Pileus: Protecting User Resources from Vulnerable Cloud Services

Research Lead: Trent Jaeger, Penn State, tjaeger@cse.psu.edu

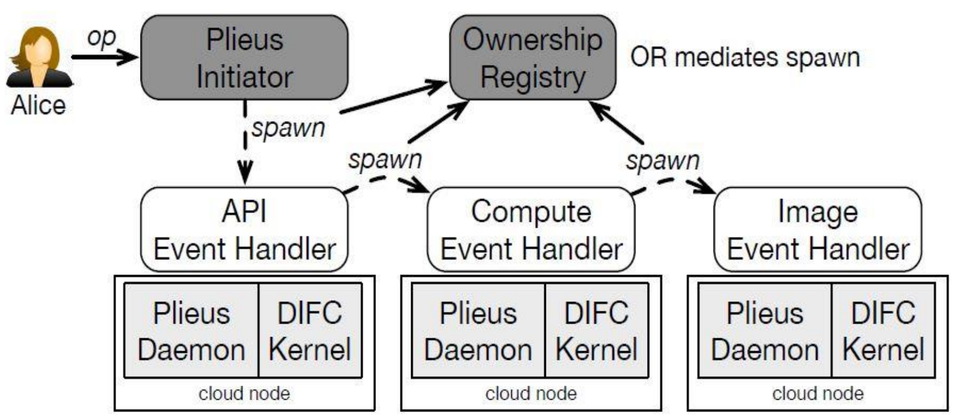
Security issues in cloud manifest themselves in mainly two forms: **insecure cloud services** and **insecure cloud architecture**.

• Insecure Cloud Service: Cloud relies on various **cloud services** to provision and manage customer resources (e.g., VM). Vulnerabilities in these cloud services can lead compromise of customers' data or computation, e.g., CVE reports **132** security vulnerabilities in OpenStack cloud services.

• Insecure Cloud Architecture: Current cloud platforms assume a TCB including each and every cloud service and the nodes they run on. Consequently, compromise of a single service or node can bring down the entire cloud.

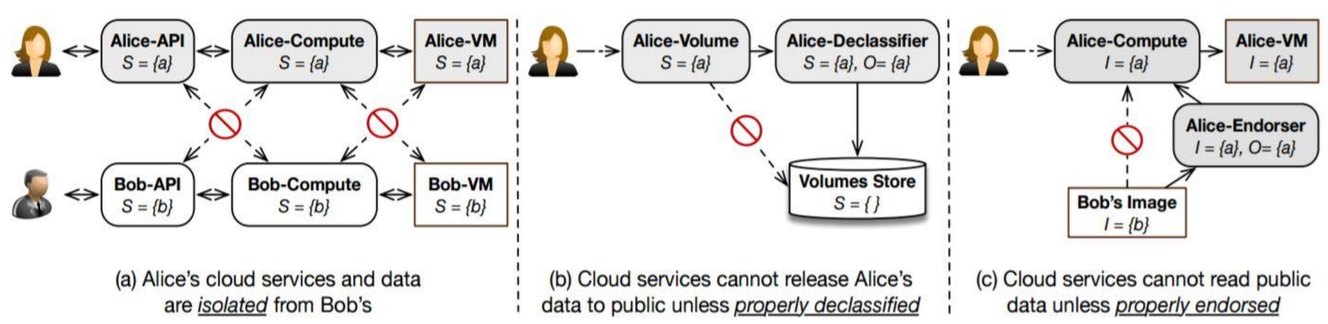
We present a framework that Minimize Permissions, Minimize Security Decisions, and Eliminate Dependence on Untrusted Nodes

Pileus Overview



DIFC in Pileus

DIFC: Decentralized Information Flow Control restricts the security decisions to only the event handlers trusted by the user. Pileus adopted concepts of security label and ownership from DIFC.



(a) Alice's cloud services and data are *isolated* from Bob's

(b) Cloud services cannot release Alice's data to public unless *properly declassified*

(c) Cloud services cannot read public data unless *properly endorsed*

Result

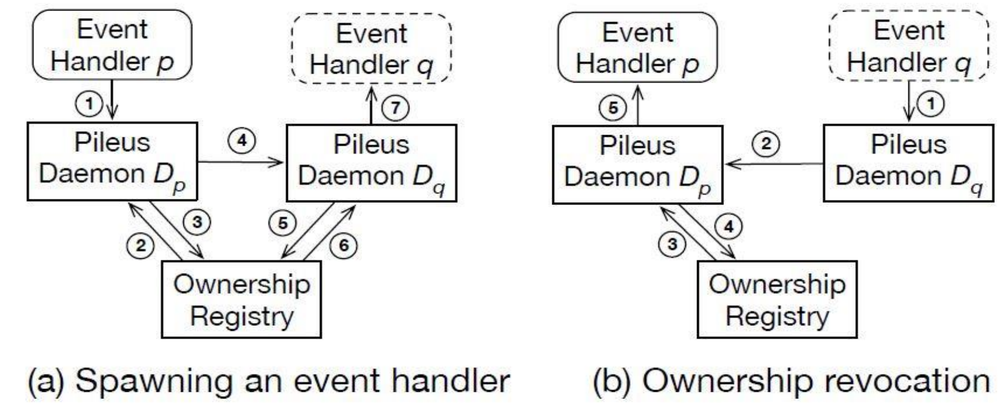
Vulnerability Mitigation: Pileus can systematically mitigate *44 out of 132* vulnerabilities reported in OpenStack.

Attack prevention: Pileus can detect and block a variety of attacks including *request forgery attacks*, *token sniffing attacks* and *request hijacking attacks*.

Category	Description	Example	#	Pileus
Unauthorized data access	Cloud services failed to enforce access control, allowing authenticated adversary to access resources private to other cloud users.	CVE-2013-2256, CVE-2012-4573	19	*Y*
Node breach	Cloud services use input provided in user requests when performing privileged operations, allowing remote adversary to arbitrarily read, write files or execute programs on a cloud node.	CVE-2011-4596, CVE-2014-0162	13	*Y*
Credential leakage	Cloud services fail to declassify vendor's secrets, allowing sensitive information (e.g., credentials) to accidentally flow out of the cloud.	CVE-2014-7231, CVE-2014-1948	10	*Y**
Data residue	Cloud services fail to clean volumes before sharing, allowing sensitive information to be leaked through data residue.	CVE-2012-5625, CVE-2013-4183	2	*Y**
Misconfiguration	Cloud services read or write files that are publicly accessible on a cloud node, allowing local adversary to escalate privilege by reading or writing these files.	CVE-2013-7048, CVE-2013-0261	6	*N**
DoS	Cloud services fail to manage system resources on a cloud node, allowing remote adversary to overwhelm the computation power of a cloud node.	CVE-2013-6437, CVE-2012-1585	30	*N**
Authentication bypass	Cloud services fail to correctly authenticate user.	CVE-2014-5253, CVE-2013-6419	28	*N*
Web attack	Web application vulnerability such as XSS and session fixation.	CVE-2014-8578, CVE-2012-2144	11	*N*
Miscellaneous	Various implementation flaws in cloud services that may lead to attack.	CVE-2013-2013, CVE-2014-7144	12	*N*

Spawn Protocol

Pileus spawn protocol prevents: 1) nodes that lack User's authority from spawning event handlers that could access user's data 2) node that fails to satisfy user's security policy from being selected as target node or given the authority to execute user's handler



(a) Spawning an event handler

(b) Ownership revocation

Future Work

- Investigate efficient and scalable intrusion detection mechanisms in cloud for both cloud applications and infrastructure.
- Extend integrity verification and monitoring to containers (e.g., docker).

Related Publications

- Y. Sun, G. Petracca, T.Jaeger. **Pileus: Protecting User Resources from Vulnerable Cloud Services**. 2016 Annual Computer Security Applications Conference(ACSAC' 16)
- Y. Sun, G. Petracca, T. Jaeger. **Making Information Flow Explicit and Controllable in Cloud**. *Technical Report NAS-TR-0184-2015*
- Y. Sun, G. Petracca, H. Vijayakumar, T. Jaeger, J. Schiffman**. CloudArmor: Protecting the Execution of Customer's Cloud**. In *Proceedings of the 2015 IEEE International Conference on Cloud Computing (IEEE CLOUD' 15).*

Sponsored by National Science Foundation and Army Research Lab