

A Modular, User-Centric Security Analysis of OpenStack

Ran Canetti†, **Marten van Dijk**‡, Jason Hennessey†, Kyle Hogant†,

Hoda Maleki‡, Mayank Varia†, Reza Rahaeimehr and Haibin Zhang‡

†Boston University, ‡University of Connecticut



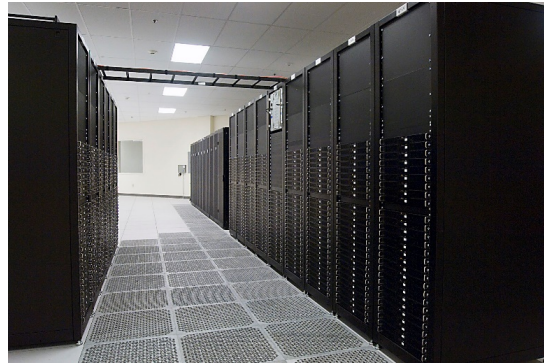
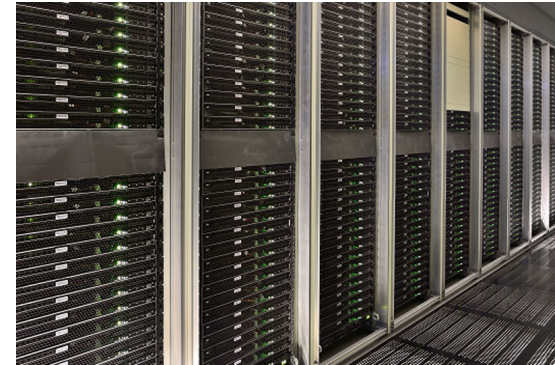
UConn

- Introduction
 - Cloud Computing
 - OpenStack
 - Universal Composability
- Universal Composability
- Analysis Approach
- Conclusion

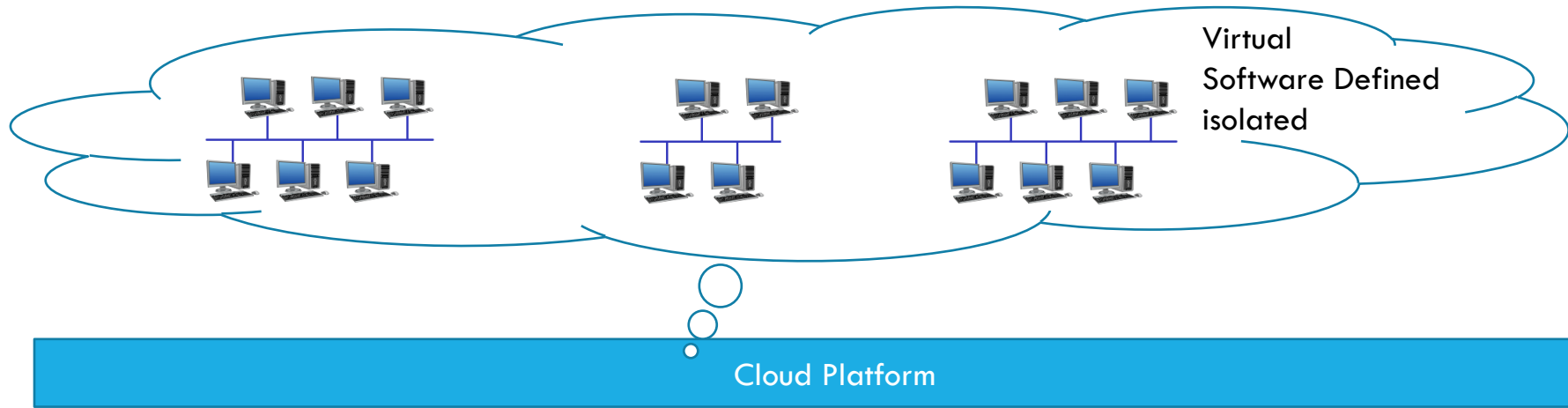


Challenges

- Deploying new applications
- Running multiple applications
- Scaling up/down the share of each application
- Different security requirements
- Protecting against the vulnerabilities of the other applications
- ...



Cloud Computing



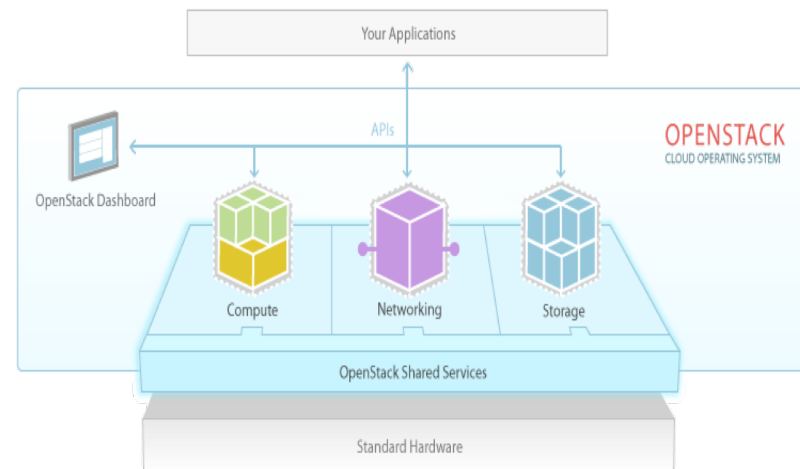
Cloud Security Issues

- Cloud Platform
 - Huge software
 - Many bugs
- Cloud serves several different applications
 - Isolation
 - Shared underlying hardware; Side channel attacks
 - Buggy code
- Cloud serves many people
 - Attackers, Hackers
 - Privacy, Confidentiality









OpenStack

- Reliable Open Source Cloud Platform
- Widely Used
 - 71% of clouds in production or full operational use
- Infrastructure as a Service (IaaS)
- Highly Modular
 - 23 main modules
 - Many plug-ins
- Community based development Model
 - More than 6500 contributors
- Rapidly growing
 - 6-month cycles
















Main Services

 SWIFT Object Storage	 KEYSTONE Identity	 NOVA Compute	 NEUTRON Networking	 CINDER Block Storage	 GLANCE Image Service
---	--	--	---	---	---



Optional Services

 HORIZON Dashboard	 CEILOMETER Telemetry	 HEAT Orchestration
 TROVE Database	 SAHARA Elastic Map Reduce	 IRONIC Bare-Metal Provisioning
 ZAQAR Messaging Service	 MANILA Shared Filesystems	 DESIGNATE DNS Service
 BARBICAN Key Management	 MAGNUM Containers	 MURANO Application Catalog
 CONGRESS Governance		



OpenStack Security Issues

- Cloud issues
- Difficulty of security analysis
 - More than 3.5 million lines of code
 - More than 6,500 contributors
- Lack of clear security model
- Not well defined APIs
- Lots of plug ins
 - VMM: KVM, XEN, Hyper-V, VMware



UCONN

Solution?

Universal Composability



Universal Composability

- General-purpose model for security analysis of protocols
- Perfect for modular systems
- Common understanding and common language
- Introduced by Ran Canetti in 2000



- Secure protocols remain secure
- Security proof based on emulation
- A protocol emulates another one,
 - if no environment (observer) can distinguish the executions
 - $P1 \approx P2$



Goals

- Better understanding of OpenStack's security guarantees (for OpenStack Users/Customers)
- Assist in identifying highest-impact security improvements (for OpenStack Developers)
- Formal definition of OpenStack security-related functionality (for Cryptographers)
- Study the security interfaces between components which has not been studied well

Steps

- Define Functionality of Ideal Cloud
- Define Functionality of Ideal Components
- Show that Components realize the Ideal Cloud Functionality
- Propose OpenStack Modifications to realize the Functionalities
- Propose Component Implementations that realize the Functionalities



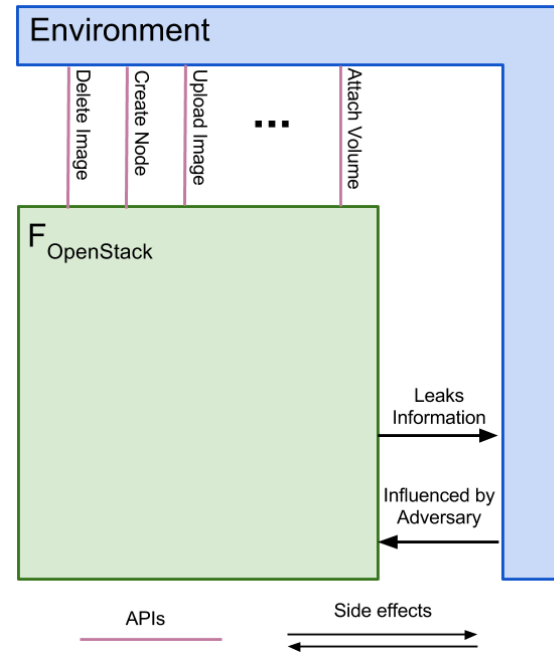
Ideal World

Ideal OpenStack

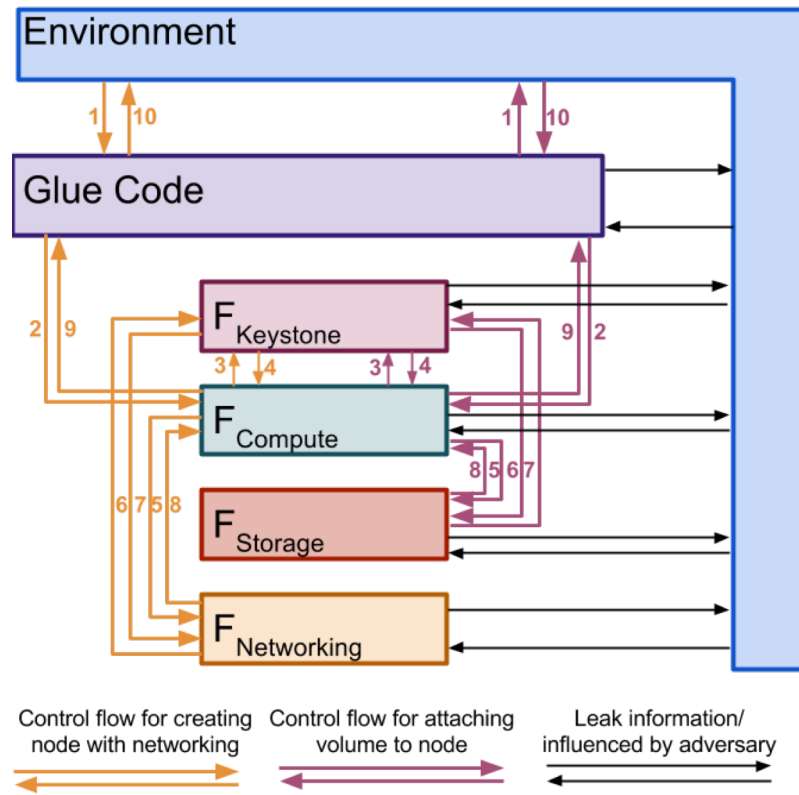
- Accurate
- No time

Ideal Functionalities:

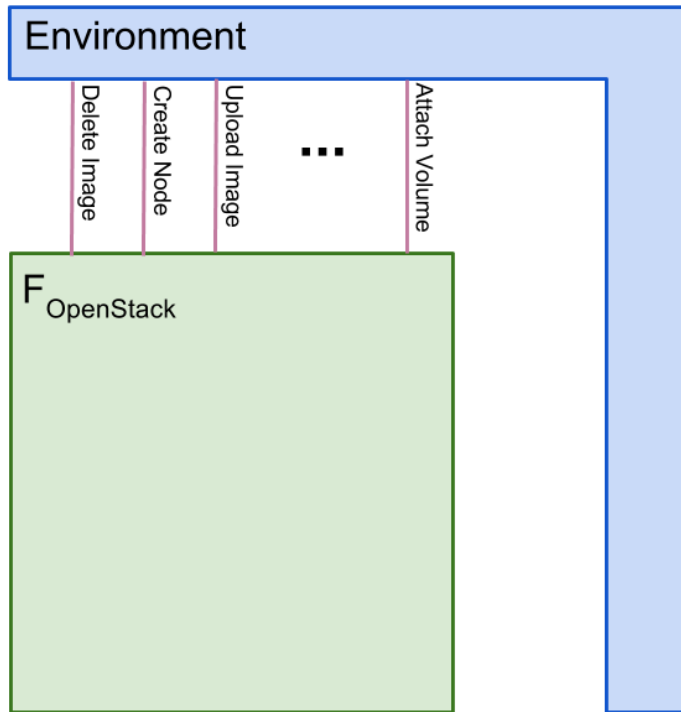
- Create Node
- Delete Node
- Upload Image
- Delete Image
- Create Volume
- ...



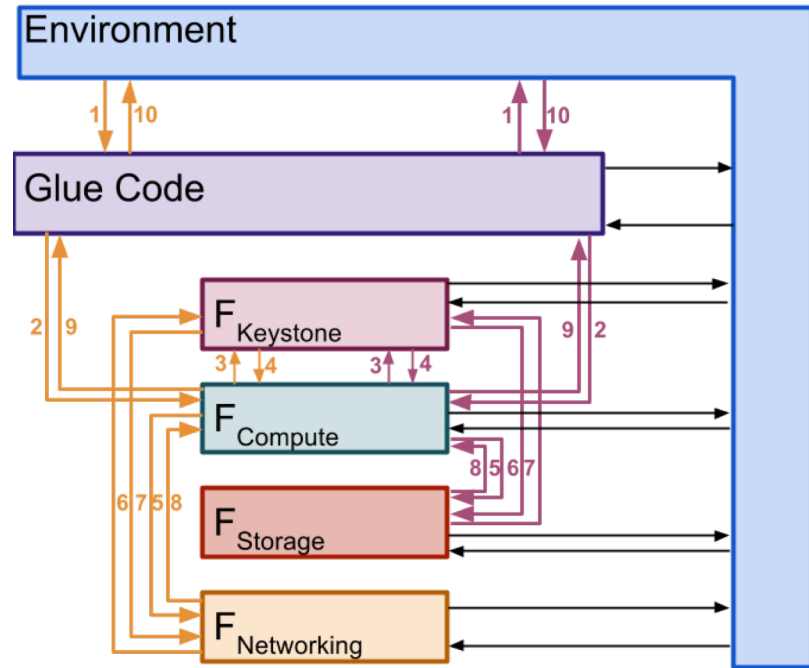
Hybrid World



Security Analysis



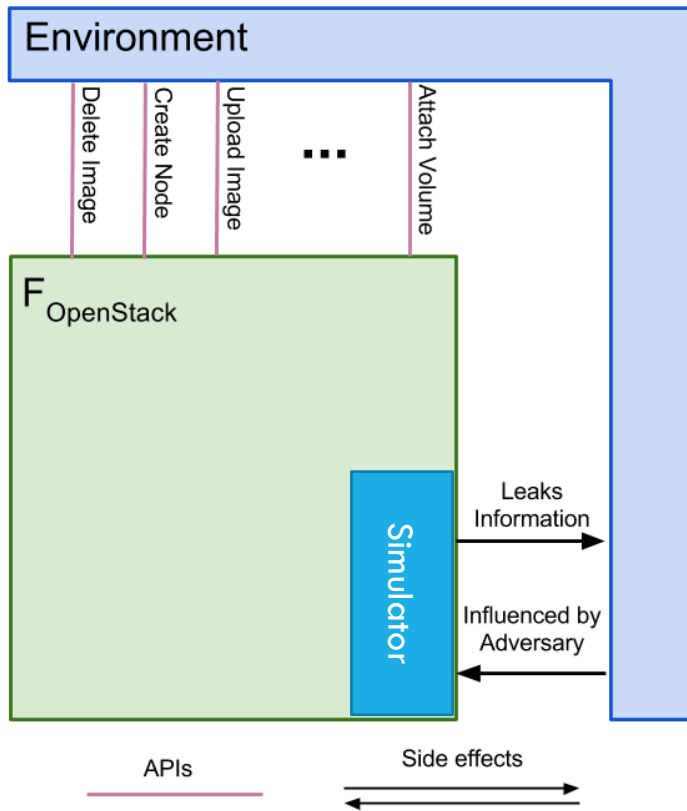
APIs



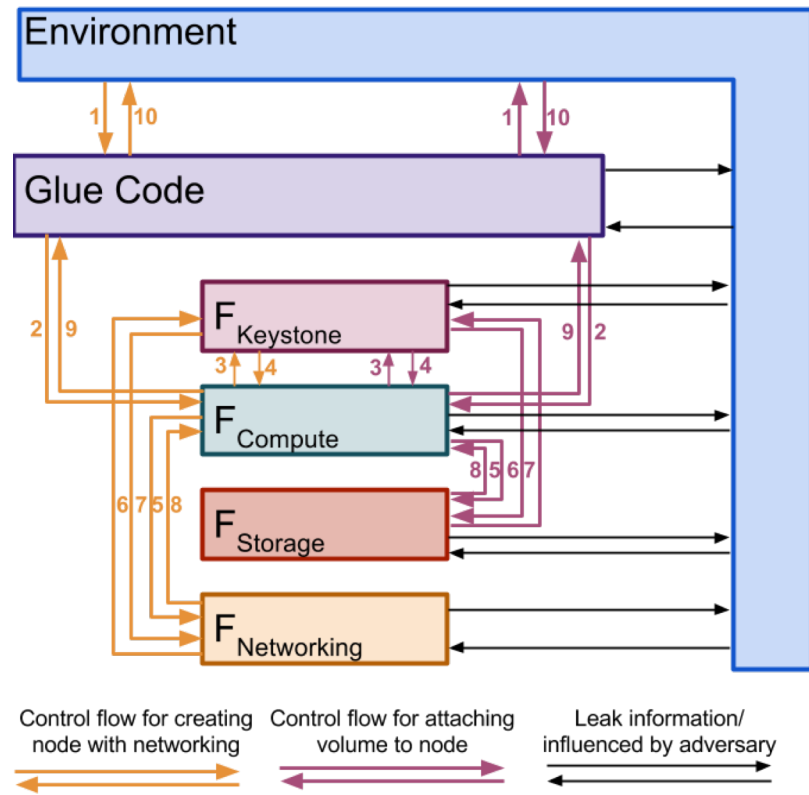
Control flow for creating node with networking Control flow for attaching volume to node Leak information/ influenced by adversary



Security Analysis



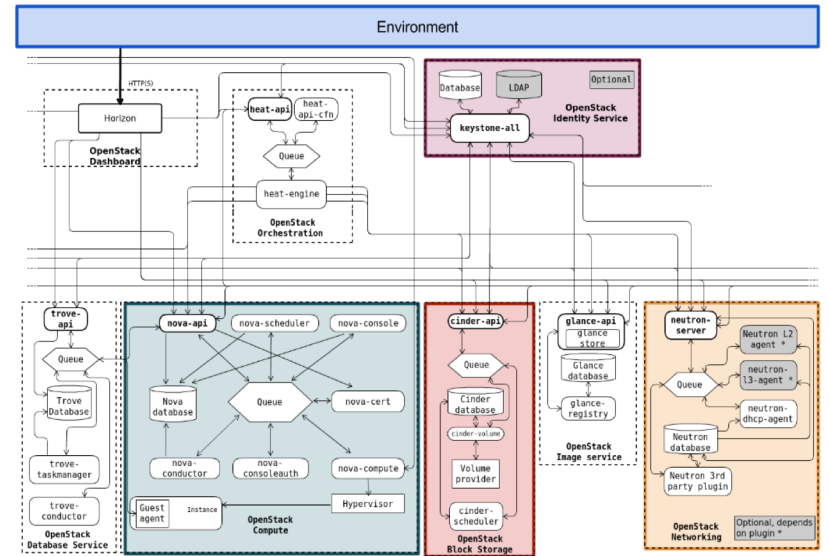
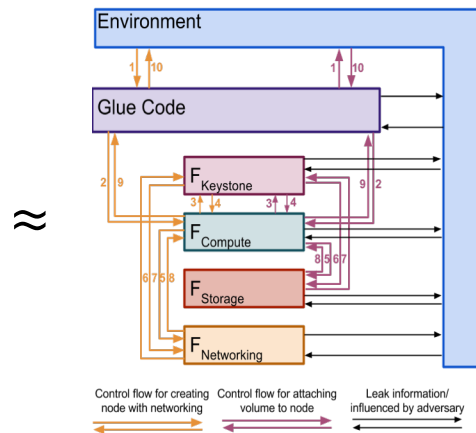
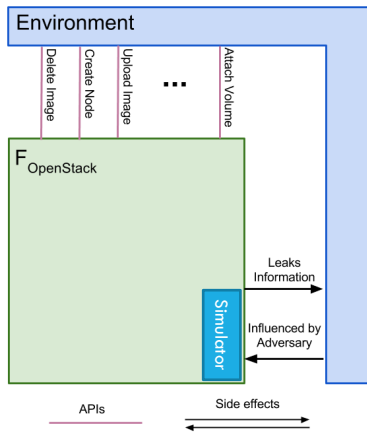
≈



Next Steps



Security Analysis



Conclusion

- OpenStack security must be analyzed
 - The security model depends on the plug-in set
- UC
 - Better understanding of cloud security model
 - Reveals security bottlenecks and concerns
 - Allows understanding to how to improve the security posture
- Needs Time and Expertise

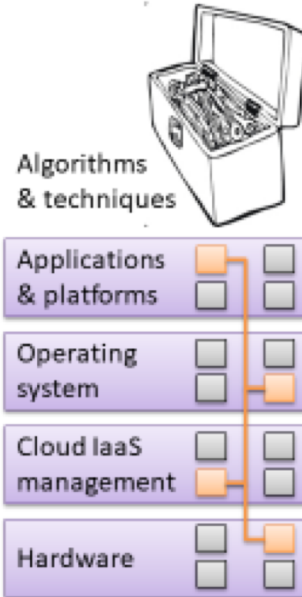
A Modular, User-Centric Security Analysis of OpenStack

Challenge:

- Cloud computing has a huge impact on society, but security concerns inhibit its uptake
- OpenStack is the prevalent open-source, non-proprietary package for managing cloud services and data centers
- Provide rigorous and holistic security analysis of OpenStack in the universally composable (UC) security framework

Solution:

- Analyze OpenStack's multiple inter-related components
- Assert the security of components individually
- Then compose to derive the overall system's security



Scientific Impact:

- *User-Centric:* Stresses the security guarantees given to users of the system
- *Modular:* Formulates security properties for individual components and deduces from these security properties of the overall service
- *Defense in Depth:* OpenStack can be improved, with minimal changes

Broader Impact:

- Showcase composable design and analysis as a viable basis for secure system design
- Impact upon the practice of cloud computing (collaboration Massachusetts Open Cloud)
- Several outreach programs to expose local-area middle and high school students and their teachers to cybersecurity

Participating Institutions: Boston University (NSF grant 1414119, "Modular Approach to Cloud Security"), MIT (1413920), Northeastern (1413964), and UConn (1413996). For more info, email marten.van_dijk@uconn.edu.



Thank You !

Lab's website: <http://scl.uconn.edu>

Other research: HW Trojans, Secure Supply Chain Management, Moving Target Defense, Secure Processor Architectures, Oblivious RAM, FHE, ... and wherever my students take me

Picture References:

- <http://sthelenslscb.org.uk>
- <http://www.dell.com>
- <https://www.openstack.org>

