Poster: Cloudtracker: Cloud-wide policy enforcement with real-time VM introspection

Mirza Basim Baig* Conor Fitzsimons* Suryanarayanan Balasubramanian* Radu Sion† Don Porter†
{*Student †Faculty} *Stony Brook University, NY, USA*
{*mbaig,crfitzsimons,sbalasubrama,sion,porter*}*@cs.stonybrook.edu*

***Abstract*—Clouds have become a high-value target for cyber attacks such as those exploiting side-channels. Current defenses are not applicable cloud-wide, prove inefficient in practice and often require non-trivial changes to deployed applications.**

Here we present CloudTracker – a suite of lightweight modules that utilize fast hypervisor level VM introspection to enforce cloud-wide security policies with no changes to the hosted applications and guest OSes. CloudTracker enables the specification and enforcement of cloud-wide policies that can efficiently and transparently mitigate side channels and other attacks.

I. Introduction

Clouds come at the cost of relinquishing critical security guarantees to third party providers. In addition to traditional security issues, today's multi-tenant virtualization based clouds feature a set of specific attack surfaces, one of which derives from the inherent existence of side channels. As numerous recent results show, tenants can no longer assume strong isolation and, due to the opaque nature of hypervisor scheduling, the tenant may end up sharing a physical machine with competitors or malicious agents.

The above scenario is not hypothetical. It is now possible to gain co-residence with a target virtual machine and mount *side channel attacks*, e.g. that leverage hardware devices e.g. the L2 cache, to bypass logical isolation and extract sensitive information such as cryptographic keys [1, 2].

To prevent such attacks tenants require guarantees of physical isolation, possibly at a higher cost, especially for highly sensitive workloads. While full physical isolation is certainly an option, it is often too expensive and defeats the cost benefit of clouds.

Initial work has attempted to provide logical isolation without support from the cloud provider by using a guest-based approach [3]. While perfectly viable, this work is limited to a particular attack vector (L2 cache) and would need to be re-engineered for any additional attacks. Further, guest-based solutions require changes to guest level applications, placing the burden of security fully onto the client. This again defeats some of the main desiderata of clouds since now each individual client application will need customized security specific modifications and support.

In contrast to guest-based approaches, involving the cloud provider in the process can lead to significantly more efficient and scalable alternatives. A key insight is that cloud-based solutions have superior monitoring vantage points and significant authority to dispatch security-related decisions, while still providing the tenant with control in the decision-making process. Client-driven security decisions can now be dictated by the tenant, while being enforced by the cloud infrastructure.

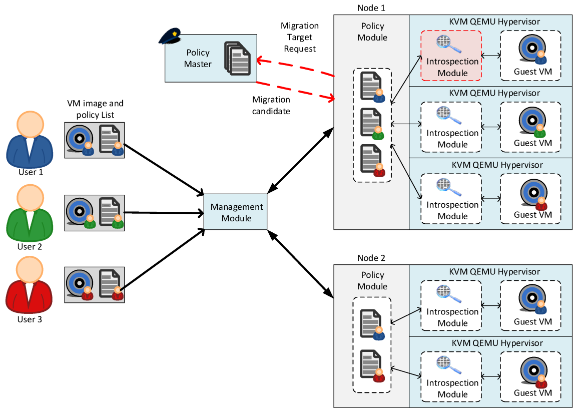

Figure 1. Tenants provide CloudTracker with VM images and security policies which are propagated automatically to relevant nodes. Policies are enforced in real time using VM introspection and callbacks.

To this end we present CloudTracker: A suite of lightweight modules that utilize fast hypervisor level virtual machine introspection to efficiently and transparently enforce cloud-wide security policies to provide a client-centric solution. CloudTracker requires no changes to the target virtual machines or applications.

References

[1] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 199–212, New York, NY, USA, 2009. ACM.

[2] E. Tromer, D. A. Osvik, and A. Shamir. Efficient cache attacks on aes, and countermeasures. *J. Cryptol.*, 23(2):37–71, Jan. 2010.

[3] Y. Zhang, A. Juels, A. Oprea, and M. Reiter. Homealone: Co-residency detection in the cloud via side-channel analysis. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 313 –328, may 2011.