

# Data Centre Virtualisation

*by* Nicholas Alexander

---

|                |                                                                           |                 |       |
|----------------|---------------------------------------------------------------------------|-----------------|-------|
| FILE           | 2104_NICHOLAS_ALEXANDER_DATA_CENTRE_VIRTUALISATION_113613_1632916423.DOCX |                 |       |
| TIME SUBMITTED | 22-MAY-2018 09:29PM (UTC+0100)                                            | WORD COUNT      | 2917  |
| SUBMISSION ID  | 89753851                                                                  | CHARACTER COUNT | 15435 |

# **Network Operating Systems and Security**

**Nick Alexander (Author)**

Networking, School of Applied Computing

UWTSD

Swansea, Wales

nalexander.147734@student.uwtsd.ac.uk

***Abstract* - The purpose of this paper is to explore the current state of affairs regarding cloud computing, the advantages and disadvantages of the different systems. Also, to investigate data loss, the effect of natural disasters on data, backups and network security.**

## **INTRODUCTION**

Traditionally, running an application required hardware and software to be purchased, installed, maintained, repaired, updated etc on site. One good aspect of this is that the business has complete control over the infrastructure and the data.

Nowadays cloud computing has shown that businesses don't need to own a resource to use it productively or securely, a plus point of this is cloud computing removes some of the burden of I.T. infrastructure, management and support from the enterprise. It reduces the time and man power usually required by I.T. staff to buy, configure, support and manage the hardware as well as removing the upfront capital expense needed to setup a large network backbone.

INFRASTRUCTURE AS A SERVICE (IaaS) is an option in which providers offer bare computing resources such as servers, storage, networking and virtualisation as a service. The provider is then responsible for maintaining these as well as the hypervisor layer and security features such as access management.

The users can access these resources through the internet and can use them to install and run applications, but the users have to do a lot of work in terms of installing, maintaining and managing the software layers, (even though they have a lot of flexibility)[1]. Typically, customers pay for what they use on a 'pay as you go' scheme, but this can work out quite hard to budget for.

PLATFORM AS A SERVICE (PaaS) takes the IaaS model a step further by hosting operating systems, middleware and other frameworks on their physical infrastructure. This means that platform providers have more responsibility - not only do they manage the underlying hardware (like an infrastructure provider does) but also offers software such as applications and operating systems[2]. This means that users need to spend less time installing, configuring and updating software and operating systems (because this is done by the provider). Instead they can spend more time on using, deploying and managing their own applications, without having to worry about the underlying stack[3]. More expensive than IaaS, but no need to buy software licenses or pay I.T. staff to install and support the software.

SOFTWARE AS A SERVICE (SaaS). In this model the entire hardware and software stack is hosted by the cloud service provider. This means that nearly all management responsibility is with the provider – they need to purchase, install, configure, upgrade, secure and manage every element of the stack. So users only have to log on and use the application, but they do have to ensure the integrity and security of the data used by the application, and also that only authorised users can access the data[4]. The responsibility of the user is diminished because the hardware and software is maintained by the provider, but this also means that the user has less control (for example over software versions).

A quick comparison of the different systems discussed so far can be seen in *Figure 1*:

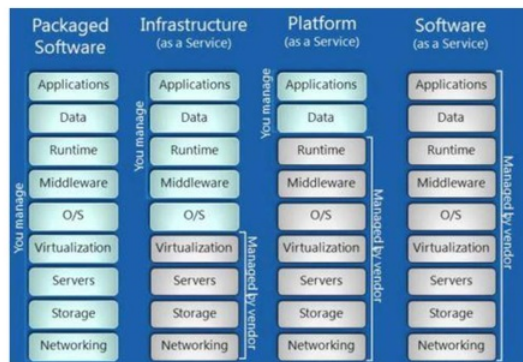


Figure 1 – A comparison of who manages which services, image courtesy of [4].

**BRING YOUR OWN DEVICE (BYOD).** With the advent of high speed broadband, the idea of ‘working from home’ or accessing applications from anywhere in the world really became popular. This resulted in a trend known as BYOD, or Bring Your Own Device, meaning that the same software and data could be accessed from the user’s own device either in the office or remotely[5]. While great in theory, a lot of people complained of the complicated Virtual Private Network (VPN) requirement, and the reduction in speed the VPN caused. Another concern with BYOD is company data being stored on someone’s home computer; the questionable age and reliability of the device; whether it has adequate security software; what would happen to the data if it was lost/stolen/broken. Also, how all of these devices could be supported by the I.T. Department.

**DESKTOP AS A SERVICE (DaaS)** addresses a lot of the BYOD concerns by allowing users to use any computer / tablet / mobile etc to access a full desktop experience. This is due to developments in ‘Client Side Virtualization’ which is a new way to host and deliver multiple applications. The benefits of this are that data isn’t stored on the user’s machine, it is only used to access the hardware and software running on the remote computer[6]. Amazon have relatively recently entered the cloud computing sector and have rapidly taken a large market share from Microsoft and Google with their AWS offering– see Figure 2:

### Worldwide cloud infrastructure services market share

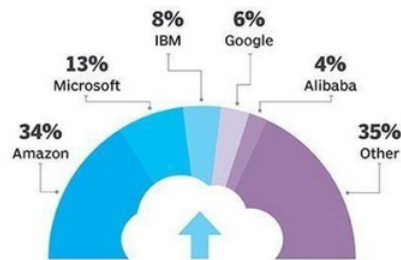


Figure 2 – Amazon’s market share of Cloud Services, image courtesy of [7].

There are advantages and disadvantages to all of the approaches listed above: One downside is that a reliable internet connection is essential – if that was to slow-down or disconnect, the entire workforce would be unable to access any of the hardware or software which they are renting. In recent years, broadband connections have become faster and more stable so this is less of an issue than it was a few years ago. This risk is counteracted by the fact that on-site hardware could also go down – in which case all of the workers would be sat waiting for the onsite I.T. staff to fix the fault. Data is stored offsite so any fire/flood/virus attack etc that could cause the local hardware to lose data is now the worry of the service provider. This should be a consideration when choosing whether to use SaaS or DaaS and also when choosing which company to use: do they have data backups remotely in case of a natural disaster for example. If their computers were to fall victim to an earthquake, volcano, bombing in a war or act of terrorism – all scenarios should be considered. Customers who are paying every month expect continuous, uninterrupted service and trust them to not lose their data even in extreme circumstances. This requires the company to setup their systems in a configuration such as a failover cluster, so that if a disaster was to strike, all services would continue to run, without any noticeable change from the user’s perspective[8].

Whoever has the responsibility of the hardware and software, (either a provider or the local / onsite setup); also has the responsibility of the security – not just against natural disasters and failures, but also against attacks. A brief overview of some common network attacks are listed below:

**DISTRIBUTED DENIAL OF SERVICE (DDoS)** attacks occurs when hackers flood a network or website so that legitimate users are denied access because it is overwhelmed[9]. The attacks are co-ordinated so that they come from multiple sources, this is achieved by previously taking control of many devices (known as zombies), these can flood the network all at once, or pulse to slow a service down which is less likely to be detected [10].

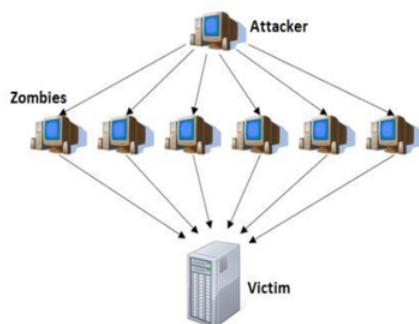


Figure 3 – DDoS attack, image courtesy of [11].

Hackers often use dedicated servers which they connect to using a Virtual Private Network (VPN), providing anonymity[12]. These hacking services have been sold on the black market, sometimes for as little as \$150 for a week-long DDoS attack[12]. It is estimated that over a million ‘Internet of Things’ (IoT) devices could have been controlled for use in coordinated DDoS attacks using malware such as ‘bashlite’, and ‘torlus’[13].

Preventing DDoS attacks is very difficult because as many as 10,000 zombie machines could be requesting information at the same time; firewalls and antivirus are essential – as they can be set to recognise unusual inbound traffic. There are companies now offering a ‘DDoS mitigation service’ for a monthly fee[14]. Other techniques to avoid attacks include ‘Intrusion Prevention Systems’ (IPS) which respond automatically, and ‘Intrusion Detection Systems’ (IDS) which require human intervention[15]. It has even been suggested that ‘game theory’ could be used to combat these attacks[9].

**ROGUE DHCP SERVERS.** In a large network, there will usually be a dedicated Dynamic Host Configuration Protocol (DHCP) server which has the responsibility of providing host computers with their IP address, subnet mask and other information. If this is compromised (often by a rogue DHCP server giving out incorrect information to the hosts) – this can lead to a loss of

connection to network services, slow speed and compromised information if linked with a ‘man in the middle attack’ (see below). To avoid this, Microsoft have required DHCP servers to need authenticating by active directory before they are accepted by hosts[16]. Microsoft created command-line software to combat rogues, called Dhcploc, but is now no longer updated[17]; graphical software has been created based on Microsoft’s version called RogueDetect[18] which can be used to test for any rogue DHCP servers present on the network.

Often with Rogue DHCP server attacks (and DDoS attacks) the hackers aim is to block network access to the DNS server. As this is required for email, internet Voip etc, if the DNS server goes down, the network can quickly be affected[19].

An important step to avoiding rogue DHCP server attacks is to ensure the server room is physically locked, all unused switch ports are disabled, and some form of MAC address security is enabled so that only the intended device can connect (such as ‘MAC sticky’).

**ADDRESS RESOLUTION PROTOCOL (ARP)** is a network protocol that builds a table of IP addresses and their associated MAC addresses (called an ARP cache). Whenever a device with an unknown MAC address is to be contacted, a message is sent to every host in the network, requesting the owner to reply. Everyone else who receives the message in error drops the packet, only the owner replies. This allows the missing information to be added to the table[20].

**ARP SPOOFING** (also called ARP Cache Poisoning), is when hackers take advantage of the ARP procedure because it is unauthenticated and hackers can ‘sniff’, or listen to the traffic between two hosts, (without them ever being aware)[11], then generate non-genuine ARP replies to either manipulate data, create a DDoS attack or a ‘Man In the Middle’ attack[11] (see below). Not all hacks are carried out by highly skilled people with years of experience, there are tools available which make packet sniffing, password capturing etc relatively easy, such as Ettercap[21]. This has somewhat been superseded by newer programs such as Bettercap[22] which is more suited to https sites. Several penetration testing programs can be found together in Kali Linux[23].

#### EVIL TWIN

In this type of attack, a hacker listens to a host which maybe requesting to connect to an Access

Point (AP) for example. The information that is passed back and forth between the host and the AP is recorded and used by the hacker to setup a rogue AP, then to de-authenticate the host from the original AP and reconnect to the rogue AP instead. The hacker can now intercept all of the traffic that was intended for the legitimate AP by impersonating it.

**MAN IN THE MIDDLE** - Here the idea of an evil twin is taken a step further, once the host has been disconnected, it reconnects to the rogue AP (unknowingly) and this then authenticates the host with the original AP, so all information first goes to the hacker before being passed on to the router. This means that the hacker gets to see all of the information (passwords, credit card details etc) that has been typed by the host before it gets to the router.

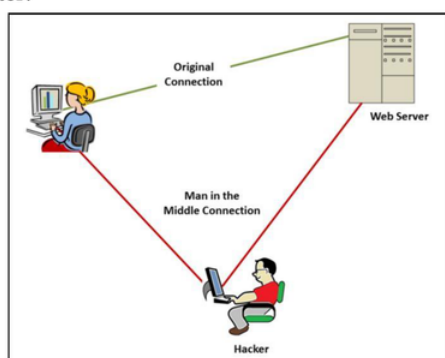


Figure 4 – man in the middle attack image courtesy of [24]

Man in the Middle (MIM) attacks can be used to steal valuable data or security details such as IDs and passwords.

One feature designed to deal with these problems is an 'SSL certificate'. If the certificate has been signed by a 3rd party such as 'Certificate Authority' (CA), this adds a layer of security which is designed to eliminate attacks such as 'man in the middle'[24] by encrypting the sent data and only the holder of the public and private key can decipher the information.

**PACKET SNIFFING** - When sending a message to a computer on a network, (particularly ARP requests because they are sent to all nodes), if the computer's address does not match the destination address in the message, the packet is dropped. But if a hacker set his network interface card to 'Promiscuous mode'[16], all packets can be accepted (regardless of the destination

address)[12]. This can be used on a wireless network or a wired one to capture packets and intercept all information transmitted by the host.

A packet sniffer is a computer program that can intercept the traffic in a network, two of the most common programs are – 'tcpdump' and 'wireshark' which analyse data as it is sent to its destination [16]. They are freely available online for network owners to be able to test their systems, but can also be very powerful tools in the wrong hands.

## CONCLUSION

If a company is deciding whether to rent computing services or to invest in purchasing computers to use locally, there are many factors to consider. If the network is onsite – disaster recovery, hacker attacks and backup scenarios must be thoroughly covered, whereas by renting the system services these considerations are the responsibility of the provider. But it needs to be checked that the company has these concerns covered, and if a disaster was to happen – whether the services would seamlessly transfer to the backup system without any disruption to the user. Part of the rental cost would be the maintenance and updating of the system behind the scenes, but this would also be an ongoing expense if hardware was installed locally. The rental expense is compared to the upfront cost of purchasing hardware, how long that hardware will likely last before it breaks down or becomes obsolete. It is highly likely that even for stand-alone home users that as internet speeds become faster, online software will take more and more of the demand away from the local machine – meaning that the storage and processing can be done in the cloud. One reason that companies would favour this setup (for homes and large enterprises) is the prevention of piracy because every online subscriber would have a genuine software license. A monthly fee is preferable for software companies - rather than sell once and wait for another purchase years later. One downside to this if it was to become more mainstream, would be the demand and extra bandwidth needed by the broadband providers.

## REFERENCES

- [1] E. Bauer *et al.*, "Towards a Security Baseline for IaaS-Cloud Back- Ends in Industry 4 . 0," pp. 427–432, 2017.
- [2] P. Golding, "Cloud Computing, Saas and PaaS," in *Connected Services: A Guide to the Internet Technologies Shaping the Future of Mobile Services and Operators*, Wiley Telecom, 2011, p. 352.
- [3] J. M. Pintos, C. N. Castillo, and F. López-Pires, "Evaluation and comparison framework for platform as a service providers," in *2016 XLII Latin American Computing Conference (CLEI)*, 2016, pp. 1–11.
- [4] A. S. Rumale and D. N. Chaudhari, "Cloud computing: Software as a service," *2017 Second Int. Conf. Electr. Comput. Commun. Technol.*, pp. 1–6, 2017.
- [5] K. Mishima, T. Sakurada, and Y. Hagiwara, "Easy Accessible Virtual Computer Room for BYOD Environment," pp. 15–16, 2018.
- [6] P. Sarkar, "Introduction to DaaS," in *Data as a Service: A Framework for Providing Reusable Enterprise Data Services*, Wiley-IEEE Press, 2015, p. 368.
- [7] margaret rouse, "What is RFID tagging? - Definition from WhatIs.com," 2017. [Online]. Available: <https://internetofthingsagenda.techtarget.com/definition/RFID-tagging>. [Accessed: 20-May-2018].
- [8] W. N. A. Qasmi, T. Siddiqui, M. K. Shehzad, A. Iqbal, and M. S. Ilyas, "A comparative study of failover schemes for IaaS recovery," in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 25–30.
- [9] E. F. I. C. Amandi EC, Eheduru GE, "Anti-DDoS Firewall; A zero-sum mitigation game model for distributed denial of service attack using linear programming," pp. 27–36, 2017.
- [10] A. Schwabach, *Internet and the law*. 2005.
- [11] R. R. Saini and H. Gupta, "A security framework against ARP spoofing," *2015 4th Int. Conf. Reliab. Infocom Technol. Optim. Trends Futur. Dir. ICRITO 2015*, 2015.
- [12] M. Goncharov, "Russian Underground 101," *Trend Micro Inc. Res.*, pp. 1–29, 2012.
- [13] C. Cimpanu, "There's a 120,000-Strong IoT DDoS Botnet Lurking Around," 2016. [Online]. Available: <https://news.softpedia.com/news/there-s-a-120-000-strong-iot-ddos-botnet-lurking-around-507773.shtml>.
- [14] D. Mitigation, "arbornetworks," 2018. [Online]. Available: <http://www.arbornetworks.com/ddos-protection-products>.
- [15] D. C. Grant, "Distributed detection and response for the mitigation of distributed denial of service attacks," *2018 Int. Conf. Inf. Netw.*, pp. 495–497, 2018.
- [16] J. Kadlec, D. Jaros, and R. Kuchta, "Implementation of an advanced authentication method within microsoft active directory network services," *Proc. - 6th Int. Conf. Wirel. Mob. Commun. ICWMC 2010*, pp. 453–456, 2010.
- [17] Microsoft, "Dhcploc Overview." [Online]. Available: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759117\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759117(v=ws.10)).
- [18] V. Rubin, "RogueDetect." [Online]. Available: <https://sourceforge.net/projects/roguedetect/>.
- [19] I. Georgiev and K. Nikolova, "An Approach of DNS Protection Against DDoS Attacks," pp. 140–143, 2017.
- [20] B. Scott *et al.*, "An interactive visualization tool for teaching ARP spoofing attack," *Proc. - Front. Educ. Conf. FIE*, vol. 2017–Octob, pp. 1–5, 2017.
- [21] M. V. Alberto Ormaghi, "Ettercap," 2018. [Online]. Available: <https://ettercap.github.io/ettercap/>.
- [22] "Bettercap," 2018. [Online]. Available: <https://www.bettercap.org/>.
- [23] K. Linux, "Our Most Advanced Penetration Testing Distribution, Ever.," 2018. [Online]. Available: <https://www.kali.org/>.
- [24] K. Judge, "The Man in the Middle: He is Coming After You!," 2015. [Online]. Available: <https://antivirus.comodo.com/blog/computer-safety/man-middle-coming/>.

# Data Centre Virtualisation

## GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

**Instructor**

**78**/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

GRADING FORM: SMU GENERIC\_GJ

**NICHOLAS ALEXANDER**

**78**

### RESEARCH-INFORMED LITERATURE



An excellent number of sources of mostly good academic credibility.

**23**

### KNOWLEDGE AND UNDERSTANDING



Very good evidence of knowledge and understanding - your discussion of different kinds of attacks, in particular, is especially good.

**25**

## ANALYSIS



Very good conclusions drawn, though your synthesis of material could be slightly better. Try not to rely too heavily on the "say one thing, cite the source you read about it from" idea - instead, try to read 3 or 4 sources on the same thing, write a combined narrative based on everything you've read, then cite all of them together.

**17**

## PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

## SKILLS FOR PROFESSIONAL PRAC.



A very well-written, professionally laid out report. Excellent work, Nick!

**13**