**CO4509 –**

**Computer Security**

Table of Contents

[Introduction 3](#_Toc35035331)

[Principles of CDN 5](#_Toc35035332)

[Cache Poisoned Denial of Service (CPDoS) 10](#_Toc35035333)

[Conclusion 13](#_Toc35035334)

[References 14](#_Toc35035335)

[Figure 1: Components of Computer Security 3](#_Toc35035336)

[Figure 2: Man in the Middle Attack 4](#_Toc35035337)

[Figure 3: Content Distribution Network 5](#_Toc35035338)

[Figure 4: Working of CDN 7](#_Toc35035339)

[Figure 5: Architecture of CDN 8](#_Toc35035340)

[Figure 6: Comparison 9](#_Toc35035341)

[Figure 7: Attack of CPDoS 11](#_Toc35035342)

# Introduction

The internet has become an essential part of everyone’s life and there are several implementation processes and components are available on the internet and computer system. Computer security is the protection of the computer system and this is used to secure the computer from the outside threat. The basic aim of this assignment is to explain every single aspect of computer security including the process of Cache Poisoned Denial of Service. In this report, the description of the content distribution network (CDN) will also be defined. In the process of computer security, multiple aspects are available and the basic aim of the assignment is to describe every possible feature and component of all of this concept (Czarny B, 2020). In the process of computer security, there are three main components are available and that component is known as (CIA) such as:

* Confidentiality
* Integrity
* Availability

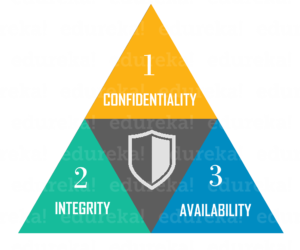


Figure 1: Components of Computer Security

Confidentiality is used to ensure that the information which is available on the computer system will be secure from the outside threat. An integration works like a protection sector which used to protect the computer system from unauthorized parties. Computer security and IT security is one of the most important concern in today’s world and there are several reasons are available which is responsible for that high tight security (Rezafard A, 2020). There are several kinds of computer attacks are available such as:

* Malware Attack
* Man in the Middle
* Phishing
* Eavesdropping
* SQL Injection
* Password Attack and others

These all are some basic and most widely famous types of computer security attacks. One of the most dangerous types of attack is malware attack and most of the cybercriminals used to apply this attack on the computer system. The cybercriminals used to send a fake email to the user’s computer and when the user access that mail and click on that particular link then the malicious software automatically get installed into their customer system and the cybercriminals can easily get the access of that computer and this process is called malware attack (Cortier V, 2020). Man in the middle is also one of the most crucial types of computer attack let’s have an example, suppose we are trying to do online shopping and for purchasing the product the user has to pay online and when the user provide their account details at that time the cybercriminals used to get access of our account and whole confidential information of our bank account automatically sends to the cybercriminal (Pullagura V, 2020).

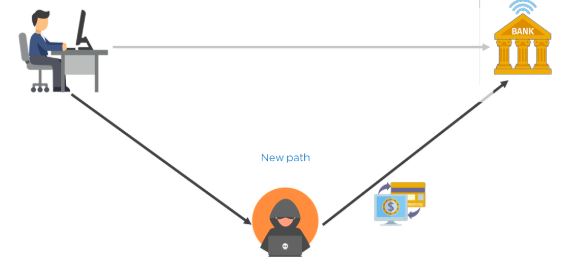


Figure 2: Man in the Middle Attack

# Principles of CDN

CDN is known as a content delivery network or content distribution network also which is a system of distributed servers of a distributed network. The content delivery network (CDN) is used to send the web information, website link and other webpage content to a user. To send the content information of the webpage content delivery network (CDN) uses a geographical location of the user so that the particular webpage can easily send to the respective user. The content delivery network (CDN) is one of the most important and very effective parts of the internet and internet technology services. The process of the content delivery network (CDN) can be easily downloaded by using some specific network connectivity and there are several of the implementation processes are available and every single process is directly or indirectly connected to each other (Silva FA, 2020). We can easily say the content delivery network (CDN) is a transparent backbone of the internet and the services of the internet which can change the content delivery of the webpage or the website. The internet directly interacts with the services of the content delivery network (CDN) and there are multiple kinds of content delivery network (CDN) services that are available which are directly or indirectly connected to each other. The content delivery network (CDN) means having the data more rapidly available on several websites hosting platform or webpages. The server-client principle is also one of the biggest aspects in the implementation of the content delivery network (CDN) which is used to directly interact with the server and client. The concept of server and client can easily understand like we can consider the server/client as sender and receiver. One person used to send the message and the other person uses to collect the message and the server-client principle is also works on this concept (Ruiz L, 2020).

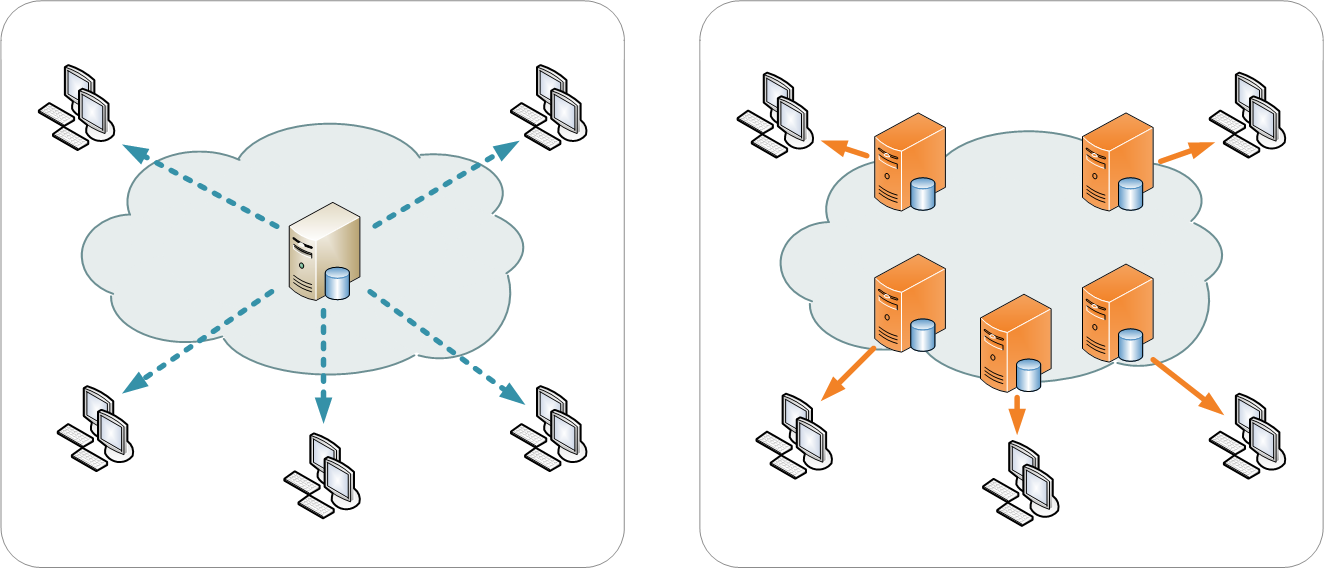


Figure 3: Content Distribution Network

The given image is an example of the concept of the content delivery network (CDN) which clearly defines the working of the content delivery network (CDN) in a very effective way. There are multiple servers and clients are available who are responsible for the working of the content delivery network (CDN). The basic reason for inventing the content delivery network (CDN) is that earlier there was a big issue in the process of transferring data from a web server to the client computer system due to multiple network or technical error. To remove this latency issue the concept of the content delivery network (CDN) has been invented which makes the data transferring process very easy from a web server to the client’s computer system. The delay interval conducts multiple errors like data factor, web factor and many more so to remove this time delay interval the concept of content distribution network was invented (Giuliano R, 2020). There are more functionality and benefits are available of the content delivery network (CDN) such as:

* Minimize server timeouts
* Incorrect data packets and jitters
* Internet data bandwidth
* Digital signals and others

These all are some additional functionality of the content delivery network (CDN). The CDN system is used to minimize the server timeouts because this uses the high network internet connectivity so that the data transfer speed automatically increases in this process. The content delivery network (CDN) also used to collect incorrect data packets from the web server so that unwanted data cannot be sent to the client’s computer system (Mazzenga F, 2020). The content delivery network (CDN) automatically corrects the speed of data bandwidth. The acceleration and control of digital signals also be managed by a content delivery network (CDN). In the global market, there are many companies are available who use the service of the content delivery network (CDN) and they are getting better results in terms of business and technology also. The redundant data transmission automatically reduced after the invention of the content delivery network (CDN). On the internet there are uncounted contents are available so in this case, there is a challenge of duplicate content also occur and to reduce that problem CDN used to analyze every single packet server send by the web browser so that the content management system can easily find out the actual source of operating for the particular content. The cache server is also one of the most important concepts of the internet which is directly connected with the services of the content delivery network (CDN) that used to define the function of the web page objects (Shattil SJ, 2020). There are several web page objects are available such as:

* PNG
* HTML
* PHP
* HTM
* BMP
* TIF
* GIF and others

These all are the type of web page objects which is contain the file entities which we don’t need to transfer anymore because all the information of data available on this web page automatically transferred to the specific client’s computer system. The current services of the content delivery network (CDN) are using in the security sector, financial insurance sector, ISP, ICP, online transaction, big and small companies, and many other fields. There are more other sectors are also available such as:

* Mobile Sector
* Healthcare Sector
* Government Strategies
* Online Gaming
* Advertising Sector and many more (Helms W, 2020)

**Working of CDN:**

In the working of CDN, the CDN needs to be on its default gateway for all incoming traffic and to make this thing happen the domain name server (DNS) configuration should be reset. After setting the root domain the point to point IP range of CDN connected with the CDN server and the server directly interacts with the client’s computer system.

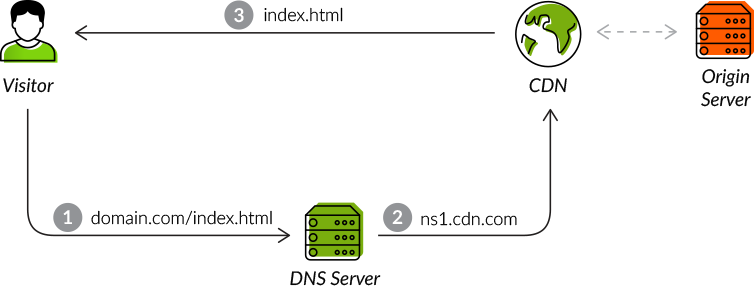


Figure 4: Working of CDN

The given image is about the working condition of a content delivery network (CDN). A DNS server connected to the CDN IP range and the CDN IP range directly connected to the client’s computer system to get the data from the webpage or the webserver (Gould K, 2020).

**The architecture of CDN:**

To send the data at a very high range by using the technological aspect the concept of the content delivery network (CDN) has been used. Which is used to minimize every data file like media files, audio files, content system and many more? In the process of the architecture of the content delivery network (CDN), one of the most effective infrastructural models are points of presence (POPs).

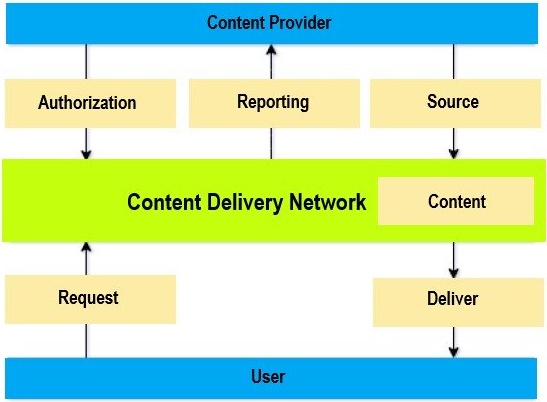


Figure 5: Architecture of CDN

The given image is about the architecture of a content delivery network (CDN). In this image the content provider directly connected with the three basic components such as authorization, reporting, and sources. The content delivery network (CDN) directly connected to the content and the server and client model approach used to request and deliver the content form the webpage server to the user’s computer system. The content provider is the entity delivering the content and the content provider used to give the permission or the authorization to deliver content. After giving the authorization the content provider demands performance analytics and user to provide the CDN services to the relevant data (Chen D, 2020).

There are some key components are also available in the process of the content delivery network (CDN) such as:

* Delivery Nodes
* Storage Nodes
* Origin Nodes
* Control Nodes

**Delivery nodes** are servers that are used to contain cache running one or more content delivery applications. The delivery nodes located very close to the end-user and the content can very easily be sorted by using the services of this node. The delivery nodes can demand the content from the original node which is one of the most effective functionalities of the content delivery network (CDN) process. The delivery node is one of the most important key components and the very essential aspect too. The user can demand the type of data and this is the responsibility of the deliver node of the content delivery network (CDN) to provide the appropriate data searched by the user. The only disadvantage in this process is sometimes data cannot be filtered due to low network connectivity or bandwidth so in this case user has to research the particular content which he or she wanted (Beck JL, 2020).

**Origin node** is the main source of the content delivery network (CDN) which is used to enable the content distribution across the entire network.

**The storage node** is used to store the information provided in the webserver. There can be different information or content that can be available from multiple webpages or web servers.

**The control node** is used to control the working of the content delivery network (CDN) so that the type of content delivery can be analyzed very effectively because in the process of the content delivery network (CDN) the content delivery process is very important and the content which is used to send by this internet service should be very appropriate as according to the search by the client (Dang N, 2020).

The service of the content delivery network (CDN) can be used in the process of web performance optimization also because the content delivery network (CDN) can increase the speed of web surfing by filtering the searched data so that the link will appear very fast and the performance of the web browser will get automatically increase and the optimization also get automatically started. Website speed optimization is very important because this process can provide a better web browser experience to the users. The speed over multiple digital platforms can easily be increase such as mobile platforms, tablet platforms, laptop platforms, desktop platform and many more.

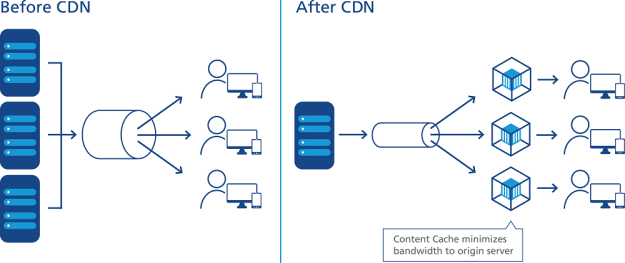


Figure 6: Comparison

The comparison diagram of the condition of before CDN and after CDN has clearly explained that after implementing the content delivery network (CDN) the number of users automatically increases because of the network speed increase (Patel V, 2020).

# Cache Poisoned Denial of Service (CPDoS)

In the process of computer security, the process of the content distribution network (CDN) is very important and very useful too but on the other hand, the concept of cache poisoned denial of services is the risk factor for the content distribution network (CDN) and the computer network functionality. The cache poisoned denial of services (CPDoS) is a new way of web cache poisoning attack. The aim of the cache poisoned denial of services is to disable the resources available on the website or the web browsers. Web caching used to enables the reuse of the services of the hypertext transfer protocol (HTTP) response. The aim of this HTTP response enables the process is to reduce the number of requests that reach the origin server, network traffic, and many other aspects. In the working of the web browser, the cache memory is most important because this is used to save the user’s access credential. Let us suppose we have logged into our G-mail account and a popup comes up which asks us to save the permanent password or not. If we click on yes then our login credentials automatically saved into the web browser but internally that login credentials automatically saved into our cache memory of the browser and this is the reason that this concept is very important in the implementation of the computer security. The cache poisoned denial of services use the HTTP header to operate their malware attacks (Nguyen HV, 2019).

**HTTP Header:**

HTTP header is a dynamic element of the HTTP protocol. In the implementation of the web browser to manage the request from a web browser to the response is managed by the HTTP header and the cache poisoned denial of services also works on the concept of HTTP header. These two components can be divided into two types such as:

* HTTP request header
* HTTP response header

Both the type of header is very important in the implementation of the web browser because both used in the process of information transferring from one source to another source. There are two components are available on which cache poisoned denial of services attack which is the webserver and content delivery network (CDN). The web server used to store the original content of the website and on the other hand, the content delivery network (CDN) used to store the copy of the cache memory of the website and the cache memory can be refreshed at a certain time only. This is one of the most important and very effective types of the implementation process and directly and indirectly connected or linked to the components of a content delivery network (CDN) and the webserver (Prabadevi V, 2019). In the modern internet world, the content delivery network (CDN) is the crucial part and needs to be very secure because this is used to send and transfer the content information resources from one end of the server to another end of the server. This is a very effective execution process of computer security. There are some other variations are also available of cache poisoned denial of services such as:

* HTTP header oversize (HHO)
* HTTP meta character (HMC)
* HTTP method override (HMO)

These all components have an impact on the implementation of the cache poisoned denial of services that are directly or indirectly connected to each other. The HHP has two-phase which are impact and mitigation. The HTTP header used to impact on the network layer of the webserver connectivity so that the speed of data transferring automatically decrease and this is one of the biggest challenge and the risk in the implementation of the cache poisoned denial of services. The working of the content delivery network (CDN) will get affected due to the process of cache poisoned denial of services and in the computer security system, this is one of the most important issues of the internet technology which is needed to be removed or recovered (Jeyanthi N, 2019).

**Cache poisoned denial of services (CPDoS) works on:**

1. This used to connect the website to an unknown content delivery network (CDN) to generate a new CDN entry.
2. The request of the attacker contains an oversized HTTP header so that multiple CDNs can connect at a single time. The CDNs allow the server to pass that HTTP header but there is no any security filter is available to filter or to analyze the content of the webpage or the web browser (Chatterjee M, 2019).
3. In the implementation of the web server, the oversized HTTP header creates an error on the webserver. By affecting the oversized HTTP header the webserver cannot be able to send the data packets and the server goes low automatically. This is one of the biggest issues of this functionality on the internet service. Most of the cybercriminals used to get the advantage of this error to down the server. The error page which occurred on the web browser is cached on the content delivery network (CDN).

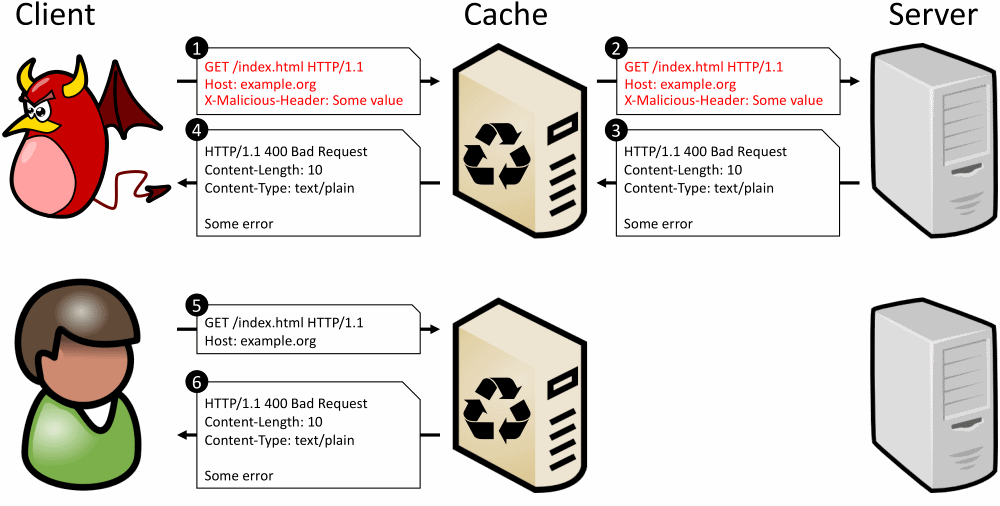


Figure 7: Attack of CPDoS

The given image is about the image explanation of cache poisoned denial of services and clearly defines the attacking functionality by differencing into client, cache, and server. These all components are directly or indirectly connected to each other and there are several implementation processes is available and every single implementation process is very effective in terms of internet service and computer security (Abraham A, 2020).

**The solution to the CPDoS Exploit:**

There can be some solution to this malware attack on the webserver and content delivery network (CDN). To examine the weakness of this exploit firstly we have to conduct a series of experiment and in this experiment, we should find out the reason of how to overcome very effectively. The exploit analyzing process includes the functionality of a practical environment. There should be a security layer implemented to the HTTP header of the web browser so that the network bandwidth of the web browser cannot be affected by the outside malware attacks or devices. The CND operates across a large geographical location and there are multiple web server locations are available and every single location is directly or indirectly connected to each other. This is used to summarize what pair of web caching systems and HTTP implemented in the process of the content management system.

**Future Preferences of CDN and CPDoS:**

There can be some future enhancement in CDN such as:

* Traffic will grow exponentially
* Consumer internet traffic will increase more by around 80%.
* Connected device will drive complexity
* CDN architectures will evolve
* Innovation and scale will drive success
* Content deliver echo system will grow to include new categories

There can be some future enhancement in CPDoS also such as:

* Application can be server less
* Application can be multitier
* The traffic or population growth will increase
* The hacking will reduce
* Route Poisoning will improve the complexity to the next level
* The problem of hidden route poisoning will be reduce

# Conclusion

The basic aim of this assignment was to describe every possible aspect of the computer security. Two concepts have been successfully describing which is CDN and CPDoS. CDN is one of the most important concepts in the process of computer security. In this assignment, every possible aspect of a content distribution network (CDN) has been successfully described and explained. This is used to send the content information from the web browser to the client’s computer system. There are multiple processes are includes and every single process is directly or indirectly connected to each other. The architecture of the CDN, working of CDN and key components of CDN has been successfully analyzed and explain in this assignment report. The error packer CPDoS has also been analyzed and explains in this assignment report which directly affects the services of the CDN and the web server or web browser.

# References

* Czarny, B., Mo, J., Rezafard, A. and Patt, D.M., OPSWAT Inc, 2020. *Computer security vulnerability assessment*. U.S. Patent 10,554,681.
* Cortier, V., 2020. Verification of Security Protocols (Invited Talk). In *28th EACSL Annual Conference on Computer Science Logic (CSL 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.
* Nukala, K.K.Y., Pullagura, V., Sahu, D., Sriramoju, J.C. and Vennapusa, L.P., CA Inc, 2020. *Generation of security policies for microsegmented computer networks*. U.S. Patent Application 15/999,552.
* Silva, F.A., Ruiz, L.B. and Loureiro, A.A., 2020, January. Content delivery in vehicular ad hoc networks. In *Anais do XXIX Concurso de Teses e Dissertações* (pp. 73-78). SBC.
* Giuliano, R., Mazzenga, F. and Vizzarri, A., 2020. Integration of Broadcaster and Telco Access Networks for Real Time/Live Events. *IEEE Transactions on Broadcasting*.
* Shattil, S.J., Genghiscomm Holdings LLC, 2020. *Content Delivery in Wireless Wide Area Networks*. U.S. Patent Application 16/569,033.
* Gonder, T., Helms, W.L., Gould, K., Chen, D., Chen, J., Yu, J., Dang, N. and Patel, V., Time Warner Cable Enterprises LLC, 2020. *Apparatus and methods for delivery of multicast and unicast content in a content delivery network*. U.S. Patent 10,531,161.
* Beck, J.L., Charter Communications Operating LLC, 2020. *Protocol and architecture for the decentralization of content delivery*. U.S. Patent 10,531,130.
* Nguyen, H.V., Iacono, L.L. and Federrath, H., 2019, November. Your Cache Has Fallen: Cache-Poisoned Denial-of-Service Attack. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1915-1936).
* Prabadevi, B., Jeyanthi, N., Udzi, N.I. and Nagamalai, D., 2019. Lattice Structural Analysis on Sniffing to Denial of Service Attacks. *International Journal of Computer Networks & Communications (IJCNC) Vol*, *11*.
* Prabadevi, B., Jeyanthi, N. and Abraham, A., 2020. An analysis of security solutions for ARP poisoning attacks and its effects on medical computing. *International Journal of System Assurance Engineering and Management*, *11*(1), pp.1-14.
* Roy, S., Morais, F.J.A., Salimitari, M. and Chatterjee, M., 2019, January. Cache attacks on blockchain based information centric networks: an experimental evaluation. In *Proceedings of the 20th International Conference on Distributed Computing and Networking* (pp. 134-142).
* Yu, Z., Xue, D., Fan, J. and Guo, C., 2020. DNSTSM: DNS Cache Resources Trusted Sharing Model Based on Consortium Blockchain. *IEEE Access*, *8*, pp.13640-13650.