SDC 19
SNIA INDIA
May 23-24, 2019
Bangalore, India
STORAGE DEVELOPER CONFERENCE

Cloud Security: Current challenges and possible solutions

Anupam Jagdish Chomal
DellEMC

Agenda

- Quick introduction to common cloud deployments
- Attacks against the bare metals
- Threats to Virtualization
- Intel MDS
- Recommendations to achieve cloud security

About ECS

- ECS is an industry-leading object storage platform
- Available as software defined, as a turnkey appliance, or as a service operated by Dell EMC
- Can be used to implement a ‘private cloud’ of object storage, or a public cloud storage, creating a smart 'hybrid cloud' approach

whoami

- Principal Software Engineer in DellEMC Elastic Cloud Storage (ECS) Security Team
- I have over 15+ years of experience in Storage, Networking, and Security domain
- My area of interest includes Network, Application and Cloud Security
- I have a Masters in Computer Science from IIT Bombay

Standard Disclaimer

- This talk represents my personal opinions and research and not those of my employer
- All data has been collected from research papers and online sites. I did not create any of the material covered in the paper
- I have taken care to mention papers / websites that I have used for this presentation in the references section. I apologize if I have missed mentioning any

Common Cloud Deployments

- Common models available in cloud deployment – hybrid and community, private, public
- Various service models provided by cloud providers – infrastructure as a service (IaaS), platforms as a service (PaaS), and Software as a service (SaaS)

Common Cloud Deployments - Contd

- Fundamentally there are two different types of clouds, public and private
- Hybrid clouds combine features of both the public and private models

Public Cloud (Co-tenancy)

- Customers share on premise and access to basic computer infrastructure like storage, servers, networks etc
- Multi-tenancy causes a host of security problems

Private Cloud

- Computer infrastructure is dedicated to a single client
- Provides enhanced level of security and privacy
- More expensive than public cloud

IaaS Vs PaaS

- With most IaaS deployment, customers share resources on a physical server
- IaaS – OS -> Runtime -> Data -> Application
- PaaS – Data -> Application
- Managing IaaS tougher than SaaS
- Some customers however require full access to dedicated physical server

Main attack vectors in a Cloud Environment

- Network
- Hypervisor
- Computing hardware
- Three types of attackers – external, internal, and cloud provider

Network based attacks

- DDoS
- CI attacks – IP/ARP spoofing & Sniffing attack
- Code Injection
  - Cross Site Scripting (XSS)
  - SQL Injection
  - Malware

What is a Bare Metal Cloud?

- It’s a public cloud service where users rent physical hardware from a cloud provider
- Public cloud are multi-tenant and the VMs hosted have to share the available resources
- Some bare metal providers – IBM's SoftLayer, RackSpace, and amazon

Denial of Service (DoS)

- DoS is one of the most command attack on the cloud
- The simplest types of attacks are Layer 3 and 4 attacks (IP and UDP/TCP in the OSI stack) eg – SYN flood
- An application layer 7 attack pretends to be a real user trying to access a web application

Attack against the Bare Metals – DDoS

- In 2016, servers of OVH were hit by a 1 Tbps DDoS attack
- The attackers used an IoT botnet compromised of compromised CCTV cameras

Attack against the Bare Metals – DDoS

- github was hit by 1.35Tbps, and a separate site by 1.7Tbps
- In general, attack against SaaS, data centers and cloud services have more than doubled since the last year

Mitigating DDoS

- Some Cloud providers use techniques like SYN cookies, rate limiting and connection limits
- Some route traffic through a load balancing infrastructure
- Others spread servers across multiple geos

Memcached reflection/amplification attack

- Memcached is used to speedup database driver websites by caching data in the RAM
- It was intended to be used on systems not exposed to the internet
- By default, memcached listens on localhost on TCP and UDP port 11211

Memcached Attack - Contd

- Memcached was open on UDP and did not require any authentication
- Spoofed IP addresses requests are send to the vulnerable UDP Memcached server which floods the target victim with internet traffic

Memcached Attack - Contd

- The Memcached server responds with a larger amount of data than the initial request
- Issue was fixed in Memcached version 1.5.6, disabling UDP by default
- Attacks as big as 260 GB per second were measured by some cloud providers

Tomorrow there will be something else!

Baseboard Management Controller BMC

- BMC is a specialized service processor that monitors the physical state of a computer using sensors & the admin access it through an independent connection.
- The BMC is part of the Intelligent Platform Management Interface (IPMI) and is usually contained in the motherboard of the device

Attack against Bare Metals – Cloudborne

- BMC can become a liability because it lets access physical admin access remotely
- Eclypsium's researchers rented out bare metal cloud server, and make alteration to its BMC's firmware
- They then went ahead and released the server only to get the exact same machine after a while

Cloudborne - Contd

- They noticed that the changes made to the BMC firmware remained
- An attacker can abuse this to access the server after it was wiped and reassigned to another customer

Threats to Hypervisor/Virtualization

- VM escape
  - Attacks the hypervisor from the VM
  - Allows the attacker to monitor or attack co-resident VMs

Threats to Virtualization - contd

- Inter VM attack
  - Attack launched from one VM to another directly
  - The Virtual Machine Monitor (VMM) is bypassed

Intel's MDS

CVE ID	CVE-2018-12126	CVE-2018-12127	CVE-2018-12130	CVE-2019-11091
Impact	Microarchitectural Store Buffer Data Sampling (MSBDS): Leaks data being stored from store buffers	Microarchitectural Load Port Data Sampling (MLPDS):Leak various internal processor buffers of data being loaded and stored	Microarchitectural Fill Buffer Data Sampling (MFBDS):Leaks already-loaded data from a processor's fill buffer	Microarchitectural Data Sampling Uncacheable Memory (MDSUM):Leaks various internal processor buffers of data being loaded and stored

Intel Microarchitectural Data Sampling (MDS)

- Allows an attacker to surreptitiously collect sensitive data in memory, such as passwords or tokens
- As part of the remediation, involves shutting off the Hyper-Threading feature in Intel chips

MDS - Contd

- Biggest impact on dense, multi-tenant public cloud providers
- Possible solutions: updating the CPU microcode, applying kernel patches, and disabling Hyper-Threading

Misconfiguration

- Private data is getting exposed not due to platform flaws but user misconfiguration
- Through 2022, at least 95% of cloud security failures will be the customer's fault – Gartner

Misconfiguration - examples

- Deep Root Analytics left a database containing personal information for 198 million US voters publicly accessible (stored on a S3 server)

Mitigation

- Decide what needs to be sent to the cloud
- Decide on security levels on your data eg.MAC
- Hire the right resources to plan, configure, and maintain your cloud presence
- Time for a cloud STIG? Atleast have a checklist read for your cloud security configuration
- Audit and monitor

Threat Modelling (OWASP)

- Identify trust boundaries to and within the system
- list actors who interact within and outside of the trust boundaries
- Identify Information flows within and to and from the trust boundaries

Threat Modelling – Contd

- Find information persistence within and out of trust boundaries
- Find potential threats and vulnerabilities to these trust boundaries

Threat Modelling – Contd

- Find threat agents that can exploit these vulnerabilities
- Evaluate the impact of exploitation of a vulnerability by a threat agent

Steps for Threat Modelling

- Create a threat model
- Analyze the findings and find ways to fix it
  - Large number of cloud deployments have security misconfiguration
- Come up with a plan to fix the issues observed
- Monitor your deployment
- Encrypt moving data

References

- https://www.sciencedirect.com/science/article/pii/S0045790616300544
- https://securityaffairs.co/wordpress/51640/cyber-crime/tbps-ddos-attack.html

References - Contd

- https://www.owasp.org/index.php/Threat_Modeling_Cheat_Sheet
- https://www.threatstack.com/blog/how-to-create-a-threat-model-for-cloud-infrastructure-security
- https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

References - Contd

- https://www.wired.com/story/voter-records-exposed-database/