**Cyber Security and Applied Cryptography Assignment**

Contents

[**Introduction:** 2](#_Toc187943712)

[**Approach:** 2](#_Toc187943713)

[**Research / Findings:** 3](#_Toc187943714)

[**Comparative Analysis:** 4](#_Toc187943715)

[**Security:** 4](#_Toc187943716)

[**Performance:** 4](#_Toc187943717)

[**Compatibility:** 5](#_Toc187943718)

[**Ease of Use and Maintenance:** 5](#_Toc187943719)

[**Use cases:** 5](#_Toc187943720)

[**Summary of protocol comparison:** 5](#_Toc187943721)

[**Detailed Technical Underpinning:** 6](#_Toc187943722)

[**Security software review:** 7](#_Toc187943723)

[**Use & analysis:** 9](#_Toc187943724)

[**Speed Test:** 9](#_Toc187943725)

[**DNS Leak Test:** 10](#_Toc187943726)

[**Security Test:** 10](#_Toc187943727)

[**Usability:** 11](#_Toc187943728)

[**Development of solutions:** 12](#_Toc187943729)

[**How OpenVPN addresses Gradgo’s vulnerabilities:** 12](#_Toc187943730)

[**Challenges:** 12](#_Toc187943731)

[**Conclusion:** 13](#_Toc187943732)

[**References:** 13](#_Toc187943733)

[**Appendices:** 13](#_Toc187943734)

# **Introduction:**

Gradgo, a graduate recruitment agency in Northampton, operates extensively on the internet to manage its business operations, making resilient data security an essential requirement. In todays interconnected online world, where the internet is integral to our everyday lives, protecting our online privacy and security is more important than ever.

Gradgo’s online activities, which likely includes handling sensitive candidate data, are vulnerable to several potential threats. These vulnerabilities may include data interception, unauthorised access through unsecured networks, phishing attempts, and even targeted cyber-attacks. Employees using public Wi-Fi hotspots, or remote working setups over unsecured channels further increases these risks.

Virtual Private Networks (VPNs) have become an essential technology to ensure secure and private online interactions, especially when using public or untrusted networks. VPN’s help protect us from some of the most common online everyday threats in cybersecurity, by protecting our sensitive information, maintaining our anonymity, and giving us greater control over our data.

As cyber-related threats become more sophisticated, and the demand for secure online communication grows, VPNs are becoming an increasingly important solution to our security needs. They provide protection for privacy, data integrity, and secure remote access, making them the perfect first line of defence on computer systems. This research paper aims to evaluate the effectiveness of VPN solutions for Gradgo, and how utilising these solutions could benefit their company’s security.

# **Approach:**

To effectively address the challenges faced by Gradco, first we must identify the specific vulnerabilities in their operations. As a recruitment agency, Gradco’s internet-based activities involved handling very sensitive data, which includes personal information about candidates, confidential communications with clients, and business documents. These everyday activities expose the company to various risks, such as data interception, unauthorised access, phishing, and compliance issues. Employees working remotely, possibly using public Wi-Fi, further increase these risks.

VPNs provide a solution to mitigate these vulnerabilities. VPNs route all internet traffic through encrypted tunnels, preventing interception during transmission, and ensuring the confidentiality and integrity of the data. VPNs also mask the organisation’s IP address by routing traffic through remote servers, improving anonymity and making it more difficult for hackers to target Gradgo’s systems. By establishing a secure, encrypted communication channel for the company, this protects sensitive data from being access by unauthorised individuals.

To evaluate the effectiveness of VPNs in addressing Gradgo’s vulnerabilities, a series of tests and research will be conducted. This includes a review of currently existing VPN technologies, a deep dive into the security features they offer, and how suitable they are for Gradgo. An experiment phase will then be conducted, in which a VPN solution, such as OpenVPN, will be deployed to test its encryption capabilities, performance, and resistance to common threats such as DNS leaks or man-in-the-middle attacks. These findings will then be used to create a detailed tailored VPN solution recommendation for Gradgo.

I will be deciding first on a VPN protocol for Gradgo to make use of, and from there will then decide the best way to execute its use, whether that be through a pre-existing VPN service, or via self-hosted means.

# **Research / Findings:**

Research into how VPNs work revealed several key insights into how VPN technology could address Gradgo’s cyber-security vulnerabilities:

The encryption protocols used by VPNs, such as AES-256, have been proven to provide protection against data interception. This means that the confidentiality of sensitive data, such as candidate records and client communications, is maintained even over public untrusted networks.

With the use of key-based encryption, VPNs create a secure channel of communication between the user, and any website or activity they perform. This means that even if an attacker happens to get onto the same network, they will not be able to decipher the traffic in the VPN as it will all be encrypted. This is important for Gradgo as it means any employees connecting to Gradgo systems remotely will not run the risk of having their data intercepted by malicious actors.

DNS leaks are an issue which can happen with VPNs, which means a suitable VPN in which this does not happen needs to be chosen for Gradgo. A DNS leak is a security flaw that occurs when requests are sent to an internet service provider’s DNS server even when the user is using a VPN to protect themselves.

A possible issue when using VPNs can be the performance impact. Due to VPNs rerouting your network traffic, it can negatively affect network performance, resulting in lower speeds. Free VPNs which often have many users all connected at the same time, are often very slow due to the load on the servers because of the number of clients connected. This means a suitable paid option or self-hosted option would need to be considered by Gradgo, so that the balance between security and performance makes the solution practical for daily operations.

As a company handling a large amount of sensitive data, Gradgo needs to be mindful of following all privacy laws such as the GDPR (General Data Protection Regulation). This states that all data must be stored with correct integrity and confidentiality. The use of VPNs within Gradgo ensures the secure handling of sensitive information, which demonstrates Gradgo’s commitment to maintaining data protection compliance.

While VPNs are highly effective in securing data, it requires proper configuration and ongoing maintenance to ensure continued protection. This also means that employees need to be trained in using the systems to maximise the benefits of the technology and to prevent its misuse.

These findings highlight the significant role that VPNs could play in enhancing Gradgo’s security. By providing secure remote access, protecting against vulnerabilities, and ensuring regulatory compliance, VPNs offer a comprehensive solution for Gradgo’s needs. In the section following this, I will compare different VPN protocols to determine the best option for Gradgo.

# **Comparative Analysis:**

For Gradgo’s needs, there are three big VPN solutions which I am going to compare, based on their security, performance, compatibility, maintenance, and use cases, to ultimately decide on a final solution which will then be tested further to evaluate the effectiveness of said solution for Gradgo’s needs. These solutions are: OpenVPN, WireGuard, and IPSec/IKEv2.

## **Security:**

OpenVPN – Highly secure, using AES-256 encryption and multiple cryptographic algorithms. It’s open-source nature allows continuous improvements and transparency.

WireGuard – Uses modern cryptography, such as ChaCha20 and Poly1305, for lightweight yet robust security. Smaller codebase minimises vulnerabilities.

IPSec/IKEv2 – Strong security when configured with AES-256 encryption. Often paired with certificates for authentication.

## **Performance:**

OpenVPN – Reliable, however, slower due to extensive encryption. Suitable for high-security environments where speed is second to security.

WireGuard – Outperforms both other protocols in speed due to its lightweight design and efficient handling of encryption. The fastest option of the three.

IPSec/IKEv2 – Faster than OpenVPN, but slower than WireGuard, especially over mobile networks. However, its ability to quickly reconnect makes it ideal for devices switching between networks frequently.

## **Compatibility:**

OpenVPN – Compatible with most platforms and supports UDP and TCP protocols. However, it does require third-party software for some platforms.

WireGuard – Growing support across platforms. Is easier to set up but still growing in enterprise environments which makes it not as good of a fit in these cases *yet*.

IPSec/IKEv2 – Widely supported by native device clients, including Windows, macOS, iOS, and Android.

## **Ease of Use and Maintenance:**

OpenVPN – Difficult to configure and maintain, but the extensive customisation options that are available make it adaptable.

WireGuard – Simple and very easy to configure, with minimal maintenance required.

IPSec/IKEv2 – Medium difficulty to configure, but benefits from native support on most devices.

## **Use cases:**

OpenVPN – Suitable for environments which require high security, such as business networks and remote work setups.

WireGuard – Best for cases where performance is key, such as mobile devices or applications where latency is critical.

IPSec/IKEv2 – Suitable for mobile users and areas that require stable, fast connections with minimal setup.

## **Summary of protocol comparison:**

OpenVPN offers great security and versatility, making it an incredibly reliable choice for Gradgo’s operations involving sensitive data. However, it may require more expertise to configure and manage, meaning additional staff may need to be hired.

WireGuard stands out for its speed and simplicity, making it a great choice for environments where performance is important. Its smaller codebase also reduces potential vulnerabilities.

IPSec/IKEv2 provides a balance of security and speed, with excellent support for mobile users.

With all these facts in mind, OpenVPN is the chosen solution for Gradgo, due to the amount of sensitive data Gradgo deal with daily, and the need to protect it, without a massive emphasis on speed.

# **Detailed Technical Underpinning:**

The following is a detailed chronological step by step explanation on how VPNs work.

VPN stands for Virtual Private Network. It is a service that establishes a digital connection between your own computer, and a remote server owned by a VPN provider. This creates a tunnel that encrypts your personal data, masks your IP address, and ensures your online experiences are private. The three main goals of a VPN are to maintain confidentiality, integrity, and availability.

A VPN works by first encrypting all data you are sending when connected to your network via whichever client software you are using. In the case of OpenVPN, the AES-256 encryption algorithm is used. This is a highly secure algorithm that uses a 256-bit key to scramble data into an unreadable form. It is a symmetric key form of encryption, meaning it uses the same key for both encryption and decryption, usually via methods like RSA, or the Elliptic Curve Diffie-Hellman, to securely exchange symmetric keys. This ensures that only authorised individuals with the correct key can access the data. A single block is composed of 16 bytes, which is a 4x4 matrix. Each byte has 8 bits in it, adding up to create a block of 128 bits. The AES algorithm is then applied to every block, encrypting the data piece by piece. AES-256 is virtually uncrackable using any brute-force method. It would take millions of years to break it using currently available technology and capabilities.

All the encrypted data is then sent through a secure tunnel to the VPN server. A VPN tunnel is a secure encrypted connection between a device and a VPN server that protects the data transferring over the internet by encapsulating data packets inside another protocol, hiding their original contents.

Since your request data is being routed through the remote VPN servers, it means your IP address is essentially being replaced by the IP address of the server you are connected to. This means that whenever the data you are sending reaches a website, it looks as if the request has come from the VPN server, and not you. From the perspective of the website you are visiting, it is as if your network is not in the equation at all.

Next, using the same encryption methods that were used to encrypt your initial requests, the VPN server takes the information send from the website you are trying to access, encrypts it, and then sends it back to you via the secure tunnel. The VPN service client you are using, then decrypts the data received from the VPN server, allowing you to access the content.

This whole process ensures that your internet activities are completely hidden from your internet service provider, the websites you visit, and any potential malicious actors attempting to eavesdrop on your activities. They are all unable to see your real IP address, the websites you are accessing, and the data that is being sent and received. Instead, all that they can see is the VPN server’s IP address and encrypted traffic.

Performance needs to be taken into consideration when using a VPN. Because your computer is having to encrypt data before it is sent, and decrypt it once it is sent back, this process can increase CPU usage and cause latency. Encryption protocols like AES-256 which are high in strength, while very secure, are likely to put a larger burden on your CPU compared to weaker encryption methods. The added overhead of encryption and tunnelling can consume more bandwidth too, which can cause issues in tasks that already consume high amounts of bandwidth such as video streaming or transferring large files.

A pressing threat which VPNs protect you from are man-in-the-middle attacks (MITM). MITM attacks occur when a malicious actor intercepts communications between two parties without their knowledge. This is often done to either obtain/modify data, or to impersonate one of the parties. By encrypting all data being transmitted between the user and the VPN server, even if an attacker was to intercept the data, the encryption renders it unreadable and therefore useless. OpenVPN uses TLS/SSL protocols, which includes authentication to verify the integrity of the communication channel, further preventing interception.

DNS (Domain Name System) leaks are one of the largest risks when it comes to using VPNs, because if a VPN is unable to prevent them effectively, the VPN becomes useless for the user. DNS leaks occur when DNS queries, which are used to translate domain names into IP addresses, bypass the secure VPN tunnel, meaning that they are sent directly to your Internet Service Provider. This exposes your browsing activity, defeating the purpose of the VPN. To prevent this, most VPNs will route DNS queries through their own encrypted tunnels, ensuring that the queries do not leak to external DNS resolvers. You can test for DNS leaks yourself by using online tools such as dnsleaktest.com. A correctly configured and working VPN should show the DNS server associated with the VPN provider instead of the one associated with your ISP.

# **Security software review:**

As stated at the end of the comparative analysis section, my chosen VPN solution for Gradgo is OpenVPN. This is for several reasons.

Firstly, when choosing a VPN solution there was the choice between self-hosting a VPN protocol or using one of the many VPN services that provide entire VPN software packages for you. These VPN services are typically aimed at the regular consumer, simplified greatly so that anyone without knowledge of VPNs can use the software. They tend to have less customisation, are far more simplistic, and can have larger performance impacts due to the frequency of other individuals using the same service. VPN protocols are what each VPN provider uses to run their VPN, and there are many open-source protocols available to the public, such as OpenVPN. Gradgo hosting their own VPN allows for more control, customisation, and exclusive use of their own service. While this is greatly beneficial for their individual needs, it means that there will need to be staff who have the knowledge and skills required to set it up and maintain it.

OpenVPN is an open-source VPN protocol that utilises SSL/TLS protocols for encryption and secure key exchange. It is compatible with a wide range of platforms, making it highly versatile for Gradgo, allowing employees to access it regardless of the device they are using. OpenVPN relies on the OpenSSL library, which supports encryption algorithms such as AES-256. It uses SSL/TLS certificates for server authentication and client authentication. It also supports multi-factor authentication and various different credential management systems. OpenVPN encapsulates data packets through an encrypted tunnel using the UDP or TCP transport protocols. OpenVPN is highly customisable. Administrators can configure OpenVPN to operate on almost any port, and allows advanced configurations, such as split tunnelling, load balancing, and multiple levels of encryption.

OpenVPN is designed to resist common attacks, such as man-in-the-middle, by ensuring authentication between the client and server. By properly configuring OpenVPN, DNS and IPv6 leaks can be prevented, ensuring anonymity for users.

While OpenVPN is highly secure, its performance can vary based on configuration. As stated previously, the use of AES-256 can add latency, although this is often negligible for most use cases, especially when self-hosting, with less traffic going to the VPN than when using a public VPN service. The overall performance, however, will be influenced by server processing power, network bandwidth, and the number of connected users. Therefore, the type of server may need to be scaled accordingly. The choice of a self-hosted server, or Virtual Private Server (VPS) will be discussed in more detail later.

Overall, OpenVPN is an excellent choice for Gradgo for several reasons. Gradgo handles sensitive personal data, including candidate information, resumes, contact details, and clients’ confidential requirements. OpenVPN’s use of AES-256 ensures that this data remains secure during transmission. Gradgo employees likely need to access internal systems remotely. With the upwards trend towards hybrid or remote working environments. OpenVPN supports secure remote access by creating an encrypted connection between remote users and the company’s internal network. OpenVPN can also be deployed on a wide variety of platforms, from cloud-based virtual private servers to on-premises servers. This flexibility allows Gradgo to adapt the solution to their budget and needs. Finally, OpenVPN is highly scalable for Gradgo, in both directions. If Gradgo gets bigger and they need to scale up their operation, their OpenVPN system can be scaled up accordingly. On the other end, if for whatever reason, Gradgo need to scale down, this can also be done, especially when using virtual private servers.

# **Use & analysis:**

Gradgo has a few options when it comes to setting up OpenVPN. The option that I have opted for, which I also think is the best choice for Gradgo, is hosting the VPN themselves on a Virtual Private Server (VPS). I happen to own a VPS currently already, so I downloaded the OpenVPN access server onto my VPS and have a working VPN connection based in the Netherlands.

For installing OpenVPN, once a VPS has been purchased from a hosting provider (I recommend Hostinger, as they have a one-click installation method when setting up the VPS) make sure to update the VPS’ operating system, and there are many OpenVPN installation scrips available on GitHub for a one-click setup. These scripts simplify the installation process by automating configuration tasks. Once configured to your desired protocol and port number, client configuration files can be generated for each user. These files will include the required credentials and encryption keys to connect to the VPN. Any user who would like to use the VPN then simply downloads the OpenVPN connect client, inputs their login credentials, and can toggle the VPN on and off whenever they please.

From here, now that I have set up my own OpenVPN system, I will conduct several tests to evaluate the performance and security of the OpenVPN solution. All tests will be ran on the same desktop used to connect to the OpenVPN client, showing performance and security both with and without the VPN connected.

## **Speed Test:**

Using Google’s internet speed test tool, the following results were gained:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Mbps Download | Mbps Upload | Latency (ms) |
| No VPN | 458 | 197 | 12 |
| OpenVPN enabled | 103 | 140 | 22 |

From these results, we can see that there was roughly a 78% decrease in download speed, 29% decrease in upload speed, and an 83% increase in latency. While on paper this looks like a large speed impact, the reason for such a large decrease in speed is for multiple reasons. Firstly, the internet connection I am using to conduct this test is very fast, and secondly, there may be a limit to the amount of bandwidth that one device can use at a time on the VPS. This means that a device with a download speed of 200Mbps, may not necessarily see a 78% decrease too, it may just decrease to around the same 103Mbps level of this conducted test. The VPS I used to host OpenVPN was very cheap as it is made for personal use since I am the sole user. Gradgo is likely to spend much more on a larger scale VPS system, meaning these speed impacts should not be as drastic.

## **DNS Leak Test:**

Using the website dnsleaktest.com, the next test will cover whether the VPN is correctly routing all DNS queries through the VPN and not outside of the secure tunnel. When running the test with no VPN enabled, it can detect the IP, ISP, and country that I am connecting to the website from.

A screenshot of a computer

Description automatically generated

As seen in the image above, with the VPN enabled, it is successfully routing all DNS traffic through the VPN tunnel, resulting in the IP, ISP, and country shown in the test, being that of my server, and not the desktop using the VPN.

## **Security Test:**

The next test will be using Wireshark to determine if data sent and received when the VPN is running is correctly encrypted. To test this, the VPN will be turned on, Wireshark will start recording, normal internet browsing will be done for a few minutes, including some downloads, and then the recorded packets will be analysed.

A screenshot of a computer screen

Description automatically generated

As you can see, when analysing the packets associated with the OpenVPN protocol (Typically UDP packets on the default 1194 UDP port configured for OpenVPN) the packet information is completely unreadable, meaning that all the data being sent and received, is correctly encrypted, and nobody can do anything with it. Even if a man-in-the-middle attack was successful, they would not be able to do anything with this data.

## **Usability:**

OpenVPN is extremely intuitive, and offers a high degree of usability, even for individuals with limited technical expertise in managing and setting up VPNs. Many VPS services offer one-click installation options for the OpenVPN server, making setup incredibly easy if you have just bought a new VPS. Even if the service you are using does not offer that, there are many one-click install scripts available online from reputable sources.

The configuration process for the OpenVPN server is made significantly easier by the availability of an extremely intuitive online graphical user interface system provided by the OpenVPN Access Server.

As a user, OpenVPN is also straightforward and easy to use. The OpenVPN Connect software, available for almost all major operating systems and mobile platforms, makes it simple to connect to your VPN server. Administrators can make the onboarding process easier by generating a configuration file specific to the user, which when sent to the user and imported into OpenVPN Connect, immediately logs them in and sets up their connection for them. There is also the option to manually input server details to log into the VPN system. Once done, it is as simple as pressing a toggle, and the VPN is turned on.

# **Development of solutions:**

Based on the findings and analysis conducted throughout this report, OpenVPN is the most suitable VPN solution for Gradgo. It stands out for is strong encryption standards, and ease of deployment. Additionally, its ability to run on a wide variety of platforms, and its intuitive online GUI for setup and configuration, make it highly usable, even with limited to no training.

For deployment instructions, refer to the OpenVPN documentation at openvpn.net, and my brief explanation on deployment in the use & analysis section of this report.

## **How OpenVPN addresses Gradgo’s vulnerabilities:**

OpenVPN successfully encrypts all data traffic, preventing Gradgo’s sensitive candidate and client information and communications from being intercepted.

OpenVPN successfully masks Gradgo’s IP addresses and ensures DNS requests are routed securely through the VPN.

OpenVPN allows employees to securely connect to Gradgo’s internal systems from any location, ensuring that they can work while minimising security risks.

Using OpenVPN demonstrates Gradgo’s commitment to data protection and complying with regulations such as GDPR.

## **Challenges:**

Costs – While VPS hosting and OpenVPN licensing are not free, the costs are relatively low compared to enterprise VPN solutions available. Gradgo can also start with a basic VPS plan and scale up based on bandwidth and user requirements.

Setup and maintenance – The initial setup requires some technical expertise, but OpenVPN Access Server and the many available one-click configuration options do simplify this process. However, for long term upkeep, it would be beneficial to hire someone with technical experience in maintaining a system like this, to ensure that it runs smoothly and does not disrupt business operations.

User adoption – Employees unfamiliar with VPNs may find their use confusing. This can be mitigated through clear communication about the reasoning behind its use, and proper training, if necessary, on how to use them.

Performance – VPN usage will introduce latency. To combat this, make sure that the server is being hosted on a reliable VPS with sufficient resources.

# **Conclusion:**

Cyber security threats are constantly evolving. To ensure the safety of sensitive data and to stay operational, companies like Gradgo will have to adopt VPNs and other security solutions. This paper has explored the critical vulnerabilities faced by Gradgo as a graduate recruitment agency and assessed how Virtual Private Network technology can effectively address these concerns.

The proposed implementation plan contains a systematic approach for Gradgo to deploy OpenVPN, allowing them to enhance their cybersecurity posture while maintaining ease of use for its team.

Investing in cybersecurity is now a necessity in our ever-evolving digital world. OpenVPN will allow Gradgo to confidently navigate the constantly changing challenges of online business operations, while maintaining their security, privacy, and long-term success.

# **References:**

<https://openvpn.net/>

<https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/>

<https://www.fortinet.com/uk/resources/cyberglossary/dns-leak#:~:text=A%20standard%20DNS%20leak%20can,connect%20to%20the%20user's%20ISP>.

<https://gdpr-info.eu/>

Ahman, Farhan et al. (2018-11) Main-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers’ Strategies. Sensors. **18**(11), pp.4040.

# **Appendices:**

**AI acknowledgement:**

I acknowledge the use of GenAI tools in line with the University Of Northampton’s GenAI policy, Category 2.

**1. Structuring or planning your assessment.**

N/A

**2. Writing style or tone.**

I used ChatGPT to check for spelling, punctuation, and grammar errors, and to help rephrase sentences where I had reused the same word or idea multiple times.

**3. Summarising content.**

I use ChatGPT to help provide context behind some of the requirements given to me on the brief, as there were lots of parts within the recommended paper structure which did not make sense / needed more explanation as to what was being asked of me.

**4. Analysis.**

N/A

**5. Ideas, concepts and arguments.**

I used ChatGPT to help explain what should go in certain sections in which the provided section headings were unclear.

**6. Content**

N/A