NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 2, Issue – 1, June 2023
E-ISSN - 2583-7559

Cybersecurity Threats Mitigation and Preventive Strategies amid COVID-19 Pandemic

Naveen Kumar Chaudhary, National Forensic Sciences University, Gandhinagar, Gujarat, India
(naveen.chaudhary@nfsu.ac.in)

Abstract— **The COVID-19 pandemic is an immense humanitarian crisis that has severely affected the society and the global economy. The rapid and unexpectedly broad disruption to businesses around the world has left companies struggling to maintain security and business continuity. There is an increased reliance on digital platform for day-to-day activities due to the imposition of lockdown, social distancing and stay-at-home orders. The cyber criminals are taking advantage of the pandemic situation and targeting people and businesses. Cyber security has taken a center stage amid COVID-19 pandemic. This paper discusses the cyber security threats the world is facing in this unprecedented crisis. The associated technical and security challenges and suggests suitable mitigation and prevention strategies that include building a secure peer-to-peer virtual private network for remote access based on an open source software platform.**

Index Terms— **COVID-19, cyber security, cyber threat, cyber-criminals, digital platform, digital security risk, work from home, remote access domain, user domain, VPN.**

1. INTRODUCTION

There was no prediction of COVID-19 and the world was not prepared to handle this pandemic on its outbreak. The pandemic that started in 2019 quickly spread across the globe and it became a global crisis. The pandemic caused a situation of acute medical and economic emergency in many countries and affected the routine life and business management [1]. As per the World Health Organisation (WHO) timeline, the first case of COVID-19 was identified on 31 December 2019 in Wuhan, China and the first case outside China was reported on 13 January 2020, in Thailand [2]. The WHO declared COVID-19, as a 'public health emergency of international significance' on 30 January 2020 [3]. The virus that causes COVID-19, has been classified as Severe Acute Respiratory Syndrome Coronavirus 2(SARS-CoV-2) [4]. In the past, there have been worse pandemics, such as Bubonic Plague, Small Pox and the Spanish Flu that killed millions of people, however their global impact was limited as communication and connectivity was not so evolved at that time [5]. The emergence of pandemic related cyber security threats is not a new trend. Ebola related cyber security threats also surfaced at its outbreak, however, the impact of such cyber threats were limited as this pandemic was mostly isolated to West Africa [6]. COVID-19 is an airborne virus that spreads through contaminated objects, surfaces and person-to-person [7]. It spreads quickly through the infected person in the absence of necessary precautionary measures. As per the WHO's COVID-19 dashboard, there were more than 18 million confirmed cases in the first week of August 2020 globally [8]. In India itself, there were more than 2 million confirmed cases in the first week of August 2020 due to COVID-19 infection [9]. The situation does not seem to improve until majority of the population is vaccinated. COVID-19 pandemic has posed many serious challenges, primarily due to its global spread out and non-availability of any effective vaccine in the beginning. The research and development work on the vaccine is on the fast track in many countries. The countries are imposing lockdown and issuing advisories to follow 'social distancing' and 'work from home' to manage the spread of the disease. The people are working from home and preferring digital mode of business to manage day-to-day activities and run their businesses. This has changed the way people live their lives and manage the routine business. There is a greater reliance on digital platform and 'online' is the new normal. Unfortunately, cyber-criminals who are always in the lookout for opportunities to target the victims for financial gains and promote their ill-intended motives are taking advantage of the situation. There is a rise in the cyber security incidents related to COVID-19 and the cyber agencies across the globe are facing difficulties in managing the cyber threats.

2. CYBER SECURITY LANDSCAPE

2.1 Digital Security Risks

The increased reliance on 'online' to conduct the business through digital platform and 'work from home policy' has heightened the digital security risk. The digital information channels, social media platforms, video streaming and cloud services

, e-mail services, conference calls and video conferencing tools are being used much more than ever before and at a much larger scale [10, 11]. The people are required to work online and many of them are working from the home. This has enlarged the less well-protected IT surface. The more intense use of internet to carry on digital online activities by the new and in-experienced users are further creating more opportunities for the cyber criminals [12]. The office premises have better cyber security arrangements. It is protected by perimeter and end point cyber security solutions. The cyber security of the enterprise is governed by their cyber security plan, which comprises of cyber security policy and crisis management plan. This kind of cyber security arrangement one does not find while working in the home environment. The home user if not aware of basic cyber security hygiene such as regular patch management, antivirus protection and safe computing practices, may put system as well as data to risk. Besides that, if user works on sensitive data while in home using unprotected or vulnerable personal computer, it increases the risk of opening the doors to hackers. The society-wide shift amid COVID-19 pandemic towards remote working has increased the cyber risk.

2.2 Cyber Security Threats

The advancement in ICT technology has set new bar for the cyber security and it has become now more challenging than ever before. The cyber criminals take advantage of emergencies and crisis, especially when there are uncertainties and people are frightened. The outbreak of COVID-19 pandemic is no different. The bad actors are using COVID-19 as a tool for their malicious deeds and they are targeting victims with varied attack tactics. There exists numerous taxonomies relating to attacks and cyber-crimes [13,14,15,16]. The UK's Crown Prosecution Service(CPS) categorises cyber-crime in two parts; cyber dependent and cyber enabled crimes[17]. A cyber dependent crime is an offence that can be committed using a computer, computer networks or other form of information communications technology [18]. A cyber-enabled crime is a traditional crime that can be increased in its scale or reach by use of computers, computers networks or other forms of information communication technology[19]. These two categories are summarized in table 1.

Table 1:Categorization of cyber crime

Cyber Crime	
Cyber dependent crime	**Cyber enabled crime**
Hacking	Financial Fraud
Malware	Phishing
Denial of Service	Pharming
Distributed Denial of Service	Extortion

The migration of people, business and process on digital platform has also given rise to high rate of cyber-crimes. There is a prediction that cyber-crime will grow more in the future and by 2021, it will touch the figure of $ 6 trillion [20].The traditional crime triangle can also describe the cyber-crime, as it specifies that for the cyber-crime to happen three factors have to exist; a victim, a motive and an opportunity [21]. The victim is the target of the attack, motive is the aspect that drives attacker to launch the attack and opportunity is the chance to commit the attack. The cyber-attack tactics has grown as a full-fledged domain and cyberspace is now recognised as the fifth realm of the warfare. The asymmetric nature of cyber-attack makes it quite a potent weapon for state and non-state actors. The countries with advanced technology and cyber skilled work force are developing offensive capabilities in cyber domain. These days it is common to read cyber offensive related news whenever the relationship between two countries turn strained due to geo-political reasons. The steep rise in the confirmed COVID-19 cases with its declaration as a pandemic is a major concern for many countries. A few countries have demanded for a greater accountability in this time of unprecedented situation. This has led to a diplomatic war between some countries and escalated alleged cyber-attacks targeting their ICT and Critical Information Infrastructure (CII). Australia in June 2020 alleged the involvement of state based cyber actor in launching malicious attack against its institutions, including health, critical infrastructure and essential services holding sensitive economic and personal data [22]. UK's National Cyber Security Centre alleged in July 2020 that the hackers have hindered their COVID-19 vaccine research [23]. USA also alleged that the state sponsored hackers are targeting US labs that are working on COVID-19 vaccine development [23]. Canada's Communications Security Establishment (CSE) has also alleged the role of cyber espionage group in hindering their vaccine research [23]. WHO reported a dramatic increase in cyber-attacks against their employees who handled COVID-19 related information [24]. The trend of Scammers impersonating WHO in emails increased and targeted the victims to channel donations to a fictitious fund and not the authentic fund repository [24]. WHO reported fivefold increase in cyber-attacks in April 2020 as compared to numbers that were observed in the same period last year [24]. The COVID-19 at the time of outbreak had immense psychological impact on the humans as not much information about this infection was available and people searched internet to find information about this pandemic. This also resulted in the rise of 'COVID' or 'corona' related domain registration with malicious intent. Palo Alto discovered, 2,022 malicious and 40,261 high-risk newly registered domains by the end of March [25]. Since the beginning of the outbreak, 90,284 new corona related domains have been registered globally [26]. The phishing attack also saw a steep rise through malicious emails and fake websites. The attackers enticed victims into opening malicious attachments or clicking phishing links. This resulted in identity impersonation and illegal access to personal accounts of the victims. The Trend Micro has linked one million spam messages to COVID-19, since January 2020 [25]. The cyber criminals spoofed supplier and client email addresses and used nearly identical email addresses to conduct Business Email Compromise attacks [25]. A report published on 24 May revealed that 2.9 crore Indian jobseekers data was released on one of the hacking forums on the dark web for free [27]. The websites have also became a vulnerable target amid the COVID-19 pandemic. Many fake websites with nearly similar sounding names surfaced soon after the announcement of PM-CARE fund in India [28, 29]. The trend of fake campaigns and disinformation in the garb of COVID-19 saw a huge surge [30]. The Brno University Hospital in the city of Brno, Czech Republic, in the middle of a COVID-19 outbreak was hit by a ransomware attack on 12 - 13 March 2020 [31]. The malware attack resulted in postponement of surgeries, shifting of patients in other hospitals and deactivating of IT systems [32]. K7 Threat Labs reported 260% surge in COVID-19 related cyber threats in India during the lockdown period from the last week of March to the first week of April 2020 [33]. As per the K7 Threat Labs reports, 'Phishing emails' were the most popular attack vector, and these emails were crafted with COVID-19 theme based messages. These malicious emails were circulated with malicious links and attachments carrying ransomware, Remote Access Trojans, Cryptominers, in the name of trusted organisations [34]. Twitter hack on 15 July 2020 is one of the highly publicised attack amid COVID-19 pandemic. The attacker hacked into the accounts of several celebrities, business executives, companies and politicians and conned people into sending bitcoin to an account [35]. Cyber security threat landscape amid COVID-19 pandemic has increased primarily because of two reasons; firstly 'work from home' policy implemented by most of the sectors and secondly the 'fear of pandemic' among people in the affected countries.

3. Technical and Security Challenges

Most of the organisations were unprepared to tackle the cyber security challenges that emerged with the outbreak of COVID-19 pandemic. The technical issues entailed that organisations, digital network operators and software developers should implement the necessary changes in a time bound manner ensuring continuity of business and level of required security. In many cases, the major challenge emerged due to the increased traffic load. The applications and networks not designed to handle the increased traffic load behaved erratically. The 'work from home' policy not only exposed firms to increased security risks and online frauds but also raised concerns over the resilience of the ICT infrastructure that supports the digital internet traffic. The Internet Service Providers(ISPs), Virtual Private Network (VPN) operators and Cloud service providers are facing unprecedented challenges to manage the demand and provide hassle free services. With the imposed lockdown, social-distancing, self-isolation and quarantines amid COVID-19 pandemic the reliance on audio and video conferencing has increased manifold to ensure the continuity of work and business. There are various platforms available for videoconferencing; Zoom, Skype, Microsoft Teams, Google Meet and WebEx. The number of daily meeting participants using Zoom videoconferencing tool increased from 10 million to 200 million from Dec 2019 to March 2020 [36]. There have been incidents when the uninvited participants have disrupted the business meetings by interjecting inappropriate languages, hateful and pornographic images [37]. Some of the videoconferencing applications allegedly exaggerated their encryption facility [36]. There have been incidents of sharing the subscriber data to social networking platform for advertisement disregarding the subscribers' privacy [36]. The inadequate user privacy policy of the videoconferencing platform gives rise to serious concerns regarding data privacy. The consumer report recently analysed the privacy policies of Microsoft Team, Google meet and Zoom and concluded that they are collecting more data then what people realise [38]. Some of the companies and countries have raised serious concerns regarding some of the popular video conferencing platforms default security settings [39]. Many countries are capturing citizen data to keep track of their movement and proximity to COVID-19 infected person. This data if breached by cyber criminals will jeopardize the individual's privacy. The state sponsored actors on espionage missions are taking advantage of COVID-19 pandemic to break into Government and Corporate IT systems. An Advanced Persistent Threat is a sophisticated hacking group that uses malware to target the victim. APT's may be backed by state or a non-state cyber actors. An APT nicknamed 'Vicious Panda' was crafted in March 2020 to attack Mongolian public sector organisations [31]. APT nicknamed 'Mustang Panda' used malware infected Microsoft word documents relating it to COVID-19, targeted Vietnamese, Taiwanese and Fillipino entities via email [31]. The varied nature of security challenges that world is facing during the COVID-19 pandemic was not seen in the earlier major pandemics that the world has faced so far. The organisations have to ensure aligning their security controls to tackle the varied nature of cyber threats imposed by COVID-19 pandemic. This entails relooking at the cyber security posture of all the seven domains of the IT infrastructure, that are; 'User Domain', Workstation Domain', 'LAN Domain', 'LAN-to-WAN-Domain', 'WAN Domain', 'Remote Access Domain' and 'System' Domain. The evaluation of gaps and optimization of all the seven domains in-line with organisational security policy.

4. Cyber Threats Mitigation and Prevention Strategies

People, Process and Technology are the three important resource pillars for maintaining the cyber security. In order to optimize the three resource pillars effectively for maintaining the healthy cyber security posture, every organization has to evolve their cyber security plan. The cyber security plan should comprise of cyber security policy and cyber crisis management plan. The important resource pillars of the cyber security were 'office premise' centric prior to COVID-19 pandemic outbreak and many of the organizations have not catered for situation like 'work from home' in their cyber security plan. The organisations that used to conduct business from a single central location or a small number of locations are finding themselves spread out at many locations. This makes security of 'Remote Access Domain' important. The 'Remote Access Domain' is one of the domains within the seven domains of a typical IT infrastructure and it comprises of the authorized users who access organization resources remotely. The access usually occurs over unsecured transports such as the internet while 'working from home' or travelling. The major security concern over the remote access is data privacy. This means that only authorized users should view or modify the data. Encryption is the most common control to protect data privacy in an untrusted environment. The strategy may include application data encryption, application connection encryption and system connection encryption. The common compliance controls that could be ensured in the 'Remote Access Domain' are shown in table 2.

Table 2: Common compliance control in the Remote Access Domain

Control Type	Components
Preventive	Proxy server, Firewalls, Intrusion Detection System, Intrusion Prevention System, User based Access Control System and Configuration change control.
Detective	Performance monitoring, traffic analysis, configuration settings monitoring and Vulnerability Assessment & Penetration Testing.
Corrective	VPN, attack intervention, business continuity and disaster recovery planning.

Virtual Private Network (VPN) provides solution for remote access as it creates encrypted communication tunnel over a public network. VPN is one of the control measures to reduce the risk, however it also has its own vulnerabilities. The major issue is user's authentication with the VPN. An attacker may gain access to the organisation's data by knowing or guessing the authorized user's VPN credentials. This kind of security vulnerability can be mitigated by applying two-factor VPN authentication. The organisations need to secure their 'Remote Access Domain' by developing a plan and selecting the right security controls. Besides that, the 'User Domain' that covers the end users of the information system have significant role to play. This domain primarily considers the role and responsibilities of the users and generally covers Acceptable Use Policy (AUP), system access policy, internet access policy and e-mail policy, however considering the awareness level that is required to handle the cyber security challenges, the organisations may consider including COVID-19 cyber awareness policy. The policy should be framed keeping the global landscape on COVID-19 cyber threat and point out specific precautionary and remedial measures against 'malicious domains', 'online scams', 'phishing', 'data harvesting malware' and 'disruptive malware (DOS/DDoS and ransomware). The users at all the levels should be encouraged to practice good cyber hygiene in general, including; software and anti-virus patch management, good password protection, enabling multi-factor authentication and installation of application from the genuine authorized repository. The advisories on safe videoconferencing measure, data privacy, important case studies with lessons learnt should be issued on a regular basis to promote cyber security awareness culture. Tabletop exercises on COVID-19 cyber security theme to be planned regularly by the organisations to evaluate their incident response, business continuity and disaster recovery plan.

5. SECURE REMOTE ACCESS BASED ON AN OPEN SOURCE SOFTWARE PLATFORM

A secure remote access using WireGuard VPN has been successfully implemented to access the Server from the remote client. WireGuard is a cross-platform communication protocol that uses free and open source software for implementing encrypted virtual private network. WireGuard uses modern cryptography peer reviewed cryptographic primitives. Curve2519 with elliptic curve Diffie-Hellman (ECDH) is used for key exchange and Chacha for symmetric encryption with Poly 1305 for message authentication [40]. WireGuard supports pre-shared key mode and uses UDP protocol for transportation. The software was initially developed for the Linux kernel but it supports cross platform implementation. The WireGuard interface has private key, listening UDP port, list of peers, public key, list of associated tunnel IPs, an endpoint IP and port that identifies the peer. The fundamental concept of WireGuard is based on a Cryptokey routing that is an association between public keys of peers and the IP addresses that those peers are allowed to use. The concept of Cryptokey routing is shown in figure 1. The session key exchange process of the WireGuard that takes place between the server and client is shown in figure 2.

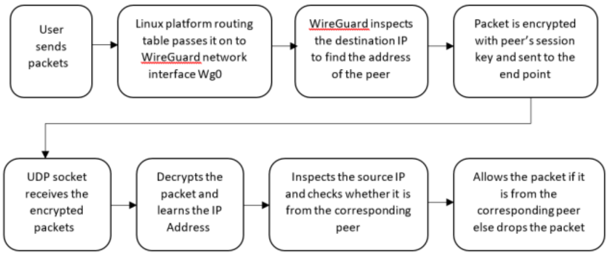

User sends packets
Linux platform routing table passes it on to WireGuard network interface Wg0
WireGuard inspects the destination IP to find the address of the peer
Packet is encrypted with peer's session key and sent to the end point
UDP socket receives the encrypted packets
Decrypts the packet and learns the IP Address
Inspects the source IP and checks whether it is from the corresponding peer
Allows the packet if it is from the corresponding peer else drops the packet

Figure 1. Cryptokey Routing

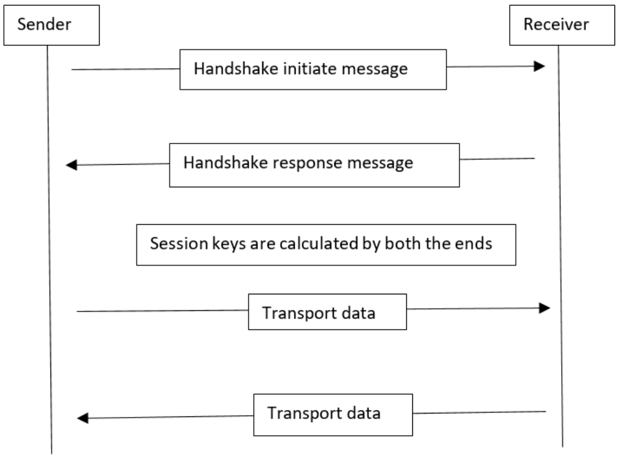

Sender
Receiver
Handshake initiate message
Handshake response message
Session keys are calculated by both the ends
Transport data
Transport data

Figure 2. Session key exchange process.

The WireGuard peer-to-peer VPN implementation has been conducted on a computer which hosts two virtual machines. The details are shown at table 3.

Table 3: The environment of the implementation

Type of Machine	Specifications
Physical Machine	Windows 10 standard x64 based processor, Intel Xeon CPU 1.60 Ghz RAM: 32 GB
Virtual Machine 1 (Server)	Ubuntu machine 20.04.2 LTS with kernel Linux 5.8.0-59-generic installed on VMWare Workstation 15 Pro, CPU: 2 processor cores RAM: 4 GB
Virtual Machine 2 (Client)	Ubuntu machine 20.04.2 LTS with kernel Linux 5.8.0-59-generic installed on VMWare Workstation 15 Pro, CPU: 2 processor cores RAM: 4 GB

The IP addresses and keys used during the installation process are shown in table 4.

Table 4: IP addresses and keys used

Description	**Server**	**Client**
Local IP Address	192.168.229.138	192.168.229.141
WireGuard IP Address	10.0.0.1	10.0.0.2
WireGuard Private key	QOsk4Be832zp7uHmo1IfaXru6k3Csh8TiE6lfGKCYU8=	SGjMR59GNDEguiaJ6hQ+K6jJegI6MgnROIxUZEl/p3I=
WireGuard Public Key	xmdU3SUeZlmy0W6uFmNgDBrEkVOVZpr77WPU1IpC7X8=	rQL4UlAPj/rpuY14YuCKlzGZGt458aGdmT7Q1lnrEDg=

The step by step WireGuard installation and configuration for creating a basic VPN connection between two peers for remote access is explained in the succeeding lines.

5.1 WireGuard Installation on Server and Client

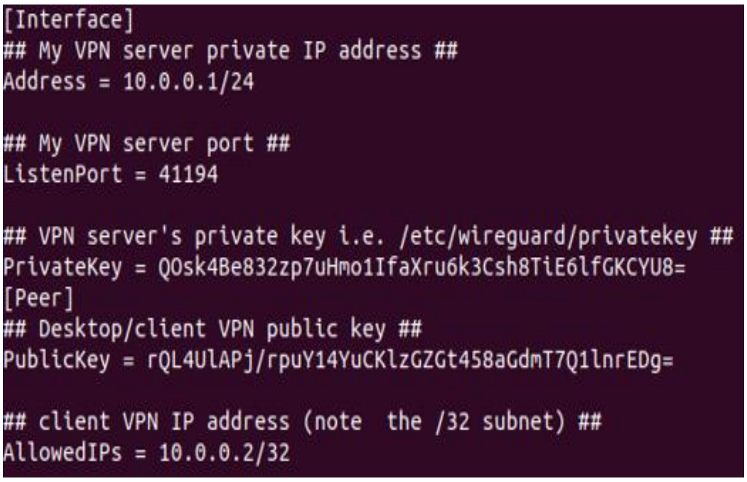
sudo apt install wireguard, this install WireGuard on server as well as client.

5.2 Create a Private and Public Key on Server and Client

wg genkey | tee privatekey | wg pubkey > publickey, this generates public and private key on both the machines.

5.3 Configure the Server

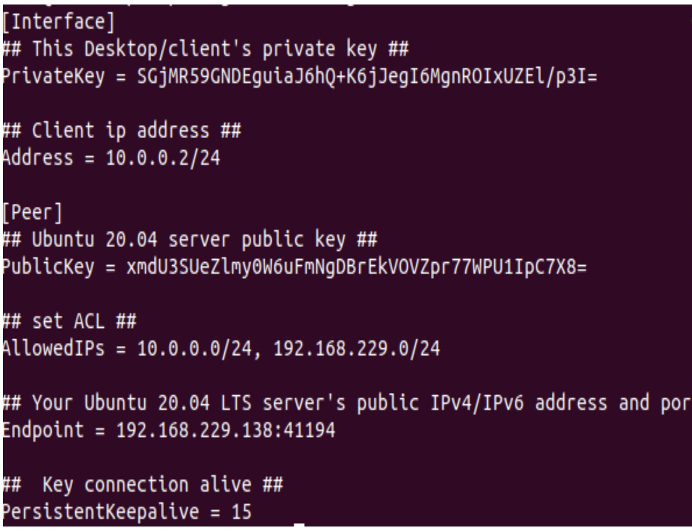
Create a new file “**/etc/wireguard/wg0.conf**” on the client server machine and insert the server private IP address, private key, listening port and client’s public key and private IP address.



```
[Interface]
## My VPN server private IP address ##
Address = 10.0.0.1/24

## My VPN server port ##
ListenPort = 41194

## VPN server's private key i.e. /etc/wireguard/privatekey ##
PrivateKey = QOsk4Be832zp7uHmo1IfaXru6k3Csh8TiE6lfGKCYU8=
[Peer]
## Desktop/client VPN public key ##
PublicKey = rQL4UlAPj/rpuY14YuCKlzGZGt458aGdmT7Q1lnrEDg=

## client VPN IP address (note  the /32 subnet) ##
AllowedIPs = 10.0.0.2/32
```

5.4 Configure the Client

Create a new file called “/etc/wireguard/wg0.conf” on the client machine and insert the client private key, IP address and server IP address with the listening port.



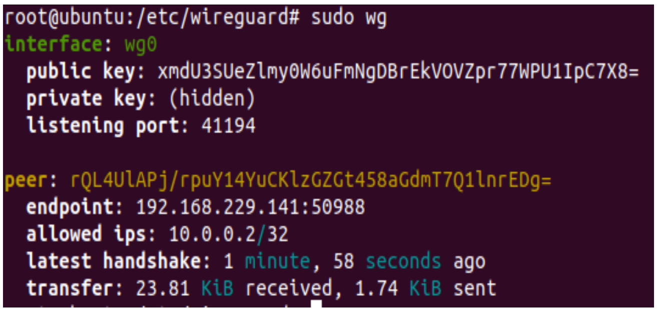
```
[Interface]
## This Desktop/client's private key ##
PrivateKey = SGjMR59GNDEguiaJ6hQ+K6jJegI6MgnROIxUZEl/p3I=

## Client ip address ##
Address = 10.0.0.2/24

[Peer]
## Ubuntu 20.04 server public key ##
PublicKey = xmdU3SUeZlmy0W6uFmNgDBrEkVOVZpr77WPU1IpC7X8=

## set ACL ##
AllowedIPs = 10.0.0.0/24, 192.168.229.0/24

## Your Ubuntu 20.04 LTS server's public IPv4/IPv6 address and port ##
Endpoint = 192.168.229.138:41194

##  Key connection alive ##
PersistentKeepalive = 15
```

5.5 Enabling and Starting WireGuard Service on Server and Client

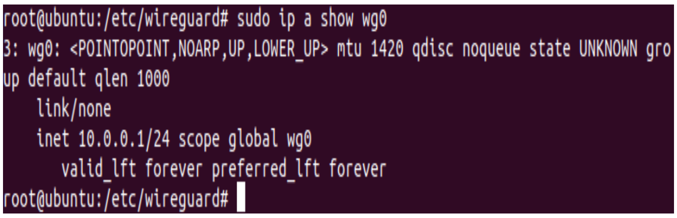
sudo systemctl enable wg-quick@wg0, it turns the WireGuard service at the boot time.
sudo systemctl start wg-quick@wg0, it starts the service.
sudo systemctl status wg-quick@wg0, it gets the service status.

5.6 Verification at Server and Client

sudo wg0
sudo ip a show wg0
This verifies that the interface named wg0 is up and running on Ubuntu Server.

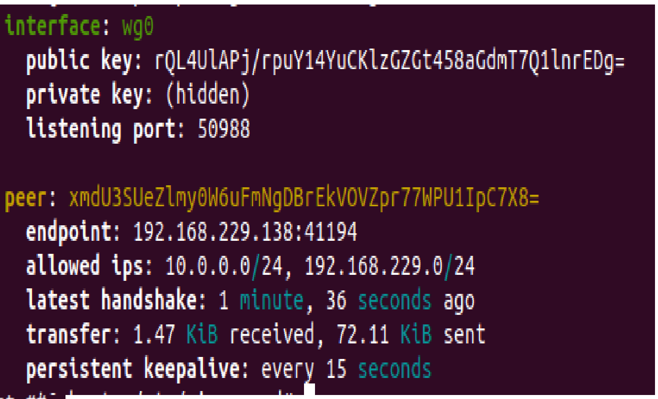


```
root@ubuntu:/etc/wireguard# sudo wg
interface: wg0
  public key: xmdU3SUeZlmy0W6uFmNgDBrEkVOVZpr77WPU1IpC7X8=
  private key: (hidden)
  listening port: 41194

peer: rQL4UlAPj/rpuY14YuCKlzGZGt458aGdmT7Q1lnrEDg=
  endpoint: 192.168.229.141:50988
  allowed ips: 10.0.0.2/32
  latest handshake: 1 minute, 58 seconds ago
  transfer: 23.81 KiB received, 1.74 KiB sent
```



```
root@ubuntu:/etc/wireguard# sudo ip a show wg0
3: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN gro
up default qlen 1000
    link/none
    inet 10.0.0.1/24 scope global wg0
       valid_lft forever preferred_lft forever
root@ubuntu:/etc/wireguard# 
```

ping –c 4 10.0.0.1
sudo wg
This verifies the secure peer-peer VPN connection at the client side.



```
interface: wg0
  public key: rQL4UlAPj/rpuY14YuCKlzGZGt458aGdmT7Q1lnrEDg=
  private key: (hidden)
  listening port: 50988

peer: xmdU3SUeZlmy0W6uFmNgDBrEkVOVZpr77WPU1IpC7X8=
  endpoint: 192.168.229.138:41194
  allowed ips: 10.0.0.0/24, 192.168.229.0/24
  latest handshake: 1 minute, 36 seconds ago
  transfer: 1.47 KiB received, 72.11 KiB sent
  persistent keepalive: every 15 seconds
```

The above process installs a secure peer-to-peer VPN connection and facilitates secure remote access between the two machines.

6. Conclusion

The COVID-19 pandemic has changed the way people live their lives and conduct their business. The concept of lockdown, social distancing, self-isolation and quarantine that came with COVID-19 pandemic has changed the societal and business norms. There is a heavy reliance on digital platform for routine day-to-day and business activities. The 'work from home' policy and fear of pandemic in the minds of the people has changed the global cybersecurity threat landscape. Cyber criminals are taking advantage of the unprecedented situation and they are targeting victims with malicious intent. The cyber-crimes have not only cost implication in terms of damage and destruction of data, forensic investigation but it at times also lead to reputational harm, identity theft and theft of intellectual property. There is a need for adopting the appropriate strategy at the individual as well as business enterprise level to manage the cyber security challenges amid COVID-19 pandemic. There is also a need to evolve effective cyber security plan at the business enterprise level duly addressing the changes that are required at 'Remote Access Domain' and 'User Domain' level. The precautionary and preventive measures against COVID-19 cyber security threats should take into account the important resource pillars of cyber security, people process and technology for forging the effective way ahead.

References

[1] Time Well, San Murugesan, "IT Risk and Resiliency-Cybersecurity response to COVID-19", vol. 22, pp. 4-20, May-June 2020.

[2] WHO Timeline - COVID-19, Who.int, 2020. [Online]. Available: https://www.who.int/news-room/detail/27-04-2020-who-timeline---covid-19. Accessed: 08 Aug 2020.

[3] WHO, "Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)," 2020. Available: https://www.who. int/ news -room/detail/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov). Accessed: 04 May-2020.

[4] Clean Link. SARS-CoV-2 And COVID-19: What's The Difference?. Available: https://www.cleanlink.com/news/article/SARS-CoV-2-

AndCOVID-19-Whats-The-Difference--25264. Accessed: 08 Aug 2020.

[5] AJ Tatemm, et el., "Global Transport Networks and Infectious Disease Spread". Journal: Advances in parasitology, 62, pp.293-343, Apr 2006.

[6] Trend Micro. Social Engineering Watch: Ebola Virus Being Used As Bait to Lure Victims. Available:https://www.trendmicro.com/vinfo/ tr/security/news/cybercrime-and-digital-threats/social-engineeringebola-virus-being-used-to-lure-victims. Accessed: 20 March 2020.

[7] WHO, "Modes of transmission of virus causing COVID-19: implications for IPC precaution recommendations," 2020. Available: https://www.who.int/newsroom/commentaries/detail/modes-of-transmission-of-virus-causingcovid-19-implications-for-ipc-precaution-recommendations. Accessed: 04 May 2020.

[8] WHO Coronovirus disease (COVID-19) dashboard. Available: https://covid19.who.int/?gclid=EAIaIQobChMIma-stZ-L6wIVUbaWCh06TARMEAAYASAAEgJVzPD_BwE. Accessed: 08 August 2020.

[9] COVID-19, dashboard. Available https://www.mygov.in/covid-19. Accessed: 08 Aug 2020.

[10] Vgl. Ella Koeze, Nathaniel Popper, The Virus Changed the Way We Internet, in: The New York Times 07.04.20. Avialbale: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html? action=click&module=Editors%20Picks&pgtype= Homepage. Accessed: 14 July 2020

[11] Statista: Media consumption increase due to the coronavirus worldwide 2020, by country. Available :https://www.statista.com/statistics/1106766/ mediaconsumption -growth-coronavirus-worldwide-by-country/. Accessed: 14 July 2020.

[12] Johannes Wiggen, "The impact of COVID-19 on cyber crime and state-sponsored cyber activities", Facts & Findings, No 391 / June 2020, pp. 1-8. Available: https://www.kas.de/en/facts-findings. Accessed: 12 July 2020

[13] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit". The Oxford Handbook of Cyberpsychology. OUP, 2019.

[14] S. O. Ciardhu ´ ain, "An extended model of cybercrime investigations," International Journal of Digital Evidence, vol. 3, no. 1, pp. 1–22, 2004.

[15] J. L. Cebula and L. R. Young, "A taxonomy of operational cyber security risks," Carnegie Mellon University, Software Engineering Institute, Tech. Rep., 2010.

[16] A. Nicholson, T. Watson, P. Norris, A. Duffy, and R. Is- 18 bell, "A taxonomy of technical attribution techniques for cyber-attacks". European Conference on Information Warfare and Security. Academic Conferences International Limited, 2012, pp. 188.

[17] CPS, "Cybercrime - prosecution guidance," The Crown Prosecution Service (CPS), Tech. Rep., 2019. Available: https://www.cps.gov.uk/ legal-guidance /cybercrimeprosecution-guidance.Accessed: 30 June 2020.

[18] M. McGuire and S. Dowling, Cyber crime: A review of the evidence Research Report, Research Report 75, Home Office, Tech. Rep., 2013. Available: https://assets.publishing. service.gov.uk/government /uploads/system/ uploads/attachment data/ file/246751/horr75-chap1.pdf. Accessed: 20 June 2020.

[19] M. McGuire and S. Dowling, Cyber crime: A review of the evidence Research Report, Research Report 75, Home Office, Tech. Rep., 2013. Available https://assets.publishing.service.gov.uk/government/uploads /system/uploads/attachment data/file /248621/horr75-chap2.pdf . Accessed 20 June 2020.

[20] Cybersecurity Ventures, 2019 official annual cybercrime report. Available: https://www.herjavecgroup.com/the-2019-officialannual-cybercrime-report. Accessed: 30 June 2020.

[21] M. Cross and D. L. Shinder, Scene of the cybercrime. Syngress Pub., 2008.

[22] Australia reports 'malicious' cyberattack by 'sophisticated state-based cyber actor': PM Morrison. The Economics Times, 19 June 2020. Available:https://economictimes.indiatimes.com/news/international/world-news/australia-reports-malicious-cyberattack-by-sophisticated-state-based-cyber-actor-pm morrison/articleshow/76464217.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, Accessed 31 July 2020.

[23] Malicious Activity Targeting COVID-19 Research, Vaccine Development, release date 16 July 2020. Available: https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/malicious-activity-targeting-covid-19-research-vaccine-development. Accessed: 31 July 2020.

[24] WHO reports fivefold increase in cyber-attacks, urges vigilance. 23 April 2020, Available: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. Accessed: 30 July 2020.

[25] Global Landscape on COVID-19 Cyberthreat. Available: https://www.interpol.int/en/Crimes/ aCybercrime/COVID-19-cyberthreats. Accessed: 30 July 2020.

[26] Live Updates: COVID-19 Cybersecurity Alerts. Available: https://cyware.com/ blog/live-updates-covid-19-cybersecurity-alerts-b313. Accessed: 16 Aug 2020.

[27] 2.9 Crore Indian Job Seekers' Data Leaked on Dark Web: Report, 24 May 2020. Available: https://www.india.com/technology/2-9-crore-indian-job-seekers-data-leaked-on-dark-web-report-4037946/. Accessed: 01 Aug 2020.

[28] Aditi Agrawal, COVID-19 Apps used by states not properly tested, says India's National Cyber Security Coordinator, 16 May 2020. Available: https://www.medianama.com/2020/05/223-covid19-apps-states-not-properly-tested-rajesh-pant/. Accessed: 31 July 2020.

[29] PM CARES COVID-19 fund: Do not fall for fake donation website. The Times of India, 21 Apr 2020.Available:http://timesofindia.indiatimes. com/articleshow/75274181cms?utm_source=contentofinterest &utm _medium= text&utm_campaign=cppst. Accessed: 30 June 2020.

[30] COVID-19: Cyber Threat Analysis, United Nations Office on Drugs & Crime. Available: https://www.unodc.org/documents/middleeastand northafrica //2020/COVID19/COVID19_MENA_Cyber_Report_EN.pdf. Accessed: 30 July 2020.

[31] Prem Mahdevan, Cybercrime Threats during the COVID-19 pandemic. Apr 2020.Available: https://globalinitiative.net/wp-content/uploads/ 2020/04 /Cybercrime-Threats-during-the-Covid-19-pandemic.pdf. Accessed: 29 June 2020.

[32] Catalin Cimpanu, Coronavirus: Business and technology in a pandemic. Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, 13 March 2020. Available: https://www.zdnet.com/article /czech-hospital-hit-by -cyber -attack-while-in-the-midst-of-a-covid-19-outbreak/. Accessed: 30 June 2020.

[33] Manu Kaushik, Most cyber-attacks in India from China, Pakistan; hackers exploit COVID-19, emulate PM CARES, 22 June 2020. Available: https://www.timesnownews.com/business-economy/economy/article/ exclusive-most-cyber-attacks-in-india-from-china-pakistan-hackers-exploit-covid-19-emulate-pm-cares/609868. Accessed: 30 July 2020.

[34] Abhijit Ahaskar, Coronavirus related cyberattacks surge by 260% during lockdown, Kerala most targeted: Report. Livemint , 21 May 2020. Available: https://www.livemint.com/technology/tech-news/coronavirus-related-cyberattacks-surge-by-260-during-lockdown-kerala-most-targeted-11590054440090.html. Accessed: 31 July 2020.

[35] Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic, 11 Aug 2020. Available: https://www.prnew swire. com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html. Accessed: 14 Aug 2020.

[36] Deagle: W.L. Deagle, et al., "To Zoom or Not to Zoom—Privacy and Cybersecurity Challenges". Available: https://news.bloomberglaw.com /us-law-week/insight-to-zoom-or-not-to-zoom-privacy-and-cybersecurity-challenges. Access: 14 Aug 2020.

[37] Boerner: R. Boerner & L. McDaniels, 27 April 2020, Fisher Phillips, Available:https://www.fisherphillips.com/resources-alerts-10-point-plan-to-protect-your-business. Accessed: 30 April 2020.

[38] A. St. John, "It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.," 2020. Available: https://www.consumerreports.org/video-conferencingservices /videoconferencing-privacy-issues-google-microsoftwebex/.

Accessed: 30 May 2020.

[39] T. Warren, “Zoom faces a privacy and security backlash as it surges in popularity,” 2020. Available: https://www.theverge.com/2020/4/1/21202584/zoom-securityprivacy-issues-video-conferencing-software-coronavirus-demandresponse. Accessed: 30 May 2020.

[40] Donenfeld, J., A “WireGuard: Next Generation Kernel Network Tunnel”. Available: https://www.wireguard.com/papers/wireguard.pdf. Accessed: 11 June 2021.