I. J. Computer Network and Information Security, **2019, 11, 36-45**
Published Online November 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.11.05

A Domains Approach to Remote Access Logical Vulnerabilities Classification

Samuel Ndichu
School of Computing and Informatics, Maseno University, Private Bag, Maseno, Kenya
E-mail: ndichu.ranji@gmail.com

Sylvester McOyowo, and Henry Okoyo
School of Computing and Informatics, Maseno University, Private Bag, Maseno, Kenya
E-mail: oyowosilver@gmail.com; okoyo.ho@gmail.com

Cyrus Wekesa
Department of Electrical and Information Engineering, University of Nairobi, Nairobi, Kenya
E-mail: cyrus.wekesa@gmail.com

Received: 16 October 2019; Accepted: 25 October 2019; Published: 08 November 2019

Abstract—Remote access facilitates collaboration and the creation of a seamless work environment. This technology enables employees to access the latest versions of data and resources from different locations other than the organization’s premises. These additional locations include home or untrusted networks not governed by the organization's security policy and baseline. Balancing between security and accessibility is a significant challenge. Remote access can be a high-security risk if not correctly safeguarded and monitored. This paper presents some technologies and methods for remote access. It then highlights security concerns, attack vectors, and logical vulnerabilities in remote access. To address these security concerns and weaknesses, we present a domains approach to logical vulnerabilities in remote access and vulnerability scoring using the Common Vulnerability Scoring System (CVSS). Domains simplify device and user authentication and separate the organization network into logical and discrete entities. The separation enables a unique security application to each domain. Vulnerability scoring enhances remediation efforts through prioritization of the logical vulnerabilities. The approach comprehensively covers all points of compromise during remote access and contributes to effective logical vulnerability management. The results of the experiments provide evidence that all remote access domains have a high severity rating of at least a 7.28 CVSS score. Our study highlights the drawbacks of the current remote access methods and technologies such as the Virtual Private Network (VPN) and shows the importance of securing all domains during remote access.

Index Terms—Remote access, logical vulnerabilities, domains, attack vectors, vulnerability scoring.

I. Introduction

Today’s networked environments are highly mobile, and remote access is necessary to be able to achieve various organizational goals and objectives. Remote access, also referred to as remote login, is the ability to access data and resources from a remote location other than the organization's facilities [1]. Remote access involves the use of different methods and technologies to allow employees access to an organization's data and resources on the road, at home, or even from remote organizational sites [2]. Use of Virtual Private Networks (VPN), Local Area Networks (LAN) and Wide Area Networks (WAN) can facilitate remote access for data and resources. To access this data remotely, employees make use of organizational or personally owned devices. This access is necessary for traveling employees, disaster recovery, business continuity, telecommuting, remote support, and vendor support.

First, an organization establishes the need for remote access. Then, it makes significant decisions on how the access is set up, what access to allow, how to handle organization policy, legal considerations and other laws and regulations, and, most importantly, how to keep everything secure [2]. The development of remote access procedures has the advantage of reducing the data access burden. However, it involves substantial investments in hardware and software. Besides, new technology and mechanisms for data protection during transmission are likely to face resistance due to the number of changes that accompany such implementations [3]. The techniques may be obsolete by the time an organization overcomes such resistance. Remote access has multiple benefits for organizations and individuals. These include, among others enabling collaboration among employees and facilitating seamless work environments. Also, it eliminates traditional barriers of geographical locations and time zones hence allowing efficient communication for individuals and organizations. Besides, it facilitates access to the most current versions of data and resources.

This data access from home networks or other untrusted networks is, in most cases, beyond organizational control. Lack of control means that the corporate security policies and baselines may or may not be met in these remote networks [4], which makes a balance between security and accessibility a hard bit to tackle and a significant challenge. Remote access can be a high-security risk if not correctly safeguarded and monitored. Tunneling is an excellent means of connecting remote users to the internal network. However, it does not assure the security of the connecting device, user, or client application. Fig.1., below, is an example of remote access compromise from [5]. This report attributed twenty-three, nine, and thirteen percent of data compromises in Point-of-Sale (POS) systems, corporate internal network, and E-commerce, respectively, to the dependence on remote access.

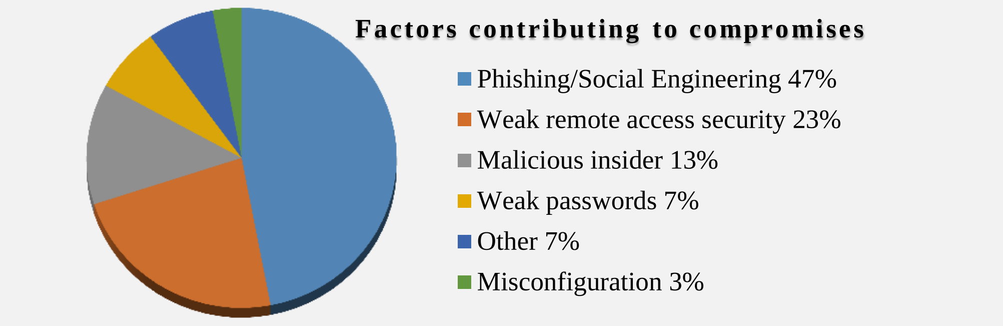

Fig.1. Factors contributing to security compromises [5].

Remote access is used to manage different locations and payment systems remotely. However, most of the time, these organizations employed remote access clients and software with weak or default credentials or configurations. These vulnerabilities resulted in compromises directly related to weak remote access security in these networks. According to this report, remote access security, malicious insider and phishing, or social engineering were among the most exploited vulnerabilities by cybercriminals in the years 2017 and 2018, resulting in 83 and 77 percent of compromises in POS and corporate networks, respectively, as shown in Fig.1., above. Weak passwords, misconfigurations, and code injection contributed to the remaining percent of compromises. The objectives of this study are to analyze remote access methods and technologies and the remote access logical vulnerabilities inherent in networked environments. To achieve the research objectives, we propose the domains approach to separate the organization network into logical, discrete entities for a unique security application to each domain and the Common Vulnerability Scoring System (CVSS) for the scoring of logical vulnerabilities in remote access.

This paper organization is as follows. Section II presents remote access technologies and methods. This section discusses remote access security concerns, attack vectors, and logical vulnerabilities. Section III presents a domains approach as a means for separation and classification of remote access vulnerabilities. Also, we perform vulnerability scoring using CVSS to show the importance of security for each of the domains. Lastly, section IV highlights the results of our research and presents the limitations of the tunneling method implemented by VPN technology. Comprehensive vulnerability management for all domains in remote access is proposed as a way forward to remote access security.

II. Remote Access Methods and Technologies

There are various technologies used in establishing remote access. One of them is by use of a line that runs between a computer and an organization’s LAN. Another one is by use of a dedicated line to establish a connection between a local LAN and a remote LAN. This type of connection provides faster data speeds, but its more expensive. Remote access can also be established by the use of existing computer networks and tunnel connections such as VPN, telnet, and Secure Shell (SSH). VPN uses the Internet to connect a remote user to data and resources using encryption and tunneling to access an organization’s network [6]. The remote device and the local system or server must have remote access software for a successful remote connection. Cable modem, Integrated Services Digital Network (ISDN), wireless network, and digital subscriber line are other means for remote access connections [7]. Another alternative is through a service provider of remote access via the Internet. An organization will rely on the security of the service provider’s infrastructure [8]. These include leased lines, Multi-Protocol Label Switching (MPLS), Frame Relay, Satellite, and Plain Old Telephone Service (POTS) modems. Other Infrastructures include microwave links, long-range fiber optics, and copper lines. POTS or ISDN, Dial-Up, WAN Links, Local Wireless, and VPN are the general categories or groups of technologies used to establish remote access.

Organizations have many options in methods for providing remote access to their data and resources.

There are four categories of remote access methods, which are commonly used by organizations and individuals [9,10], namely, tunneling, portals, remote desktop access, and direct application access.

A. Security Concerns

Remote access technologies, for example, VPN, allow users to connect to remote networks through the internet from any geographical location. Remote access gives rights and privileges as any other user connected locally [11]. This access is necessary for employees working from an offsite location, home, or traveling. Remote access technologies and devices are usually exposed to external threats. Hence they require additional protection compared to technologies accessed locally [10,12]. Despite its multiple benefits and advantages, remote access has several drawbacks [9]. Major security concerns for remote access are malware from remote devices, unwanted applications, loss of data and information, unauthorized access by hackers, lack of or weak physical security, unsecured networks, and access to internal resources. It is vital to analyze the criticality of data or resources to which a remote user wishes to connect. A security classification system is necessary to be able to award data and resources protection level that is equal to their value [8]. This system ensures the alignment of the level of effort required to establish and manage controls to the business impact resulting from a compromise. It is crucial to consider an understanding of resources the organization is willing to assign to control access to data and resources. To map the controls required, one must understand the threats and possible attack vectors.

Attack vectors and logical vulnerabilities

According to [8], remote access can be compromised at various points, beginning from the remote user and device, following the connection to the data or service to the data and resources accessed. These make the different attack vectors in remote access. Some of these include impersonation, captured or guessed user credentials, social engineering, malware, cloning, eavesdropping, sniffing, interruption, data injection or modification, hijacking, or man-in-the-middle attack, replay attack, and a denial-of-service attack.

Remote access vulnerabilities stem from several reasons. Devices used for remote access generally have weaker protection compared to standard client devices. Many of these devices do not have enterprise firewalls, antivirus, and a lack of physical security controls. The lack thereof is attributed to the fact that, in most cases, the enterprise does not manage the remote devices. Also, these devices are most of the time used in hostile environments and lack proper configurations. Besides, remote access communications are carried over untrusted networks [12]. Passive attacks involve listening or observing data without modifying. Eavesdropping is listening in and or observing other user's traffic. Sniffing is using a network to observe clear text messages. Protocols or approaches that send username and password information in clear text are the most easily compromised. These include Post Office Protocol 3 (POP3), Telnet, and rlogin [6]. Data interception and modification is possible in numerous ways. Identity Spoofing is making packets so that they look like they came from a different sender. This modification involves the use of information about transmission senders and receivers stored in the IP packet headers [8]. One common mode of attack is for an attacker to sniff on a public network, for example, the Internet. The attacker looks for packets that come from a source that is trusted by a particular firewall. The attacker then constructs and sends packets through the firewall after discovering a transmission source.

User vulnerabilities are numerous. For example, sometimes, have notes with sensitive information such as login credentials left lying on their desks or workbenches. Other users are sometimes too careless when they allow others to watch them log into a system. Other user vulnerabilities involve the use of social engineering to gain user login credentials. Awareness training and user education are useful for mitigating and remediating user vulnerabilities. Administrator vulnerabilities include failure to keep up to date with new vulnerabilities, patches, and fixes. Vendors post information, updates, and patches for their products on websites. Some vendors also provide email notifications. Others also supply automatic updates. Operating system hardening is a crucial practice to safeguard against remote access vulnerabilities, which involves disabling or removing all unnecessary applications, services, and protocols.

Attack vectors exploit vulnerabilities in remote access devices, users, methods, and technologies leading to unauthorized disclosure of information, corruption, destruction of data and disruption, or denial of services. To manage these logical vulnerabilities in remote access effectively, we will present a domains approach capitalizing on the various points of compromise in remote access. As evident in the attack vectors above, vulnerabilities are in the remote device or user, access method, or local data or resource. These points of compromise will form the basis of classification for logical vulnerabilities in the domains approach to remote access. The following Table 1., below presents the remote access domains and their corresponding vulnerabilities for different attack vectors. The domains are classified according to the environment and phase of remote access. As is the common practice, securing just the second domain would lead to data compromises in the other two domains as remote access vulnerabilities are evident in each of these domains.

Table 1. Remote access domains, vulnerabilities, and attack vectors. In "()" are the vulnerabilities for a specific domain [8].

Remote device and user domain	Remote access method domain	Local data or resource domain
a. User or device impersonation. (Lack of physical controls).	a. Listening or observing by third parties along the communication channel, that is eavesdropping or sniffing. (Transmission in clear text).	a. Attack and compromise of local communication software listening for requests. (Such as poor configurations, lack of updates and patches).
b. Captured or guessed user credentials. (Weak password policy).	b. Communication interruption. (Transmission in clear text).	b. Impersonation of valid remote device or user. (Inadequate remote device validation setup, lack of encryption, and mutual authentication protocols).
c. User intimidation or coercion for credentials or to perform unwarranted activities - social engineering. (Lack of user education and awareness training).	c. Data injection or modification. (Transmission in clear text)	c. Denial-of-service attack to an authentication server such as radius server or RAS. (Such as poor configurations, lack of updates, and patches).
d. Compromise to the remote device by malware. (Such as lack of firewalls, antivirus, updates, and patches).	d. Hijacking after communication initiation or interception during initiation - a man-in-the-middle attack. (Insecure communication protocol and poor configuration).	d. Denial-of-service attack to communicate outward on devices such as modem and router. (Such as poor configurations, lack of updates, and patches).
e. Cloning or impersonation of the local data, resource, or system to obtain user credentials or other information by domain name poisoning. Such as poor configurations, lack of updates, patches).	e. Communication replay - a replay attack. (Lack of tagging for encrypted components, e.g., with sessionid and number).	

III. Methodology

A. A Domains Approach

The origin of the network domain is in the cellular network. It is used to differentiate between the wired and wireless segments of a mobile network. The wired part could include physical infrastructure such as a router, base station, switch, server, among others. Wireless consists of the radio frequency spectrum. Various network nodes and links (subnets) are interconnected to provide cellular service. The wireless connects a cell phone to a base station, and the wired (network domain) facilitates the rest of the communication. A domain is based on various relationships such as network setup, location, and business.

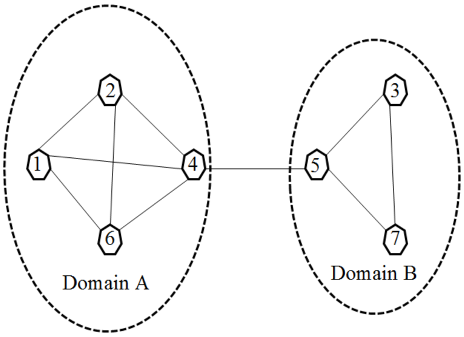

Fig.2. Two domains communication system [14].

Fig.2., above shows two domains communication system with two subnets, domain A and domain B. Domain A has four nodes, and domain B has thee nodes with each of the nodes being interconnected using links within a subnet. Subnet one is connected to subnet two using a single link.

Trust relationship

Trust relationship refers to nodes trusting a single certificate authority to issue certificates for public keys in a specific domain. Nodes can validate certificates for each other within a domain. In the case of cellular networks, an authentication center is used to hold cryptographic keys used by subscribers for authentication within a domain.

Key distribution center.

Each node has a protected channel used for communication with a centralized key distribution center. The key distribution center is used either to distribute a key to two communicating nodes or to relay protected information between two communicating nodes.

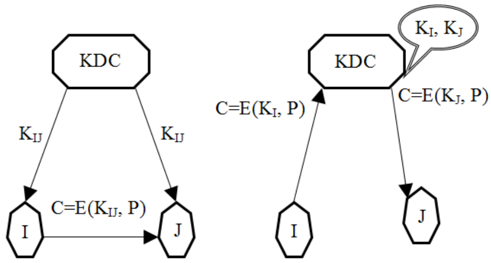

Fig.3. Distribution, and relay using a key distribution center [14].

In Fig.3., above, the key distribution center in the first instance distributes key K_{IJ} between nodes I and J so that they can securely initiate communication. In the second instance, the key distribution center relays the communication by decrypting the message with the key K_I shared with node I, and then encrypting the message with the key K_J shared with node J.

After a review of methods, technologies, security concerns, attack vectors, and logical vulnerabilities in remote access, it is evident that remote access has weaknesses in three areas or points. This research identifies these points as the domains of vulnerabilities in remote access. These include vulnerabilities in the remote device and user, transmission media, and local data, system, or resources. Adopting a domain approach will standardize an organization's logical vulnerability management and simplify device and user authentication [13]. Also, they enhance user access to multiple systems. Domains separate the organization network into logical, discrete entities for a unique security application to each domain [13]. This separation enhances and simplifies the mapping of different security controls for remote access to each of the identified domains. The approach ensures comprehensive coverage of each area or point of compromise during remote access. Fig.4., below, is a domains approach to remote access security based on the derived vulnerability categories in remote access. As shown in the Fig.4., we separate or divide a networked environment into three domains. These domains form the basis of classification for vulnerabilities in remote access. They include:

a. The remote device and user. (The physical location of the user and the type of remote device).
b. The remote access method. (Internet or part of an organization's network).
c. The local data, system, or resources.

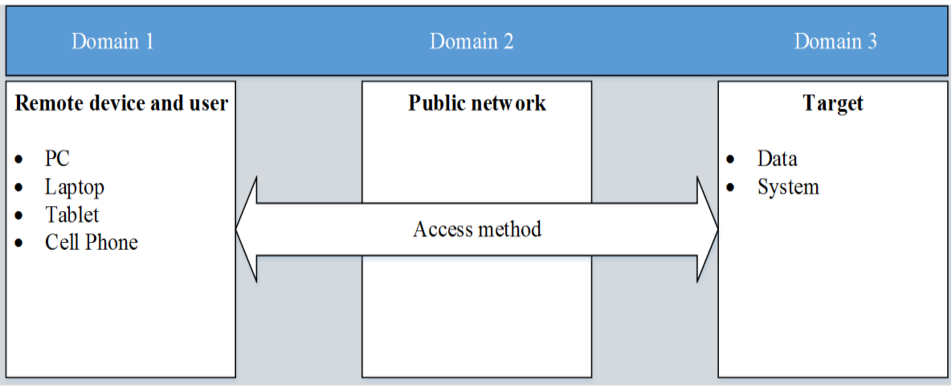

Fig.4. A domains approach to remote access logical vulnerabilities

Data and resources will virtually be connected to provide access to organizational information. Take a case of a remote user accessing data and resources from home. This user has a variety of devices, which could include a laptop, a desktop, and a tablet. The approach places the user and his/her devices in a remote device and user domain. The user accesses the organization's data and resources over a public network, in this case, the internet, which is in the access method domain. The last domain contains the data, resources, or system the remote user intends to access. This domain is in a data center on the organization's premises and probably in a different geographical location. Domain's approach for logical vulnerabilities in remote access comprehensively covers all points of compromise during remote access. It enhances the security process by ensuring that security is uniquely applied to each domain, thereby effectively managing vulnerabilities in all aspects of remote access. This approach is instrumental in the protection of confidentiality, ensuring integrity, and maintaining availability during remote access.

B. Logical Vulnerabilities Scoring

Vulnerability scoring is the process of rating identified vulnerabilities to prioritize them for remediation. Various vulnerability scoring systems exist. The most common include vulnerability analysis scale by SANS institute, proprietary scoring system by Microsoft, numeric scoring system by Computer Emergency Readiness Team Coordination Center (CERT/CC-US), and CVSS by Forum of Incident Response and Security Teams (FIRST) [15]. Other examples include:

a. Common Vulnerabilities and Exposures (CVE) by MITRE Corporation. CVE is a list of security vulnerabilities and exposures. It provides common names for known vulnerabilities and exposures, acting as a reference point for information exchange on security tools and products. CVE enhances interoperability for security products.
b. Open Web Application Security Project (OWASP). It is a risk rating methodology for web application vulnerability assessment.
c. Qualys by Qualys Inc. It is a web-based platform for vulnerability management. This scoring system is available as software as a service. Its vulnerability categories are vulnerabilities, potential vulnerabilities, and information gathered.

This research adopts the CVSS for the scoring of logical vulnerabilities in remote access. The reason for using CVSS is because it enables the performance of statistical analysis on vulnerabilities and vulnerability properties. It results in standardized vulnerability scores from the normalization of vulnerability scores across all software and hardware platforms [15]. CVSS is an open framework where anyone can see the individual characteristics used to derive a score, and it is easier for risk prioritization since vulnerability scores show the importance of a given vulnerability compared to other vulnerabilities. Organizations and individuals who publish ratings are required to adhere to its guidelines by providing the score and the scoring vector string. It is composed of the base, temporal, and environmental metric groups, and each has a set of metrics [16]. The base metric group is the inherent and fundamental qualities of a vulnerability that are constant over time and user environments. The temporal metric group is the qualities of a vulnerability that change over time. Analysts or product vendors specify the base and temporal metrics. The environmental metric group is qualities specific to a particular user environment specified by a user.

The base group defines fundamental qualities of a vulnerability resulting in an accurate representation of a vulnerability. If there is a need to relate a vulnerability to a specific environment, then temporal and environmental groups can be added to refine the results of the vulnerability representation. This combination enhances the decision-making process during the mitigation of vulnerabilities [15]. After assigning values to the base metrics, the base equation calculates a score and creates a vector string, which is a text string that contains the values assigned to each metric. Others can use this vector string to understand how that particular score was derived. Each use case is unique, and the base score and vector string alone may be enough to score a vulnerability. We obtain a temporal score by combining temporal metrics and the base score using the temporal equation. Combining environmental metrics with the temporal score using the environmental equation results in an environmental score. The final score is rated low (0.1-3.9), medium (4.0-6.9), high (7.0-8.9) or critical (9.0-10.0) as per CVSS v3. Table 2., below shows the CVSS group metrics and vectors.

Table 2. Base, temporal and environmental metrics and vectors [15,16].

Base metrics	**Temporal metrics**	**Environmental metrics**
a. Attack Vector (AV): Network (N), Adjacent Network (A), Local (L), Physical (P)	a. Exploitability (E): Unproven (U), Proof of Concept (P), Functional (F), High (H), Not Defined (X)	a. Security Requirements (CR, IR, AR): Low (L), Medium (M), High (H), Not Defined (X)
b. Attack Complexity (AC): High (H), Low (L)	b. Remediation Level (RL): Official Fix (O), Temporary Fix (T), Workaround (W), Unavailable (U), Not Defined (X)	**Modified Base Metrics:**
c. Privileges Required (PR): High (H), Low (L), None (N)	c. Report Confidence (RC): Unknown [U], Reasonable (R), Confirmed (C), Not Defined (X)	b. Modified Attack Vector (MAV): Network (N), Adjacent Network (A), Local (L), Physical (P), Not Defined (X)
d. User Interaction (UI): None (N), Required (R)		c. Modified Attack Complexity (MAC): High (H), Low (L), Not Defined (X)
e. Scope (S): Unchanged (U), Changed (C)		d. Modified Privileges Required (MPR): High (H), Low (L), None (N), Not Defined (X)
f. Confidentiality Impact (C): None (N), Low (L), High (H)		e. Modified User Interaction (MUI): None (N), Required (R), Not Defined (X)
g. Integrity Impact (I): None (N), Low (L), High (H)		f. Modified Scope (MS): Unchanged (U), Changed (C), Not Defined (X),
h. Availability Impact (A): None (N), Low (L), High (H)		g. Modified Confidentiality (MC): None (N), Low (L), High (H), Not Defined (X)
		h. Modified Integrity (MI): None (N), Low (L), High (H), Not Defined (X)
		i. Modified Availability (MA): None (N), Low (L), High (H), Not Defined (X)
Vector: AV:[N,A,L,P]/AC:[H,L]/PR:[H,L,N]/UI:[N,R]/S:[U,C]/C:[N,L,H]/I:[N,L,H]/A:[N,L,H]	**Vector:** E:[U,P,F,H,X]/RL:[O,T,W,U,X]/RC:[U,R,C,X]	**Vector:** CR:[L,M,H,X]/IR:[L,M,H,X]/AR:[L,M,H,X]/MAV:[N,A,L,P,X]/MAC:[H,L,X]/MPR:[H,L,N,X]/MUI:[N,R,X]/MS:[U,C,X]/MC:[N,L,H,X]/MI:[N,L,H,X]/MA:[N,L,H,X]

Base, temporal and environmental equations

Base Score (BS) is a function of the Impact Subscore (ISc) and Exploitability Subscore (ESc) equations,

$$\begin{aligned} &If\ (ISc \leq 0)0\ else, \\ &SU^{4}\ Round\ up\Big(Min\big[(I+E),\ 10\big]\Big) \\ &SC\ Round\ up\Big(Min\big[1.08\times(I+E),\ 10\big]\Big) \end{aligned} \tag{1}$$

ISc is defined as,

$$\begin{aligned} &SU\ \ 6.42 \times ISc_{Base} \\ &SC\ \ 7.52 \times \left[ISc_{Base} - 0.029\right] - 3.25 \times \left[ISc_{Base} - 0.02\right]^{15} \end{aligned} \tag{2}$$

Where,

$$ISc_{Base} = 1 - \left[\left(1 - I_{Conf}\right) \times \left(1 - I_{Integ}\right) \times 1 - I_{Avail}\right] \tag{3}$$

ESc is defined as,

$$8.22 \times AV \times AC \times PR \times UI \tag{4}$$

Temporal Score (TS) Score,

$$Round\ up\left(BS \times ECM \times RL \times RC\right) \tag{5}$$

Environmental Score (ES),

$$\begin{aligned} &If\ \ \left(M.ISc \le 0\right) 0\ else, \\ &If\ \ M.SU\ \ Round\ up \left(\begin{matrix} Round\ up \\ \left(Min\left[\left(M.I + M.E\right), 10\right]\right) \\ \times ECM \times RL \times RC \end{matrix} \right) \\ &If\ \ M.SC\ \ Round\ up \left(\begin{matrix} Round\ up \\ \left(Min\left[1.08 \times \left(M.I + M.E\right), 10\right]\right) \\ \times ECM \times RL \times RC \end{matrix} \right) \end{aligned} \tag{6}$$

Modified Impact Subscore (M.ISc),

$$\begin{aligned} &If\ \ M.SU\ \ 6.42 \times \left[ISc_M\right] \\ &If\ \ M.SC\ \ 7.52 \times \left[ISc_M - 0.029\right] - 3.25 \times \left[ISc_M - 0.02\right]^{15} \end{aligned} \tag{7}$$

Where,

$$ISc_M = Min \left[\begin{bmatrix} 1 - \left(1 - M.I_{Conf} \times CR\right) \\ \times \left(1 - M.I_{Integ} \times IR\right) \\ \times \left(1 - M.I_{Avail} \times AR\right) \end{bmatrix}, 0.915 \right] \tag{8}$$

Modified Exploitability Subscore (M.ESc),

$$8.22 \times M.AV \times M.AC \times M.PR \times M.UI \tag{9}$$

The definition of “Roundup” is the smallest number, specified to one decimal place, which is equal to or higher than its input.

IV. Results and Discussion

Adopting the domains approach, we group the logical vulnerabilities in remote access into the three domains; remote device and user, remote access method, and local data, resource, or system. Each of these domains has its distinct remote access attack vectors and logical vulnerabilities. We scored each of the vulnerabilities using CVSS v3.0. BS, ISc, ESc, TS, ES, and MISc stands for the base score, impact subscore, exploitability subscore, temporal score, environmental score and modified impact subscore, respectively. The scores are derived using the CVSS calculator with its working principles presented in equations (1) to (9) These equations results with the BS, ISc, ESc, TS, ES, and MISc scores which are used to calculate the overall CVSS score for a remote access domain. For this scoring, the assumption is that of a particular remote access scenario without any security mechanism implementation. This assumption is essential for vulnerability prioritization during remediation. Table 3., below presents the base, temporal, environmental scores, and vector strings for each of the vulnerabilities.

Table 4., presents a summary of the results of the remote access logical vulnerability scoring using CVSS. Out of the scored fourteen vulnerabilities, remote device or user impersonation, i.e., IP spoofing, scored a rating of 6.1. This score places it as a medium rating. The rest thirteen vulnerabilities scored a high rating of between 7.3 and 8.6. These scores show the importance of security in remote access as almost every vulnerability in remote access is a potential point of security compromise. Any score between 0.1 and 3.9 would warrant minimum attention when it comes to vulnerability remediation. An analysis of variance (ANOVA) for means of these three remote access domains vulnerability rating provides evidence of statistical significance with F = 8.3413, a critical value of 0.05, and critical F = 3.9823. Therefore, since the F statistic is bigger than the critical value, we can conclude that there is statistical significance in these domains means.

The charts below, Fig.5., present the lowest, highest, and average CVSS scores in each domain of remote access. The lowest in the remote device and user domain scored a 6.1, which is a medium rating. The highest in the same domain scoring an 8.1 rating, which is a high rating. In the remote access method, the lowest score was 8.5, and the highest was 8.6, both a high rating. In the local data or system domain, the lowest was 7.6, and the highest was 8.5, which is a high rating for both. The average for each domain rated between 7.28 and 7.85, which is a high severity rating. Remote access vulnerability score was an average of 7.9, which is a high severity rating. Securing just the remote access method will leave a communication network 7.28 and 7.85 vulnerable in the remote device and local resource, respectively. The results go to show the importance of security in each of the three domains of remote access. Therefore, remediation of logical vulnerabilities in remote access would require a comprehensive approach that addresses all three domains in remote access.

Table 3. Remote access base, temporal, environmental scores, and vector strings.

Domain	Vulnerability	Score							Vector string
		BS	ISc	ESc	TS	ES	MISc	OS	
Remote Device and User	Impersonation/spoofing	6.1	3.7	1.8	5.7	6.1	5.0	**6.1**	AV:L/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:L/MAC:H/MPR:N/MUI:R/MS:C/MC:L/MI:L/MA:L
	Captured/guessed credentials	8.5	5.3	2.5	7.4	7.4	5.3	**7.4**	AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H/E:U/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:N/MUI:N/MS:C/MC:L/MI:L/MA:H
	Intimidation/coercion/social engineering	8.6	6.0	1.8	7.5	7.5	6.0	**7.5**	AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:N/MUI:R/MS:C/MC:H/MI:H/MA:H
	Remote device malware	8.5	5.3	2.5	8.1	8.1	5.3	**8.1**	AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H/E:H/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:N/MUI:N/MS:C/MC:L/MI:L/MA:H
	Local system cloning/DNS Poisoning	7.9	6.0	1.3	7.3	7.3	6.0	**7.3**	AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:H/E:F/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:N/MAC:H/MPR:H/MUI:N/MS:C/MC:H/MI:L/MA:H
Remote Access Method	Eavesdropping/sniffing	6.8	4.0	2.2	6.5	8.5	5.9	**8.5**	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:H/RL:O/RC:C/CR:H/IR:X/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:H/MI:N/MA:N
	Communication interruption	6.8	4.0	2.2	6.5	8.5	5.9	**8.5**	AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H/E:H/RL:O/RC:C/CR:X/IR:X/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:X/MI:X/MA:H
	Data injection/modification	8.7	5.8	2.2	8.3	8.6	6.0	**8.6**	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N/E:H/RL:O/RC:C/CR:H/IR:H/AR:X/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:N
	Hijacking/interception/man-in-the-middle attack	9.0	6.0	2.2	8.6	8.6	6.0	**8.6**	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
	Communication replay/replay attack	9.0	6.0	2.2	8.6	8.6	6.0	**8.6**	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
Local Data, Resource or System	Local communication software Attack	6.8	4.0	2.2	6.5	8.5	5.9	**8.5**	AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H/E:H/RL:O/RC:C/CR:X/IR:X/AR:H/MAV:N/MAC:H/MPR:N/MUI:N/MS:C/MC:X/MI:X/MA:H
	Remote device/user Impersonation	8.1	6.0	1.4	7.7	7.7	6.0	**7.7**	AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:L/MAC:H/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
	DoS attack to authentication server	8.0	6.0	1.3	7.6	7.6	6.0	**7.6**	AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:N/MAC:H/MPR:H/MUI:N/MS:C/MC:H/MI:H/MA:H
	DoS attack to communication devices	5.8	4.0	1.3	5.6	7.6	5.9	**7.6**	AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H/E:H/RL:O/RC:C/CR:X/IR:X/AR:H/MAV:N/MAC:H/MPR:H/MUI:N/MS:C/MC:X/MI:X/MA:H

Table 4. Remote access logical vulnerabilities CVSS scores.

Domain	Vulnerability attack vector	CVSS Score
1. Remote Device and User	Impersonation/spoofing	6.1
	Captured/guessed credentials	7.4
	Intimidation/coercion/social engineering	7.5
	Remote device malware	8.1
	Local system cloning/DNS Poisoning	7.3
2. Remote Access Method	Eavesdropping/sniffing	8.5
	Communication interruption	8.5
	Data injection/modification	8.6
	Hijacking/interception/man-in-the-middle attack	8.6
	Communication replay/replay attack	8.6
3. Local Data or Resource	Local communication software Attack	8.5
	Remote device/user Impersonation	7.7
	DoS attack to an authentication server	7.6
	DoS attack to communication devices	7.6

Low (0.1-3.9) *Medium (4.0-6.9)* *High (7.0-8.9)* *Critical (9.0-10.0)*

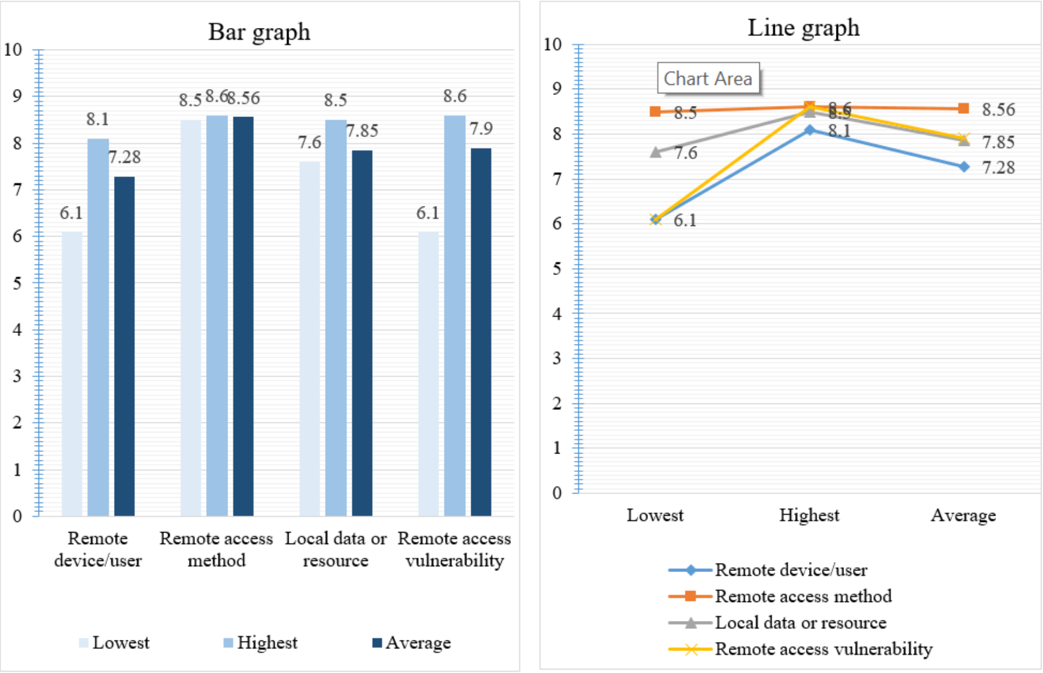

Fig.5. Remote access domains CVSS scores.

V. Conclusion

Organizations are not securely using remote access methods and technologies such as VPN, which results in compromises originating from vulnerabilities in remote access. VPN is a mature technology, and the most implemented means of remote access. It is a technology used to hide information from sniffers on the internet. The technology uses encryption and works based on tunneling. However, VPN has several drawbacks; it cannot enforce security policies since it does not analyze data packets, cannot regulate access since it does not perform authentication, cannot detect mistakes or misuse since it does not check the data packet contents and can potentially allow high-risk devices onto the network. Home or offsite devices are an example of devices at high risk. Take a case where a trusted offsite or home device is hacked or owned, and this risks the network that trusts this device. This compromised device can facilitate the spreading of malicious code from such a remote device to the internal network. Therefore, tunneling based on VPN alone is not adequate to secure remote access because VPN aims at ensuring just one of the identified domains (remote access method) is secure. As future work, there is a need for a comprehensive security model for remote access that takes into account all the three domains in remote access. This model will enhance the remediation process for logical vulnerabilities in remote access. In our future work, we will be developing a remote access security model based on the management of vulnerabilities in these remote access domains. This model will take into account both managed and unmanaged devices for remote access.

ACKNOWLEDGMENTS

The research was supported in part by the Higher Education Loans Board through Grant HELB/45/003/VL.1 of Postgraduate Award 2014/2015.

REFERENCES

[1] Scarfone, K., and Souppaya, M. (2007). User's Guide to Securing External Devices for Telework and Remote Access, *NIST Special Publication 800-114.*

[2] Harbert, S. (2011). Trends in Remote and Mobile Information Access Technologies. *Technology Focus,* Volume 23, №3, Fall 2011.

[3] Blakemore, M. (2001). The Potential and Perils of Remote Access in Confidentiality, Disclosure, and Data Access. *Theory and Practical Application for Statistical Agencies,* Elsevier, Pp.315-340.

[4] Harrell, J. (2014) The Evolution of the Threat Landscape and the Need for a Live Intelligence-based Approach to Security. *Norse-corp* August 2014.

[5] Trustwave. (2018) Trustwave global security report. *Seventh annual edition, Pp.8-27.*

[6] Nedeltchev, P. (2003). Troubleshooting Remote Access Networks. *Cisco Press.*

[7] Robichaux, P. (1999). Remote Access Twenty-Four Seven. *SYBEX, Network Press.*

[8] Homeland Security. (2011) Configuring and Managing Remote Access for Industrial Control Systems. *Control Systems Security Program, Center for the Protection of National Infrastructure, National Cyber Security Division, Pp.19-32, April 2011.*

[9] Scarfone, K. (2009). Security for Enterprise Telework and Remote Access Solutions. *Computer Security Division Information Technology Laboratory,* National Institute of Standards and Technology, NIST.

[10] NIST SP 800-46 Guide to Enterprise Telework and Remote Access Security. *Recommendations of the National Institute of Standards and Technology,* Revision 1.

[11] CISA. (2016) Protection of Information Assets. *CISA Review Manual 26Th Edition,* Chapter 5, Pp.353-383.

[12] Scarfone, K., Souppaya, M. and Hoffman, P. (2009) Guide to Enterprise Telework and Remote Access Security. *Recommendations of the National Institute of Standards and Technology, NIST SP 800-46 Revision 1,* June 2009.

[13] Arconati, N. (2002) One Approach to Enterprise Security Architecture. *SANS Security Essentials GSEC version 1.3,* SANS Institute 2002.

[14] Chen, L. D., and Gong G. (2008). Communication System Security, *Chapter 3,* Chapman and Hall/CRC, Pp.1-2.

[15] Mell, P., Scarfone, K. and Romanosky, S. (2007) A Complete Guide to the Common Vulnerability Scoring System. *Version 2.0,* June 2007.

[16] Hanford, S. (2014) CVSS v3, Preview 1: Base, Temporal, and Environmental Metrics. *CVSS Special Interest Group (CVSS-SIG),* June 2014.

Authors' Profiles

Samuel Ndichu holds an MSc in Data Communication and BSc in Information Technology from KCA University, Kenya. He is a Computer Science Ph. D. candidate in the School of Computing and Informatics, Maseno University, Kenya. His MSc thesis was focused on developing a framework to evaluate information security preparedness in law enforcement agencies. His current research interests include information and network security.

Sylvester McOyowo holds a Ph. D. degree in Computer Science from the Peoples' Friendship University. He is the Dean, School of Computing and Informatics, and a lecturer at the Department of Computer Science Maseno University, Kenya. His main teaching and research interests include Research Methods, Digital, and Analogue Electronics, and he is a Ph.D. supervisor to Mr. Ndichu.

Henry Okoyo holds a Ph. D. degree in Computer Science from the University of Manchester, an MSc degree in Microprocessor Engineering and Digital Electronics from the former University of Manchester Institute of Science and Technology (UMIST), and a BSc degree from the University of Nairobi, Kenya. He is a lecturer at the Department of Computer Science, School of Computing and Informatics, Maseno University, Kenya. His main teaching and research interests include Artificial Intelligence, and he is a Ph.D. supervisor to Mr. Ndichu.

Cyrus Wekesa holds a Ph. D. degree in Electrical Engineering from the University of Tokushima, Japan, and an MSc, and a BSc in Electrical Engineering from the University of Nairobi, Kenya. He is currently an associate professor in the school of Engineering, University of Eldoret, Kenya. His teaching and research interests include and Information Security, Telecommunications and Computer Networks, Computer Architecture, and Electronics, and Distributed Systems, and he is a Ph.D. supervisor to Mr. Ndichu.

How to cite this paper: Samuel Ndichu, Sylvester McOyowo, Henry Okoyo, Cyrus Wekesa, "A Domains Approach to Remote Access Logical Vulnerabilities Classification", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.11, pp.36-45, 2019. DOI: 10.5815/ijcnis.2019.11.05