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

# Seeding Clouds with Trust Anchors

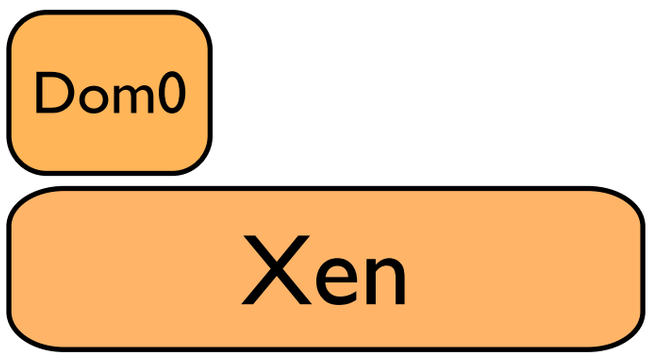
**Joshua Schiffman**, Thomas Moyer,
Hayawardh Vijayakuamar,
Trent Jaeger, and Patrick McDaniel
CCSW '10

# Hurdles to Cloud Adoption

- Clouds offer customers a platform for on-demand resources and reduced administrative effort
- However, fears of **data loss** and **security breaches** have stifled adoption by many businesses
- We propose increasing the **transparency** of cloud platforms to build trust in them

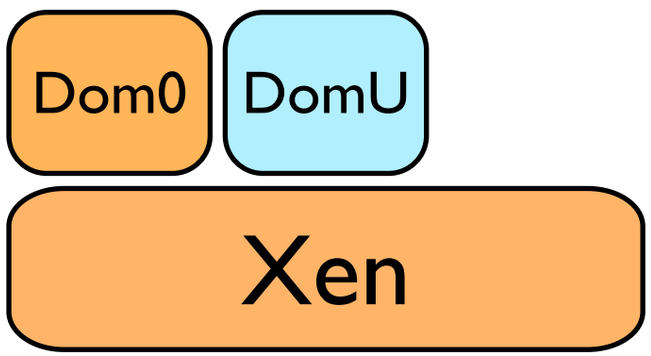
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



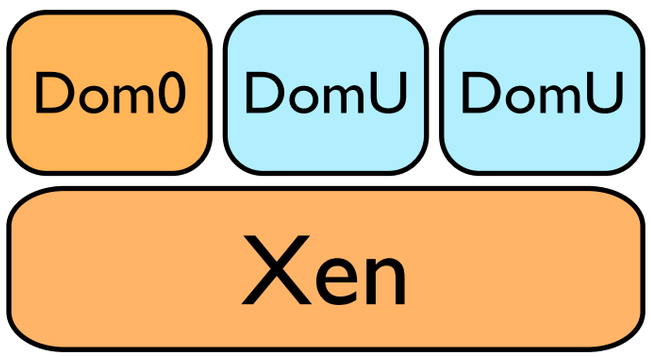
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



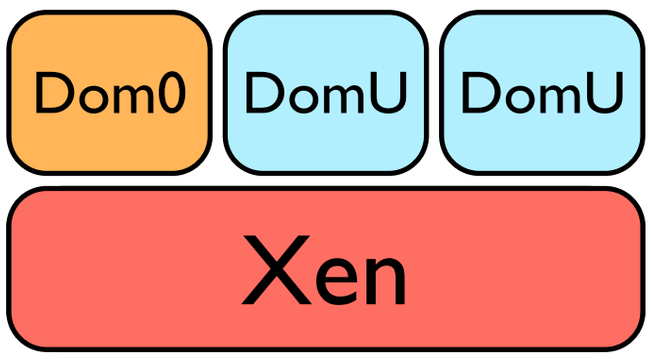
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



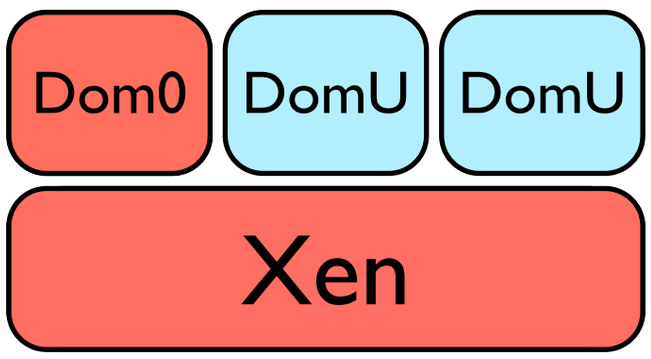
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



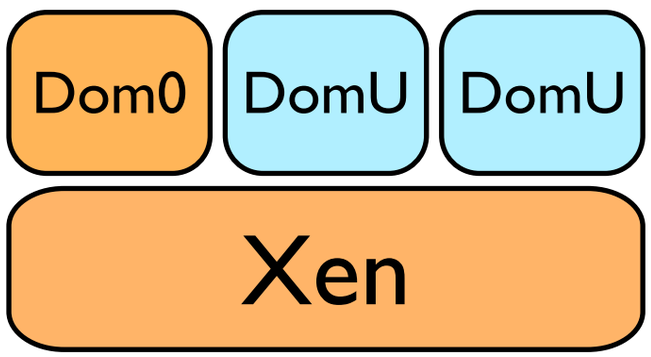
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



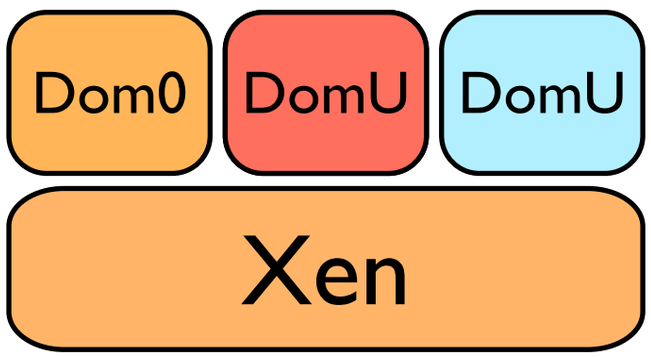
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



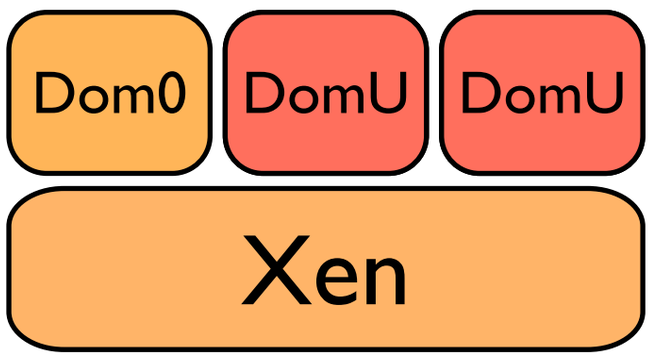
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



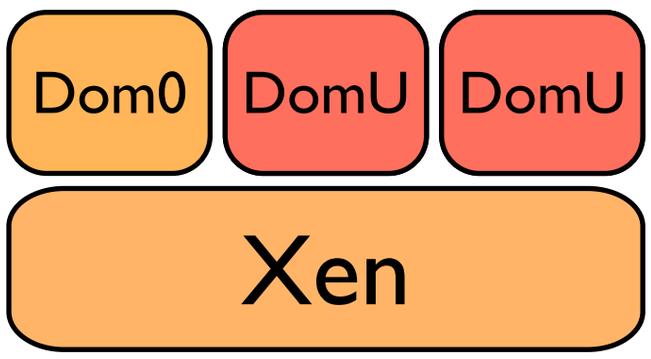
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



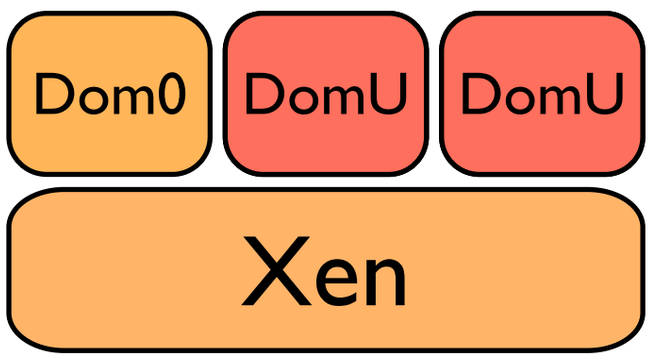
# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



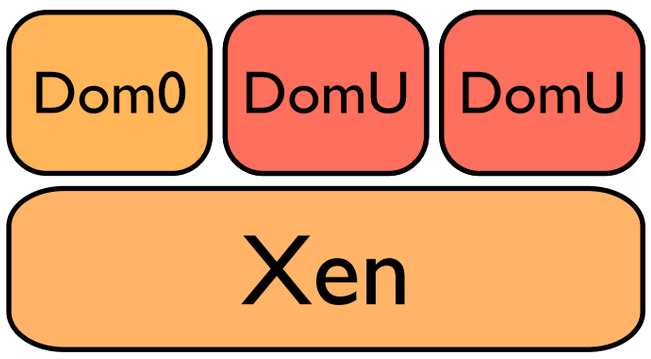

# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



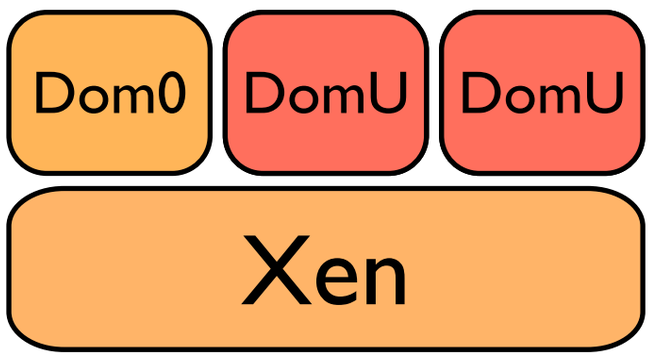

# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components



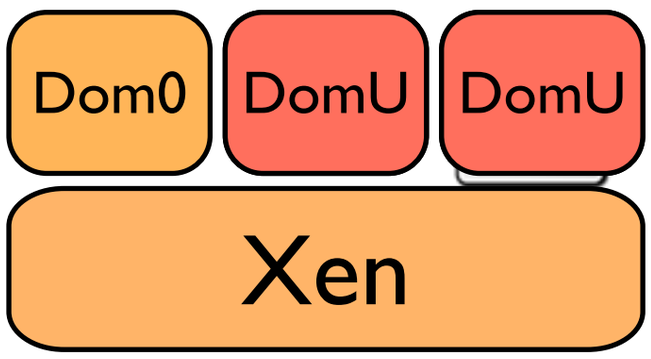

# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components




# Uncertainty in Clouds

- Customers are concerned with:
  - Host and VM integrity
  - VM isolation / protection
  - Data leakage
- Need to verify integrity of those components

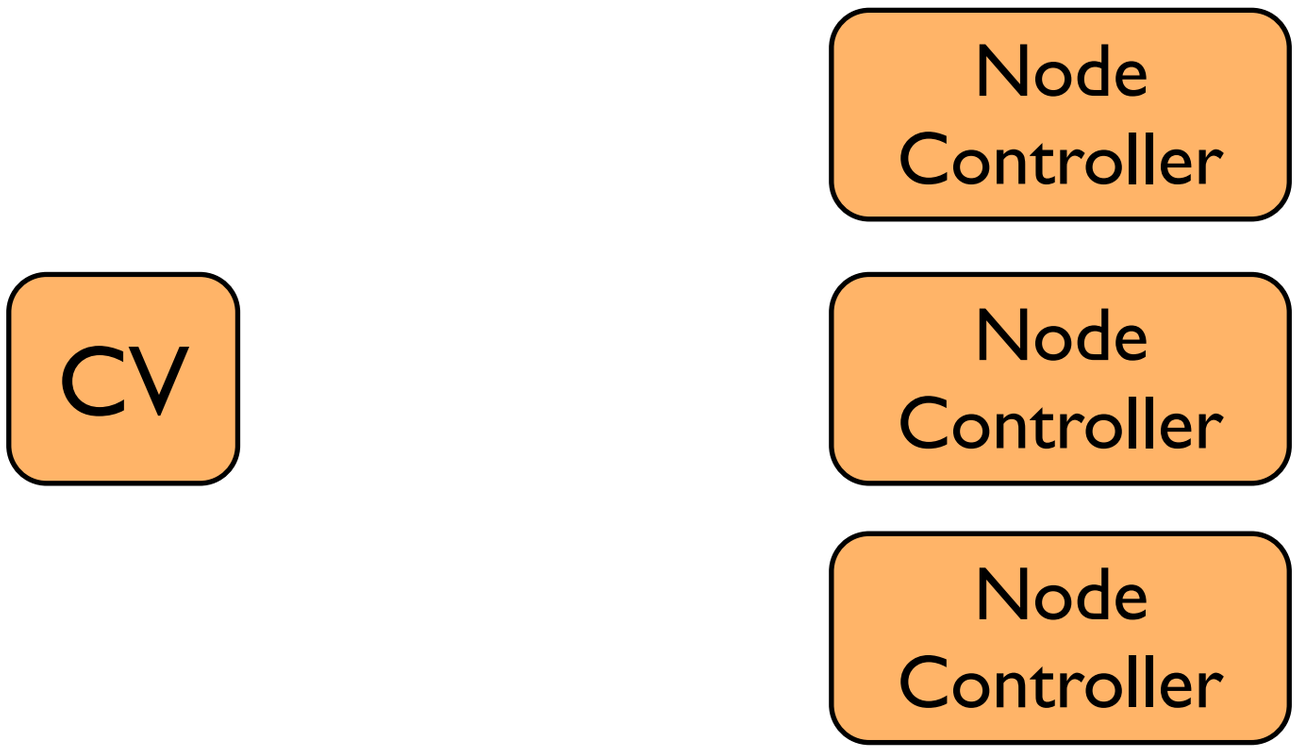



# Cloud support for proofs

- Clouds offer a unique administrative environment for integrity measurement
  - Physical security, internal PKI, consistent components
  - Centralized administration over many systems
- Focus on using hardened / proven components
  - Assured hypervisors (e.g., SEL4) and code
  - Verifiable enforcement policies

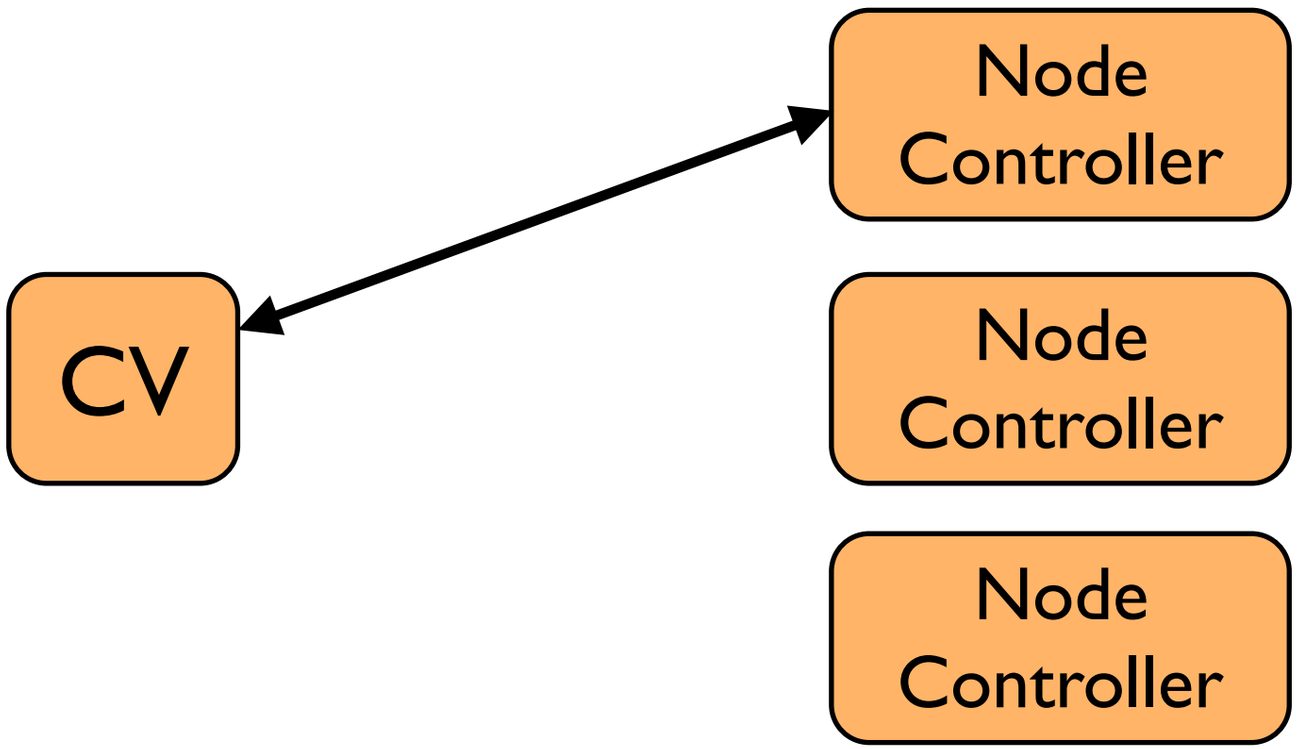
# Cloud Verifier

- We propose a Cloud Verifier (CV) mechanism to enable verification of cloud platforms by proxy
  - Verifiable component in the cloud
  - Monitors the integrity of VM hosts using a public integrity criteria



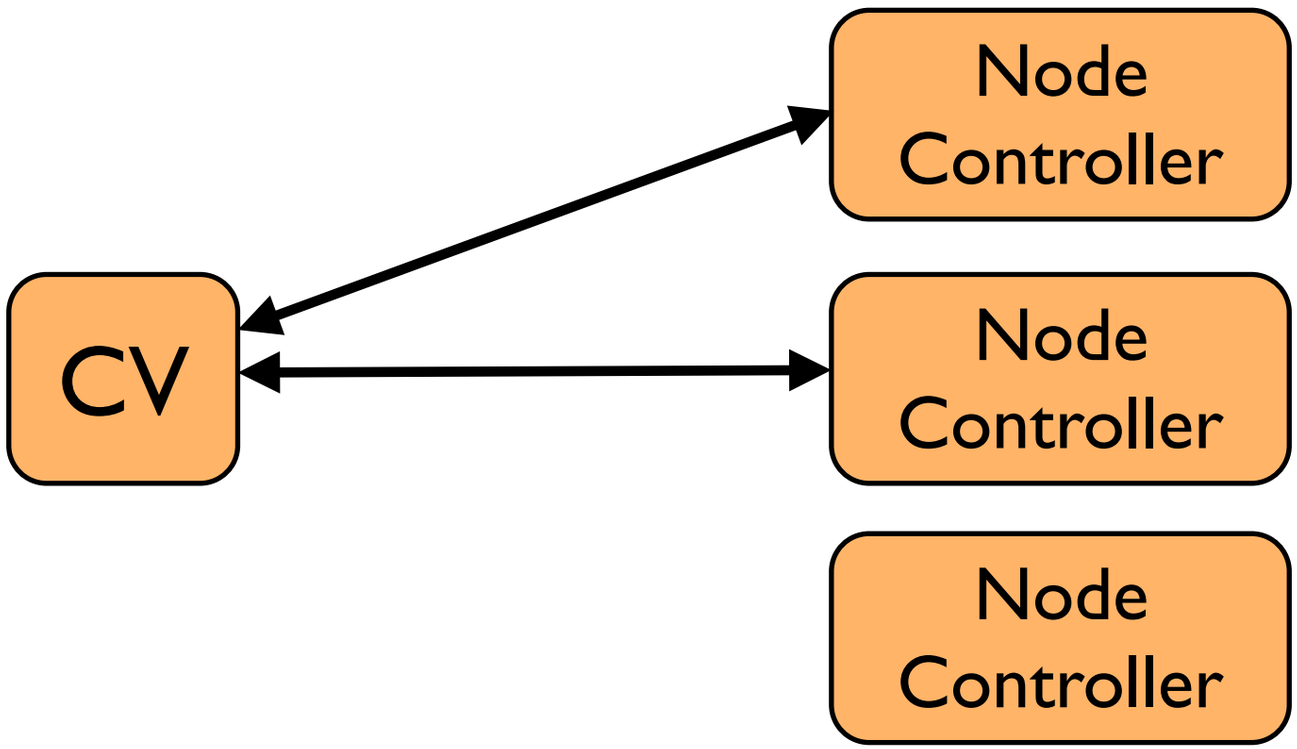
# Cloud Verifier

- We propose a Cloud Verifier (CV) mechanism to enable verification of cloud platforms by proxy
  - Verifiable component in the cloud
  - Monitors the integrity of VM hosts using a public integrity criteria



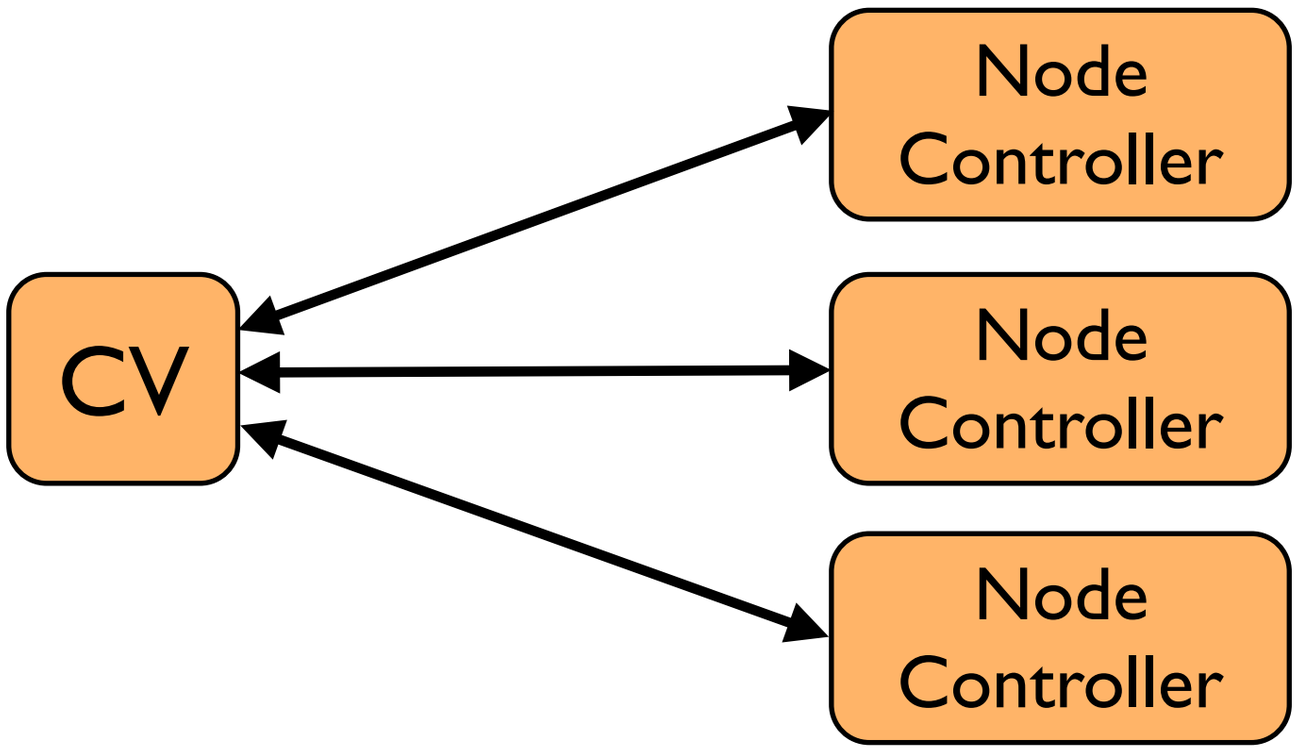
# Cloud Verifier

- We propose a Cloud Verifier (CV) mechanism to enable verification of cloud platforms by proxy
  - Verifiable component in the cloud
  - Monitors the integrity of VM hosts using a public integrity criteria



# Cloud Verifier

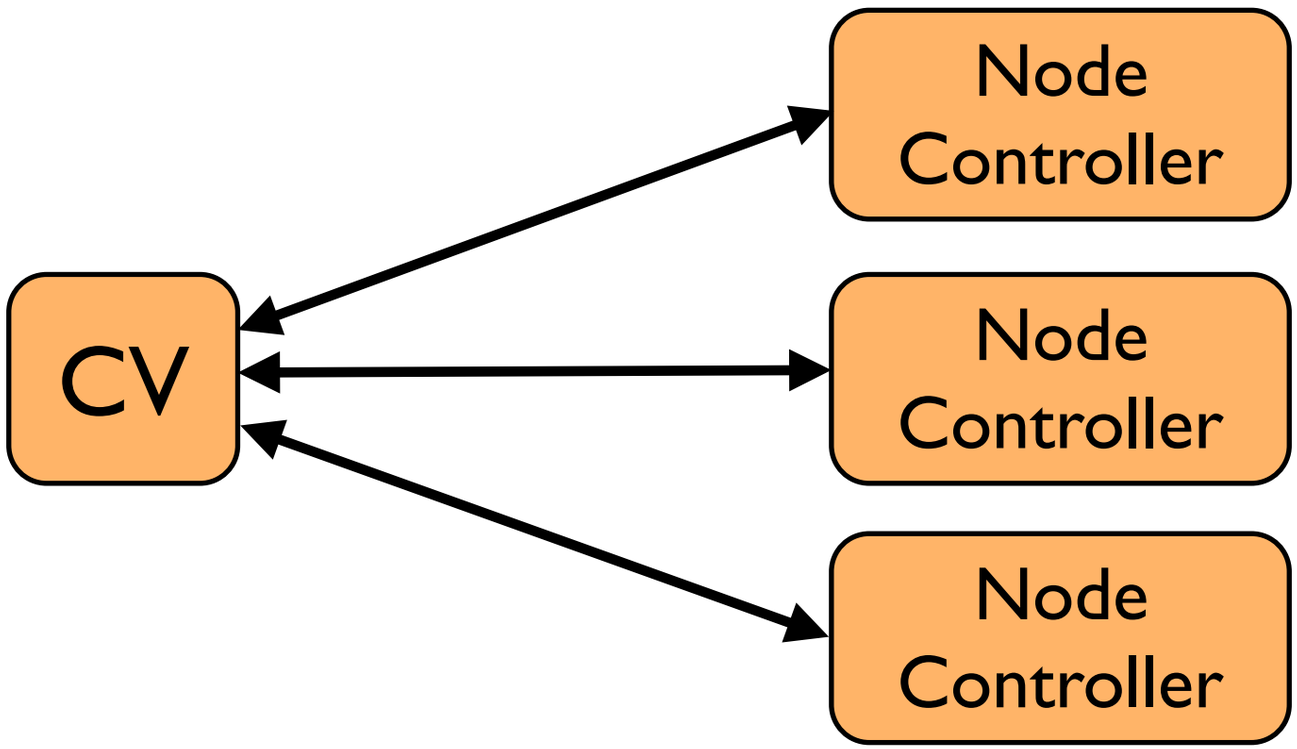
- We propose a Cloud Verifier (CV) mechanism to enable verification of cloud platforms by proxy
  - Verifiable component in the cloud
  - Monitors the integrity of VM hosts using a public integrity criteria



# Cloud Verifier

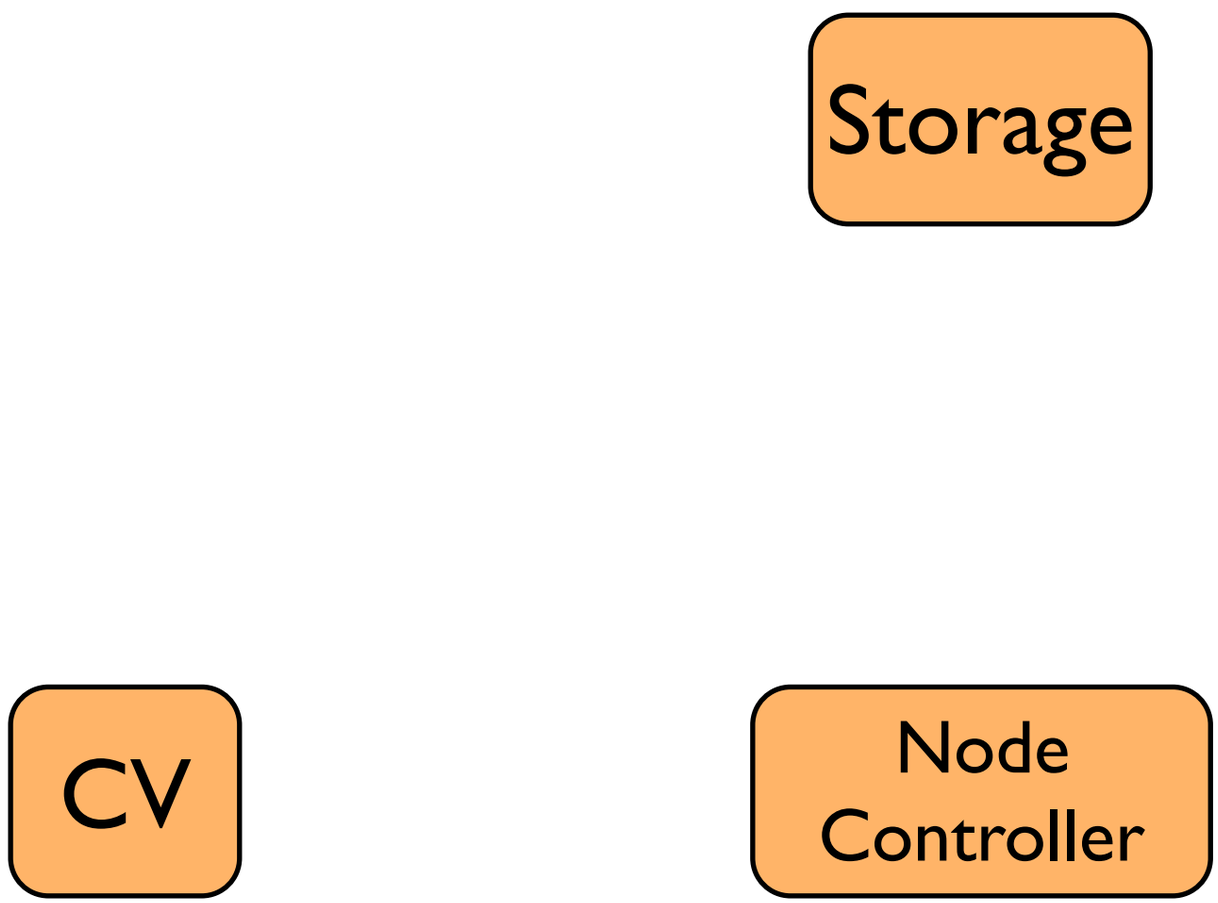
- We propose a Cloud Verifier (CV) mechanism to enable verification of cloud platforms by proxy
  - Verifiable component in the cloud
  - Monitors the integrity of VM hosts using a public integrity criteria

Integrity Criteria



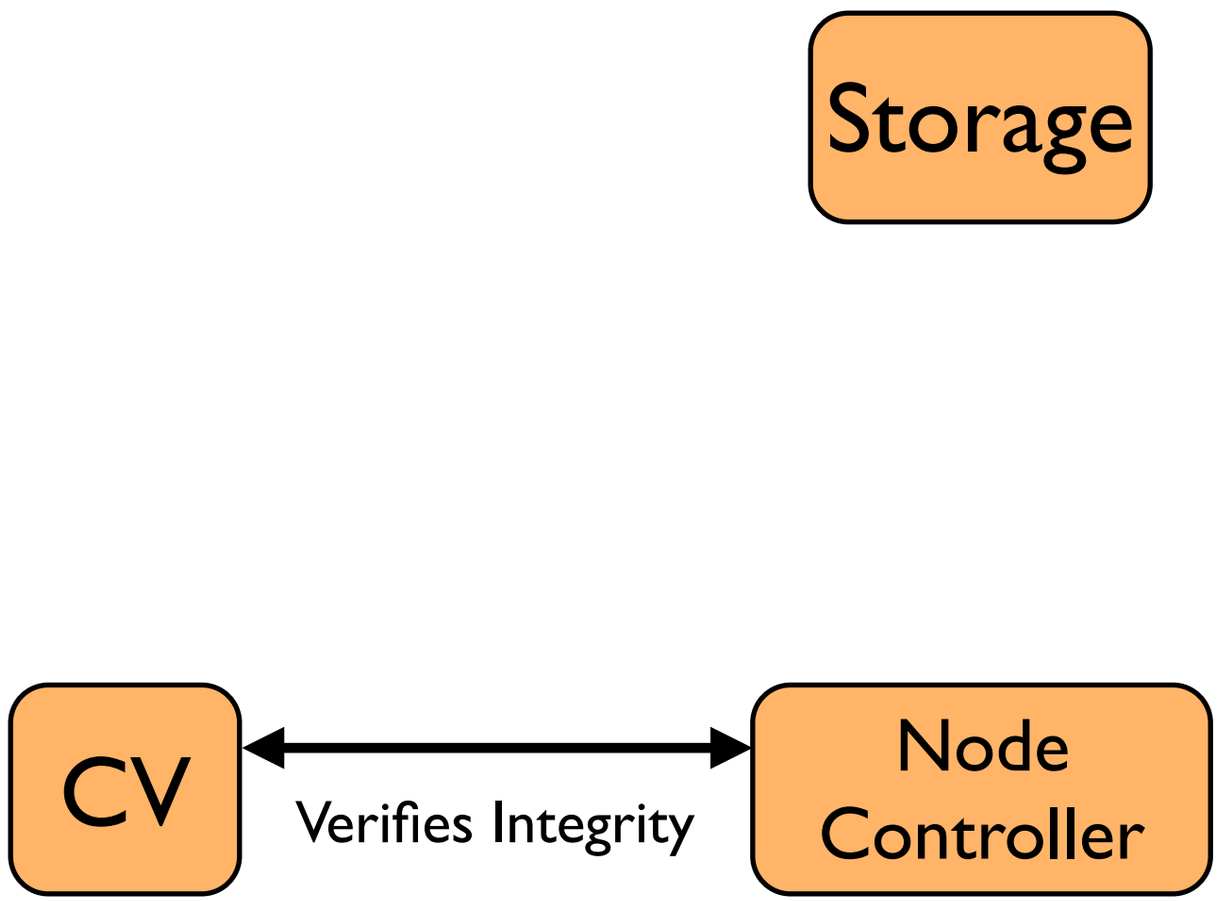
# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key



# Customers using the CV

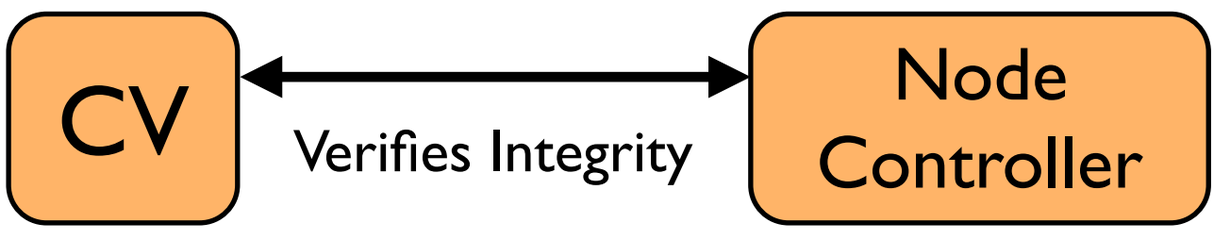
- CV then vouches for integrity of a VM's host using a signed public key



# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

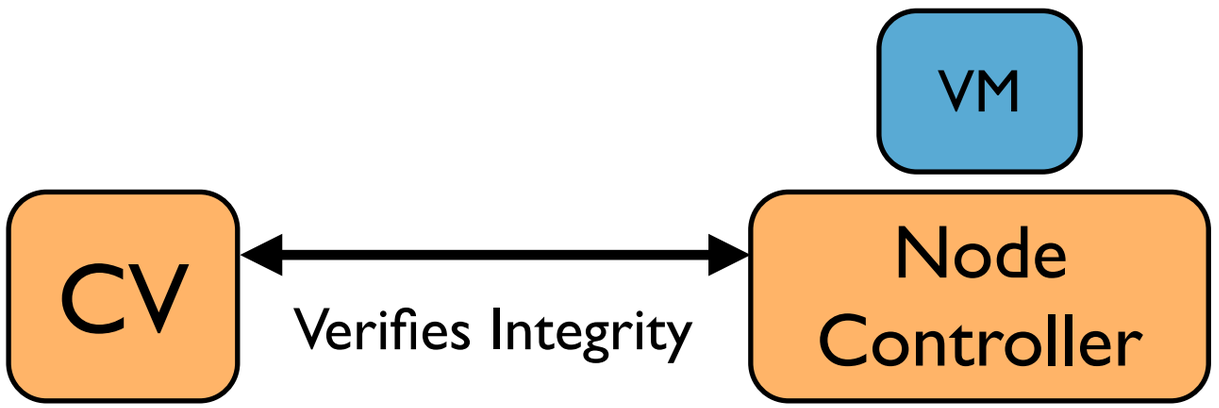
Storage



# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

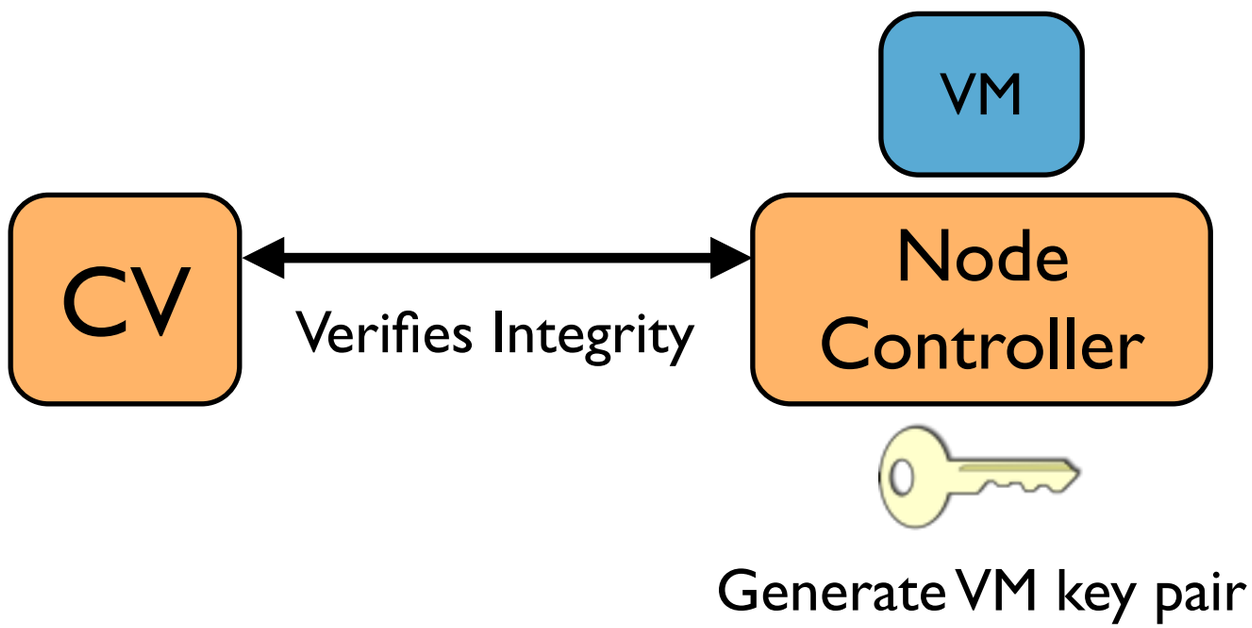
Storage



# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

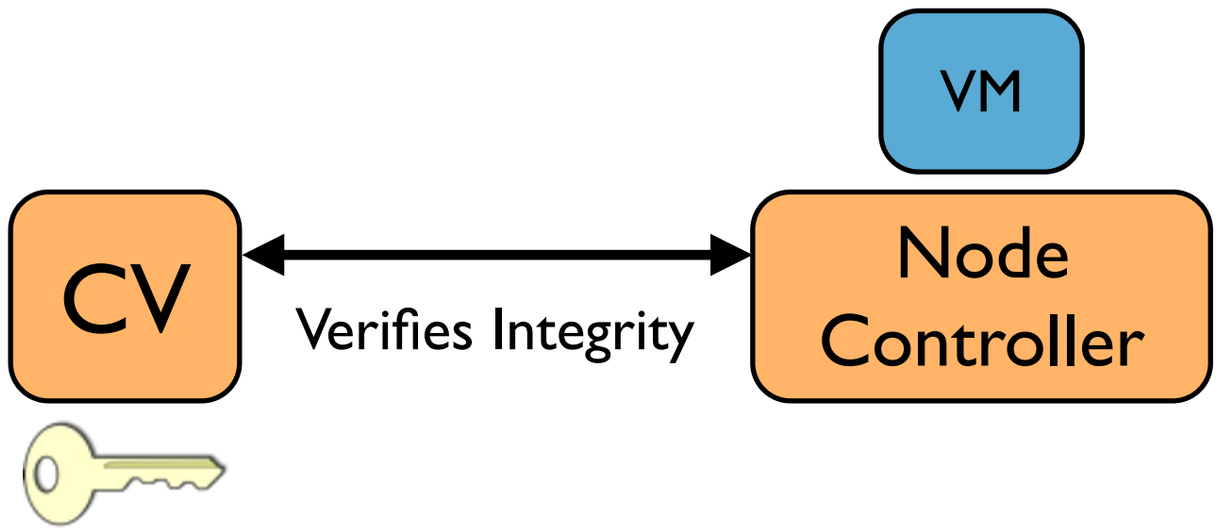
Storage



# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

Storage

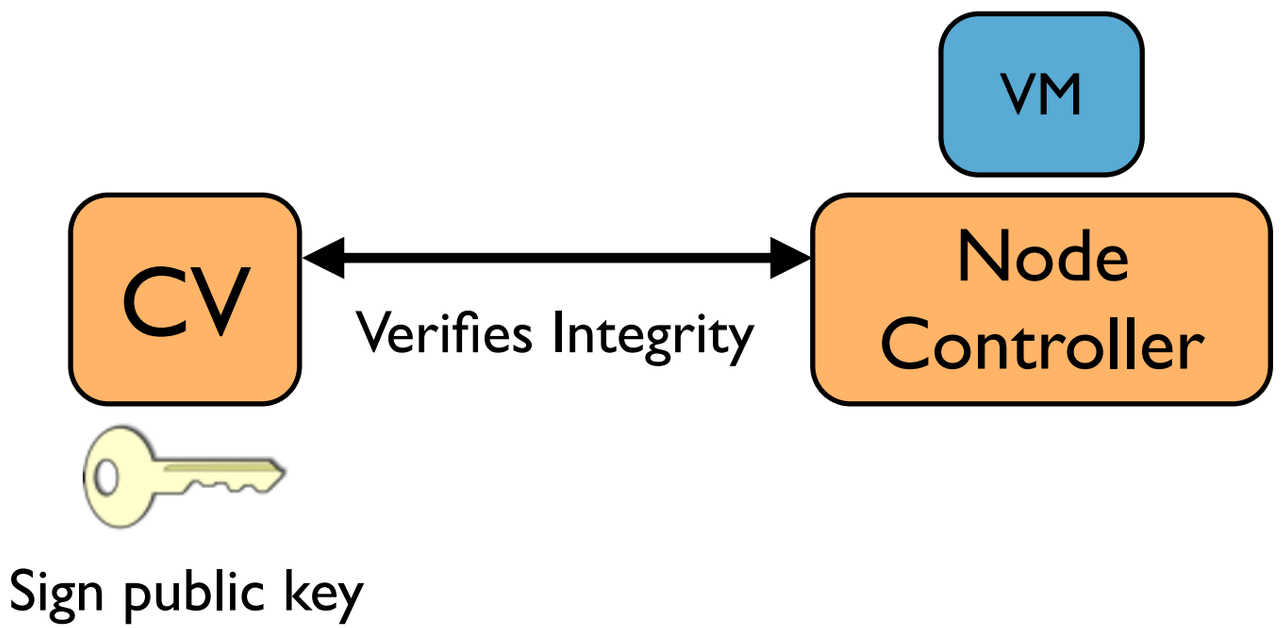



Generate VM key pair

# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

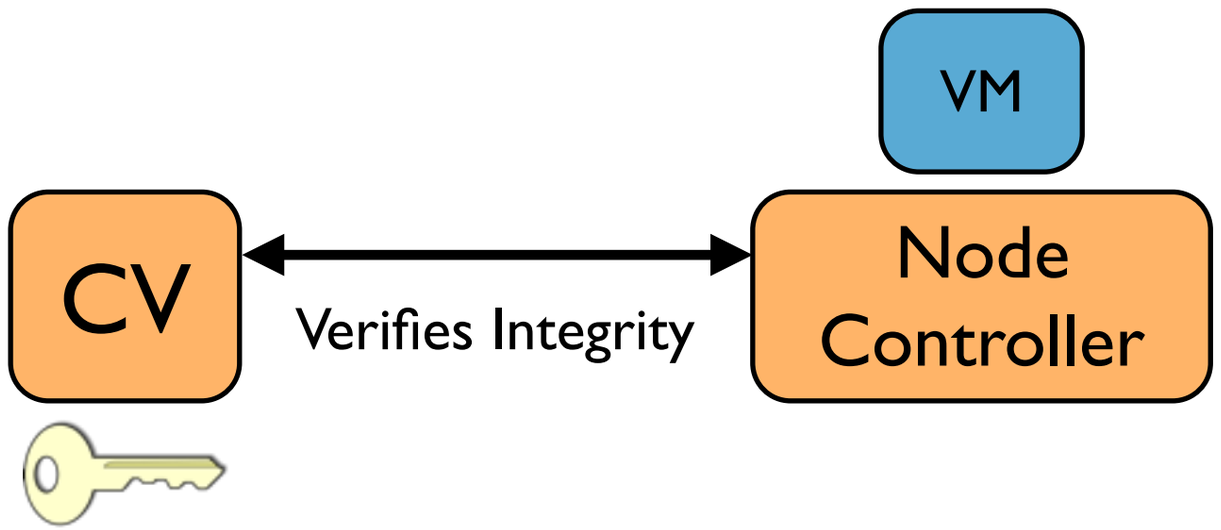
Storage



# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

Storage

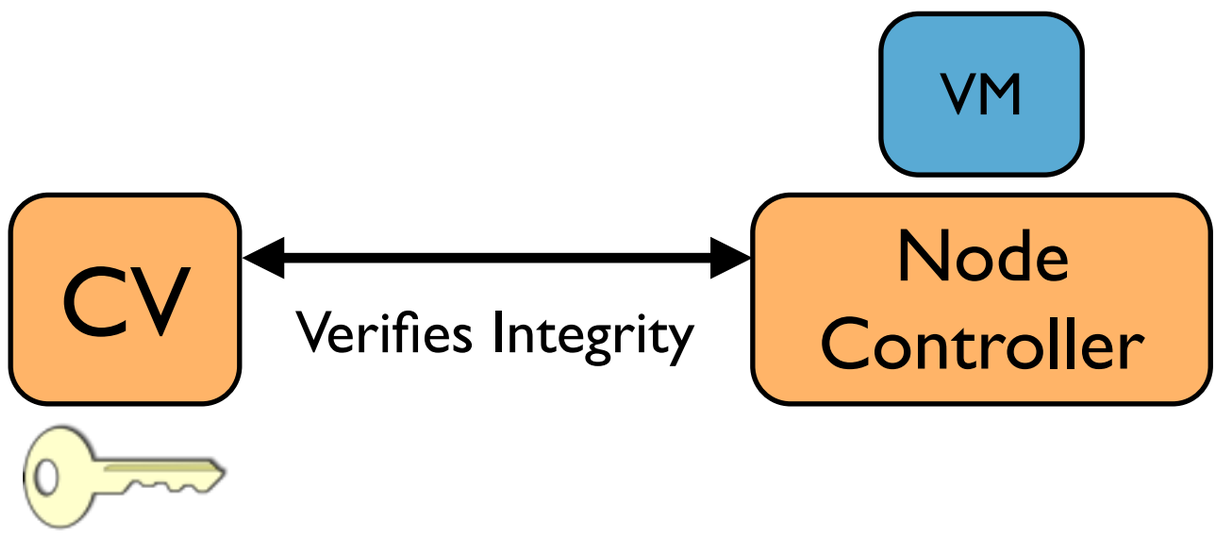


# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key

Storage

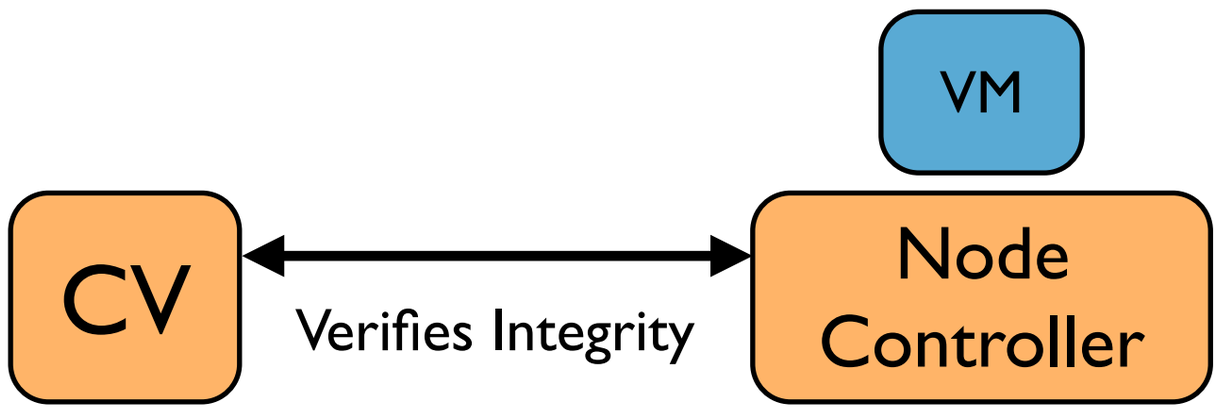
Get VM key



# Customers using the CV

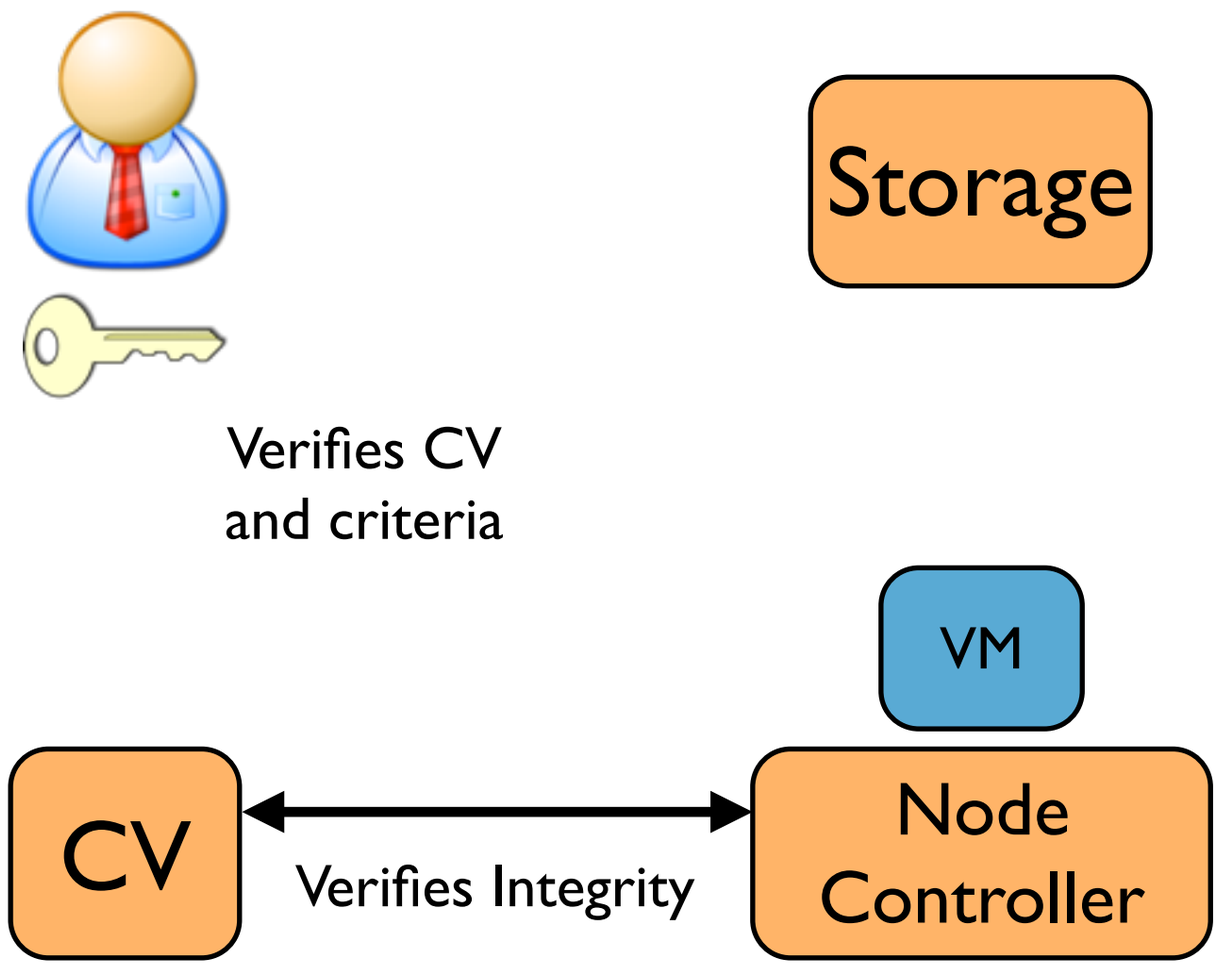
- CV then vouches for integrity of a VM's host using a signed public key

Storage



# Customers using the CV

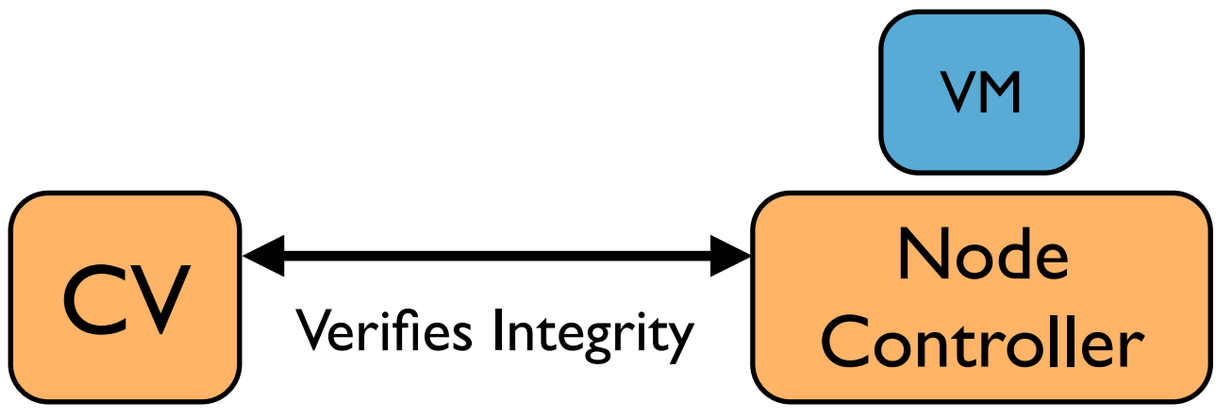
- CV then vouches for integrity of a VM's host using a signed public key



# Customers using the CV

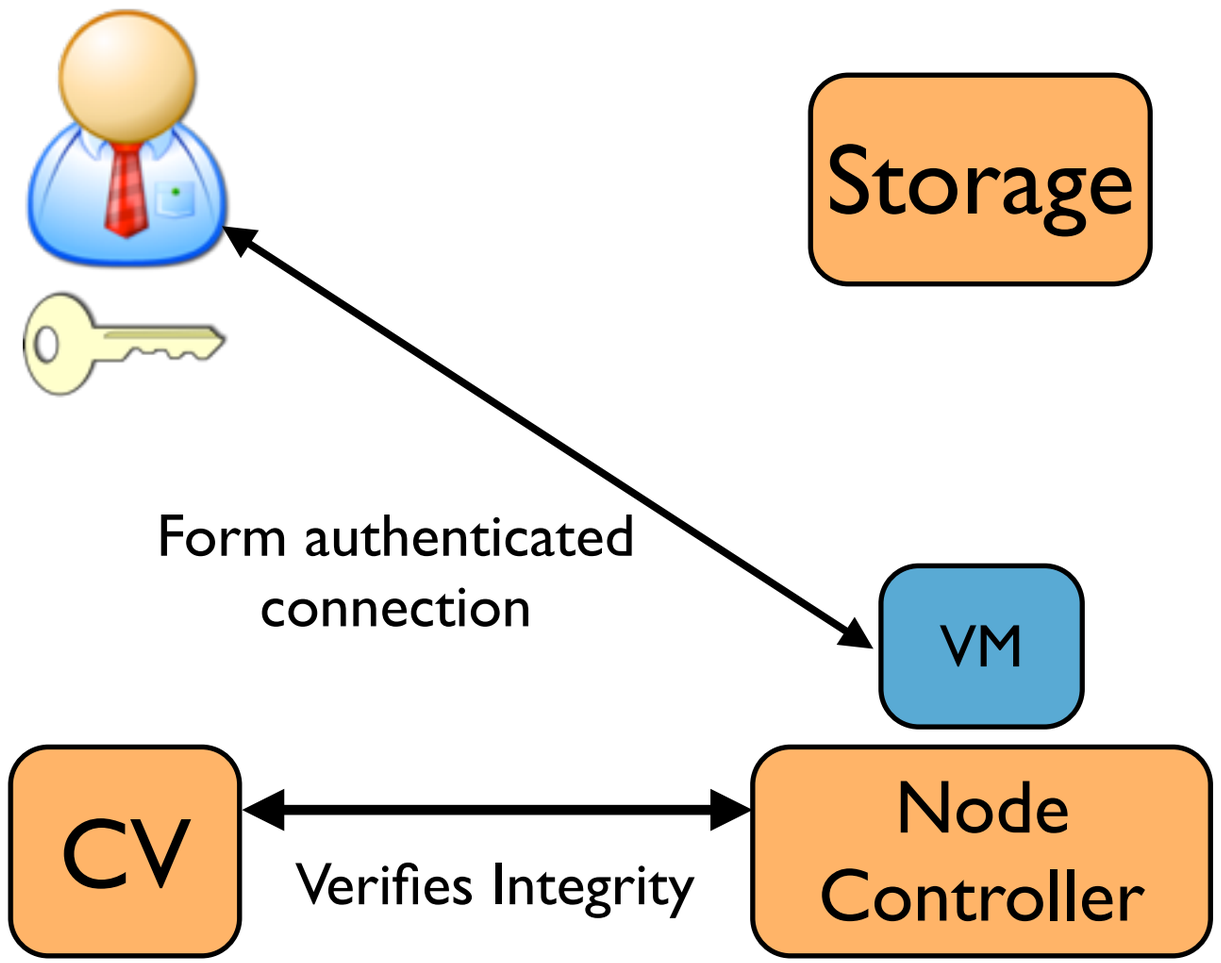
- CV then vouches for integrity of a VM's host using a signed public key

Storage



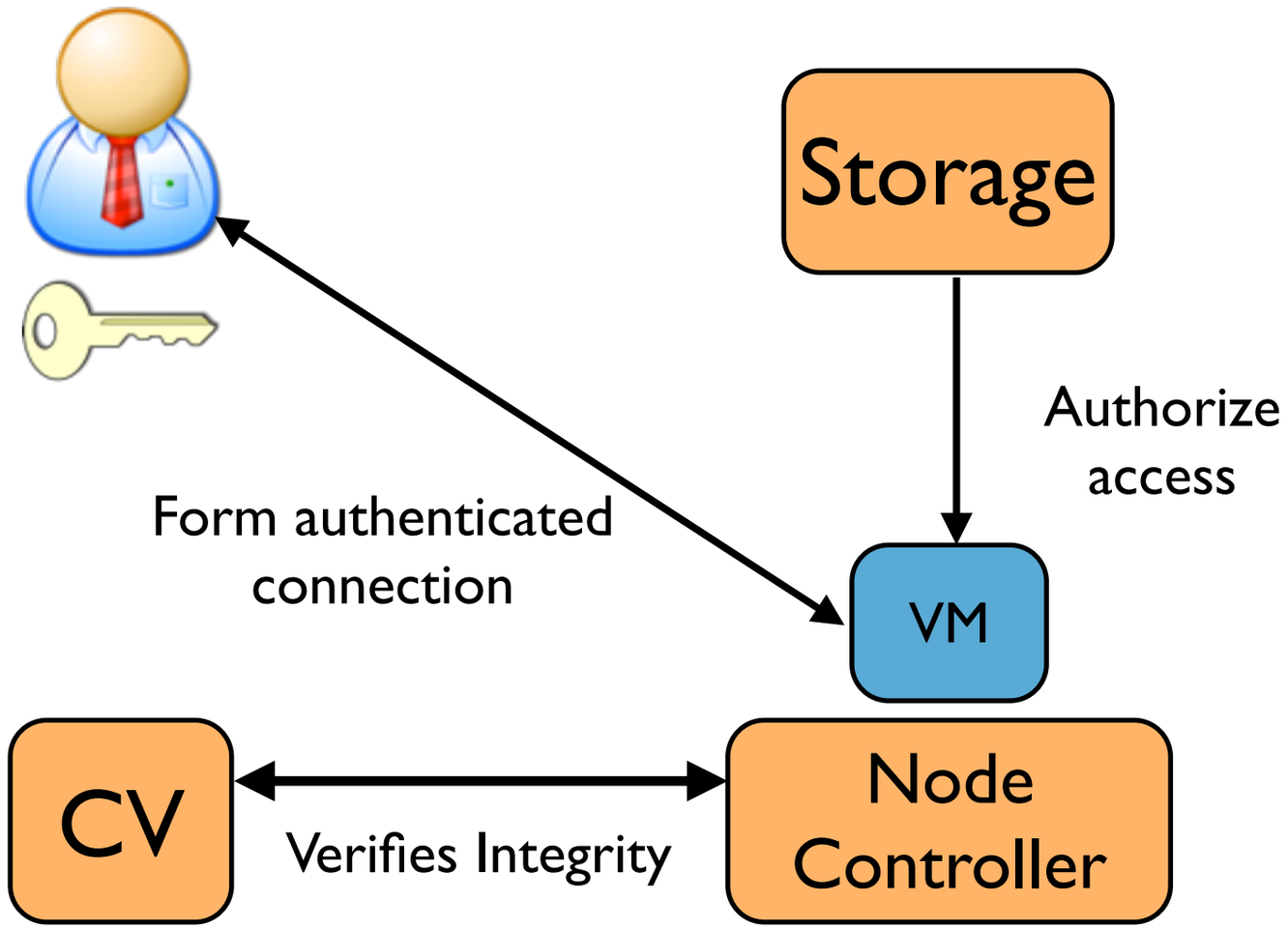
# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key



# Customers using the CV

- CV then vouches for integrity of a VM's host using a signed public key



# Transparency Challenges

- How can customers verify these proofs?
  - Custom distributions
  - Copious amount of details and systems
- How can this be done efficiently?
  - Clouds operate at Internet scale
  - Commodity trusted hardware is slow

# Integrity Criteria

- Current integrity measurement approaches are very system configuration specific
  - Difficult to assess arbitrary data and custom code
  - Resolution of measurement is often insufficient
- Require an integrity criteria that focuses on integrity properties achieved by a system
  - Establish a verifiable origin for data
  - Leverage enforcement to minimize measurements
  - Enable verifiers to compare requirements

# Performance

- Constructed a testbed using Eucalyptus
  - Configured nodes using network-based ROTI installation
- Attestations take ~1 second to produce
- CV generates asynchronous attestations
  - Using an attested time server to provide nonces
  - Handle over 7,000 requests per second

# Further Challenges

- CV Scalability
- Enforcing customer security requirements
- Key revocation and remediation

# Questions?

Joshua Schiffman (jschiffm@cse.psu.edu)

http://www.joshschiffman.org/

*SIIS Laboratory* (http://siis.cse.psu.edu)