Virtual Machine Introspection

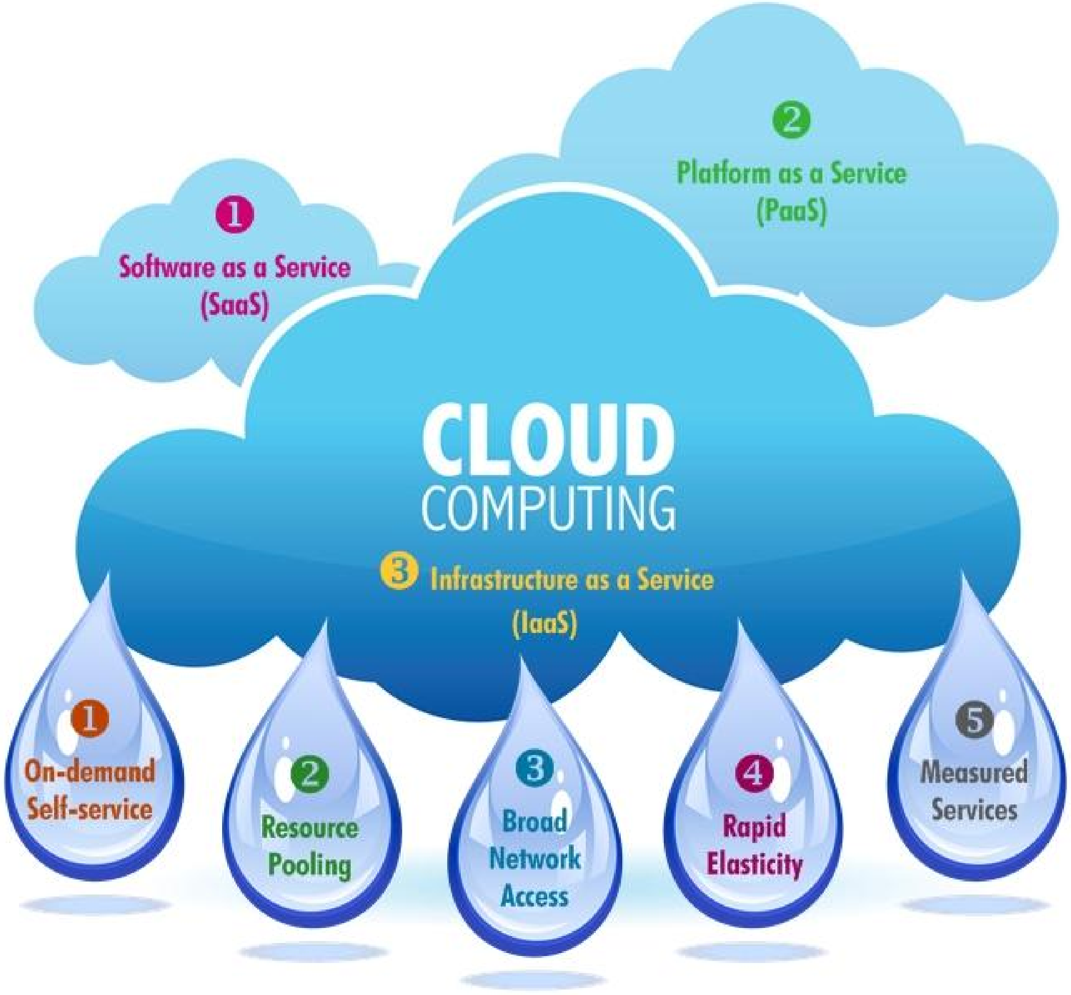
By Neel Shah

Background

- Static
- $$$$$$
- Inaccessible
- Hard to manage
- Disaster prone
- Annoying

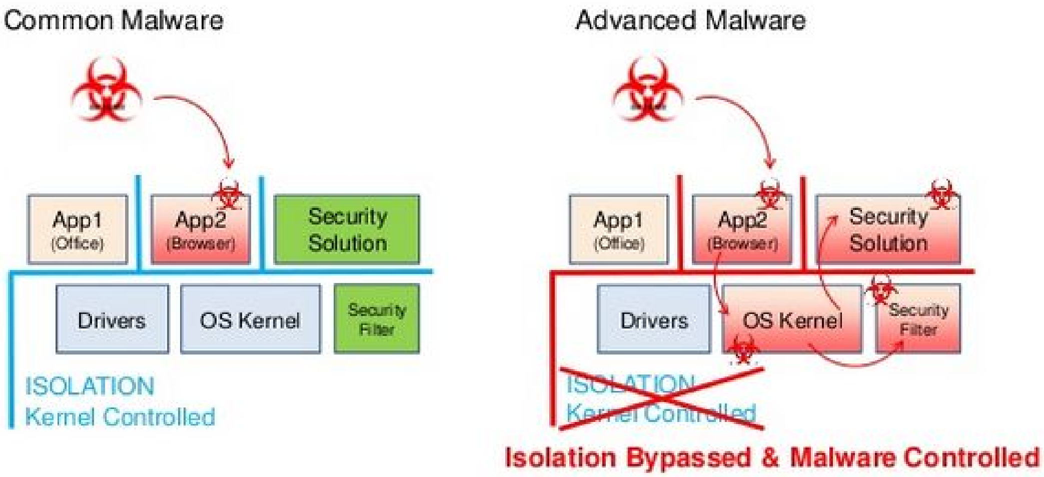
professionallyevil
22 DEFCON
HACK NAKED
HACKER
My other computer is your computer
HACK FTW
GET

Those were the dark ages.


1
Software as a Service
(SaaS)
2
Platform as a Service
(PaaS)
CLOUD
COMPUTING
3 Infrastructure as a Service
(IaaS)
1
On-demand
Self-service
2
Resource
Pooling
3
Broad
Network
Access
4
Rapid
Elasticity
5
Measured
Services

Modern Malware and Anti-Malware

- Anti-malware on same domain as malware
- Modern malware evades anti-malware software
- Modern Malware disables anti-malware software



Security and Reliability

- What happens if your service breaks?
  - As a service provider, uptime or quality of service is vital
- Can you prevent things from breaking before they do?
- Anti-malware isn’t good enough, what do we do?
  - Modern malware can evade anti-malware or even disable it completely

Virtual Machine Introspection

Virtual Machine Introspection

- Laser beam capable satellite
- Expose Linux Kernel data structures
- Monitor VM in real-time
- VM is not aware of monitoring

Virtual Machine Introspection

- Existing hardware virtualization technologies
- Mark interesting guest operating system pages
- Use hooks to monitor Kernel events:
    - Kernel module changes
    - New user processes
    - Stack/heap allocation
    - Memory is being paged
- Event based introspection to assure no malicious activity

Virtual Machine Introspection

- Protect against malicious code execution/activity
- Inject remediation tools into guest

libbdvmi

- Bitdefender’s virtual machine introspection library
- On-the-fly OS detection and decision making
- Event based introspection
- Allows mapping guest pages into userspace

My Senior Design Project

- Leverage libbdvmi’s features:
  - Event-based introspection
  - Page mapping into userspace
- Mark “special” pages to be monitored
- If there is a fault, copy remote data into mapping

References

http://security.stackexchange.com/questions/34261/what-is-virtual-machine-introspection

https://www.linux.com/news/virtual-machine-introspection-security-innovation-new-commercial-applications

https://blog.xenproject.org/author/rc/