Journal of Information Security, 2020, 11, 161-175
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Remote Access Communications Security: Analysis of User Authentication Roles in Organizations

Ezer Osei Yeboah-Boateng, Grace Dzifa Kwabena-Adade

Faculty of Computing & Information Systems (FoCIS), Ghana Technology University College, Accra, Ghana
Email: eyeboah-boateng@gtuc.edu.gh

How to cite this paper: Yeboah-Boateng, E.O. and Kwabena-Adade, G.D. (2020) Remote Access Communications Security: Analysis of User Authentication Roles in Organizations. *Journal of Information Security*, **11**, 161-175.
https://doi.org/10.4236/jis.2020.113011

Received: June 17, 2020
Accepted: July 14, 2020
Published: July 17, 2020

Abstract

Remote access is a means of accessing resources outside one's immediate physical location. This has made employee mobility more effective and productive for most organizations. Remote access can be achieved via various channels of remote communication, the most common being Virtual Private Networks (VPNs). The demand for remote access is on the rise, especially during the Covid-19 pandemic, and will continue to increase as most organizations are re-structuring to make telecommuting a permanent part of their mode of operation. Employee mobility, while presenting organizations with some advantages, comes with the associated risk of exposing corporate cyber assets to attackers. The remote user and the remote connectivity technology present some vulnerabilities which can be exploited by any threat agent to violate the confidentiality, integrity and availability (CIA) dimensions of these cyber assets. So, how are users and remote devices authenticated? To what extent is the established connection secured? With employee mobility on the rise, it is necessary to analyze the user authentication role since the mobile employee is not under the monitoring radar of the organization, and the environment from which the mobile employee connects may be vulnerable. In this study, an experiment was setup to ascertain the user authentication roles. The experiment showed the process of 2FA in user authentication and it proved to be an effective means of improving user authentication during remote access. This was depicted via the use of what the user has (mobile phone/soft-token) as a second factor in addition to what the user knows, *i.e.* password. This authentication method overcomes the security weaknesses inherent in single-factor user authentication via the use of password only. However, the results also showed that though 2FA user authentication ensures security, the remote devices could exhibit further vulnerabilities and pose serious risks to the organization. Thus, a varied implementation was recommended to further enhance the security of remote access communication with regards to the remote user authentication.

Keywords

Remote Access, Communications Security, User Authentication, 2FA, Virtual Private Network (VPN), Telecommuting, Threats, Vulnerabilities

1. Introduction

Many businesses today are utilizing the Internet and its technologies as vital business tools than ever before [1]. The benefits of IT as a tool for business cannot be overemphasized. Almost every organization leverages some aspects of IT in their daily operations. Some opportunities businesses utilized include employee mobility via remote access technologies, improved production via enterprise resource planning technologies, competitive advantage via user-friendly and customer-focused products among others.

Remote access is basically the ability to grant access to an authorized entity from distant locations for the purposes of computing and networking. Various types of remote access are available, such as virtual private network (VPN), desktop sharing or privilege access management (PAM).

Globalization has made employee mobility or telecommuting a necessary part of most organizations, and therefore most companies have adopted mechanisms to allow staff effectively access corporate resources while away from the work premise. While employee mobility enhances productivity, it comes with a myriad of cyber risks that could be exploited for successful attacks. Negligence on the part of the remote user could result in catastrophic consequences for any organization [1]. It is therefore necessary to enhance the security of IT infrastructure as well as user authentication methods to mitigate possible vulnerabilities inherent in user authentication. Verizon [2] reported password leaks as a major contributor to data breaches relating to remote access and connectivity. Most users tend to use the same password across several accounts due to human challenges in recalling and/or use different passwords. A single compromised password could afford the attacker access to several other accounts or resources accessible to the user.

Many research works have proposed password replacement schemes to curb security concerns with user authentication. With two-factor authentication (2FA), stolen password attacks could be prevented since the attacker must validate a second factor before gaining access to the user's account. In recent times, huge IT organizations such as Google, Microsoft, Facebook among others, have implemented two-factor authentication mechanism in their services. 2FA enhances single factor authentication and provides a layer of security by requesting the user to be authenticated twice before access to requested resources is granted. 2FA relies on existing password authentication (something the user knows), in addition to something the user has such as hardware token or something the user is such as fingerprint pattern. While 2FA does not promise total security, when implemented properly, it ensures that attacks are made difficult for the attacker. For example, remote impersonation attacks can easily be overcome by 2FA such that should a user's password be stolen or guessed, the attacker would need to have access to the second factor such as the hardware token, the soft-token generated on the user's phone, etc. before access can be granted. 2FA could be implemented in many forms such as one-time password (OTP), Accept/Reject Buttons, QR Code Scanning, hardware tokens such as Ron Rivest, Adi Shamir and Leonard Adleman (RSA) SecurID, etc.

This study assumes that 2FA is usable if properly implemented with users properly trained to be aware of cyber security implications [3].

The succeeding sections review literature relevant to the study, the methodological approach adopted for the study, the findings of the study presented to show packet capture information that will be relevant to a malicious actor and finally, conclusions and recommendations offered.

2. Literature Review

According to the U.S Code, information security is ensuring that information and information systems are safeguarded with the aim of providing confidentiality, integrity and availability [4]. Information security is to ensure that information and information systems do not get into wrong hands to be manipulated or used for wrong or harmful purposes. There is dearth of literature on the use of IT as a tool to curb human weaknesses in information security. Most literature focus on user training to increase security awareness. A 2018 UK-based cyber report indicated that most large corporate institutions prioritize cyber security as compared to smaller organizations, and therefore provide cyber awareness training for staff [5]. However, in Africa, training is not commensurate to cyber-attacks [6]. Most organizations do not provide training, while others wait until an attack happens or in most cases provide training which has very little information security content. These, coupled with other factors, contribute to the ever-increasing successes in cyber-attacks since threat agents are working round the clock with sophisticated tools at their disposal. One could not agree less with [7] that it is about time organizations realize that while training is important, it is imperative to complement it with technical mechanisms to minimize the user weaknesses in the cyber security chain.

2.1. Remote Access Connection

Remote access refers to reaching data or resources which is outside one's immediate location. Remote access in the corporate sense could either be in the form of telecommuting or workers accessing corporate resources from outside the corporate network or in the form of technical support firms accessing a user's machine from a remote location for technical assistance [8]. Previously, remote access connection was established via traditional dial-up technologies. Dial-up technology was expensive due to either an organization procuring a leased dedicated circuit from public switched telephone network (PSTN) or by privately installing wired circuits [9]. Currently virtual private network (VPN) technologies have replaced traditional dial-up methods. Irrespective of the means used to establish remote access, some technologies need to be in place to implement the access connection and to establish communication. Some of these technologies include the protocols required to establish connection between a client and remote server, as well as protocols to secure the transmission of data between the endpoints in the connection. Additionally, there must be in place an access method and control mechanism to facilitate communication between the client and remote server as well as ensure only legitimate users have access to resources remotely.

- Remote Desktop is a type of remote access method that enables a user to reach and control another computer from a remote location as though the remote computer is local. The remote user can see, take control of, and interact with the remote computer. Remote desktop access requires the installation of supported software on both local and remote computers for a successful connection and communication. Remote desktop is usually used by technical staff to aid users remotely on technical or other user support needs. It is also employed by system and network administrators to control, administer and support systems and users on the network [8].
- Virtual Private Network (VPN) is an extension of a local area network by establishing a tunnel between two endpoints via technologies such as Secure Socket Layer (SSL), Open VPN, etc. VPN enables a remote user to be part of a corporate network and access corporate resources. Most VPN implementations make use of Layer 2 Tunneling Protocol (L2TP) which allows service providers to enable remote dialup VPN access for customers. To protect data in transit over the public Internet, data is encrypted and encapsulated via IP Security (IPSec) technology. This ensures that, data in transit via the tunnel cannot be eavesdropped on or intercepted by man-in-the-middle attacks [10]. Due to these security measures provided in the implementation of VPN connections, organizations have a level of security reliance on VPN to improve productivity since workers can access resources from any location outside the work premise.
- VPN connectivity could be implemented in two variations which are client-to-site and/or site-to-site connections. Client-to-site connections involve corporate network and a remote user, whereas site-to-site involves two (2) or more corporate networks.
- Other methods include Wide Area Network (WAN), integrated services digital network (ISDN) or digital subscriber line (xDSL) [11].

2.2. User Authentication

2.2.1. User Authentication Factors

An authentication factor is a credential that is required whenever a user needs to validate their identity to access a system. There are basically three broad categories of factors commonly deployed in user authentication, each of which is described below [12]:

- Knowledge-Based Factors

Knowledge-based factors refer to something the user knows. Examples of such factors include password, personal identification number (PIN), etc. knowledge-based factors are mostly used in single-factor authentication where the user is required to provide a valid username and corresponding password to access a system.

- Possession-Based Factors

Possession-based factors refer to something the users have in their possession. Examples of such factors include hardware token device, a smart phone, security USB drive, etc.

- Inherence Factors

Inherence factors are "something the users are made of" and are metrics intrinsically owned by authorized users or entities. They typically manifest as biometric-based factors, which include fingerprints, facial, retina or voice patterns, etc.

2.2.2. User Authentication Types

Described below are some common authentication types available, according to [13].

- Password Authentication

Password authentication is the most common type of user authentication [14]. It is also referred to as a single factor authentication (SFA). It requires the user to input a secret that is known to them. This secret could be a password, a PIN or a pattern. Lamport [15] was the first to introduce password authentication. Research shows that this type of authentication is less secure and has been prone to several cyber-attacks such as password guessing, brute force attacks, phishing among others.

- Two-Factor Authentication (2FA)

Two-factor authentication is a type of authentication that complements single-factor authentication to provide an additional layer of security. This is achieved by means of requesting the user to type in a code from a software or hardware token after entering a valid username and password. 2FA was designed to resolve some known vulnerabilities with SFA [16]. While this type of authentication does not offer hundred percent security, it is better and safer than single-factor authentication. 2FA was first proposed by [17] and has gone through many evolutions towards an enhanced authentication mechanism. Some variations of 2FA include smart cards, hardware security tokens, soft-based tokens among others.

- Biometric Authentication

The United States Department of Homeland Security defines Biometrics as unique physical properties that can be used for automatic recognition [18]. Biometric authentication relies on user physiological characteristics for authentication purposes. Some physical characteristics include iris colour, fingerprint pattern, facial recognition among others. This authentication methods seeks to improve upon 2FA and overcome some security challenges present in 2FA. Biometric authentication was first introduced by [19], who proposed the first three-factor authentication method based on biometrics. Three-factor authentication improves upon SFA by assuring physical presence of the user.

2.3. User Authentication Role in Remote Access Connection

Remote access to corporate resources via VPN requires a remote client to initiate the connection. The remote client is the computer user who could be at home, in a coffee shop, at a friend's workplace or at a public Internet café. Irrespective of location, the remote connection requires the user to first have Internet connectivity, and then to authenticate via the remote access client application installed and configured on their machine, to access corporate resources. While single factor authentication is considered insecure, VPN inherently does not foster strong user authentication mechanism [20]. Additionally, users can misplace their authentication credentials, share with friends and family, inadvertently yield credentials to threat agents via social engineering attacks, fall prey to shoulder surfing, or compromise the computing machine to be used as a command and control unit to infest their corporate network due to negligence on the source of Internet connectivity used remotely. These actions or inactions by the user could result in a threat agent gaining unauthorized access to corporate resources which could have ripple adverse implications on the organization. The use of additional authentication factors for remote access, such as one-time-password, in addition to single factor authentication could alert the user to take necessary action against any connection that they or anyone they have shared credentials with have not initiated. Where computer authentication is implemented, this could further make it harder to threat agents to gain access and thereby mitigate inherent risks.

3. Experimental Methodology

3.1. Experimental Design

Design of experiment is basically a design of activities geared towards describing and explaining an observed concept of information or difference in conditions, typically within set limits, and that are occasioned to prove the concept or otherwise. In this study, the design experiment consisted of 3 key phases, as follows:

- Identification phase:

In this phase, the remote user logs on to the VPN client with a valid username. The VPN client communicates with the firewall for authentication.

- Authentication phase

The firewall is configured with Remote Authentication Dial-In User Service (RADIUS) server which points to the IP address of Microsoft Active Directory

(AD). Microsoft Active Directory is the centralized user database that contains every information required to successfully authenticate the user [21]. During the authentication phase, user inputs logon credentials, the hash value is passed to the AD via firewall RADIUS for the AD to confirm if the credentials are valid by matching it to the AD's hashed value of stored user credentials. If successful, the VPN client prompts user for token. The firewall communicates with the user via email for initial setup of token. Subsequent tokens are generated on the authentication app. After successful validation of token, a secure connection is established between the remote user and the corporate network.

- Secure Tunnel Establishment

In this phase, the network is monitored for IPSec tunnel establishment negotiation protocols. Communication protocols being used in the VPN tunnel establishment process are also monitored to analyze any possible attacks that could be initiated against the protocols.

3.2. Experimental Setup

- Remote User

The remote user is a staff with a valid username and password. The username is for identification and the password is for authentication. For 2FA, the user email ID is also registered in the firewall with 2FA option enabled for remote connectivity (Table 1).

- Remote Client

The remote client is the corporate laptop assigned to staff for corporate work. The remote client has a VPN client installed and configured for remote access. Table 2 depicts the specifications for both the remote client and the VPN client.

Table 1. Remote User Credentials.

No.	Remote User	Username	Password	Email ID
1	Staff-1	Remote_User1	**********	remoteuser1@internet.com
2	Staff-2	Remote_User2	**********	remoteuser2@internet.com
3	Staff-3	Remote_User3	**********	remoteuser3@internet.com
…	…	…	…	…
n	Staff-n	Remote_Usern	**********	remoteusern@internet.com

Table 2. Specifications of remote and VPN clients.

Remote Client Specifications	VPN Client Specifications
Model: HP EliteBook	Brand: FortiClient VPN
Operating System: Windows 10 Pro	Version: 6.2.1.0831
RAM: 8 GB	FortiToken Mobile Version: 4.6.0.0098
HDD: 500 GB	
Processor: Intel Core i7 (8th Gen)	

- Authentication Server

The authentication server contains details about registered users and laptops. Microsoft Active Directory (AD) is used for this experiment. HP ProLiant 380 Gen9 server was used running Windows Server 2012 Standard R2.

3.3. Network Traffic Monitoring Tool

- Wireshark

Wireshark is a free downloadable software which is compatible with windows operating systems. It was used to capture packets of data as they traverse the communication link between the remote user the corporate network.

- FortiGate 100E (Firewall)

The firewall records logs on user and network activity. These logs were also monitored and analyzed for network traffic.

3.4. Experimental Process

In **Figure 1**, the authentication process flow is described. In the first phase, the user supplied valid username and password which were authenticated from Microsoft AD via RADIUS configured on the firewall. This is depicted as XAUTH (extended authentication) in the firewall interface. Upon successful XAUTH, the second phase is initiated where the user is prompted by the VPN client to provide a soft-token generated on the mobile authentication App. Upon successful token validation, the remote connection is successfully established. The user can then access corporate resources such as files servers, print services among others.

Below is a description of the flow of activities as depicted in the figure:

1) Remote user opens FortiClient and enters username and password;

2) The username and password are transported over the Internet to the Firewall;

3) The Firewall confirms the username and password validity (Single Factor Authentication) from the Microsoft Active Directory via RADIUS authentication;

4) A successful Single Factor Authentication is communicated by the Active Directory to the Firewall;

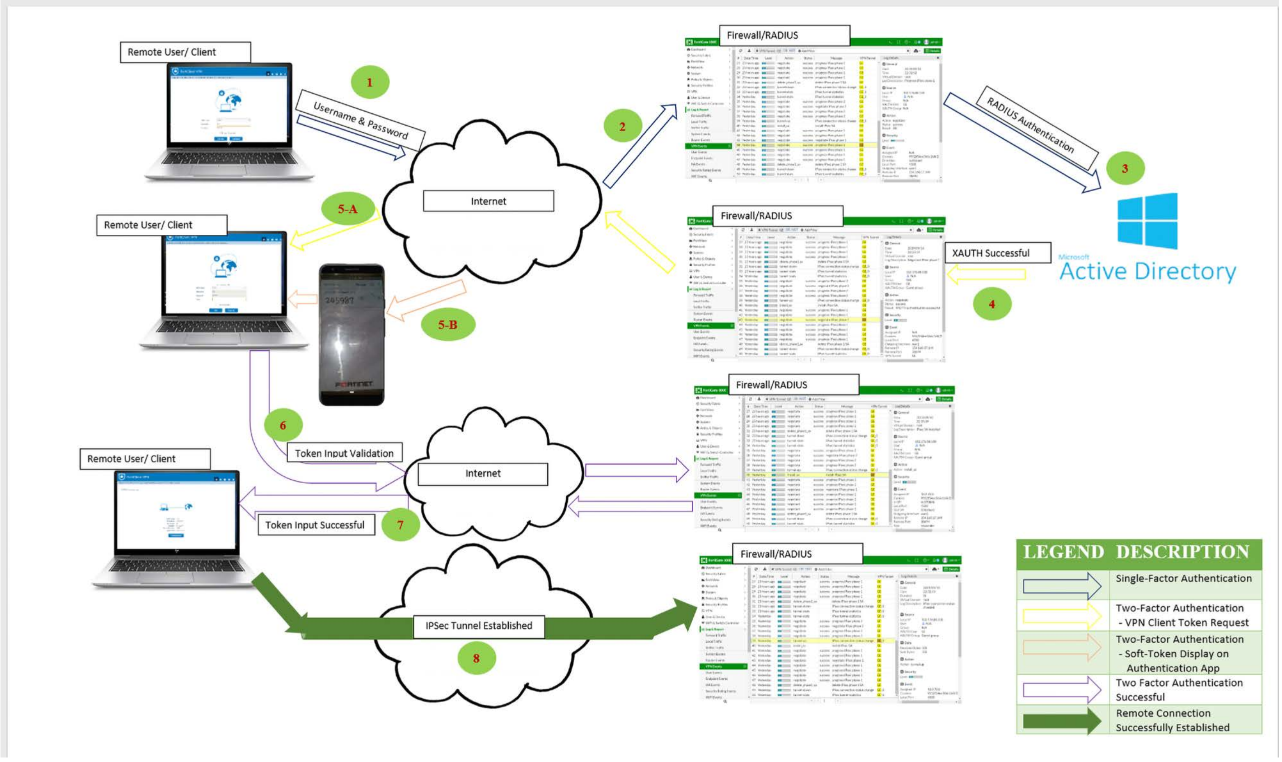
5A) Successful Single Factor Authentication is communicated to the Remote Client via the FortiClient and requested to provide a second factor (*i.e.* the soft-generated token) for authentication;

5B) The soft-generated token is displayed on the Mobile FortiToken and the user enters it in the FortiClient's Token field;

6) The token inputted by the user is validated by the Firewall (*i.e.* second factor authentication);

7) A successful two factor authentication is communicated between the firewall and the FortiClient; and

8) A secure IPSec tunnel is established between the firewall and the remote client, providing the remote user secure access to the corporate network and resources.



LEGEND	DESCRIPTION
⇨	Single-Factor Authentication
⇨	Two-Factor Authentication - VPN Client Token Request
⇨	Two-Factor Authentication - Soft-Token Display on Authentication App
⇨	Two Factor Authentication Successful
➡	Remote Connection Successfully Established

Figure 1. User authentication & remote access connection (Source: Fieldwork).

4. Findings and Data Analysis

4.1. Findings

Presented below in the ensuing sections are the findings of the experiment.

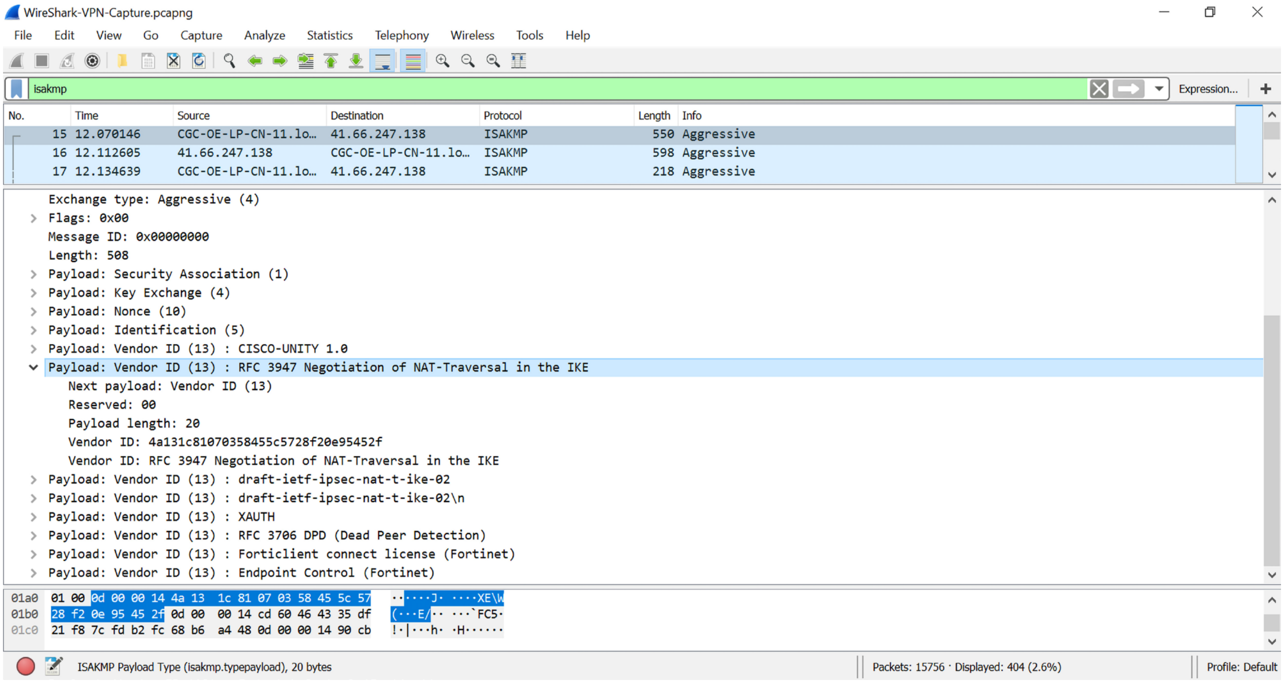
Figure 2 depicts the remote client information detailing the IP addresses used in the sessions. It displays both source and destination IP addresses associated with the query and the connection parameters.

Figure 3 depicts the network address translation (NAT) traversal techniques used in Internet Key Exchange (IKE) negotiations, in accordance with IETF RFC 3947. Basically, NAT traversal is a networking technique use in establishing and maintaining IP-based connections across the NAT-based gateways establishing the VPN connections. Technically, the gateways exchange keys to establish the secure VPN communications channel between them. As a prelude, they authenticate each other and negotiate a way to encrypt subsequent communications for establishing the session [22].

As indicated earlier, Figure 3 dealt with the negotiation aimed at establishing the VPN connection. Then, in Figure 4 appropriate encryption and integrity check are performed on all ISAKMP messages between the entities. Further the IKEv1 negotiation is initiated to establish how the entities will use security services to communicate securely, utilizing IPSec security associations (SAs).

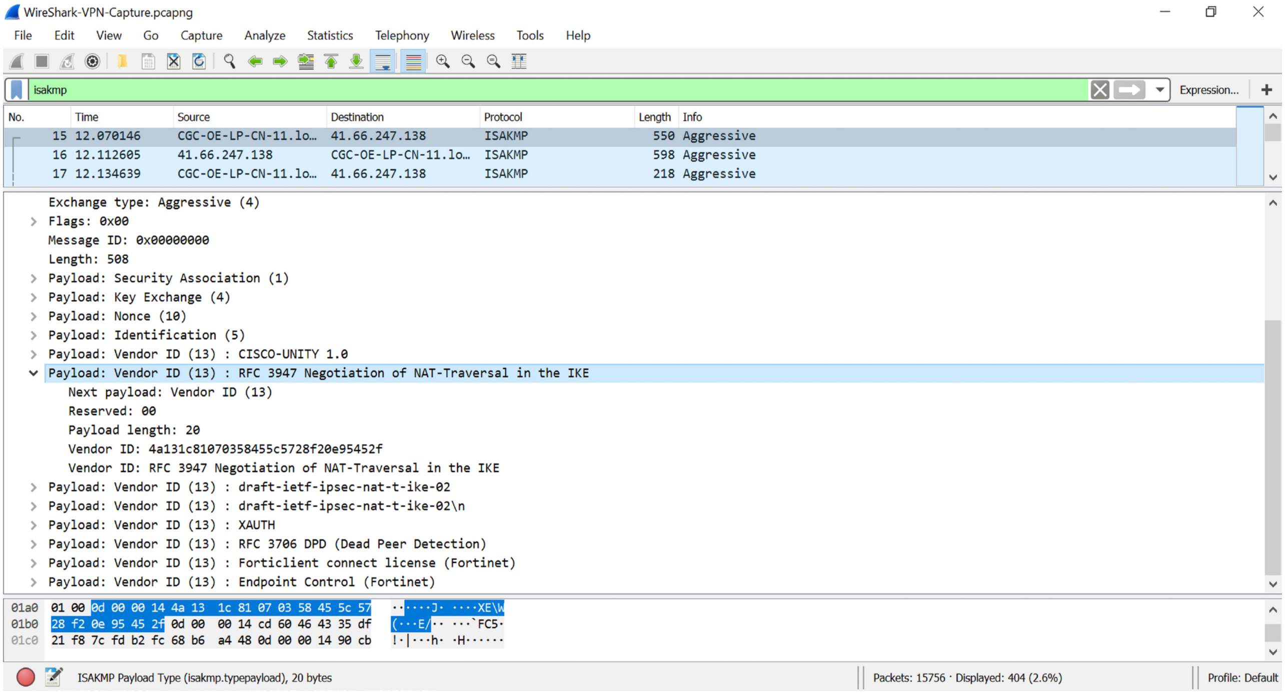
4.2. Data Analysis

The research utilized descriptive data analysis with data obtained from the experiment conducted. The experiment provided data such as the factors used in user authentication, the factors used in remote access communications as well as the impact these factors have on remote access security. Some of the factors include use of password as an authentication factor, remote host details such as IP addresses, authentication protocols among others.



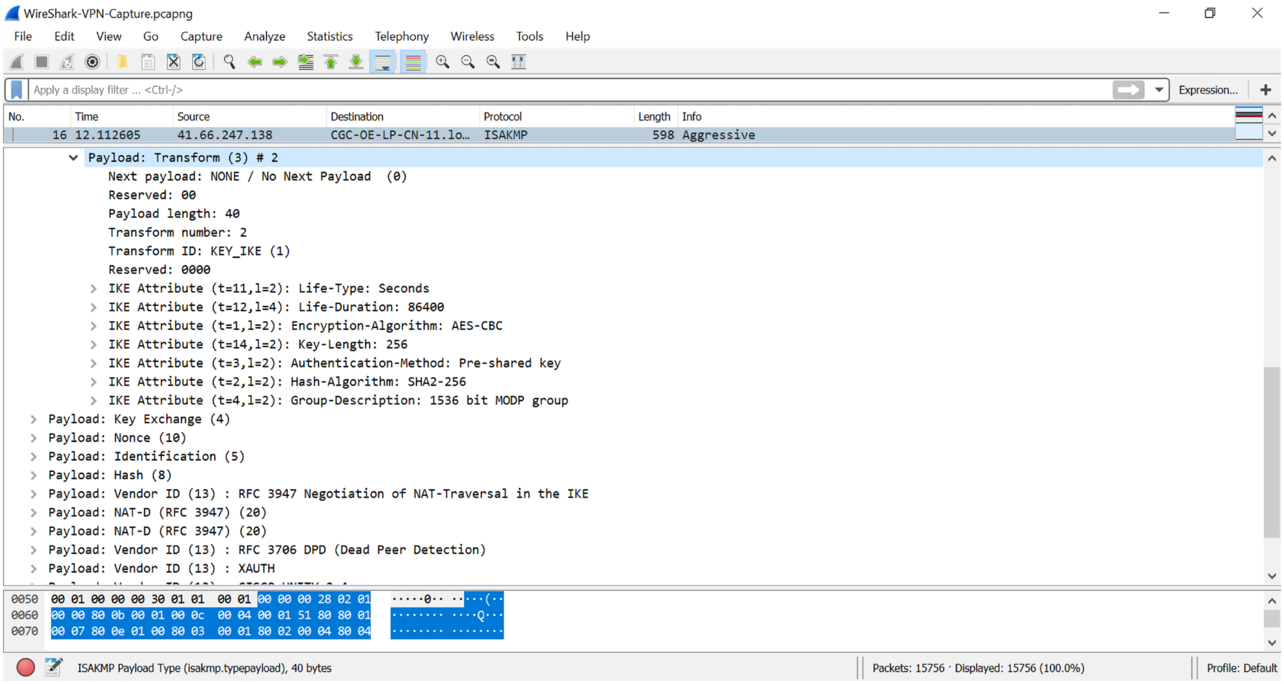
```
isakmp

No.  Time       Source               Destination          Protocol  Length  Info
  15 12.070146  CGC-OE-LP-CN-11.lo…  41.66.247.138        ISAKMP       550  Aggressive
  16 12.112605  41.66.247.138        CGC-OE-LP-CN-11.lo…  ISAKMP       598  Aggressive
  17 12.134639  CGC-OE-LP-CN-11.lo…  41.66.247.138        ISAKMP       218  Aggressive

    Exchange type: Aggressive (4)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 508
  > Payload: Security Association (1)
  > Payload: Key Exchange (4)
  > Payload: Nonce (10)
  > Payload: Identification (5)
  > Payload: Vendor ID (13) : CISCO-UNITY 1.0
  v Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
      Next payload: Vendor ID (13)
      Reserved: 00
      Payload length: 20
      Vendor ID: 4a131c81070358455c5728f20e95452f
      Vendor ID: RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
  > Payload: Vendor ID (13) : XAUTH
  > Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  > Payload: Vendor ID (13) : Forticlient connect license (Fortinet)
  > Payload: Vendor ID (13) : Endpoint Control (Fortinet)

01a0  01 00 0d 00 00 14 4a 13  1c 81 07 03 58 45 5c 57   ······J· ····XE\W
01b0  28 f2 0e 95 45 2f 0d 00  00 14 cd 60 46 43 35 df   (···E/·· ···`FC5·
01c0  21 f8 7c fd b2 fc 68 b6  a4 48 0d 00 00 14 90 cb   !·|···h· ·H······

ISAKMP Payload Type (isakmp.typepayload), 20 bytes    Packets: 15756 · Displayed: 404 (2.6%)    Profile: Default
```

Figure 2. Remote client IP address (Source: Fieldwork).



```
isakmp

No.  Time       Source               Destination          Protocol  Length  Info
  15 12.070146  CGC-OE-LP-CN-11.lo…  41.66.247.138        ISAKMP       550  Aggressive
  16 12.112605  41.66.247.138        CGC-OE-LP-CN-11.lo…  ISAKMP       598  Aggressive
  17 12.134639  CGC-OE-LP-CN-11.lo…  41.66.247.138        ISAKMP       218  Aggressive

    Exchange type: Aggressive (4)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 508
  > Payload: Security Association (1)
  > Payload: Key Exchange (4)
  > Payload: Nonce (10)
  > Payload: Identification (5)
  > Payload: Vendor ID (13) : CISCO-UNITY 1.0
  v Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
      Next payload: Vendor ID (13)
      Reserved: 00
      Payload length: 20
      Vendor ID: 4a131c81070358455c5728f20e95452f
      Vendor ID: RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
  > Payload: Vendor ID (13) : XAUTH
  > Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  > Payload: Vendor ID (13) : Forticlient connect license (Fortinet)
  > Payload: Vendor ID (13) : Endpoint Control (Fortinet)

01a0  01 00 0d 00 00 14 4a 13  1c 81 07 03 58 45 5c 57   ······J· ····XE\W
01b0  28 f2 0e 95 45 2f 0d 00  00 14 cd 60 46 43 35 df   (···E/·· ···`FC5·
01c0  21 f8 7c fd b2 fc 68 b6  a4 48 0d 00 00 14 90 cb   !·|···h· ·H······

ISAKMP Payload Type (isakmp.typepayload), 20 bytes    Packets: 15756 · Displayed: 404 (2.6%)    Profile: Default
```

Figure 3. NAT traversal in IKE negotiations (Source: Fieldwork).


WireShark-VPN-Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.   Time       Source          Destination          Protocol  Length Info
   16 12.112605  41.66.247.138   CGC-OE-LP-CN-11.lo…  ISAKMP       598 Aggressive

      Payload: Transform (3) # 2
         Next payload: NONE / No Next Payload  (0)
         Reserved: 00
         Payload length: 40
         Transform number: 2
         Transform ID: KEY_IKE (1)
         Reserved: 0000
       > IKE Attribute (t=11,l=2): Life-Type: Seconds
       > IKE Attribute (t=12,l=4): Life-Duration: 86400
       > IKE Attribute (t=1,l=2): Encryption-Algorithm: AES-CBC
       > IKE Attribute (t=14,l=2): Key-Length: 256
       > IKE Attribute (t=3,l=2): Authentication-Method: Pre-shared key
       > IKE Attribute (t=2,l=2): Hash-Algorithm: SHA2-256
       > IKE Attribute (t=4,l=2): Group-Description: 1536 bit MODP group
  > Payload: Key Exchange (4)
  > Payload: Nonce (10)
  > Payload: Identification (5)
  > Payload: Hash (8)
  > Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: NAT-D (RFC 3947) (20)
  > Payload: NAT-D (RFC 3947) (20)
  > Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  > Payload: Vendor ID (13) : XAUTH

0050  00 01 00 00 00 30 01 01  00 01 00 00 00 28 02 01   ·····0·· ···(··
0060  00 00 80 0b 00 01 00 0c  00 04 00 01 51 80 80 01   ········ ····Q···
0070  00 07 80 0e 01 00 80 03  00 01 80 02 00 04 80 04   ········ ········

ISAKMP Payload Type (isakmp.typepayload), 40 bytes    Packets: 15756 · Displayed: 15756 (100.0%)    Profile: Default
```

Figure 4. IKEv1 negotiation parameters (Source: Fieldwork).

Attack Vectors on Remote User Authentication

- Remote User Details

✧ Passwords

Passwords were hashed and were therefore not visible in Wireshark [23]. However, recent research from Ruhr-University showed a vulnerability with IPSec VPN. An aspect of the VPN connection under review was password-based login. From their experiment, weak passwords could easily be compromised and make it possible to attack Internet Key Exchange (IKE) protocols [23]. There are several studies that indicate the risks associated with weak passwords. Some system administrators, though expected to know better, use weak passwords or set up systems with default passwords which could have dire consequences if exploited [14] [24].

- Remote Host Details

✧ IP Address:

Wireshark captured the remote user's laptop IP address as well as the IP address of the corporate endpoint on which the VPN terminates (FortiGate Firewall, in this experiment). While public knowledge of an organization's IP address does not pose much threat to any organization, human errors could provide a means for malicious actors to exploit network devices which have public IP address configured. For example, if the firewall used in this experiment has the factory default password unchanged, a malicious actor sniffing the network and getting to know the public IP address of the firewall could try to hack into the corporate network. This malicious agent could initiate a router hacking, denial of service attack or DNS spoofing [25].

- Authentication Protocols

There are several authentication protocols used in IPSec VPN. Two main ones are:

✧ Authentication Header (AH) protocol

AH protocol is defined in RFC 2402. It provides data integrity by validating the source of the IP packets and protects against replay attacks [26].

✧ ESP

ESP protocol is defined in RFC 2406. ESP provides encryption. Confidentiality, integrity and protects against replay attacks [26].

VPN authentication methods are in public domain and are therefore known to the public. However, it is important to implement VPN with protocols that are current and provide optimum security.

- Tunnel Negotiation Protocols

✧ Internet Key Exchange (IKE)

Prior to remote connection establishment, the remote peer (remote client) and corporate peer (firewall) negotiate on pre-configured parameters to ascertain the validity of each other. This is via Internet Key Exchange (IKE) protocol. There are two (2) versions of IKE, which are IKEv1 and IKEv2. IKEv1 is obsolete and has been succeeded by IKEv2, however, most VPN implementations continue to use IKEv1. IKEv1 and IKEv2 have been showed to be vulnerable to deliberate error codes that allow threat agents to launch a man-in-the-middle attacks against IPSec VPN [27].

Phases involved in IKE negotiations are:

- IPSec Phase 1

IPSec phase 1 negotiation could either be main mode or aggressive mode. In main mode exchange, the remote client and corporate peer authenticate each other in multiple rounds with encrypted information while in aggressive mode, parameters are exchanged in a single message with unencrypted authentication information. Authentication parameters could be a pre-shared key or a digital certificate. For this experiment, pre-shared key was used, with aggressive mode.

- IPSec Phase 2

IPSec phase 2 negotiation uses quick mode for the parameters exchange. Exchange in phase 2 is encrypted.

5. Conclusions

This research work was able to demonstrate that 2FA enhances security of the user authentication role in remote access communications. This was depicted via the mobile token which proved that an attacker will need to acquire both single factor as well as the user's phone, for a successful attack. A proper implementation of 2FA will serve as a first line mechanism of strengthening the user authentication role and thus improve remote access security. While not a total security mechanism, it is a first-hand means to frustrate an attacker's efforts.

The increasing rate at which technology is advancing has led to many changes in the way corporate institutions operate. Remote working has become part of many organizations as well as the introduction of various mobile devices to the corporate network. However, organizations face a myriad of security issues associated with the freedom IT provides or its ubiquitous nature. While it is convenient for users to work from any location and from any device, it may not be the safest of choices for an organization's cyber assets. There is therefore the need to implement and enforce end user remote authentication policies and solution, complemented with result-driven training and awareness programs to safeguard corporate resources. The user is consistently the greatest risk factor to an organization's information security and must therefore be given optimum attention to mitigate consequences of user authentication vulnerabilities. Businesses need to enhance the kind of training and cyber awareness provided to end users, however, training alone will not be enough to mitigate cyber threats [7]. Businesses need to conduct regular security assessments, monitor network traffic for any malicious activities and adopt improved authentication mechanisms to mitigate loopholes in user authentication security. While Cisco recommends 2FA as a solution to security in remote user access, [28] [29] believe that the only solution to authentication vulnerabilities is to adopt biometric authentication. This is because, biometric authentication offers sure proof of genuine user being present. However, from this study, biometric authentication only cannot suffice in remote connection security. The remote device must also be authenticated even if the genuine user is present. Thus, the proposed future works recommended device authentication as a second factor in addition to soft-token 2FA. The next section discussed proposed modifications that could be considered in similar work.

6. Recommendation

Based on the findings from the experiment, the study recommends the adoption of true 2FA solution. This study considers a true 2FA solution to be one that authenticates both user and device before remote access is granted. In this kind of 2FA, the user is authenticated with username and password as single factor, and then authenticated via digital certificate of the connecting laptop in addition to soft-token generated on authentication app. The digital certificate is deployed to the connecting client via Simple Certificate Enrolment Protocol (SCEP). Complementing soft-token with laptop authentication ensures a high degree of validity of the remote user since it will be rare for a hacker to obtain both user laptop and phone to successfully masquerade as a genuine user.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Yeboah-Boateng, E.O. (2013) Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availablity (CIA). Center for Communications, Media & Information Technologies (CMI), Aalborg University,

Copengahen, 1-217.

[2] Zaw, T. and Yew, R. (2017) Data Breach Investigations Report (DBIR) from the Perspective. https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf

[3] Gilsenan, C. (2018) Two Factor Authentication (2FA): What Is It? How Does It Work? Why You Should Care! https://www.allthingsauth.com/2018/02/22/two-factor-authentication-2fa

[4] United States Code (2011) United States Code, 2010 Edition, Supplement 5, Title 44 Public Printing and Documents.

[5] Department for Digital, Culture, Media & Sport (2018) Cyber Security Breaches Survey 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

[6] Serianu Limited (2018) Sacco Cybersecurity Report 2018 Demystifying Cbersecurity for Saccos. https://www.serianu.com/downloads/SaccoCyberSecurityReport2018.pdf

[7] Serianu Limited (2017) Africa Cyber Security Report. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

[8] Pinola, M. (2019) What Is Remote Access? https://www.lifewire.com/what-is-remote-access-2377975

[9] Jyothi, K.K. and Reddy, D.I.B. (2018) Study on Virtual Private Network (VPN), VPN's Protocols and Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, **3**, 919-932.

[10] Younglove, R.W. (2001) IP Security What Makes It Work. *Computing & Control Engineering Journal*, **12**, 44-46. https://doi.org/10.1049/cce:20010107

[11] Yfantis, V. (2018) What Is Remote Access Control? https://www.parallels.com/blogs/ras/remote-access-control

[12] Rouse, M. (2014) Authentication Factor. https://searchsecurity.techtarget.com/definition/authentication-factor

[13] SolarWinds MSP (2019) Common Network Authentication Methods. https://www.solarwindsmsp.com/blog/network-authentication-methods#

[14] Ponemon Institute (2019) The 2019 State of Password and Authentication Security Behaviors Report. https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf

[15] Lamport, L. (1981) Password Authentication with Insecure Communication. *Communications of the ACM*, **24**, 770-772. https://doi.org/10.1145/358790.358797

[16] Krol, K., Philippou, E., De Cristofaro, E. and Sasse, A.M. (2015) They Brought in the Horrible Key Ring Thing! Analysing the Usability of Two-Factor Authentication in UK Online Banking. https://doi.org/10.14722/usec.2015.23001

[17] Chang, C.-C. and Wu, T.-C. (1991) Remote Password Authentication with Smart Cards. *IEEE Proceedings* (*Computers and Digital Techniques*), **138**, 165-168. https://doi.org/10.1049/ip-e.1991.0022

[18] Department of Homeland Security (2019) Biometrics. https://www.dhs.gov/biometrics

[19] Juels, A. and Wattenberg, M. (1999) CCS '99 Proceedings of the 6th ACM Conference on Computer and Communications Security. Kent Ridge Digital Labs, Singapore.

[20] Talabis, M.R.M., McPherson, R., Miyamoto, I. and Martin, J.L. (2015) Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, Waltham.

[21] Microsoft (2017) Active Directory Domain Services Overview. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[22] Fortinet (2019) FortiAuthenticator 6.0.0 > Administration Guide. https://docs.fortinet.com/document/fortiauthenticator/6.0.0/administration-guide/942259/what-to-configure

[23] Ruhr-University Bochum (2018) Security Gaps Identified in Internet Protocol "IP-sec". https://www.sciencedaily.com/releases/2018/08/180814134201.htm

[24] Yeboah-Boateng, E.O. and Boadi, E.B. (2015) An Assessment of Corporate Security Policy Violations Using Live Forensics Analysis. *International Journal of Cyber-Security and Digital Forensics*, **4**, 1-10. https://doi.org/10.17781/P001385

[25] Mortensen, P. (2019) Can a Hacker, That Knows My IP Address, Remotely Access Accounts I Have Left Logged in on My Computer? https://security.stackexchange.com/questions/186929/can-a-hacker-that-knows-my-ip-address-remotely-access-accounts-i-have-left-log

[26] Juniper Networks (2019) Overview of IPSec. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/overview-of-ipsec.html#id-11440337

[27] Seals, T. (2018) Researchers Break IPsec VPN Connections with 20-Year-Old Protocol Flaw.

[28] Song, S. (2008) SSL VPN Security. https://www.cisco.com/c/en/us/about/security-center/ssl-vpn-security.html

[29] Syed Idrus, S.Z., Cherrier, E., Rosenberger, C. and Schwartzmann, J.-J. (2013) A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences*, **7**, 95-107.