

Cloud Computing and Cybersecurity

by Paul Lawrence

FILE	3346_PAUL_LAWRENCE_CLOUD_COMPUTING_AND_CYBERSECURITY_1 13613_1043028669.DOCX		
TIME SUBMITTED	23-MAY-2018 11:46PM (UTC+0100)	WORD COUNT	5349
SUBMISSION ID	89818591	CHARACTER COUNT	32620

Cloud Services and Cybersecurity

Paul M Lawrence (P152216) Undergraduate Student, Mcomp Computer Networks
University of Wales Trinity St David, Swansea, Mount Pleasant Campus
plawrence.152216@student.uwtsd.ac.uk

Abstract – The focus of this paper is to research and analyse modern centralised computing models and the cybersecurity challenges that they present in the technological age we live in today.

Keywords-component; *Datacentere, Security, Redundancy, Failover, Exploit, Vulnerabilty, Cloud Computing, IaaS, PaaS, SaaS, DaaS*

I. AN INTRODUCTION TO CENTRALISED COMPUTING

Centralised computing has come around full circle in the last decade [1], from the advent of locally centralised mainframe [2] [3] computing in 1944, developed by IBM called the Automatic Sequence Controlled Calculator (ASCC) [4] shown in *figure 1*. The philosophy behind mainframe computing was essentially to build a very large computer that has terminals (clients) directly connected to it, that each shared the memory and computational resources housed within the mainframe to reduce the costs for businesses utilising this very expensive technology of the day.[5]



Figure 1:IBM: Automatic Sequence Controlled Calculator (ASCC)
[4]

ASCC is a very primitive relative of today's computationally powerful servers [6] that provide the modern centralised computing models of today, that deliver services remotely to end clients from large datacentres around the globe via the Internet shown in *figure 2*.



Figure 2: Google Datacentre located in Iowa, USA [7]

This modern remotely centralised model is most commonly referred to as 'cloud' computing [8].

II. CLOUD COMPUTING: OVERVIEW

The ethos behind cloud computing is to aggregate expensive server hardware and the computational power that they possess within one location i.e. datacentres that can then be delivered remotely to end clients. Portions of these server's hardware resources i.e. Central Processing Unit (CPU) and memory (non-volatile and volatile) housed within the datacentres are then remotely leased to end clients using various virtualisation platforms i.e. Virtual Machines (VM's) [9], containerisation [10] etc to perform various computational tasks and/or to store large amounts of data for a fee. [11]

This modern cloud computing model is only practical within the Internet age we live in today because of the infrastructure that has been put in place over the last 20 years to deliver high speed data throughput to residential homes and businesses around the world, making centralised computing a viable alternative to expensive modern in-house services once again. [12]

III. CLOUD COMPUTING: 'X AS A SERVICE'

X as a Service (XaaS) [13] is a generic marketing term used within the IT industry to describe a network infrastructure services model that can be delivered remotely to end clients across a public Wide Area Network (WAN) i.e. the Internet. Companies whom provide these services are referred to as Cloud Service Providers (CSP). The CSP leaders in this industry are; Amazon Web Services (AWS) [14], Microsoft Azure [15] and Google Compute Engine (GCE) [16].

There are many versions of 'X as a Service' currently available within today's market that can be broken down into three main cloud service models that are utilised by Small-to-Medium Businesses (SMB) and Corporations for services tailored for their business needs.

The three main cloud service models can be found in *figure 3*.

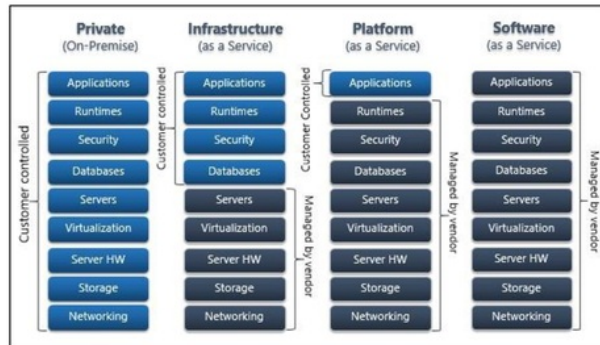


Figure 3: XaaS Comparison Diagram [17]

a. Infrastructure as a Service (IaaS)

IaaS provides a client with a leased portion of a datacentre's underlying network infrastructure i.e. Servers, Storage Area Network (SAN) etc that is managed by the CSP. This model allows the client to implement, configure and manage their own; virtual machines, business applications, web applications, storage etc to run a range of customised services for their business through a secure Hyper Text Transport Protocol Secure (HTTPS) web browser interface that uses Secure Socket Layer (SSL) and Transport Layer Security (TLS) for encrypted communications, that is delivered to the clients end devices via the Internet. [18], [19]

Advantages:

- An economically viable solution for non-IT companies who can't afford an expensive networking infrastructure and large IT team.
- Clients have full control of there Virtual Machines and can either use pre-configured versions or configure their own instances and run whatever software services they need.
- IaaS is considered the most secure cloud model currently available because of the granular control over data, VM's etc with an option for a virtual firewall instance to be installed within each VM.

Disadvantages:

- Advanced network administration knowledge is needed to maintain and configure these services, also the clients are responsible for backing up all of there data.

- Relies heavily on a stable Internet connection with high throughput, without WAN connectivity access to services is not possible.
- Can be very expensive if services aren't monitored correctly and are being paid for when they are not being used as the CSP subscription uses an itemised billing system that can confuse most non-IT companies i.e. per CPU cycles used, RAM used, Storage used, services used, VM instances etc.

b. Platform as a Service (PaaS)

PaaS provides clients with the underlying datacentre network infrastructure similar to IaaS. In this model everything including the database, middleware etc is managed by the CSP, apart from the applications and the user data generated by the applications, allowing web application developers to use the infrastructure as a test bed for web application development/management and then to publish their applications for end users to utilise. Vendor applications can also be run in this model by the client. Configuration and WAN delivery of this service is identical to IaaS. [20], [21]

Advantages:

- Minimum networking knowledge required and no large overheads of infrastructure costs.
- Granular control over applications/user data for user analytics and performance metrics of software.
- System integration support between cross platforms for software applications.

Disadvantages:

- No control of Virtual Machines and the underlying infrastructure processing the data that could potentially pose a security risk.
- Patching and updating of software applications is down to the client that will cost money and time.
- This model uses a shared platform with other customers that could pose a security risk.

c. Software as a Service (SaaS)

SaaS provides clients with applications such as Outlook E-Mail, Office 360, Dropbox etc to clients/businesses that can be accessed via a web browser eliminating the need for installation, patches, configuration, servers etc. This model is a plug and play model as the CSP manages the underlying network infrastructure, patches, servers, applications and middleware. [22], [23]

Advantages:

- Minimum networking knowledge required and no large overheads of infrastructure costs.
- Best value for money out of all the CSP models because only the software that is being used is paid for by the client and not the underlying network infrastructure.
- The underlying network infrastructure and software are all provided by and managed by the CSP for rapid deployment of applications.

Disadvantages:

- The client has no control of the data being processed for business analytics etc
- Only a limited amount of applications available for this service.
- The CSP has full control and transparency of client data that could become a major security and data protection issue.

d. Desktop as a Service (DaaS)

DaaS offers clients a secure virtual desktop solution for their businesses and staff that they can access via a web browser anywhere in the world that contains individual staff members user data that is all stored at the CSP's SAN. The underlying network infrastructure is managed and maintained by the CSP and the service subscription is per unit of virtual desktop instances. [24], [25]

Advantages:

- No networking knowledge is needed, local server or SAN for user roaming data. OS licenses and Patches are also managed by the CSP.
- Offsite workers can access their business data via the Internet.
- Cost effective and configuration/administrative free alternative to Virtual Desktop Infrastructure (VDI). [26]

Disadvantages:

- Business applications such as Outlook E-Mail, Office 365 must be bought separately, installed and managed by in house IT staff. Only default Windows OS applications are provided with the service.
- Less administrative control and security over business data i.e. intellectual property etc.

- All data is stored at the CSP so if there was an outage staff would not be able to access the companies data.

IV. CLOUD INFRASTRUCTURE SECURITY

Within the information age we live in today, data is referred to as the new 'oil' because it is a very lucrative and powerful resource for businesses and governments around the world. Therefore, datacentres that hold this vast amount of data i.e. personal, intellectual, financial etc are increasingly under attack by malicious actors who aim to steal/manipulate the data and/or disrupt the networks where it is contained for personal and/or political gain. Within cybersecurity no network can be 100% secure so network engineers have to create solutions to mitigate a high percentage of attacks and put in place measures to minimise damage to a network when a successful attack occurs. [27] [28] [29] [30]

There are many ways to attack a network and the data that it contains. Hackers and/or security professionals often engineer ingenious methods to exploit a networks vulnerability using various tools i.e. Metasploit framework [31], Kali Linux penetration testing Operating System (OS) [32] etc. Some of the most common attacks that are used against networks and the defences used against them are:

a. Remote Exploitation

Remote exploitation of a computer system or network is an attack launched by an attacker via the Internet to a server, end devices and/or internetworking devices to exploit known web facing service vulnerabilities utilised by servers and end devices such as; Hyper Text Transport Protocol (HTTP), File Transfer Protocol (FTP), Secure Shell (SSH), Telnet, Server Message Block (SMB), Simple Mail Transfer Protocol (SMTP), Secure Socket Layer (SSL) etc using custom exploit scripts written in scripting languages such as; 'Ruby' and 'Python' to exploit these known vulnerabilities within a web facing service to gain access to the network and/or device. [33], [34] [35]

The most vulnerable OS's to this style of attack using a combination of two exploits called 'Eternal blue and Double Pulsar' [36] are; Windows 7 client OS and below, also Windows Server 2012 and below. This attack exploits a vulnerability within the Server Message Block architecture of these OS's that is no longer patched by Microsoft. [37]

To minimise remote exploitation attacks, a hardware firewall [38] should be designed into the network topology to perform a deep packet inspection of inbound packets entering the network asymmetrically, along with digital network certificates [39] authenticated by a trusted server. Furthermore, an Intrusion Prevention System (IPS) [40] or honeypot [41] could be designed into the network for added security.

It is also crucial that OS vendor patches [42] are kept up to date to further secure all the end devices and servers housed within the network that utilise these Internet facing services. All OS's

that are no longer supported by the vendor should also be upgraded.

b. Password Cracking

Password cracking is a method used by hackers to infiltrate a password protected network domain, software application, OS login etc to gain access to the private information the password is securing using various cryptographic tools and techniques [43] such as 'John the Ripper' [44], 'Cain and Able' [45], and 'Brutus' [46]. The most common password attacks are:

Dictionary attack: This attack utilises a large text file that contains commonly used passwords by end users that are autonomously entered into the password field by the cracking tool until it finds the correct one. [47]

Brute Force: A brute force password attack is the most rudimentary of the two methods, it is not designed as a targeted approach but to instead try every possible combination of passwords until it finds the correct one. This method can take from a few minutes to a millennium to crack a password depending on the amount of characters that a required by the password field and the computational power available to the cracking tool. [48]

To mitigate password cracking attacks against networks and the devices that are housed within them, a network security policy [49] should be created and enforced with a section that highlights a minimum password complexity such as an alphanumeric system with no less than 8 characters that should be changed every 30 days to prevent a brute force attack. Common words, names, countries etc should also be refrained from being used to minimise the threat posed from a dictionary attack. Passwords that are authenticated by a server should also have a maximum try timeout of three attempts to further prevent passwords being cracked remotely.

Password lists stored within a database for authentication within a network should never be stored in plain text but rather hashed using Secure Hashing Algorithm (SHA) – 256 bit with salting [50], [51] in the event the database is infiltrated and the password list is stolen, making the list illegible to the attacker.

c. Malware

Malicious software (Malware) [52] is a term used to describe computer code designed to corrupt, disable and/or infiltrate computer systems/networks that is created by malicious actors.

There are three main categories of malware:

Virus: Computer code that copies itself at the source corrupting and/or destroying data. [53]

Trojan Horse: A trojan is a file that is bound with a trusted file such as an image that looks seemingly innocent and trustworthy but creates a backdoor network connection into a device in the background for a hacker to access the system though the networks firewall without the victim's knowledge. [54]

Worm: A worm is a malicious piece of code that has the ability to pivot through a network infecting many devices with its payload i.e. trojan and/or virus. [55]

Within an enterprise or SMB network up to date endpoint security software i.e. anti-malware, anti-virus, personal firewall etc from a reputable company such as Symantec [56] or MacAfee [57] should be implemented on all end devices and servers to quarantine any malware that may infiltrate end device within the network before it can cause damage to mitigate this threat. [58] [59]

d. Social Engineering

Social engineering within cyber security is the art of manipulating a person into unwittingly revealing secure information such as; passwords, maiden names, first pet names etc so that a malicious actor can leverage this information to access a network or end device. [60]

To mitigate this issue cyber security training should be given to all staff who have access to the company network, also appropriate network privileges [61] should be applied depending how senior the staff members role is within a company to minimise the damage of such an attack.

Modern social engineering techniques involve using phishing E-mails [62] that claim to be from a trusted company but when a link contained within the E-mail is clicked malware is downloaded onto the victims device and then creates a reverse Transmission Control Protocol (TCP) [63] connection back to the attacker for remote access of the victims device and/or install ransomware [64] in the form of a worm on the device that could pivot through the network infecting more devices, with a payload that could encrypt [65] sensitive documents that can't be decrypted without the encryption key, this form of attack is commonly used within ransomware attacks.

To mitigate this issue an E-mail threat scanner [66] should be implemented at the E-Mail server and all personal E-Mail should be blocked within the company network. Universal Serial Busport (USB) should also be disabled to prevent malware entering the network locally [67].

e. Denial of Service (DOS)

A Denial of Service (DOS) [68] attack is a basic but very effective attack on a network that can cripple the networking infrastructure for long periods of time preventing the network services from being used by customers/business clients. The most common version of this attack functions by malicious actors continuously sending large amount of data to a server to overwhelms its resources and/or network bandwidth, forcing it to shut down denying services to genuine end users. A single DOS attack will not interrupt services within a datacentre because they have a multitude of resources and load balancing internetworking devices. [69]

The most devastating form of this attack that is targeted at datacentres is called a Distributed Denial of Service (DDOS) [70] attack. A DDOS attack functions the same as a DOS attack but instead of just one device sending large amounts of data continuously to a server, there are multitudes of compromised devices from around the world called 'bots' [71] controlled by a malicious actor all configured to execute a DOS attack simultaneously to the same target causing a DDOS attack. [72]

A large-scale version of this attack with more than a million bots collaboratively sending upwards of 300Gb/s of data cannot be completely mitigated but rather managed to minimise the downtime of the effected devices. The largest ever DDOS attack was orchestrated in 2018 to the datacentres of 'GitHub' a software hosting company that received over 1.35 Tb/s of data that compromised of 126.9 million packets per second targeted at their servers causing the servers to crash for 20 minutes due to a DDOS mitigation 3rd party company intervening that 'GitHub' retain their services for. [73], [74]

Continuous monitoring of traffic entering the network is an essential tool to pre-empt and prepare for a DDOS attack to load balance traffic from the targeted service or protocol to more devices within the datacentre or remote site. [75]

DDOS protection tools are also available on the market such as; 'SiteLock' [76] that protect against DDOS attacks up to 300Gb/s by autonomously distributing and protecting traffic effected at the application, transport and network layers of the Open Systems Interconnections (OSI) model. 3rd party DDOS specialist companies are also available for companies to retain there services for a fee as previously discussed. [77]

V. NETWORK SECURITY AUDITING

Within a datacentre, security is of utmost importance for reasons previously discussed. A team of network security professionals are often employed to keep the datacentre secure. These professionals will install and analyse security monitoring software such as 'NetFort: LANGuardian' [78] to continuously audit and monitor all traffic coming in and out of the network with E-Mail alerts and traps (alarm triggers) configured to alert security staff of breaches and/or threats to the network. Using this data, a comprehensive threat analysis model can be created to identify the most common attacks against the datacentre and also any identified weak points within the network topology that may need additional configuration or security devices. [79] [80]

VI. REDUNDANCY

Redundancy is a key feature within networking in general but specifically to datacentres that must be available 24 hours a day 7 day a week. As previously discussed, within cyber security it's not 'if' an attack happens but 'when', so all eventuality's need to be carefully thought of and planned pre-emptively. [81]

In the event that data was lost, and/or the infrastructure was disabled from a cyber security attack or natural disaster, datacentres make copies of all data both locally and remotely

using a Redundant Array of Independent Disks (RAID) [82] that are configured for mirroring (copying) of all data onto two or more disks. These backup disks will be kept offline and often in a separate location to prevent them also becoming corrupt or damaged in the event of a catastrophe. [83]

A datacentre company usually consists of two or more datacentres that are built in separate location for redundancy purposes. The two or more datacentres are configured within a failover cluster [84], so they can function at the same time, combining resources i.e. computational power etc for efficiency and throughput to the customers/clients. In the event one of the datacentres went offline because of a natural disaster or cyber security attack, the other datacentre(s) would seamlessly takeover that datacentres work load, this process would be transparent to the end user. [85]

Datacentre redundancy is very expensive for these companies, but it is imperative in today's cyber security climate for a business to keep customers/clients data safe and maintain a trustworthy reputation within the industry. [86] [87]

VII. CONCLUSIONS

Cloud computing offers many benefits as identified within this report but there is still a long way to go before all IT operations can be outsourced to CSP's without impacting the businesses that utilise them, from efficiency to security. Many network engineers refer to network architectures as snowflakes because no two networks are the same due to the bespoke nature of companies and their business requirements that can't be outsourced as a one size fits all solution.

IaaS attempts to offer a customised networking solution to clients, but without control of the overarching infrastructure and the engine that runs the network, a lot of compatibility issues will arise whilst trying to implement complex business solutions such as; Bring Your Own Device (BYOD) Mobile Device Management (MDM), Voice and Video collaboration tools, multi-vendor services such as; Windows and Linux, user privilege management and security, along with multiple Domain Name Service (DNS) instances etc.

With the new General Data Protection Regulations (GDPR) [88] coming into force as of May 2018 companies may be more reluctant to utilise XaaS because of the inherit data security issues that exist within these CSP models, such as; the lack of control and transparency of user data within the CSP infrastructure that could be lost or stolen by malicious actors which would incur massive fines as per the new GDPR that could bankrupt alot of SMB's. Therefore, at this present time XaaS although a novel idea is still in its infancy for larger business to adopt as its only IT solution.

VIII. REFERENCES

- [1] B. . Radenkovic and P. . Kocovic, *From mainframe to cloud*, vol. 1. 2014.
- [2] "Chapter 3: History of Mainframes."
- [3] Computer History Museum, "Timeline of computer history," *Exhibits*, 2015. [Online]. Available: <http://www.computerhistory.org/timeline/>.
- [4] IBM, "IBM Archives: IBM's ASCC (a.k.a. The Harvard Mark I)," *ibm.com*, 2018. [Online]. Available: https://www-03.ibm.com/ibm/history/exhibits/markI/markI_intro.html. [Accessed: 23-May-2018].
- [5] J. Laprise and N. Ensmenger, "Think Piece The Purloined Mainframe: Hiding the History of Computing in Plain Sight," *IEEE Ann. Hist. Comput.*, vol. 31, no. 3, pp. 83–84, 2009.
- [6] K. Mershad, H. Artail, M. Saghir, H. Hajj, and M. Awad, "A Study of the Performance of a Cloud Datacenter Server," *IEEE Trans. Cloud Comput.*, pp. 1–1, 2015.
- [7] datacenterknowledge, "Google Data Center FAQ, Part 2 | Data Center Knowledge," *datacenterknowledge.com*, 2018. [Online]. Available: <http://www.datacenterknowledge.com/google-data-center-faq-part-2>. [Accessed: 23-May-2018].
- [8] S. P. Mirashe and N. V Kalyankar, "Cloud Computing," *Communications of the ACM*, 2010. [Online]. Available: <http://portal.acm.org/citation.cfm?doid=358438.349303%5Cnhttp://arxiv.org/abs/1003.4074>.
- [9] O. Tickoo, R. Iyer, and D. Newell, "Modeling Virtual Machine Performance: Challenges and Approaches VMM or Hypervisor," *Proc Sigmetrics Work. hotmetrics*, pp. 55–60, 2009.
- [10] C. Costache, O. Machidon, A. Mladin, F. Sandu, and R. Bocu, "Software-defined networking of Linux containers," in *Proceedings - RoEduNet IEEE International Conference*, 2014.
- [11] W. Machines, L. Barroso, and U. Hölzle, *The Datacenter as a Computer*, vol. 24. 2013.
- [12] Internet Society, "Brief History of the Internet," *What is the Internet? - Internet Facts & Statistics*. p. 17, 2001.
- [13] C. Computing and D. Mining, "an Overview of Cloud Comput Ing and Knowled Ge Management," *Knowl. Manag.*, vol. 1, no. 1, pp. 25–30, 2011.
- [14] Amazon, "Amazon Web Services (AWS)- Cloud Computing Services," *Amazon Web Services, Inc.*, 2016. .
- [15] Microsoft, "Microsoft Azure," *Microsoft*, 2016. [Online]. Available: <https://azure.microsoft.com/en-in/>.
- [16] Google, *Google Compute Engine*. 2013.
- [17] zdnet, "XaaS: Why 'everything' is now a service | ZDNet," *zdnet.com*, 2017. [Online]. Available: <https://www.zdnet.com/article/xaas-why-everything-is-now-a-service/>. [Accessed: 23-May-2018].
- [18] M. Kozlovsky, M. Töröcsik, T. Schubert, and V. Pósemé, "IaaS type Cloud infrastructure assessment and monitoring," in *Information Communication Technology Electronics Microelectronics (MIPRO), 2013 36th International Convention on*, 2013, pp. 249–252.
- [19] C. Heinle and J. Strebel, "IaaS adoption determinants in enterprises," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6296 LNCS, pp. 93–104.
- [20] D. Beimborn, T. Miletzki, and S. Wenzel, "Platform as a service (PaaS)," *Bus. Inf. Syst. Eng.*, vol. 3, no. 6, pp. 381–384, 2011.
- [21] G. Kulkarni, P. Khatawkar, and J. Gambhir, "Cloud Computing-Platform as Service," *Cloud Comput. as Serv.*, no. 2, pp. 115–120, 2011.
- [22] K. Brown, C. W., & Nyarko, "Software as a Service (SaaS)," *Cloud Comput. Serv. Deploy. Model. Layers Manag. Layers Manag.*, p. 50, 2012.
- [23] W. T. Tsai, X. Y. Bai, and Y. Huang, "Software-as-a-service (SaaS): Perspectives and challenges," *Sci. China Inf. Sci.*, vol. 57, no. 5, pp. 1–15, 2014.
- [24] K. Fanning and C. D. M., "DaaS: A Cost-Savings Strategy," *J. Corp. Account. Financ.*, vol. 26, no. 5, pp. 15–20, 2015.
- [25] S. Dembecher, "Having the mind in the cloud: Organizational mindfulness and the successful use of desktop as a service," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2014, pp. 2137–2146.
- [26] Citrix, "What is VDI? - Citrix," *citrix.co.uk*, 2018. [Online]. Available: <https://www.citrix.co.uk/glossary/vdi.html>. [Accessed: 23-May-2018].
- [27] European Big Data Value Association, "European Big Data Value Strategic Research and Innovation," *BigDataValu.eu*, no. July, pp. 1–45, 2014.
- [28] M. Mahrt and M. Scharrow, "The Value of Big Data in Digital Media Research," *J. Broadcast. Electron. Media*, vol. 57, no. 1, pp. 20–33, 2013.
- [29] Forbes, "Here's Why Data Is Not The New Oil," *forbes.com*, 2018. [Online]. Available: <https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#7b3a3c113aa9>. [Accessed: 23-May-2018].
- [30] Cloud Security Alliance, "Top Threats to Cloud Computing," *Security*, no. March, pp. 1–14, 2010.
- [31] Rapid7, "Metasploit Framework," *metasploit.rapid7.com*, 2018. [Online]. Available: <https://metasploit.help.rapid7.com/docs/msf-overview>. [Accessed: 23-May-2018].
- [32] Offensive-Security, "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," *kali.org*, 2018. [Online]. Available: <https://www.kali.org/>. [Accessed: 23-May-2018].
- [33] M. Conover, *Hacking Exposed Linux : Linux Security Secrets and Solutions, Third Edition*. 2008.
- [34] C. C. Palmer, "Ethical hacking," *IBM Syst. J.*, vol. 40,

- no. 3, pp. 769–780, 2001.
- [35] Microsoft, “Chapter 3: Security Design Guidelines for Web Services | Microsoft Docs,” *microsoft.com*, 2010. [Online]. Available: [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649737\(v=pandp.10\)](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649737(v=pandp.10)). [Accessed: 23-May-2018].
- [36] hackingarticles.com, “Exploit Remote Windows PC with Eternalblue & Doublepulsar Exploit in Metasploit,” *hackingarticles.com*, 2018. [Online]. Available: <http://www.hackingarticles.in/exploit-remote-windows-pc-eternalblue-doublepulsar-exploit-metasploit/>. [Accessed: 23-May-2018].
- [37] microsoft.com, “Microsoft Security Bulletin MS17-010 - Critical | Microsoft Docs,” *microsoft.com*, 2018. [Online]. Available: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>. [Accessed: 23-May-2018].
- [38] J. Gill and K. Zunnurhain, “Determining the Penetration Threshold for an ASA 5500 Firewall,” in *Proceedings of the SouthEast Conference on - ACM SE '17*, 2017, pp. 149–153.
- [39] R. Tidd and G. Heesacker, “Digital Signatures and Certificates,” *CPA J.*, no. May, pp. 60–61, 2008.
- [40] A. A. Abdelkarim and H. H. O. Nasereddin, “Intrusion Prevention System,” *Int. J. Acad. Res.*, vol. 3, no. 1, pp. 432–434, 2011.
- [41] H. D. Steps, “A HoneyPot Deployment Plan,” *Honeypots Wind.*, pp. 35–59, 2005.
- [42] F. Araujo, K. W. Hamlen, S. Biedermann, and S. Katzenbeisser, “From Patches to Honey-Patches,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, 2014, pp. 942–953.
- [43] S. Gold, “Cracking passwords,” *Netw. Secur.*, vol. 2010, no. 8, pp. 4–7, 2010.
- [44] SID, “How to Crack Passwords in Kali Linux Using John The Ripper,” *Latest Hacking News*. 2016.
- [45] Oxid, “Cain & Abel,” *oxid.it*, 2018. [Online]. Available: <http://www.oxid.it/cain.html>. [Accessed: 23-May-2018].
- [46] Darknet, “Brutus Password Cracker - Download brutus-aet2.zip AET2,” *darknet.org*, 2018. [Online]. Available: <https://www.darknet.org.uk/2006/09/brutus-password-cracker-download-brutus-aet2zip-aet2/>. [Accessed: 23-May-2018].
- [47] infosec, “Online Dictionary Attack with Hydra,” *infosecinstitute.com*, 2018. [Online]. Available: <https://resources.infosecinstitute.com/online-dictionary-attack-with-hydra/#gref>. [Accessed: 23-May-2018].
- [48] B. Danczul, J. Fuß, S. Gradingner, B. Greslehner, W. Kastl, and F. Wex, “CuteForce analyzer: A distributed bruteforce attack on PDF encryption with GPUs and FPGAs,” in *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 2013, pp. 720–725.
- [49] Sans, “SANS - Information Security Resources | Information Security Policy Templates |,” *sans.org*, 2018. [Online]. Available: <https://uk.sans.org/security-resources/policies>. [Accessed: 23-May-2018].
- [50] L. Latinov, “MD5, SHA-1, SHA-256 and SHA-512 speed performance,” *automationrhapsody.com*, 2017. [Online]. Available: <https://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/>.
- [51] C. Dobraunig, M. Eichlseder, and F. Mendel, “Analysis of SHA-512/224 and SHA-512/256,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9453, pp. 612–630.
- [52] B. Witten and C. Nachenberg, “Malware Evolution : A Snapshot of Threats and Countermeasures in 2005,” in *Malware Detection*, 2007, pp. 3–15.
- [53] infosec, “InfoSec - Types of Virus & Malicious Codes and Protective Measures,” *infosec.gov.uk*, 2018. [Online]. Available: https://www.infosec.gov.hk/english/virus/types_v.html. [Accessed: 23-May-2018].
- [54] Kaspersky, “What is a Trojan Virus? | Trojan Definition | Kaspersky Lab UK,” *kaspersky.co.uk*, 2018. [Online]. Available: <https://www.kaspersky.co.uk/resource-center/threats/trojans>. [Accessed: 23-May-2018].
- [55] kaspersky, “What is a Computer Worm? | Kaspersky Lab UK,” *kaspersky.co.uk*, 2018. [Online]. Available: <https://www.kaspersky.co.uk/resource-center/threats/viruses-worms>. [Accessed: 23-May-2018].
- [56] Symantec, “Symantec - Global Leader In Next-Generation Cyber Security | Symantec,” *symantec.co.uk*, 2018. [Online]. Available: <https://www.symantec.com/en/uk>. [Accessed: 23-May-2018].
- [57] McAfee, “Security Solutions: Endpoint, Cloud, Network, Antivirus, Malware | McAfee,” *McAfee.com*, 2018. [Online]. Available: <https://www.mcafee.com/uk/index.html>. [Accessed: 23-May-2018].
- [58] Symantic, “Internet Security Threat Report 2015,” 2017.
- [59] B. Potter and G. Day, “The effectiveness of anti-malware tools,” *Comput. Fraud Secur.*, vol. 2009, no. 3, pp. 12–13, 2009.
- [60] P. Muehleis, “Social engineering,” *J. Am. Dent. Assoc.*, vol. 141, no. 5, p. 500; discussion 500-501, 2010.
- [61] ITGovernance, “Access control and administrative privilege management,” *itgovernance.co.uk*, 2018. [Online]. Available: <https://www.itgovernance.co.uk/access-control-and-administrative-privilege>. [Accessed: 23-May-2018].
- [62] us-cert, “Avoiding Social Engineering and Phishing Attacks,” *us-cert.gov*, 2009. [Online]. Available: <https://www.us-cert.gov/ncas/tips/ST04-014>. [Accessed: 23-May-2018].
- [63] infosecurity, “Writing Reverse TCP Exploit,” *infosecurity.com*, 2018. [Online]. Available:

- <https://resources.infosecinstitute.com/stack-based-buffer-overflow-in-win-32-platform-part-5-writing-reverse-tcp-exploit/#gref>. [Accessed: 23-May-2018].
- [64] J. E. et al. . Dunn, "Ransomware," *Wikipedia*, 2012. [Online]. Available: <https://en.wikipedia.org/wiki/Ransomware>.
- [65] U. S. D. of C. / the N. T. I. S. (N.I.S.T.), "Advanced Encryption Standard (AES)," 2001.
- [66] Barracuda, "E-Mail Threat Scanner," *barracuda.com*, 2018. [Online]. Available: https://www.barracuda.com/email_scan. [Accessed: 23-May-2018].
- [67] infosec, "The Security Awareness Hazards of Removable Media," *infosecinstitute.com*, 2018. [Online]. Available: <https://resources.infosecinstitute.com/category/enterprise/securityawareness/removable-media/#gref>. [Accessed: 23-May-2018].
- [68] Q. Gu and P. Liu, "Denial of Service Attacks," in *Handbook of Computer Networks*, vol. 3, 2012, pp. 454–468.
- [69] M. McDowell, "Understanding Denial-of-Service Attacks," *Security Tip*, 2009. [Online]. Available: <http://www.us-cert.gov/ncas/tips/st04-015>.
- [70] F. Lau, S. Rubin, and M. Smith, "Distributed denial of service attacks," *Syst. Man, Cybern.*, 2016.
- [71] C. Lebeuf, M. A. Storey, and A. Zagalsky, "Software Bots," *IEEE Softw.*, vol. 35, no. 1, pp. 18–23, 2017.
- [72] B. B. Gupta, R. C. Joshi, and M. Misra, "Distributed Denial of Service Prevention Techniques," *Int. J. Comput. Electr. Eng.*, pp. 268–276, 2010.
- [73] wired, "A 1.3-Tbs DDoS Hit GitHub, the Largest Yet Recorded | WIRED," *wired.com*, 2018. [Online]. Available: <https://www.wired.com/story/github-ddos-memcached/>. [Accessed: 23-May-2018].
- [74] thehackernews, "Biggest-Ever DDoS Attack (1.35 Tbs) Hits Github Website," *thehackernews.com*, 2018. [Online]. Available: <https://thehackernews.com/2018/03/biggest-ddos-attack-github.html>. [Accessed: 23-May-2018].
- [75] S. Mansfield-Devine, "DDoS: Threats and mitigation," *Netw. Secur.*, vol. 2011, no. 12, pp. 5–12, 2011.
- [76] sitelock, "DDoS Protection | Anti-DDoS | SiteLock," *sitelock.com*, 2018. [Online]. Available: <https://www.sitelock.com/ddos-protection>. [Accessed: 23-May-2018].
- [77] infosec, "InfoSec - Securing Your Outsourcing IT Tasks," *infosec.gov.hk*, 2018. [Online]. Available: https://www.infosec.gov.hk/english/business/other_da ddosa.html. [Accessed: 23-May-2018].
- [78] netfort, "LANGuardian - Deep Packet Inspection Software.," *netfort.com*, 2018. [Online]. Available: <https://www.netfort.com/languardian/>. [Accessed: 23-May-2018].
- [79] L. Obregon, "Infrastructure Security Architecture for Effective Security Monitoring Infrastructure Security Architecture for Effective Security Monitoring GIAC (GCIA) Gold Certification," *sans.org*, 2015.
- [80] info-security, "Network Security News and Articles - Infosecurity Magazine," *info-security-magazine.com*, 2018. [Online]. Available: <https://www.infosecurity-magazine.com/network-security/>. [Accessed: 23-May-2018].
- [81] baesystems, "Cyber security breaches: it's not, if but when | BAE Systems," *baesystems.com*, 2018. [Online]. Available: <https://www.baesystems.com/en/cybersecurity/multimedia/cyber-security-breaches--it-s-not--if-but-when>. [Accessed: 23-May-2018].
- [82] sansdigital, "What is RAID? - Sans Digital - Your One-Stop Storage Solution," *sansdigital.com*, 2018. [Online]. Available: <http://www.sansdigital.com/what-is-raid.html>. [Accessed: 23-May-2018].
- [83] Sans, "Backup & Recovery | SANS Security Awareness," *sans.org*, 2017. [Online]. Available: <https://www.sans.org/security-awareness-training/ouch-newsletter/2017/backup-recovery>. [Accessed: 23-May-2018].
- [84] B. Mohammed, M. Kiran, K. M. Maiyama, M. M. Kamala, and I. U. Awan, "Failover strategy for fault tolerance in cloud computing environment," in *Software - Practice and Experience*, 2017, vol. 47, no. 9, pp. 1243–1274.
- [85] Cisco-Meraki, "Datacenter Redundancy (DC-DC Failover) Deployment Guide - Cisco Meraki," *meraki.com*, 2018. [Online]. Available: [https://documentation.meraki.com/MX-Z/Deployment_Guides/Datacenter_Redundancy_\(DC-DC_Failover\)_Deployment_Guide](https://documentation.meraki.com/MX-Z/Deployment_Guides/Datacenter_Redundancy_(DC-DC_Failover)_Deployment_Guide). [Accessed: 23-May-2018].
- [86] Microsoft, "Confidence in the trusted cloud | Microsoft Azure," *microsoft.com*, 2018. [Online]. Available: <https://azure.microsoft.com/en-gb/overview/trusted-cloud/>. [Accessed: 23-May-2018].
- [87] stratoscale, "Security and Trust in the Cloud vs. Your Private Data Center," *stratoscale.com*, 2018. [Online]. Available: https://www.stratoscale.com/blog/datacenter/security_trust_cloud_vs_your_private_data_center/. [Accessed: 23-May-2018].
- [88] J. Day, "General Data Protection Regulation Guide," *GDPR Guide*. pp. 4–24, 2017.

IX. BIBLIOGRAPHY

- Odom, Wendell CCNA 'Routing and Switching' 200-105 official cert guide cisco press (2016)
ISBN-10: 1-58720-580-7
- Bruno, Anthony; Jordan, Steve CCDA 'Cisco Network Design' 200-310 official cert guide (2016)
ISBN-10: 1-58714-454-9
- Hucaby, David CCNA 'Wireless' 200-355 official cert guide (2016)
ISBN-10: 1-58714-457-3

Santos O, Stuppi J, Cisco CCNA security 210-260 official
cert guide (2016)
ISBN: 1587205661

Robinson, Tony Building Virtual Machine Labs: A Hands-
On Guide
ISBN-10: 1546932631

Cloud Computing and Cybersecurity

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

88/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

GRADING FORM: SMU GENERIC_GJ

PAUL LAWRENCE

88

RESEARCH-INFORMED LITERATURE

A huge number of sources correctly utilised. I can



see you've made a real effort to seek authoritative, academic material first and used web sources only when necessary, and sought credible online sources. Really excellent work here.

27

KNOWLEDGE AND UNDERSTANDING



Extremely good evidence of knowledge and understanding - great depth of research, tons of detail well beyond the scope of what was asked, or what would be expected of a level 5 student.

28

ANALYSIS



Excellent analysis - you obviously really took on board my feedback from the previous assignment about synthesis - this was done really well in this work. Valid conclusions derived and well put together.

21

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



A very nicely-presented, well written report - a few minor typographical errors don't detract from an overall excellent report - really well done, Paul!

12