Cyber Security Audit of Top Four Technologies- A Short Note

Scott Sawyer
MIT Sydney Australia

Abstract : Cybersecurity and networking play a major role in todays interconnected world. The ultimate aim of this report is to discuss and provide insight into 4 areas of the cybersecurity and networking realm, from threats such as SQL Injection Attacks, through to technologies such as Load Balancing, Blockchain for the Internet of Things and Cloud Computing. As such, this report will be broken up into 4 sections to address each item individually.
Key terms: Cloud security, Load balancing, SQL injection attacks etc.

SQL Injection Attacks

SQL injection attacks remain to be a significant attack vector employed by threat actors within the realm of cybersecurity and networking. Such attacks are employed against the various database technologies in use today which include but are not limited to MySQL/MariaDB, PostgreSQL and Microsoft SQL (MSSQL) Servers. They work by exploiting known vulnerabilities in web applications such as unvalidated inputs coming from parameters parsed on the URL address line of a browser. As an example, if whilst browsing an online store you click on an item and the URL address changes to something like https://shop.example.com/product.php?id=352, the website has created a query internally to gather the data for item 352 from its database. This in itself would likely only return one record as a specific ID has been specified by the address line. However, a threat actor could attempt to manipulate the address line in an effort to enter extra arbitrary but valid SQL code into the query generated by the web applications backend processes in an attempt to gather or return more results than originally intended. Conversely the code being added may be designed to delete data from the database. It is this manipulation of the calling code that makes up the injection attack.

According to the Imperva website, a company who specialises in web application firewall technologies, common SQL injection queries can be as simple as adding “OR 1=1” to the address line which if used with the example address provided above could return all product ID’s and any other fields the website is programmed to display within the query presented, to the addition of “; DROP TABLE USERS” which would delete if it existed in the database attached to the web application being exploited the USERS table. [1] In more complex scenarios, attackers could attempt to use the UNION operator in a bid to tack on their own SQL SELECT statements into the injection attack. This could result in the return of unauthorised data from within other parts of the database such as usernames and passwords.

There have been a number of recent attacks using SQL injection to facilitate the theft of data. One such example according to Sergiu Gatlan of BleepingComputer is the theft of email addresses and password hashes from the company Freepik, a company who controls one of the largest graphic resource sites in the world. It along with its sister site Flaticon had 8.3 million email addresses and password hashes stolen from their sites databases using targeted SQL injections. Of the resulting breach, BleepingComputer reports that "3.55 million users had passwords hashed using bcrypt and a further 229 000 users had MD5 Salted hashes." [2] The breach resulted in Freepik force resetting the accounts of those members that had salted MD5 hashed passwords, and informing the users with compromised bcrypt passwords to update their credentials. Additional to these measures according to the article, "FreePik is now utilising bcrypt exclusively to secure its password hashes and has employed security experts to do a full audit of internal and external security measures." [2]

In order to defend against SQL Injection attacks, the employment of a web application firewall (WAF) is often a good way to help filter the data being sent to web application servers. WAF's use intelligent heuristics to scan submitted data to a website, looking for variables that match one or more threat signatures. If this is found, the WAF will either block the request thus stopping the attack or will strip the malicious data from the request and allow the legitimate portion to proceed.

Additional to the use of a WAF, ensuring your web application's code is not using unvalidated parameters when requesting data for return will ensure that only data that is valid will be returned to the user.

Load Balancing Algorithms

Load Balancing is the process of diverting network traffic between multiple physical or virtual resources providing the same service. This is important from a security perspective as it provides resilience against attacks such as distributed denial of service. Load Balancing can be achieved using a number of algorithms such as round robin, weighted round robin and least connection.

The round robin algorithm works by assigning connections based on a list of resources that can service the requests. In its simplest form, it simply goes down the list of resources irrespective of the attributes of the nodes that are servicing the requests. Once the algorithm reaches the end of the resource list, it loops and begins again from the top. The weighted version of this algorithm works in a similar way to the round robin method described above but does take a weighting score into consideration when determining where to send the connection request. The weighting is often set by an administrator taking into consideration the attributes of the servers that are servicing a web application. Servers with better configurations or more resources are given a higher weight. The advantages of using the round robin algorithm are that requests are shared equally amongst the listed

nodes, and if the weighted version is used, then this is taken into consideration too. However, the round robin algorithm also does not take into consideration items such as the existing load on a server. This protocol will still send the request to the server when it comes up next on the list of servers to be utilised.

The least connection algorithm takes a list of nodes that are capable of servicing requests for a given resource and sends requests to the node that is servicing the least number of active concurrent connections. This provides an advantage over the round robin algorithm because it does take into consideration server loads when determining its next available. However, like the vanilla flavour of round robin, it does not take into consideration the capabilities of a given node when it sends its connections to service the requests.

Given the way these algorithms work, it is my opinion that it is possible for load balancing algorithms to compromise the security of a network, especially if the load balancer itself is compromised. A compromised load balancer could be used to establish a base of operations into a network and provide a platform for further incursion into a network. From the algorithm standpoint, given the nature of the way they work, an attacker need only add a compromised server into the list of servicing nodes in order to capture data such as usernames and passwords when the algorithm sends requests to the infected node.

Blockchain and the Internet of Things (IoT)

The term IoT is defined by the Internet Engineering Task Force (IETF) as a "network of physical objects or 'things' embedded with electronics, software, sensors, actuators, and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices." [3] As a result, IoT objects are generally small in size and limited in their computational power and storage. These limitations often become a problem when it comes to the security of these devices as the more secure algorithms require computational power that is often beyond the limitations of these devices.

Blockchain is a technology that is used to create a decentralised ledger network that is capable of verifying the transactions conducted within it. Due to its decentralised nature, blockchain comes with the advantage of robustness as losing a node or 2 will not generally cause the chain of transactions to lose integrity or validity. Within a blockchain network, individual transactions for execution are grouped into blocks and this block is sent to each participating node within the blockchains network for validation. Validation occurs on an individual node using a mathematical calculation which is based on predetermined and agreed upon rules. This is called the blockhash. When a node has successfully validated the block, the node cryptographically timestamps the validated block and adds it to the end of its blockchain. When over half of the nodes in a blockchain network have validated the block successfully, the block is deemed to have obtained 'consensus'. At this time, the validated block is cryptographically timestamped, hashed and added to the end of the blockchain ledger. This hash

also uses the calculated hash of the previous block to create a chain of blockchain hashes. It is this state that is then shared amongst the blockchain network for the processing of subsequent blocks and the transactions that were held within that block are processed as validated transactions.

Given the above process, you may ask what blockchain has to do with the IoT. We said before that IoT devices are limited in their computational power and storage so full-blown encryption of data is generally not possible, however there is sufficient processing power available to create and calculate hashes. As blockchain works with hashes and not full encryption, it becomes suitable for use with lower powered IoT devices. Furthermore, due to blockchains robustness and decentralisation, "there is no single point of failure or vulnerability, except with the clock needed for timestamping" [4]. This enables blockchain to ensure security within an IoT domain.

Cloud Computing

Cloud Computing is becoming ever increasingly important sector within the computing world. Large organisations are working to reduce their infrastructure footprints and are turning to cloud computing technologies to augment or in some instances replace their existing infrastructure.

Cloud computing works by charging a customer for the resources that are used on a demand basis. Resources are generally located in geographically strategic datacentres and are allocated to customers based on the service models that are selected. The main advantage to the use of cloud computing technology is the flexibility and scalability it affords a company based on the companies demands and requirements. There are 4 main service models within cloud computing, Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Function as a Service (FaaS). Figure 1 below explains the 4 service models.

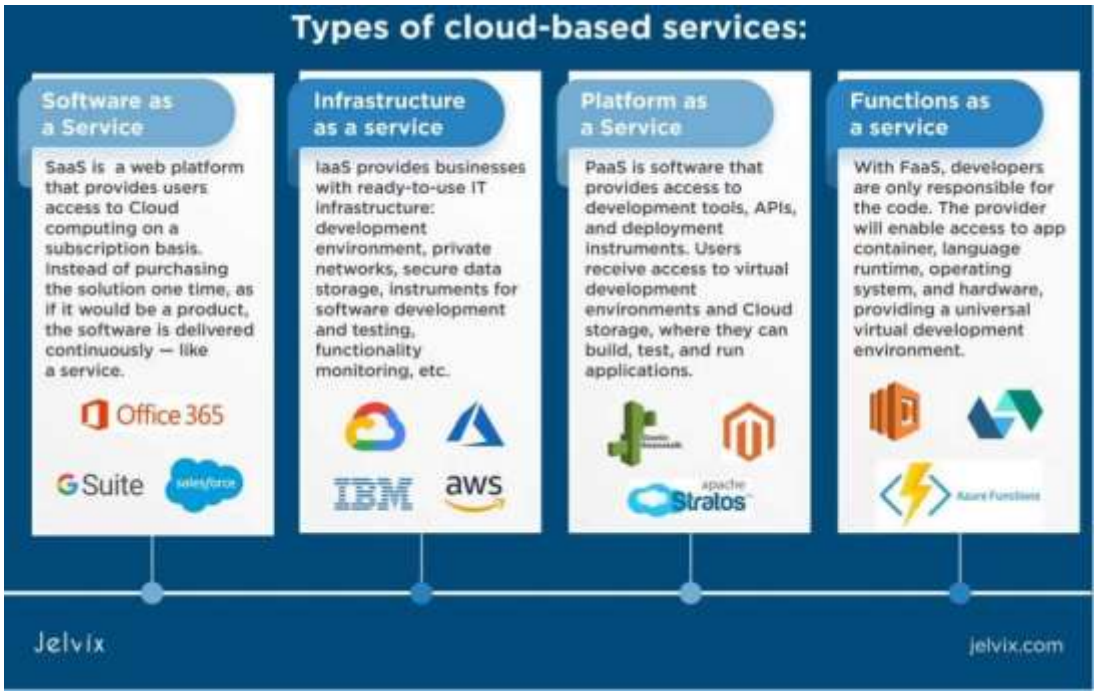

Figure 1: Types of cloud-based services. Source: Adapted from *[5]*

As cloud computing infrastructure and services generally reside outside of the organisations traditional network borders, additional security protections such as 2 factor authentication (2FA) are employed by organisations that utilize these services. The principle of having 'something you know' and 'something you have' enables organisations to validate the potential users of these systems are indeed authorised to access them.

Two common cloud computing IaaS products are Microsoft Azure and Amazon AWS. Both products provide scalable infrastructure solutions to organisations who want to utilize cloud computing technologes. Table 1 below lists the major differences between the Microsoft Azure and Amazon AWS platforms

	Amazon AWS	Microsoft Azure
Availability Zones	61 Zones	140 Zones
Database Services	MySQL, Oracle, DynamoDB	MS SQL, SQL Sync
Networking Services	Public IP/Elastic IP, Virtual Private Cloud, Heavily configurable firewall	Auto IP assignment, Load-balancing, Azure Connect
Ecosystems	AWS has has an expensive partner ecosystem	Small ecosystem with very few linux options
Support for big data	Elastic Band Storage system is ideal for large amounts of data	Standard storage has many big data issues, thus requirement for premium storage.

Table 1: Differences between Microsoft Azure and Amazon AWS products. Source: Adapted from *[6]*

Conclusion:

As can be seen from table 1 above, both products have a number of advantages and disadvantages. However, determining which product is better is highly dependent on the context in which the product is to be used. For example, if your organisation is primarily Microsoft based and doesn't have a large data storage requirement for the cloud, Microsoft Azure may be the better option as it integrates more cleanly into the existing Microsoft environment using its Azure Connect technology. This being said, if your organisation uses Linux infrastructure and services, the versatility of the AWS ecosystem may prove to provide a better experience for that organisation.

References

[1] Imperva, "SQL (Structured query language) Injection," [Online]. Available: https://www.imperva.com/learn/application-security/sql-injection-sqli/. [Accessed 25 September 2021].

[2] S. Gatlan, "Freepik data breach: Hackers stole 8.3M records via SQL injection," BleepingComputer, 21 August 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/freepik-data-breach-hackers-stole-83m-records-via-sql-injection/. [Accessed 25 September 2021].

[3] Internet Engineering Task Force, "The Internet of Things at the IETF," [Online]. Available: https://www.ietf.org/topics/iot/. [Accessed 26 September 2021].

[4] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IEEE IT Professional,* vol. 19, no. 4, pp. 68-72, 2017.

[5] C. Kirill Yusov, "Different Types of Cloud Service Models," [Online]. Available: https://jelvix.com/blog/cloud-service-models. [Accessed 26 September 2021].

[6] D. Taylor, "Azure vs. AWS: What is the Difference Between AWS and Azure," 28 August 2021. [Online]. Available: https://www.guru99.com/azure-vs-aws.html#3. [Accessed 26 September 2021].