Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 1 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Security Investigation on Remote Access Methods of Virtual Private Network

By Peter S. Nyakomitta & Dr. Silvance O. Abeka
Jaramogi Oginga Odinga University

Abstract- Remote access is one of the prevalent business trends in today's computing pervasive business environments. The ease of access to internal private networks over the internet by telecommuter devices has given birth too many security threats to the endpoint devices. The application client software and data at rest on the endpoint of remote access methods such as: Tunneling, Portal, Desktop Applications and Direct Access do not offer protection for the communication between the VPN gateway and internal resources. This paper, therefore investigate the security pitfalls of remote access for establishing virtual private network methods. To address these challenges, a remote access method to secure endpoint communication is proposed. The study adopted investigative research design by use of empirical review on the security aspect of the current state VPN Remote Access methods. This necessitates the review of the research article on the current state and related works which leads to critiques and offer proposed solution to remote access endpoint VPN. The scope of this study is limited to secure virtual private network endpoint data communication. In this paper, an investigation of these access technologies given.

Keywords: remote access, tunneling, portal, desktop application, direct application, gateway.

GJCST-E Classification: C.2.m

Strictly as per the compliance and regulations of:

Security Investigation on Remote Access Methods of Virtual Private Network

Peter S. Nyakomitta [α] & Dr. Silvance O. Abeka [σ]

Abstract- Remote access is one of the prevalent business trends in today's computing pervasive business environments. The ease of access to internal private networks over the internet by telecommuter devices has given birth too many security threats to the endpoint devices. The application client software and data at rest on the endpoint of remote access methods such as: Tunneling, Portal, Desktop Applications and Direct Access do not offer protection for the communication between the VPN gateway and internal resources. This paper, therefore investigate the security pitfalls of remote access for establishing virtual private network methods. To address these challenges, a remote access method to secure endpoint communication is proposed. The study adopted investigative research design by use of empirical review on the security aspect of the current state VPN Remote Access methods. This necessitates the review of the research article on the current state and related works which leads to critiques and offer proposed solution to remote access endpoint VPN. The scope of this study is limited to secure virtual private network endpoint data communication. In this paper, an investigation of these access technologies given.

Keywords: remote access, tunneling, portal, desktop application, direct application, gateway.

Abbreviations: Virtual Private Network (VPN), Layer 2 Forward (L2F), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPsec).

I. Introduction

An enterprise network normally consists of many remotely connected sites located far away from each other. Traditionally, leased lines connections utilizing frame Relay and Asynchronous Transfer Mode (ATM) were used to provide connectivity among these customer sites. The growth of this network made it become a costly solution and a challenge for network scalability. Virtual Private Network (VPN) came as an alternative which provide flexible solutions, such as securing communication between remote telecommuters and organization's servers, regardless of where telecommuters are located. Sandeep et al, (2016), in their article describe a Virtual Private Network (VPN) as the traditional approach for an end-to-to end secure connection between two endpoints through use of public or shared telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. The VPN establishes tunnels between servers in a site-to-site VPN, clients and servers in a client-to-site VPN (Avani and Ankita, 2017). The approach opted to investigate the security in remote access methods since most large corporations, educational institutions, and government agencies uses VPN technology to enable telecommuter to securely connect to a private network.

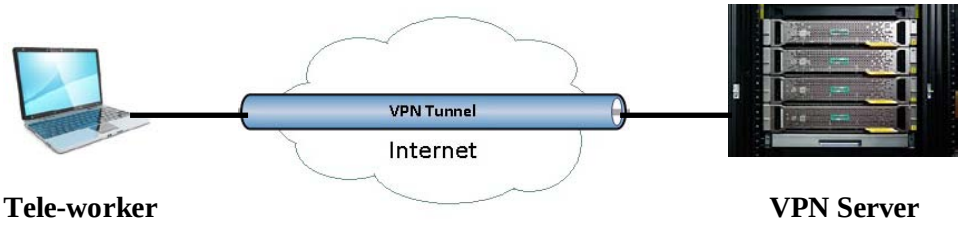

Figure 1: Remote Access VPN Architecture

It can be conceptualized as creating a tunnel from one network to another, with encrypted data travelling through the tunnel before being deciphered at its destination. Telecommuters can connect to their corporate LAN or any other LAN regardless of where the telecommuters are located (Rashikala, 2013). They can access resources such as email and documents as if they were connected to the LAN as normal.

All teleworkers authenticate themselves with the VPN server, which is protected by a firewall. Once a user is connected to the network, an internal firewall guarantees that access is available only to the required resources (Butts and Shenoi, 2011). When a data packet is transmitted from a teleworker, it sends it through a VPN gateway, which adds an Authentication Header for routing and authentication. The data is then encrypted and, finally, enclosed with an Encapsulating Security Payload which contains the decryption and handling instructions.

Author α σ: Department of School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya. e-mail: pnyakomitta@yahoo.com

The receiving VPN server strips the header information, decrypts the data, and routes it to its intended destination. A VPN allows the provisioning of a virtual "tunnel" connecting the two endpoints. The traffic within the VPN tunnel is encrypted so that other users of the public internet cannot eavesdrop by intercepting communications (Tarek and Yasser, 2011). By implementing a VPN, a company can provide access to the internal private network to clients around the world at any location with access to the public internet.

Remote access VPN is one of the prevalent business trends in today's ubiquitous computing era which deploy use of secure remote access to corporate resources by establishing an encrypted tunnel across the network. It is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.

According to Rajamohan, (2014), they allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. While a firewall protects the systems and data on a LAN from unauthorized access, it does nothing to protect the confidentiality and integrity of traffic traversing the Internet on its way to and from the LAN. That's the role of a virtual private network, or VPN. VPN technology provides encryption and tunneling functions for networked traffic across the Internet. Data is encapsulated in an IP "wrapper" that travels over the Internet. When data is sent, it must be wrapped and encrypted by a gateway using an encryption algorithm. At the other end of the communication link, the destination gateway must "unwrap" the data, decrypt it, and route it to its destination.

II. Remote Access VPN Methods

This section presents the state-of-the-art Remote Access VPN Methods for establishing virtual private network. The remote access methods are most commonly used for teleworkers. This section describe four categories based on their high-level architectures and the security implications. The categories include: tunneling, portals, remote desktop access, and direct application access. The sub-section below gives an investigation of mote access in VPN, as follows.

a) *Tunneling*

Many remote access methods offer a secure communications tunnel through which information can be transmitted between networks, including public networks such as the Internet. According to Murugiah and Karen, (2016), tunneling involves establishing a secure communications tunnel between a telework client device and a remote access server, often a virtual private network (VPN) gateway buy use of cryptography to protect the confidentiality and integrity of the transmitted information between the client device and the VPN gateway. The VPN gateway can take care of user authentication, access control and other security functions for teleworkers. The tunnel uses cryptographic protocols like IPsec, SSL and SSH tunnels to protect the confidentiality and integrity of the communications. The figure 2.shows the tunneling architecture used to set tunneling remote access.

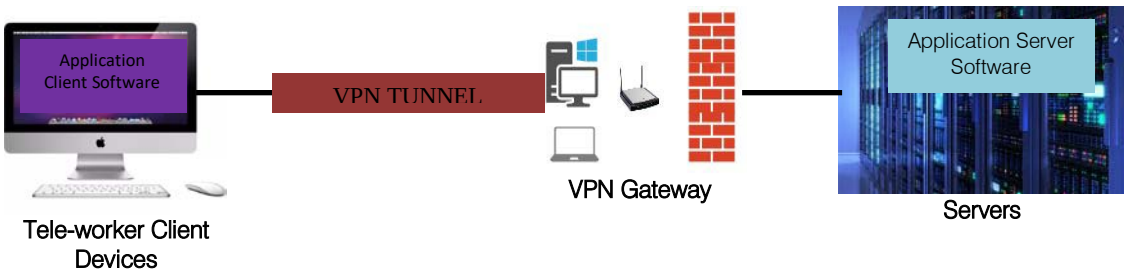

Figure 2: Tunneling Architecture

Once a VPN tunnel has been established between a teleworker's client device and the organization's VPN gateway, the teleworker can access many of the organization's computing resources through the tunnel. To use this application of VPN, users must either have the appropriate VPN software on their client devices or be on a network that has a VPN gateway system on it. The VPN gateway can control access to the parts of the network and the types of access that the teleworker gets after authentication. For example, a VPN might allow a user to only have access to one subnet, or to only run particular applications on certain servers on the protected network. In this way, even though the cryptographic tunnel ends at the VPN gateway, the gateway can add additional routing to the teleworker's traffic to only allow access to some parts of the internal network.

b) *Portals Applications*

A portal is a server that offers access to one or more applications through a single centralized interface (Murugiah and Karen, 2016). A teleworker uses a portal client on a telework client device to access the portal. The application client software is installed on the portal

server, and it communicates with application server software on servers within the organization. The Figure 3 shows the basic portal solution architecture. The portal protects communications between the client devices and the portal, and portals can also authenticate users and restrict access to the organization's internal resources.

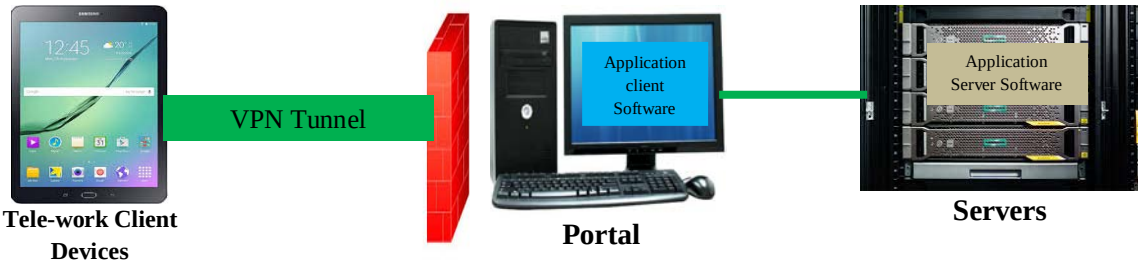

Figure 3: Portal Architecture

In terms of security, portals have most of the same characteristics as tunnels: portals protect information between client devices and the portal, and they can provide authentication and access control. The application client software and data at rest resides on the portal server which then get transferred to the client devices which are then typically stored on the client devices much more temporarily than data for a tunneled solution is. Having the application client software centralized gives an organization more control over how the software and data is secured as opposed to more distributed remote access solutions. Portals limit the access a teleworker has to particular application clients running on the portal solutions.

c) Desktop Application Access

A remote desktop access solution gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the user's own computer at the organization's office, from a telework client device. The solution allows the user to access all of the applications, data, and other resources that are normally available from their PC in the office. Figure 4, shows the basic remote desktop access architecture.

Figure 4: Remote Desktop Access Architecture

Remote desktop access uses a proprietary protocol, Remote Desktop Protocol (RDP) to enables users to interfaces with another computer through a graphical interface. It allows users to gain access to the desktop of another computer. According to (Karen, Paul and Murugiah, 2009), the remote desktop access software protects the confidentiality and integrity of the remote access communications and also authenticates the user to ensure that no one else connects to the internal workstation. However, because this involves end-to-end encryption of the communications across the organization's perimeter, the contents of the communication are hidden from the network security controls at the perimeter, such as firewalls and intrusion detection systems. A remote desktop access client program is installed on each telework client device, and it connects directly with the teleworker's corresponding internal workstation on the organization's internal network.

d) Direct Application Access

With direct application access, remote access can be accomplished without using remote access software. A teleworker can access an individual application directly, with the application providing its own security like communications encryption, user authentication. According to Murugiah and Karen (2016), one of the most common examples of direct application access is Web-based access to email, also known as Webmail. The teleworker runs a Web browser

and connects to a Web server that provides email access. The Web server runs HTTP over SSL (HTTPS) to protect the communications and the Webmail application on the server authenticates the teleworker before granting access to the teleworkers email. The Figure 5, shows the high-level architecture for direct application access.

Figure 5: Direct Application Access Architecture

The application client software installed on the telework client device initiates a connection with a server, which is typically located at the organization's perimeter. The direct application access architecture is generally only acceptable if the servers being accessed by the teleworkers are located on the organization's network perimeter or in a public-facing cloud, and not internal networks. Servers that are directly accessible from the Internet should already be well-secured to reduce the likelihood of compromise. Many organizations choose to provide direct application access to only a few lower-risk applications that are widely used, such as email, and use tunnel or portal methods to provide access to other applications, particularly those that would be at too much risk if they were directly accessible from the Internet.

III. Related Work

In (Ernest et al, (2015) proposed advanced technologies to provide tremendous support for network administrators by implementing a secure remote system administration app that runs on android smartphones to aid them administer their servers remotely when they (network administrators) are out stationed using their smartphones. The android app developed in eclipse establishes a secure connection with a remote server running a PHP application. The app was developed based on the Remote Frame Buffer (RFB) protocol. The RFB protocol, a display protocol has some security lapses including being vulnerable to Man-In-The-Middle (MITM) attack using a few tools and techniques (Masthan, Kumar and Prasad, 2013). This paper therefore incorporated a self-signed Secure Socket Layer (SSL) certificate in the android app to enable secure encrypted connections to be established between the android app and the remote server to ensure end-to-end security against attacks such as Man-In-The-Middle (MITM). The secure RFB protocol proposed and implemented in the android app was compared with other existing software for remote system administration such as Remote Desktop (RDP), and RFB protocols using ICMP ping command. The results show that the average response time of the RDP protocol was 436ms, that of the RFB protocol was 496ms and that of the android app which is based on a proposed secure RFB protocol was 474ms. The proposed android app which will act as an interface to the network server will connect to the server using Virtual Private Network (VPN) technology.

With this system, a system administrator can create a user remotely, create, view and modify text files remotely, check network status, shutdown a server and set user privileges. The system was developed based on a proposed secure RFB protocol with self-signed Secure Socket Layer (SSL) certificate incorporated into this RFB protocol to ensure end to- end encrypted connections between the smart device (client) and server. Mobile Devices Management (MDM) applications are developed to address some of the challenges associated with mobile devices (such as policy management, software distribution, and inventory management) that are not related to BYOD security. MDM functionality is similar to that of PC configuration life-cycle management (PCCLM) tools; however, mobile-platform specific requirements are often also included in MDM suites (Gartner, 2014).

On their paper, (Kumari and Khan, 2014) proposed a symmetric key and smart card-based remote user password authentication scheme that was intended to provide anonymity while resisting all known attacks. On their part, (Shehzad et al, 2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security Comm. Networks. 8:3782–3795 proposed a supplemented scheme to overcome security weaknesses of the scheme proposed in (Kumari and Khan, 2014). The authors claim to have analyzed the security of the proposed scheme in random oracle model which confirmed the robustness of the scheme against all known attacks.

A study by (Madhusudhan and Hegde, 2017), pointed out that two robust remote user authentication schemes using smart cards that were claimed to defend against ID-theft attacks, reply attacks, undetectable on-line password guessing attacks, off-line password guessing attacks, user impersonation attack, server counterfeit attack and man-in-the-middle attack. In (Gartner, 2014), the authors discuss that a smart-card based remote user authentication scheme consisting of four phases, which include initialization, registration, login, and authentication has been proposed.

A wireless body area network (WBAN) is a system that provides automatic health monitoring and sends crucial health-related data remotely to the doctors with the help of body sensors. The protection of these health records is therefore very critical to prevent malicious and fraudsters accessing these data and impersonating the patients. These networks have an authentication system as their backbone because a lapse in such technologies could lead to the death of a patient. In (Salama, Taha, and Elmahdy, (2015), a scheme known as PMAS is proposed for mutual authentication between the sink (patients' personal cellular phone) and sensor nodes focused on the advanced idea behind the Diffie-Hellman key exchange scheme. Here, a trusted third party (TTP) distributes keys (public and private) to the medical sensor node and sink (mobile / cellular phone).

Recently, elliptic curve cryptography (ECC) has been implemented widely in multi-factor authentication. It is basically a public key encryption technique based on elliptic curve theory that can be used to create smaller keys, which yields faster and more efficient algorithms as a result (Chande, et al, 2016). It was developed to reduce computational costs while providing the same level of security as other similar operations such as modular exponentiation and it finds applications in authentication protocols involving smart cards, RFIDs, wireless networks, digital signatures and other authentication techniques.

IV. Critique of the Current Remote Access Technologies

The four remote access methods discussed above were noted to have a number of security setbacks that render them ineffective in VPN deployments. To start with, Tunneled IP traffic may not receive the intended level of inspection or policy application by network-based security devices unless such devices are specifically tunnel aware. This reduces defense in depth and may cause security gaps. This security weakness applies to all network-located devices and to any end-host-based firewalls whose existing hooking mechanisms would not show them the IP packet stream after the tunnel client does decapsulation or before it does encapsulation. In addition, IP addresses inside tunnels are not subject to ingress and egress filtering in the network they tunnel over, and hence may allow malicious content into internal networks. Moreover, if the encapsulated IP packet specifies source routing beyond the recipient tunnel client, the host may forward the IP packet to the specified next hop. This may be unexpected and contrary to administrator wishes and may have bypassed network-based source routing controls.

On the part of portals applications, Tomas (2014) point out that they are faced with challenges regarding authentication including user identification, authorization, auditing or logging and session management. Desktop application access face screen sharing security setback that allow an attacker to penetrate an enterprise's defenses. In addition, many enterprises permit or fail to regulate the use of third-party file storage services to facilitate remote access to data, and when files end up in cloud-based repositories, enterprises lose control. On its part, direct application access requires the use of IPv6 exclusively to distribute addressing to connecting endpoints. This presents a larger management problem when it comes to client addressing and identification.

Due to the setbacks noted in the four access methods discussed above, a number of protocols have been developed to address some of these challenges. Unfortunately, these protocols also introduce vulnerabilities that render them insecure. For instance, the RFB protocol, a display protocol has some security lapses including being vulnerable to Man-In-The-Middle (MITM) attack using a few tools and techniques (Ernest et al, 2015). Despite the fact that RFB protocol uses encrypted passwords and network, any communication over the network is vulnerable and can be attacked by a Man-In-The-Middle (MITM) by using a few tools and techniques. In addition, the applications of VNC which are developed based on RFB protocol are generally slower, offer fewer features and security options than Remote Desktop (RD) which is based on the RDP protocol (Masthan, Kumar and Prasad, 2013). Though the data sent between the server and client is encrypted, the RDP protocol may be prone to Man-In-The-Middle attack because there is no verification of the identity of the server when setting up the encryption keys for a session.

Although businesses are mainly concerned with maintaining security, employees are worried about preserving the convenience they need to work from their mobile devices, as well as the privacy they expect regarding the personal information on the device (Morufu et al, 2015). One of the biggest challenges for organizations is that corporate data are being delivered to devices that are not managed by the IT department. This has security implications for data leakage, data theft, and regulatory compliance. Thielens, (2013), noted that the real BYOD challenge is security and that the real security challenge is not actually about the devices, it is

about controlling access from the devices to the corporate data. Moreover, Vignesh and asha, (2015), points out that sensitive data on organization and personal data are present in these devices and such any attack on these devices can expose these data.

Many enterprises view most of the MDM applications as a solution to the security challenges of BYOD. However, MDM does not completely address the security challenges of BYOD. MDM does not prevent a hacker from attacking an employee's device or a thief from stealing it and accessing sensitive data. Data leakage, distributed denial of service (DDoS), and malware are the most challenging security threats to BYOD (Gartner, 2014). Further, Manmeet, Chen and Zakiah, (2017), explain that security threat in the paradigm of BYOD creates a great opportunity for hackers or attackers to find new attacks or vulnerabilities that could possibly exploit the students' mobile devices and gains valuable data from them.

Gokulakrishnan, Jayanthi, and Thulasi, (2014) point out that VPN does not provide strong user authentication by default. This means that users can enter a simple username and password to gain access to an internal private network from home or via other insecure networks. On its part, the Point-to-Point Tunneling Protocol (PPTP) which is the most widely supported VPN protocol among Windows users establishes the tunnel, but does not provide encryption (Alshalan et al 2016). In their paper, Muhammad et al, (2016) discuss that a number of users employ mobile VPN clients to either circumvent censorship or to access geo-blocked content, and more generally for privacy and security purposes. Their experiments reveal that several instances of VPN applications that expose users to serious privacy and security vulnerabilities, such as use of insecure VPN tunneling protocols, as well as IPv6 and DNS traffic leakage. In addition, a number of mobile VPN applications actively perform TLS interception while other applications inject JavaScript programs for tracking, advertising, and for redirecting e-commerce traffic to external partners.

Another study by Varmarken et al, (2015), pointed out that some VPN applications implement tunneling protocols without encryption despite promising online anonymity and security to their users. In addition, it was noted that other VPN applications do not tunnel IPv6 and DNS traffic through the tunnel interface respectively due to lack of IPv6 support, mis-configurations or developer-induced errors. Both the lack of strong encryption and traffic leakages can ease online tracking activities performed by in-path middle-boxes such as commercial WiFi APs harvesting user's data and by surveillance agencies.

As Shehzad et al, (2015) points out, a symmetric key and smart card-based remote user password authentication scheme that was intended to provide anonymity while resisting all known attacks is still vulnerable to anonymity violation attack as well as smart card stolen attack. Chin-Ling et al, 2018) demonstrated that schemes that the two robust remote user authentication schemes using smart cards are still vulnerable to ID-theft attack, off-line password guessing attacks, undetectable on-line password guessing attacks and user impersonation. This is particularly true in situations where the user lost a smart card or the malicious legal user. In addition, the smart-card based remote user authentication scheme consisting of four phases has been shown by Gartner, (2014) to be vulnerable to offline password guessing attack under their non-tamper resistance assumption of the smart cards; and it fails to provide forward secrecy.

The challenge of the WBAN authentication is that TTP distributes all the credentials without applying any cryptographic functions or any mathematical computations. It dictates that the insider person can identify different keys of various users easily. Once important credentials are available with any malicious internal person, then he/she can distribute confidential data to others illegally.

Swapnoneel and Chanchal, (2017) point out that mutual authentication has been introduced in remote user verification and access control. However, a password can be compromised during transmission if an efficient scheme is not followed. To address this problem, elliptic curve cryptography (ECC) has been implemented widely in multi-factor authentication. However, the computational cost of one bilinear pairing (an important operation of ECC) is about twice as high as that of one modular exponentiation operation at the same security level. Therefore, the computationally-intensive nature of ECC leaves a security loophole in the protocols that use it. An attacker can force the server or client to repeatedly perform ECC operations in order to clog them, resulting in one or all of them wasting resources by performing unnecessary computations.

V. Proposed Solution

In recent years, mobile devices have replaced desktop personal computers as the primary computing platform for many users. This trend brings to the workplace where nowadays the employees use their personal owned mobile devices to access company's data. BYOD causes a lot of cyber-attacks towards the users and the organization. The proposed solution for BYOD addresses the shortcomings noted in some of the remote access technologies such as platform integrity that lacks in tunneling, authentication such as user identification, authorization, auditing or logging and session management that lacks in portals applications, regulation of file storage services to facilitate remote access to data, a feature that is missing in desktop application access, client addressing and identification that is lacking in direct application access as shown in Figure 6 below.

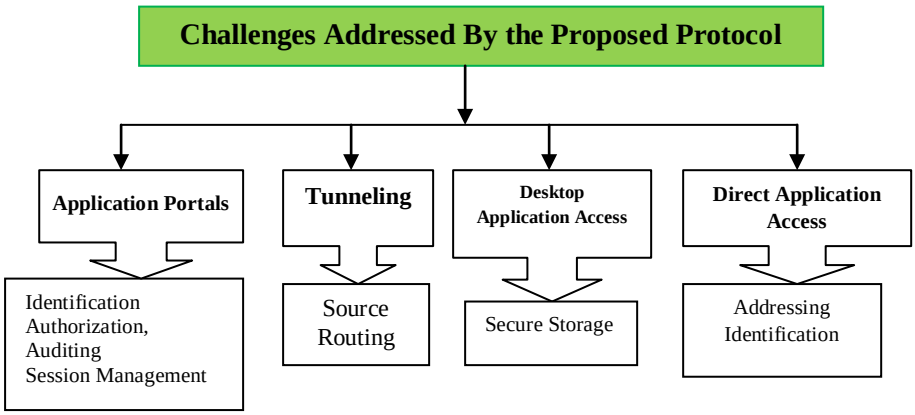

Figure 6: Problems Addressed By the Proposed Protocol

a) Architecture of the Proposed Protocol

The conventional remote access technologies have been noted to have a number of setbacks related to identification, authorization, auditing, session management, source routing, secure storage and addressing. Figure 7 shows the architectural design of the proposed protocol. As this figure shows, the proposed protocol will comprise of six attack prevention mechanisms namely IP scanning, hashing, MAC and IP based identification and addressing, digital certificates, one time passwords (OTP) and logging capability. IP scanning will be effective against source routing attacks where attackers make use of intranet IP addresses so as to fool the firewall against inspecting the traffic utilizing these internal IP addresses.

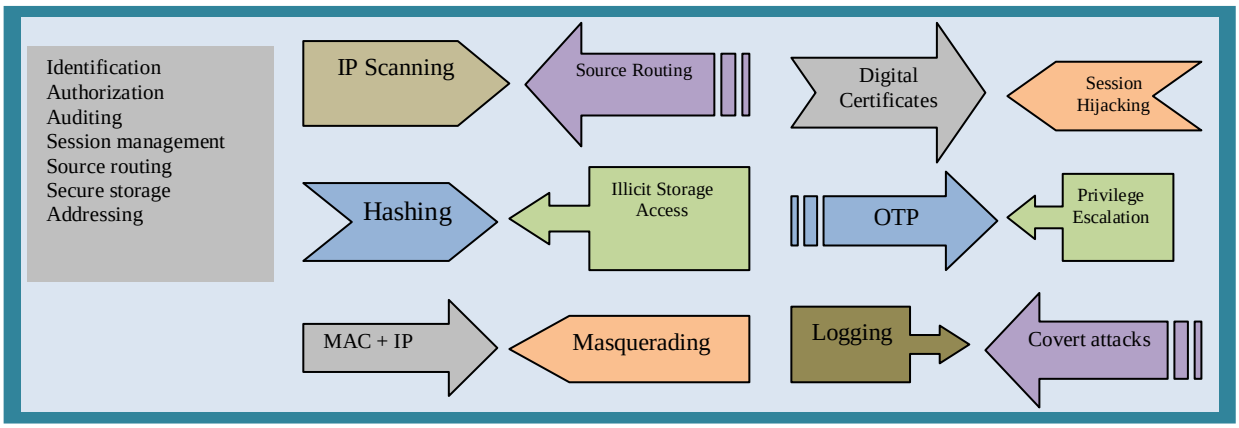

Figure 7: Proposed Protocol Architecture

The other salient feature of the proposed protocol is its hashing activity for any requested storage access to ensure secure storage of this vital organizational resource. To prevent masquerading attacks using false identification and addressing, the proposed protocol will utilize a combination of media access control (MAC) and IP address of the client and server machines for identification and addressing. Session management will be secured using digital certificates that will serve to protect the VPN communication against session hijacking attacks. On the other hand, one time passwords (OTP) will be instrumental in curtailing privilege escalation for authorized users such that once they accomplish any authorized activity, they require another set of authorization for the next activity. Covert attacks will be prevented by the proposed protocol's logging feature that will facilitate auditing during forensic analysis.

b) Secure Remote Access Method (SRAM)

Table 3.2 confirms that to secure VPN connections, a layered protection approach is necessary. The proposed VPN protection protocol will be implemented in all the four layers of the TCP/IP stack. Figure 3.2 shows the implementation design of the proposed protocol

Table 3.2: Layered Attacks and their likely target

TCP Layer	Attacks to be Prevented
Application Layer	Fingerprinting, Reconnaissance
Transport Layer	Modifications, replay
Network Layer	Source routing, packet redirection
Physical Layer	Masquerading attacks

As this figure illustrates, the proposed Secure Remote Access Method (SRAM) will be implemented in the region between the VPN end devices and the firewall. This is because the packets moving in the regions between the two firewalls are protected by SSL and TLS via the VPN tunnel.

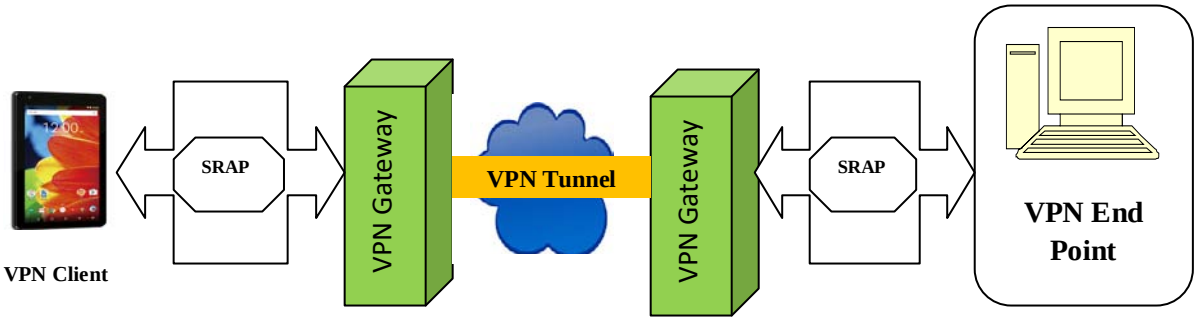

Figure 8: Proposed Secure VPN Access Method

As such, most attacks are only possible immediately these packets exit the tunnel and are passed through firewalls. All the layered protection discussed above will therefore implemented in the regions between firewalls and VPN endpoints (VPN client and VPN server).

VI. Conclusion and Recommendation

In this study, an investigation of remote access methods for establishing virtual private network a has been carried out. From this examination, it has been noted that all of them fall short of endpoint security, making it possible for attackers to carry out unauthorized data transfers from their victim machines due to lack of cryptographic protocols for securing the data that reside at the client device.

Towards the end of this paper, a protocol that could potentially address the security gap endpoint remote access client devices has been provided. One of the pillars of this protocol is encryption that would help enciphered the content of the data at the endpoint device and secondly component of this protocol is the dual-factor authentication that will requires the presence of two or more factors to prove the authenticity of the account holder. Owing to its security entropy, this protocol is therefore recommended for implementation in remote access methods for establishing virtual private network.

References Références Referencias

1. P. Sandeep et al, (2016). "A Survey of Mobile VPN Technologies." IEEE Communications Surveys & Tutorials 18.2 (2016): 1177-1196.
2. P. Avani and G. Ankita (2017), A Survey of VPN Performance Evaluation. International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Volume: 5 Issue: 5, pp 409 – 413
3. W. Rashikala, (2013). An Empirical Test-bed Analysis of a Virtual Private Network Protocol. UNITEC Institute of Technology, New Zealand.
4. J. Butts and S. Shenoi (2011): Critical Infrastructure Protection V, IFIP AICT 367, pp. 185–199,
5. S. Tarek and A. Yasser, (2011). Effective and Extensive Virtual Private Network. Journal of Information Security, 2011, 2, 39-49.
6. P. Rajamohan (2014).An Overview of Remote Access Vpns: Architecture and Efficient Installation. Ipasj International Journal of Information Technology (Iijit).
7. S. Murugiah and S. Karen (2016), Guide to Enterprise Telework, Remote Access, and Bring Your Own.S. Karen, H. Paul and S. Murugiah (2009). Guide to Enterprise Telework and Remote Access Security. National Institute of Standards and technology.
8. S. Murugiah and S. Karen, (2016).Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. NIST Special Publication 800-46 Revision 2.
9. Device (BYOD) Security. NIST Special Publication (SP) 800-46 Rev. 2.
10. D. Ernest et al, (2015).A Comparative Study Of Remote Access Technologies and Implementation of a Smartphone App for Remote System Administration Based on a Proposed Secure RFB Protocol. International Journal of Science and Engineering Applications. Volume 4 Issue 4, pp. 163-168.
11. K. Masthan, S. Kumar and V. Prasad, (2013) Virtual Network Computing of User Appliances. International Journal of Computer Science and Mobile Computing. Volume 2, Issue 8. pp. 132.
12. Gartner. (2014). Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018. Gartner Newsroom.
13. S. Kumari and MK. Khan, (2014). More secure smart card-based remote user password authentication scheme with user anonymity. Security and Communication Networks 2014; 7(11): 2039–2053.

14. A. Shehzad et al, (2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security Comm. Networks. 8:3782–3795.
15. R. Madhusudhan and M. Hegde, (2017). Security bound enhancement of remote user authentication using smart card. J. Inf. Secur. Appl. 2017, 36, 59–68.
16. H. Salama, S. Taha, and H. Elmahdy, (2015). PMAS: A proposed mutual authentication scheme for wireless body area networks. In Information and Communication Technology Convergence (ICTC), 2015 International Conference on (pp.636-641). IEEE.
17. Chande, et al, (2016). A CAE Scheme Using ECC Based Self Certified PKC. J. Comput. Sci. Vol. 12, pp. 527–533.
18. O. Morufu et al, (2015). A Review of Bring Your Own Device on Security Issues. SAGE Open. Pp. 1-11.
19. J. Thielens, J. (2013). Why API are central to a BYOD security strategy. Network Security, 2013, 5-6. doi:10.1016/S1353- 4858(13)70091-6.
20. U. Vignesh and S. Asha, (2015). Modifying security policies towards BYOD. 2nd International Symposium on Big Data and Cloud Computing. Vol.50, pp. 511 – 516.
21. Gartner, (2014). Gartner says less than 0.01 percent of consumer mobile apps will be considered a financial success by their developers through 2018. Gartner Newsroom.
22. M. Manmeet et al, (2017).Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm. International Journal of Advanced Computer Science and Applications. Vol. 8, No. 2, pp. 53-62.
23. J. Gokulakrishnan and V. Thulasi, (2014). "A Survey Report On Vpn Security & Its Technologies." Indian Journal of Computer Science and Engineering (IJCSE) 5.4 (2014): 3-5.
24. A. Alshalan, et al, (2016). "A Survey of Mobile VPN Technologies." IEEE Communications Surveys & Tutorials 18.2 (2016): 1177-1196.
25. I. Muhammad et al, (2016). An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. IMC. Pp.1-16
26. Varmarken et al, (2015). AntMonitor: A System for Monitoring from Mobile Devices. In ACM (C2B(I)D), 2015.
27. A. Shehzad, (2015). An enhanced privacy preserving remote user authentication scheme with provable security. Security Comm. Networks. 8:3782–3795.
28. C. Chin-Ling et al, (2018). An Improvement on Remote User Authentication Schemes Using Smart Cards. MDPI. 7, 9; pp. 1-19.
29. R. Swapnoneel and K. Chanchal, (2017). Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols. MDPI. Vol.1, Issue 9, pp. 1-25.