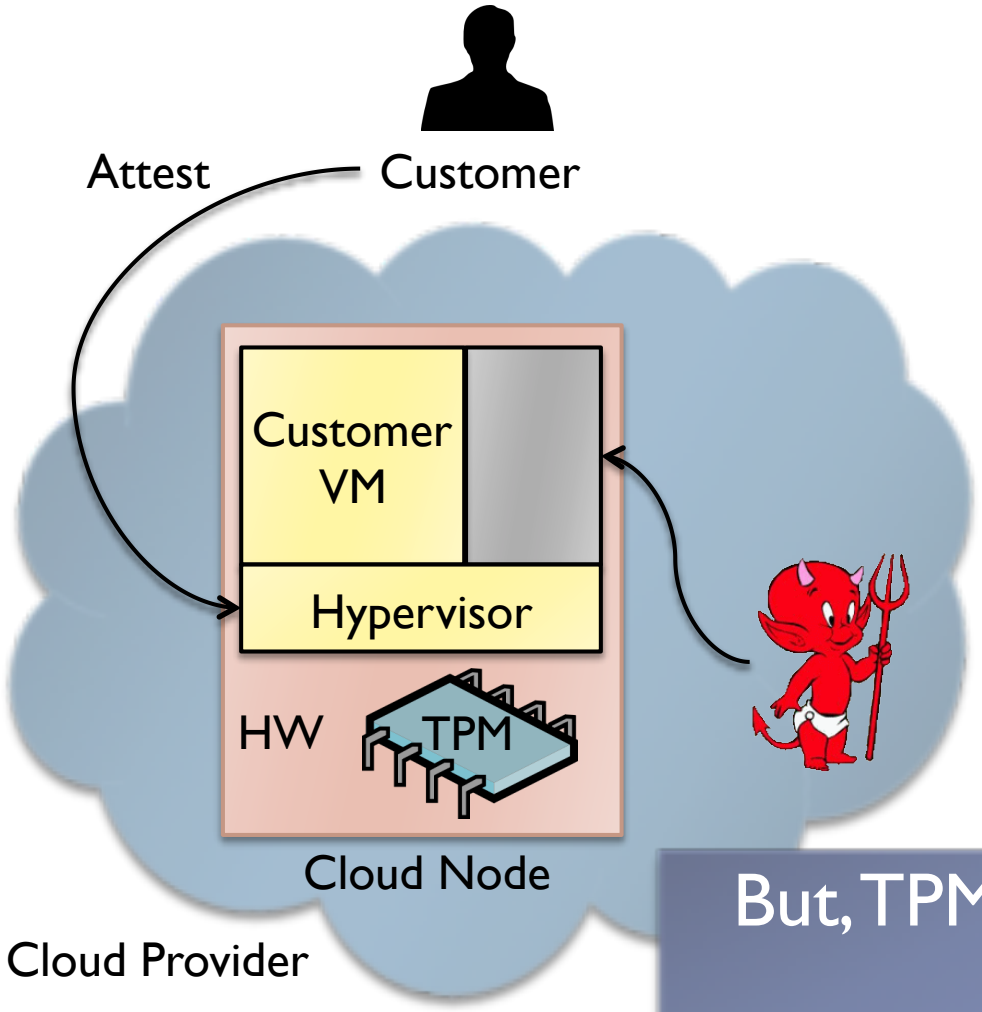
MPI-SWS[1], CITI / Universidade Nova Lisboa[2], Microsoft Research[3]

Managing the Cloud is Complex & Error-Prone



Cloud software admins. can compromise customers' data

Trusted Computing Can Help Mitigate Threats



1. Newer hypervisors can offer protection from SW admins.
   - e.g., nested virtualization: CloudVisor [SOSP'11], Credo [MSR-TR]
2. Trusted computing can attest cloud node runs "correct" hypervisor
   - Trusted Platform Module (TPM)

But, TPMs alone ill-suited for the cloud

Our Contributions

1. Policy-sealed data abstraction
   - Data is handled only by nodes satisfying customer-chosen policy
   - Examples:
     - Handle data only by nodes running CloudVisor
     - Handle data only by nodes located in the EU

2. Use attribute-based encryption (CP-ABE) to implement abstraction efficiently
   - Binds policies and node attributes to node configurations
   - Ciphertext-Policy Attribute-Based Encryption [Bethencourt07]

Excalibur incorporates both contributions

Excalibur Addresses TPM Limitations in Cloud

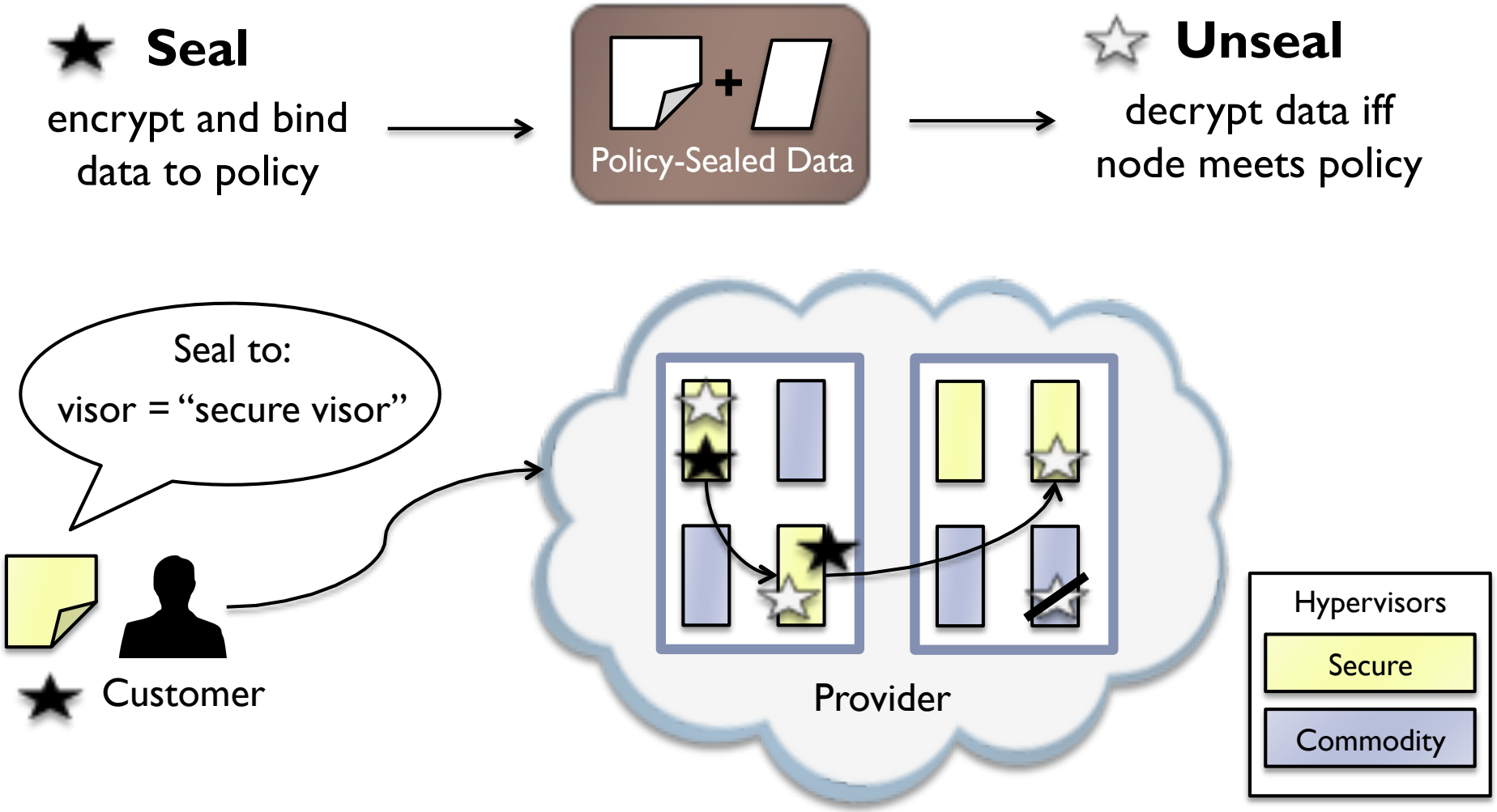
Policy-sealed data

- Enables flexible data migration across cloud nodes
  - Customer data accessible to any node that satisfies the customer policy
- Hides node's identities and low-level details of the software
  - Only high-level attributes are revealed

Attribute-based encryption

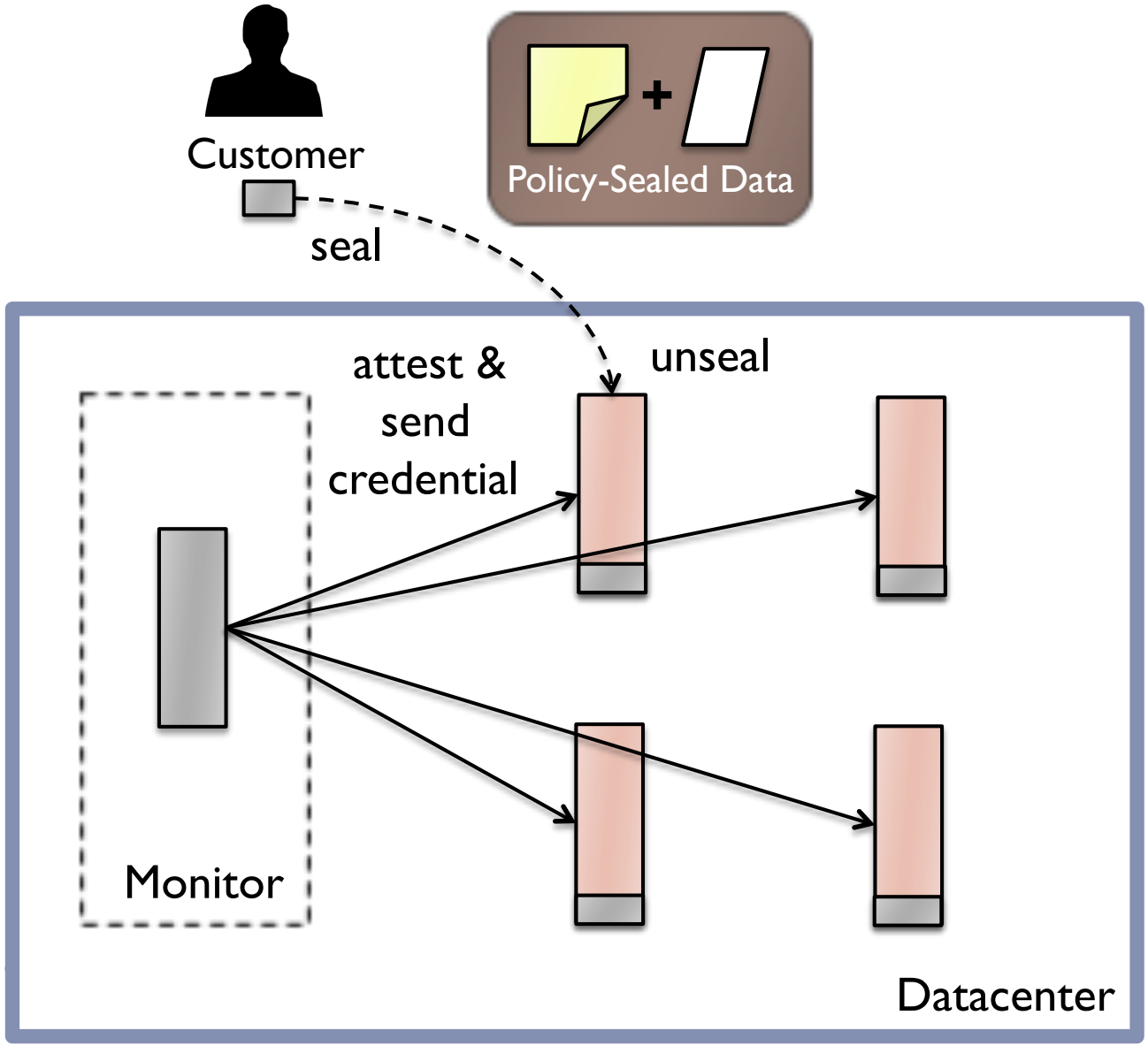
- Masks TPMs' poor performance
  - Enforcing policies does not require direct calls to TPMs

Policy-Sealed Data

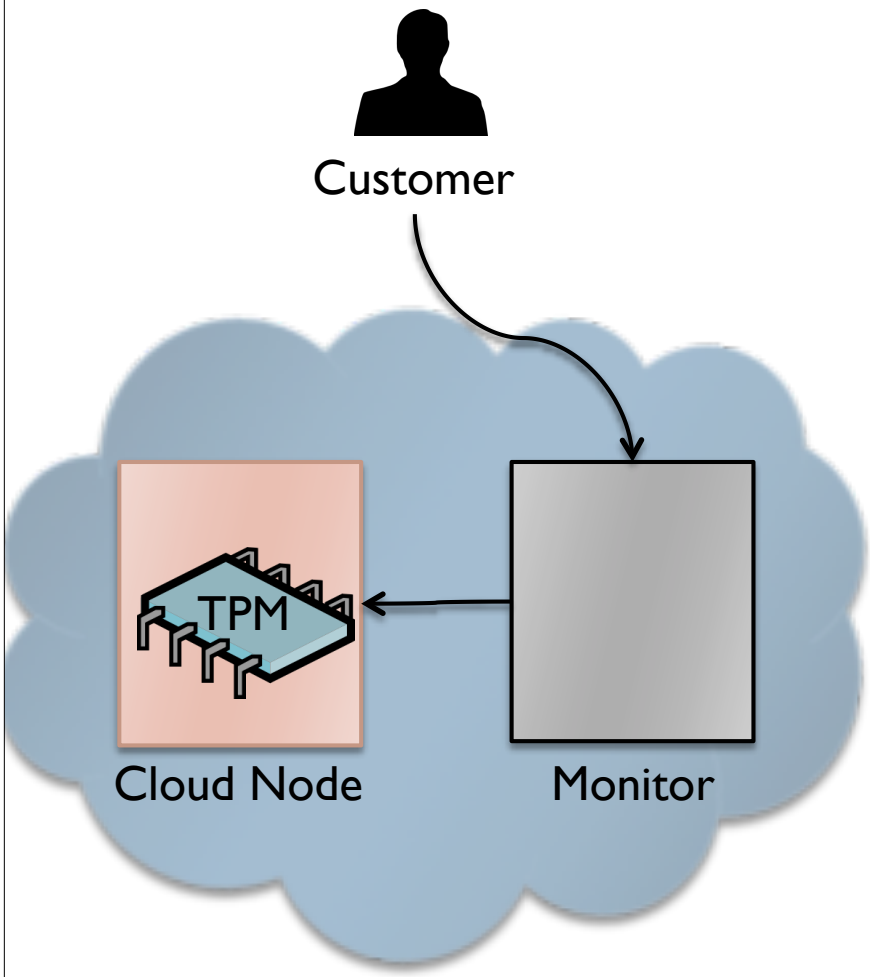


Excalibur Architecture

- Check node configurations
  - Monitor attests nodes in background
- Scalable policy enforcement
  - CP-ABE operations at client-side lib



Excalibur Mediates TPM Access w/ Monitor

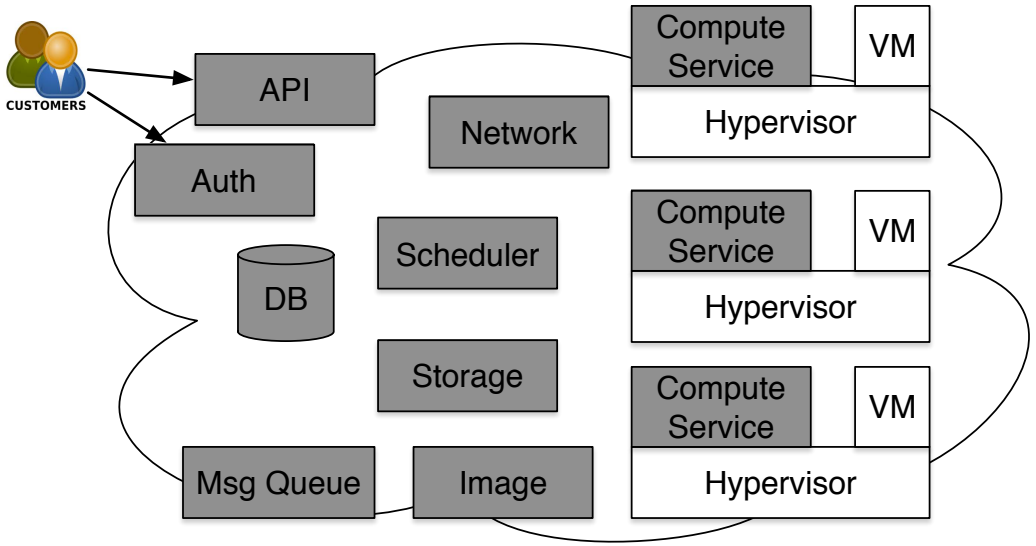


Monitor goals:

- Track node ids + TPM-based attestations
  - Hides low-level details from users
- Track nodes' attributes that cannot be attested via today's TPMs
  - e.g., nodes' locations (EU vs. US)
- Form the cloud's root of trust
  - Customers only need to attest the monitor's software configuration

IaaS Cloud Platform

- IaaS clouds rely on a variety of *cloud services* to provision and manage *users' data* (e.g., VM and container)



IaaS service vendors:

IaaS software stack vendors:

Vulnerabilities in Cloud Services

PENNSTATE 1855

CVE Details
The ultimate security vulnerability datasource

Log In Register

(e.g.: CVE-2009-

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendor
Vendor
Product
Product
Version
Other :
Microsoft
Bugtraq
CWE D
About
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :

Openstack : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **162** Page : 1 (This Page) 2 3 4

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	C
1	CVE-2016-7498	399		DoS	2016-09-27	2016-09-28	6.8	None	Remote	
OpenStack Compute (nova) 13.0.0 does not properly delete instances from compute nodes, which allows remote authenticated users to cause a denial of resize state. NOTE: this vulnerability exists because of a CVE-2015-3280 regression.										
2	CVE-2016-5363	254		DoS Bypass	2016-06-17	2016-06-20	6.4	None	Remote	
The IPTables firewall in OpenStack Neutron before 7.0.4 and 8.0.0 through 8.1.0 allows remote attackers to bypass an intended MAC-spoofing protection intercept network traffic via (1) a crafted DHCP discovery message or (2) crafted non-IP traffic.										
3	CVE-2016-5362	254		DoS Bypass	2016-06-17	2016-06-21	6.4	None	Remote	
6	CVE-2016-2140	200		+Info	2016-04-12	2016-04-21	3.5	None	Remote	
The libvirt driver in OpenStack Compute (Nova) before 2015.1.4 (kilo) and 12.0.x before 12.0.3 (liberty), when using raw storage and use_cow_images is arbitrary files via a crafted qcow2 header in an ephemeral or root disk.										
7	CVE-2016-0757	284			2016-04-13	2016-04-18	4.0	None	Remote	
OpenStack Image Service (Glance) before 2015.1.3 (kilo) and 11.0.x before 11.0.2 (liberty), when show_multiple_locations is enabled, allow remote auth data by removing the last location of an image.										
8	CVE-2016-0738	399		DoS	2016-01-29	2016-03-03	5.0	None	Remote	
OpenStack Object Storage (Swift) before 2.3.1 (Kilo), 2.4.x, and 2.5.x before 2.5.1 (Liberty) do not properly close server connections, which allows remot consumption) via a series of interrupted requests to a Large Object URL.										
9	CVE-2016-0737	399		DoS	2016-01-29	2016-03-03	5.0	None	Remote	

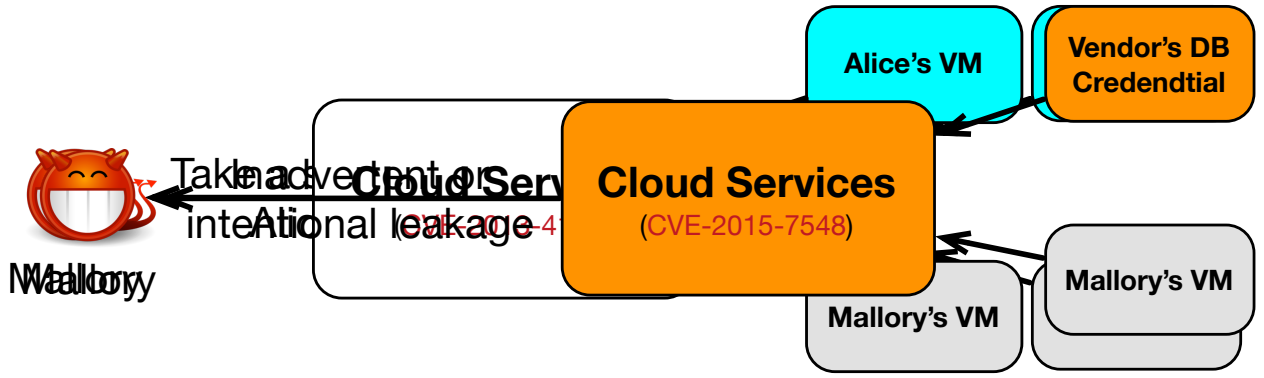
Of Exploits Descending

e Date	Score	Gained Access Level
5-14	5.8	None
efore 4.8.0.1, when SAML-based authent		
2-12	6.0	None
M virtual machines, which allows remote		
2-12	4.0	None
sitive password information for root accou		
1-16	5.0	None
e keys via a listSslCerts API call.		
2-10	5.0	None
request withou		
		None
sers to list net		
		None
restarted, whi		
		None
.x before 3.0.6 Patch C uses a hash of a		
5-27	5.0	None
.x before 3.0.6 Patch C allows remote att		
0-07	4.3	None
e attackers to inject arbitrary web script		
;" and (6) unspecified "list view" edit fiel		

Over 150 vulnerabilities reported !

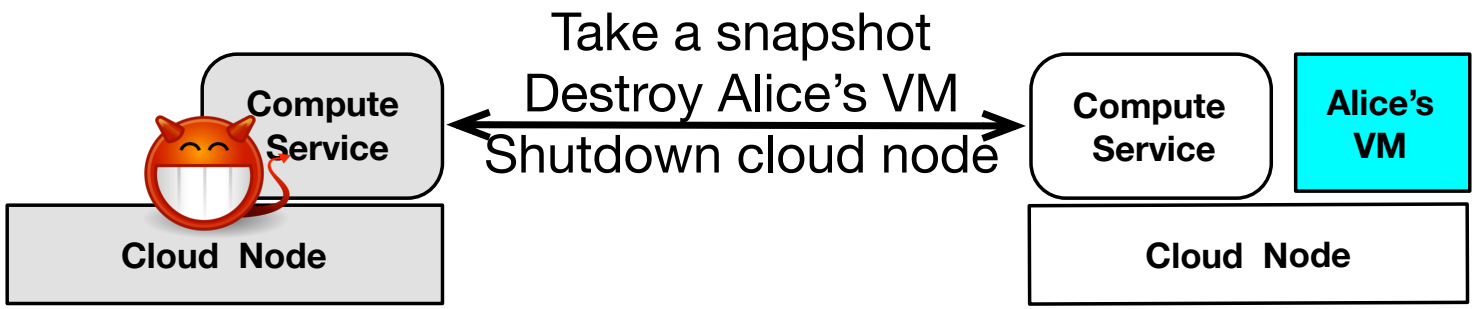
Attacks via Service Vulnerabilities

- Cloud services run with *all users' permissions*, and even *cloud vendor's permission*
  - Confused deputy attacks
  - Inadvertent or intentional data leakage
  - Problem compounded by the need of cloud services to make critical security decisions over users' data



Attacks via Flawed Trust Assumption

- Cloud services *fully trust each other*
  - Once an adversary controls a cloud service or node (e.g., via hypervisor vulnerabilities), she can perform arbitrary operations on benign cloud nodes via cloud service interactions
  - Compromise of one cloud service can lead to data compromise cloud wide
  - A user's TCB includes each and every cloud service & node

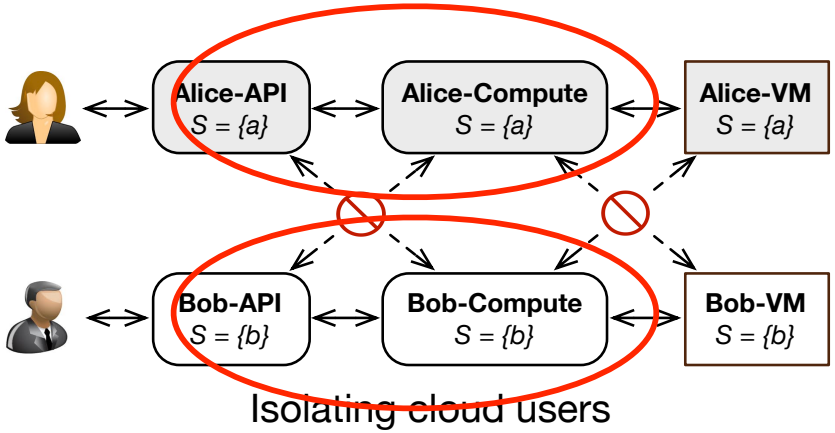


Insight

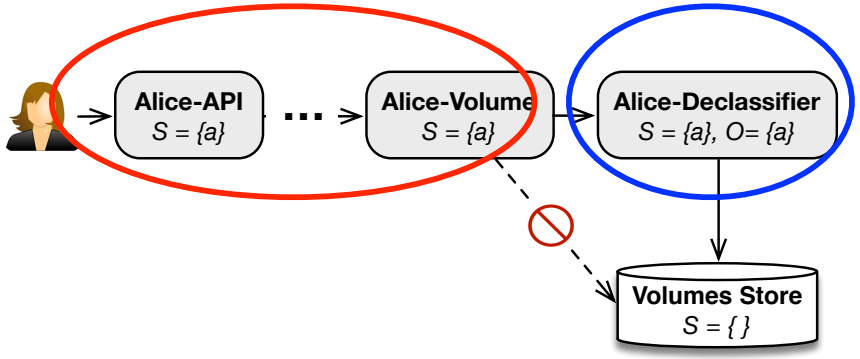
- Cloud services themselves *cannot control data propagation* due to vulnerabilities
  - Information flow control (IFC) over cloud services
- Compromised cloud services and nodes have *unlimited access* to any user's data on any cloud node
  - Bound the data accessibility of a cloud node to the users that are using (thus trusting) the cloud node
  - Decentralized security principle: a user's data security does not depend on system components that the user does not trust [Arden 2012]

DIFC over Cloud Services

- Enforce *Decentralized Information Flow Control* (DIFC) over cloud services to mitigate cloud service vulnerabilities
  - Confine cloud services to individual users' security labels
  - Cloud services must *explicitly declassify or endorse* data using *ownerships*



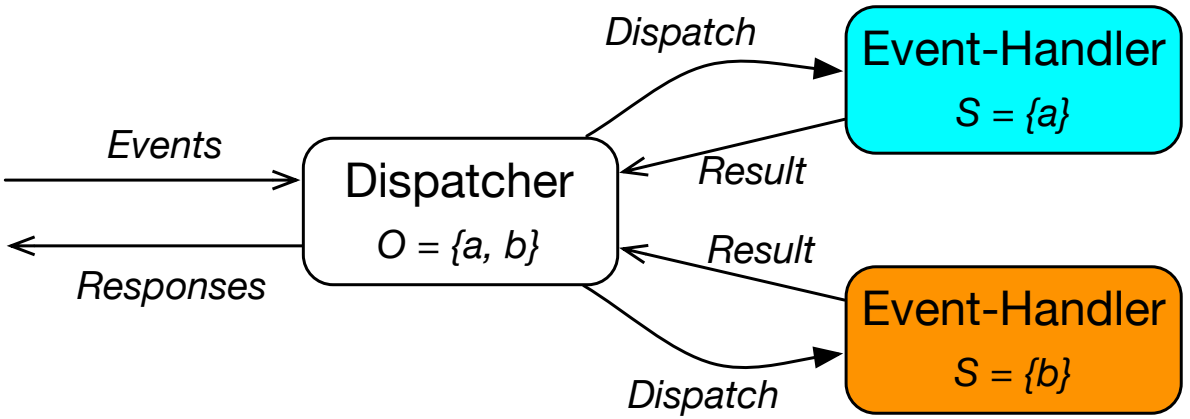
Isolating cloud users



Export protection

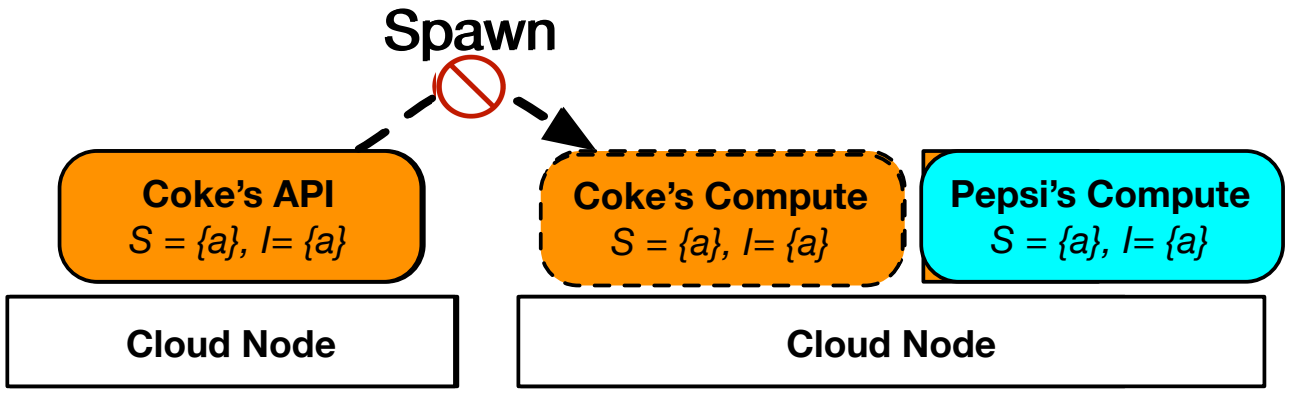
Control of Cloud Services

- Cloud services(stateless) —> ephemeral *event handlers*
  - [*Insight*] Cloud services are constructed using event dispatch loop [Efstah. 05]
  - Dispatcher on a cloud node spawns event handlers on-demand with users' labels



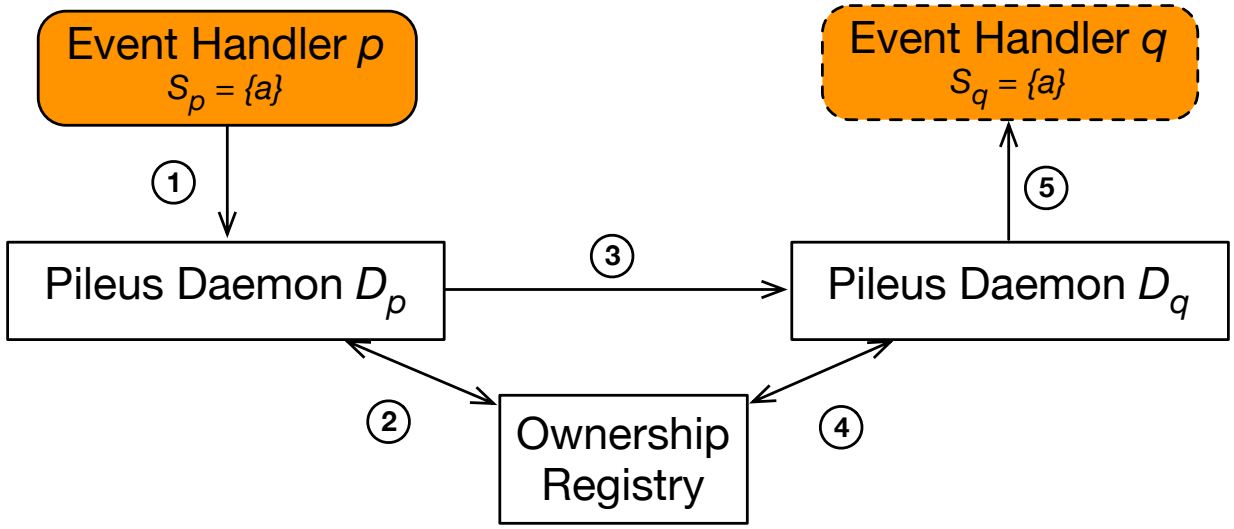
Spawning Event Handlers

- Requirements:
  - [who can spawn] prevent nodes that do not have a user's authority from spawning event handlers that may access that user's data
  - [where can it spawn] prevent nodes that fail to satisfy cloud policy (e.g., CoI) from being selected to execute the user's event handler
  - [best place to spawn] find the "ideal" cloud node to spawn



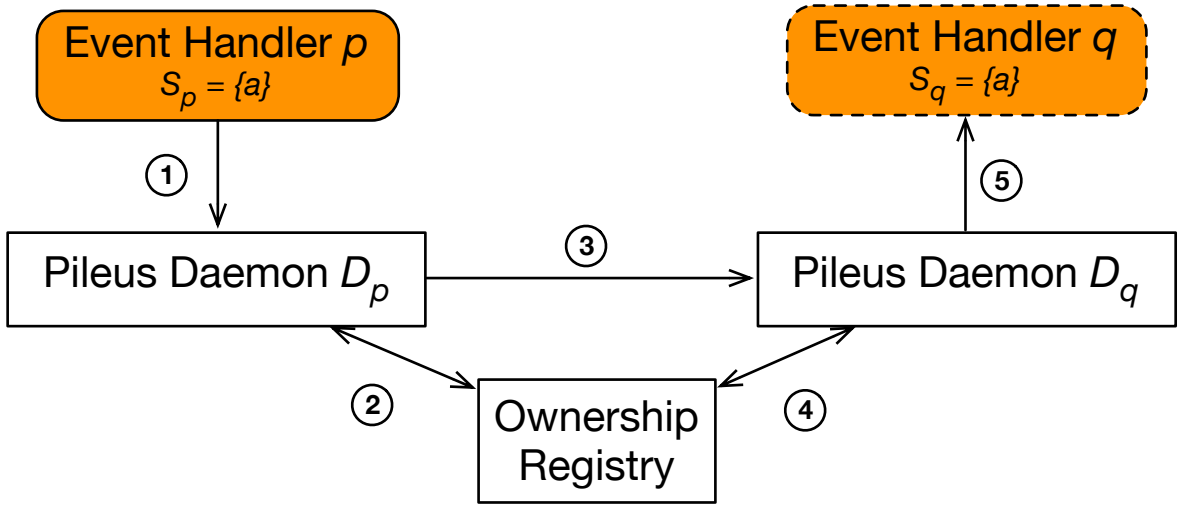
Spawn Sketch

- Daemon (dispatcher) needs to be delegated with *authority* to spawn new event handlers with ownership capabilities
  - *authority* = {*ownership*, *node*, *auth*}
  - Having the authority indicates the node is trusted by the user



Capability (Ownership) Delegation

- *centralized control* over authority distribution:
  - [who can spawn] only a cloud node trusted with a user's authority can spawn on other cloud nodes with the user's label
  - [where can it spawn] enforces mandatory cloud policy (e.g., ICAP)
  - [best place to spawn] most compatible security requirements



Mitigating Vulnerabilities

- Pileus blocks 6* zero-day OpenStack vulnerabilities that were newly reported after Pileus's deployment

	CVE ID	Affected Cloud Service	Mitigated
1	CVE-2015-1195	Image Service (Glance)	Yes
2	CVE-2015-1850	Volume Service (Cinder)	Yes
3			
4			
5			
6	CVE-2015-3221	Network Service (Neutron)	No*

Systematic mitigation of 1/3 vulnerabilities reported in OpenStack

OpenStack on Pileus

PENNSTATE 1855

- Pileus does not block normal cloud operations
  - Cloud services are confined as-is in majority of cloud operations
  - Few requires declassification and endorsement
    - When an operation causes *data flow across user boundaries* (i.e., resource sharing)
  - Declassifiers and endorsers are simple
    - Volume declassifier (50 SLOC), image endorser (150 SLOC)

Type	Number of cloud operations	Example
DIFC-aware	13	nova boot
DIFC-unware	135	nova volume-attach
Total	148	

Conclusion

- Pileus is a model and system that protects users' data from vulnerable cloud services
  - It mitigates cloud service vulnerabilities by enforcing Decentralized Information Flow Control (DIFC)
  - It addresses the mutual trust assumed by cloud services and nodes by enforcing Decentralized Security Principle (DSP)