CloudArmor: Protecting Cloud Instances by Validating Client Commands

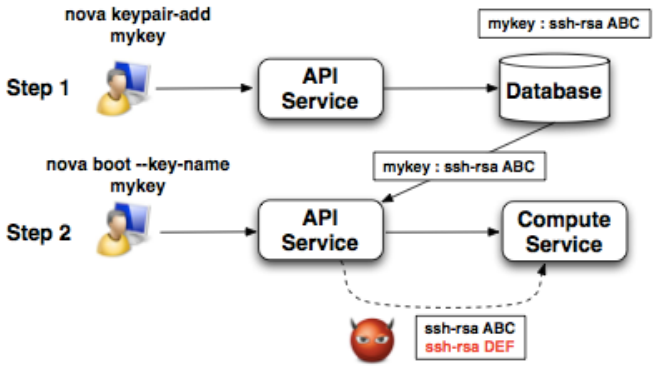
Yuqiong Sun, Giuseppe Petracca, Hayawardh Vijayakumar,
Josh Schiffman and Trent Jaeger

In order to launch an instance in cloud, cloud users must **trust the entire Cloud Infrastructure**, which comprises various **cloud services**. However, these cloud services are open to a variety of **Security Threats**, resulting in an **untrustworthy cloud infrastructure.**

• Cloud Insider: Accidental or intentional misconfiguration of computing environment by cloud Admin. (23% of data loss in data centers are due to misconfiguration, according to DataLossDB)

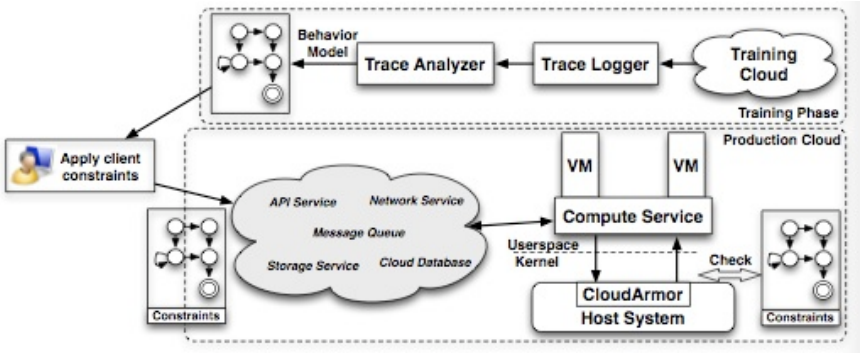
• Cloud Service Vulnerabilities: Design flaws and implementation bugs in cloud services lead to compromise. (75 reported cloud service vulnerabilities in CVE database)

Key Injection Attack



- **Goal**: Obtaining privileged access (root) to victim's instance.
- **Means**: Through compromised cloud API service, attacker modifies the SSH connection key stored in user's instance, which allows attacker to gain privileged access just like the user.
- **General Form of Attack**: To manage their instances, clients submit commands to cloud. Cloud transforms client commands into sequences of operations performed within cloud to achieve such functionality. Compromised cloud services can tamper with the transformation (e.g. order of operations, values associated with operations etc.) in order to launch an attack.
- **Root Cause**: Unregulated privileges in untrustworthy cloud.

CloudArmor: Build and Enforce a Cloud Behavior Model



- **Phase 1 (Training Phase)**: Build a cloud behavior model that describes legal cloud transformations for a specific cloud environment using dynamic analysis.
- **Phase 1.5**: Apply client specific constraints (e.g. specific keys, images etc.) to further tighten the model.
- **Phase 2 (Production Cloud)**: Enforce cloud behavior model at runtime using CloudArmor, a kernel level mechanism that validates operations performed by cloud.

CloudArmor Evaluation

- **Model Precision**: Our model has an *Average Branching Factor close to 1* and up to *90% of operation arguments* validated. This means our model is tight and affords only very little freedom to compromised cloud services to launch attacks.
- **False Alarms**: With less than *40 training runs*, our model covers a significant amount of corner cases, resulting in a detected false alarm rate close to zero. This means CloudArmor framework requires only little training efforts and can be quickly deployed for a cloud environment.
- **Performance**: CloudArmor imposes less than *2% runtime performance overhead* to client VMs.
- **Cloud TCB Reduction**: CloudArmor restricts what cloud services can do therefore eliminating the need to trust them. This results in a *reduction of cloud TCB by 92%*.

PUBLICATIONS

- Y. Sun, G. Petracca, H. Vijayakumar, T. Jaeger, J. Schiffman. **CloudArmor: Protecting Cloud Instances by Validating Client Commands**. *Technical Report*, NSRC, Pennsylvania State University, University Park, PA, US.
- J. Schiffman, Y. Sun, H. Vijayakumar, T. Jaeger. **Cloud Verifier: Verifiable Auditing Service for IaaS Clouds**. *IEEE First International Workshop on Cloud Security Auditing (CSAW' 13)*. Santa Clara, CA, USA, 2013

Sponsored by National Science Foundation grants CNS-1117692 and CNS-0931914