Jobber: Automating Inter-Tenant Trust in The Cloud

Andy Sayler
andrew.sayler@colorado.edu
University of Colorado

Eric Keller
eric.keller@colorado.edu
University of Colorado

The rise of cloud computing has significantly shifted the way we host our digital infrastructure. Today, companies often host their sites and services in large multi-tenant data centers. Understandably, recent research has explored mechanisms to isolate tenants. In this poster, we explore the opposite end of the spectrum – enabling tenants to securely collaborate.

Multi-tenant data centers can offer many advantages over traditional private data centers such as the ability to dynamically grow and shrink the size of a deployment in response to the load on the service. An untapped benefit, however, is that the collocation of multiple services in these data centers also offers numerous possibilities for inter-tenant optimization and cooperation. For example, service providers and service consumers that happen to be tenants in the same data center should be able to benefit from the increase in network performance and decrease in network cost associated with their collocation.

Such collaboration, however, should not come at the cost of decreased security. Tenants are only willing to use shared infrastructure if they can be reasonably assured that their networked systems will be properly protected. Traditionally, this protection is provided by statically configured firewalls that allow access to specific services on specific machines while blocking access to everything else [1]. Unfortunately, even in private data centers, statically configured firewalls are prone to human error and misconfiguration. The highly dynamic nature of multi-tenant data centers only exasperates this issue. Furthermore, traditional firewalls do not allow the flexibility required to properly optimize connections between collocated, interacting tenants.

Dynamic multi-tenant data centers require a dynamic, multi-tenant aware, security mechanism. Toward this end, we present Jobber: a highly dynamic network security system designed to handle both the dynamic nature of cloud data centers and the desire for optimized inter-tenant communication inherent in multi-tenant data centers (Figure 1).

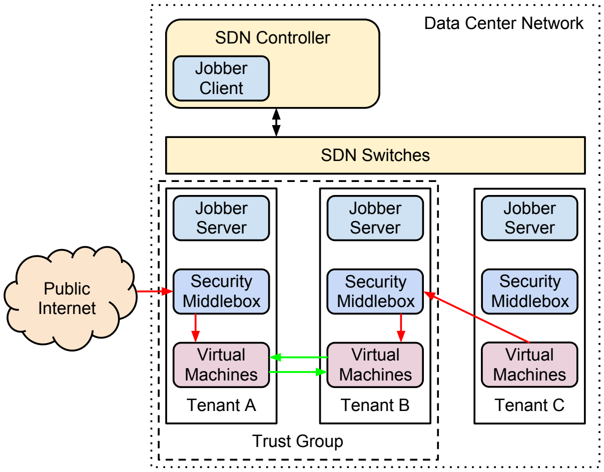

Figure 1: Jobber dynamically enables direct communication between trusted tenants (green arrows), while forcing communication from untrusted tenants and sources through additional security systems (red arrows).

Instead of relying on statically configured rules, Jobber builds and leverages a trust network between tenants to dynamically determine if a communication attempt between tenants should be allowed or denied. We employ techniques from Introduction Based Routing (IBR) [3] to realize this capability. Jobber, through theories proposed in IBR, effectively places a market value on good behaviors, encouraging well behaved tenants to form inter-tenant trust relationships while isolating misbehaving tenants.

Jobber can be deployed on both today's cloud platforms using existing APIs, as well as on future cloud platforms using SDN techniques. In the SDN case, Jobber enforces its dynamic security polices by interacting with the controller in an OpenFlow-capable network [4]. When the OpenFlow controller detects an inter-tenant flow, it queries the designated Jobber server for each relevant tenant to decide whether it should allow, drop or forward the flow through some additional infrastructure. In the poster we will expand on the design and motivation of Jobber, and present our initial proof-of-concept prototype using the Floodlight [2] OpenFlow controller framework.

References

[1] Amazon ec2 security groups. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html.

[2] Floodlight. http://floodlight.openflowhub.org/.

[3] FRAZIER, G., DUONG, Q., WELLMAN, M., AND PETERSEN, E. Incentivizing responsible networking via introduction-based routing. *Trust and Trustworthy Computing 6740* (2011).

[4] MCKEOWN, N., AND ANDERSON, T. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review 38*, 2 (2008).