Scientific Research Publishing

Journal of Information Security, 2022, 13, 337-362
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cybersecurity: Identifying the Vulnerability Intensity Function (*VIF*) and Vulnerability Index Indicator (*VII*) of a Computer Operating System

Ranju Karki*, **Chris P. Tsokos**

Department of Mathematics and Statistics, University of South Florida, Tampa, USA
Email: *ranjukarki@usf.edu, ctsokos@usf.edu

How to cite this paper: Karki, R. and Tsokos, C.P. (2022) Cybersecurity: Identifying the Vulnerability Intensity Function (*VIF*) and Vulnerability Index Indicator (*VII*) of a Computer Operating System. *Journal of Information Security*, **13**, 337-362.
https://doi.org/10.4236/jis.2022.134019

Received: September 5, 2022
Accepted: October 25, 2022
Published: October 28, 2022

Abstract

The objective of the present study is to define two important aspects of the computer operating system concerning the number of its vulnerabilities behavior. We identify the **Vulnerability Intensity Function (** *VIF*), and **the Vulnerability Index Indicator (** *VII*) of a computer operating network. Both of these functions, *VIF* and *VII* are entities of the stochastic process that we have identified, which characterizes the probabilistic behavior of the number of vulnerabilities of a computer operating network. The *VIF* identifies the rate at which the number of vulnerabilities changes with respect to time. The *VII* is an important index indicator that conveys the following information about the number of vulnerabilities of Desktop Operating Systems: the numbers are increasing, decreasing, or remaining the same at a particular time of interest. This decision type of index indicator is crucial in every strategic planning and decision-making. The proposed *VIF* and *VII* illustrate their importance by using real data for Microsoft Windows Operating Systems 10, 8, 7, and Apple MacOS. The results of the actual data attest to the importance of *VIF* and *VII* in the cybersecurity problem we are currently facing.

Keywords

Cybersecurity, Operating Systems Vulnerabilities, Stochastic Process, Vulnerability Intensity Function, Vulnerability Index Indicator

1. Introduction

Today's world revolves around technology (or computer reliant world). Information technology affects nearly all work environments such as business, education, finance, health care, security, communications, and employment, including our personal life. Thus, protecting these networks, devices, and data from unauthorized sources is the most important priority of many vendors. Cybersecurity is the field of study of protecting computers, networks, mobile devices, and data from intruders. It is also referred to as electronic information security or information technology security. It mainly focuses on securing computer systems against unauthorized access. This study contributes to the study of vulnerability aspects of the cybersecurity field. Even if one uses a high level of security measures, sophisticated hardware, and software, they are prone to attack. None of the hardware, software, network architectures, and devices is developed to the 100% free of vulnerabilities. In cybersecurity, vulnerability is a weakness, flaw, or error that can permit an attacker to reduce systems information assurance. It is the combination of three elements. They are systems susceptibility to the flaw, attacker access to the flaw, and an attacker's capability to exploit the flaw.

The objective of the present study is to accomplish three important and useful aspects of the number of vulnerabilities of the Microsoft Operating Systems (MOS) which share 76.1% of the world market, and Apple Mac Operating Systems (AOS) which share 16.1% of the world market, respectively.

First, we want to develop/identify the stochastic process that characterizes the probabilistic behavior of MOS and AOS. By identifying this stochastic process, we can obtain useful information about the number of vulnerabilities of MOS and AOS.

Secondly, we introduce a new definition of the subject study, namely **Vulnerability Intensity Function (*VIF*)** which identifies analytically and graphically the rate at which the number of vulnerabilities changes as a function of time for a MOS.

Thirdly, we introduce the **Vulnerability Index Indicator (*VII*)** for MOS and AOS. The *VII* is monitoring the number of vulnerabilities of the respective OS at a specific time of interest. This indicator conveys three possible behaviors of OS at the desired time, the number of vulnerabilities increases, the number of vulnerabilities remains the same, or the number of vulnerabilities decreases. This decision monitoring indicator conveys very important and useful information concerning the behavior of MOS and AOS at a specific time of interest, respectively which is essential for strategic planning.

1.1. Operating System

The Operating System (OS) is one of the core components (software) of the computer system. It manages the computer's memory and processes, including its hardware and software functions. Some of the important functions of an OS are disk management, memory management, process management, booting, loading and execution, device controlling, printing controlling, User Interface (UI), and data security. The User Interface (UI) of the OS allows us to enter and receive information from the computer system without knowing how to speak the computer's language. The operating system coordinates the software and hardware to the computer's Central Processing Unit (CPU), memory, and storage so that we can have the assigned works executed. Thus, it requires the development of very complex software with a number of functionaries to execute a certain assignment. It is almost impossible to have OS free from vulnerabilities. This causes tremendous security risks to software companies, developers, and individual users. An attacker can compromise the OS via vulnerabilities then the whole computer system is in the control of the hacker. They can block system access, gather information, or gain access to more computers in a network. It would disrupt the normal operation of OS. Also, it can cause significant damage to important IT assets and infrastructures. To recover from these situations, we need to apply immense resources and budgets, which can cause massive financial losses.

Figure 1 shows the worldwide market share of Desktop OS according to Statcounter Data [1]. Microsoft dominates all other desktops OS with 76.1% of its share. Figure 2 shows the market share of the different types of Windows operating as of August 2021. According to Statcounter Data [1], out of 76.1% market coverage of Windows Operating System, market share of Windows 10, Windows 7, Windows 8.1, Windows 8, Windows XP, and Windows Vista are 78.36%, 15.98%, 3.62%, 1.15%, 0.61%, and 0.28%, respectively. Based on the popularity of Windows among users, Windows 10, Windows 7, Windows 8, and Windows 8.1 are selected for the present study. In addition, according to Statcounter Data, the worldwide market share of Apple Desktop OS is 16.1%. We have considered the total number of vulnerabilities of Mac OS X and MacOS.

The major versions of Microsoft Desktop OS are Windows 95, Windows 98, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, and Windows 11. Each version of OS, MS Windows has something in common and a lot of additional features, tools, and applications. There are many versions of MacOS such as Mac OS X 10.0, Mac OS X 10.1, OS X 10.8, MacOS 10.12, and more.

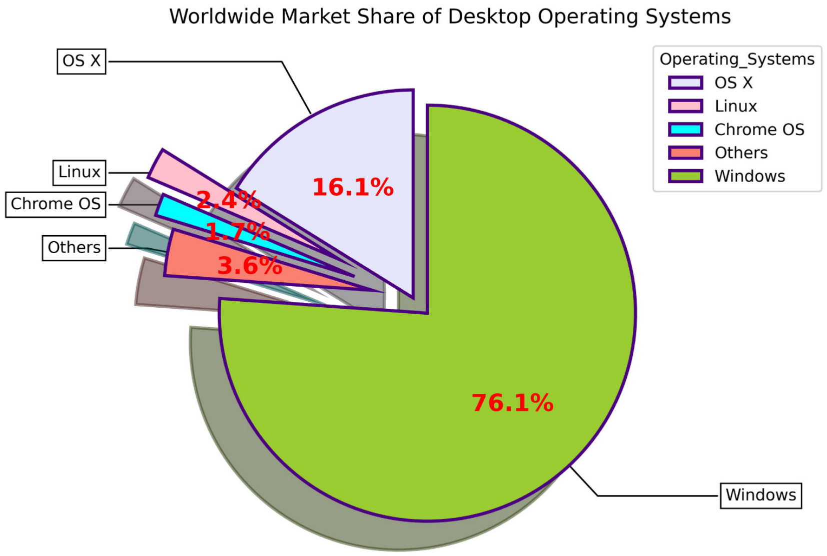

Figure 1. Worldwide market share of Desktop Operating Systems [1].

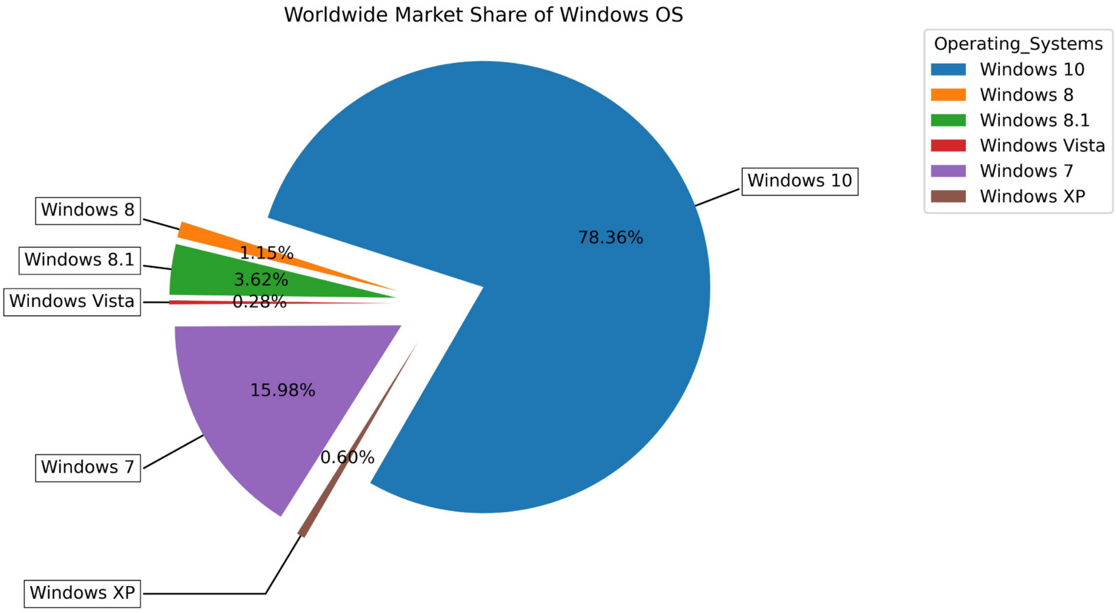

Figure 2. Worldwide market share of Windows Operating Systems [1].

They continuously update and upgrades new versions of OS to keep up with rapidly developing today's technological world. If we compare the security features of these OS, the newer version is superior to the older version. For example, by default, Windows 10 regularly scans the device for malware, viruses, and security threats and downloads the security updates automatically. There are many security features added to Windows 10 such as Windows defender application guard, user account control Windows, defender exploit guard, and Microsoft BitLocker, among others. Despite having tight security features, there are growing numbers of vulnerabilities in Windows OS. The newest version of Desktop Operating Systems offers tremendous application availability; consequently, new vulnerabilities are continuously emerging. If we can monitor the number of vulnerabilities in Desktop OS, we will be able to determine if vulnerabilities are increasing, decreasing, or remaining the same. This kind of information is very important to IT and managers to address the behavior of vulnerabilities in MOS and AOS. The quantitative analysis of the number of vulnerabilities can help IT security professionals to perform, scheduled security testing and development of security patches promptly, among others.

1.2. Review of Some Important Recent Research on Cybersecurity

The National Vulnerability Database (NVD) and other open source vulnerability databases are the main sources for researchers to study remaining aspects of the cybersecurity problem. Authors of [2] proposed a stochastic model for security evaluation based on vulnerability exploitability scores and attack path behavior by structuring the attack graph for small case scenarios. This model allows us to estimate the Expected Path Length and the Minimum number of steps to reach the target with probability one. Authors of [3] proposed statistical models that could evaluate the "Risk Factor" of a particular vulnerability at a time "t" more conveniently without going through the Markovian process. Finally, they also present a new set of Non-Linear Statistical Models that can be used in estimating the probability of being exploited as a function of time. In [4], the authors present a Non-Homogeneous Stochastic Model that allows the computer system administrators to predict the time that the system is most vulnerable to an attack in terms of the Expected Path Length (EPL) by using a network system of two computers subject with three vulnerabilities as a base model. In [5], the authors proposed a stochastic predictive model, based on the Markovian process, to evaluate the risk to the entire computer network.

Many research [6]-[14] showed the usefulness and validity of machine learning techniques in the evaluation of software vulnerabilities, such as predicting the number of vulnerabilities and the time length until exploitation, if they are exploitable. Pokhrel, Rodrigo, and Tsokos, [13], proposed a time series-based predictive model, using linear and non-linear approaches, to predict the number of vulnerabilities of a given operating system and thereby assist vendors in monitoring their OSes. Edkrantz and Said [11] studied the correlations in the vulnerability data from NVD and the Exploit Database (EDB). They applied Support Vector Machines (SVM), K-Nearest-Neighbors (KNN), Naive Bayes, and Random Forests ML algorithms to predict the exploit status of vulnerabilities. They include CWE variables, CVSS scores, parameters, vendors, words, references, and length of the text summary as variables of interest. Considering the binary classification, the SVM with Radial Basis Function (RBF) kernel has the best performance with a prediction accuracy of nearly 83%. Bozorgi, Saul, Savage, and Voelker [9] used the Open Source Vulnerability Database (OSVDB) and the CVE database to find how likely a vulnerability could be exploited and how soon. They extracted a very large number of features, many of which are binary variables. By using linear Support Vector Machines (SVMs), they were able to reach a false positive rate of 12.5% and approximately 90% accuracy. Zhang, Caragea, and Ou [14] used NVD and apply some machine learning algorithms such as Radial Basis Function (RBF) network, Sequential Minimal Optimization (SMO), Multilayer Perceptron (MLP), and simple logistic to develop a predictive model that predicts time to next vulnerability for the software Linux, Linux OSes and Mozilla web browser. The input variables were the software's name, software's version, software's CVSS, and vulnerability's published time. The SMO has the best performance with prediction accuracy of approximately 70% with the false positive rates of their predictive models are about 40%. Fray [6] used the vulnerability data of computer Operating Systems (OS) such as Microsoft, Apple, and Linux are the focus of this research from the CVE details website from January 1999 to March 2019. The predictive models were developed using the vulnerabilities details such as CVE ID Number, Vendor, vulnerability level, CVSS Score, Confidentiality Impact, Integrity Impact, Availability Impact, Access Complexity, Authentication, year, denial of service, gaining access along with their introduced factors Polarity, Subjectivity, Frequency, NumAttacks, and Days which were significant to the models' performance. The Random Forest machine learning algorithm had the best performance in predicting the vulnerability level and how likely it would be for attackers to cause Denial of Service to the system, with 93% precision, recall, F1-score, and accuracy. On the other hand, K nearest neighbors, Logistic Regression, and Gaussian Naive Bayes algorithms did not perform well, having evaluation metrics of 77% or less. The author [12] analyzes the reported vulnerabilities associated with four operating systems (Windows, Mac, Cisco IOS, and Linux) and four web browsers (Internet Explorer, Safari, Firefox, and Chrome) on NVD. They introduce an approach for predicting the cumulative number of software vulnerabilities and it is more accurate than Vulnerability Discovery Models (VDMs) in most cases. The author approaches using a Neural Network Model (NNM) to model the nonlinearities related to vulnerability disclosure. Nine common Vulnerability Discovery Models (VDMs) such as Rescorla's Quadratic, linear, Gamma-based, Weibull-based, Normal-based, AML, Younis's Folded, Rescorla's Exponential, and NHPP Power law are used to compare their prediction capabilities with the researcher?€?s approach. As the study shows that NNMs are accurate predictions of software vulnerabilities.

2. Methods

2.1. Data Description

The vulnerability data that is used in the present study was obtained from the National Vulnerability Database (NVD) [15]. It is the U.S. government repository that integrates publicly available vulnerability information and provides common references to industry information. The NVD was launched in 2005, is a product of the National Institute of Standards and Technology (NIST) Computer Security Division, and is sponsored by the Department of Homeland Security's National Cybersecurity and Communications Integration Center, and by Network Security Deployment. It is used for security management and compliance as well as automatic vulnerability management. All the reported vulnerabilities have been assigned a Common Vulnerabilities and Exposures (CVE) identifier. The CVE List was launched by MITRE Corporation as a community effort in 1999. There are over 1,500,000 CVEs created in the NVD starting from the 1990s to the present.

We have obtained the number of vulnerabilities for each Operating System from 10-31-09 to 08-31-21 from NVD. We structure the data with respect to time (monthly intervals). The total number of vulnerabilities for each operating system is a cumulative number of vulnerabilities reported in a monthly interval from the NVD database. We have included the total number of vulnerabilities of Windows 8 and 8.1 together to calculate the total number of vulnerabilities of Windows 8 since Windows 8.1 is the upgraded version of Windows 8. Apple's Operating system has different names depending on different times. For example, the first version of the Apple Operating System was called Mac OS X from its resealed date in 2001 to 2012. Then, it was called OS X until 2016. From 2016 to now, we called MacOS. We have included the total number of vulnerabilities of all versions of MacOS.

The following Table 1 shows the summary of the descriptive analysis of our data. It includes the name of the operating systems, data collection period (time), the total number of vulnerabilities (total), mean, median, the standard deviation of the data. Thus, the data suggest a positively skewed distribution of the number of vulnerabilities.

Our study started by accumulating the total number of vulnerabilities per month for Windows 7, Windows 8, Windows 10, and MacOS.

Figure 3 displays the time series patterns of Windows 7, Windows 8, Windows 10, and MacOS. After comparing patterns, we can conclude that Windows 10 has the highest number of vulnerabilities discovered compared to Windows 7 and Windows 8. Additionally, MacOS has the highest number of vulnerabilities among all four operating systems. A possible interpretation is that this means the systems for discovering the vulnerabilities present in the latest software are becoming more sensitive as technologies are rapidly developing. Nowadays, IT personnel, users, and vendors are more concerned with cybersecurity than before, so they are reporting the vulnerabilities to NVD promptly. Among Windows, Windows 10 is supposed to be more secure than others since it has many

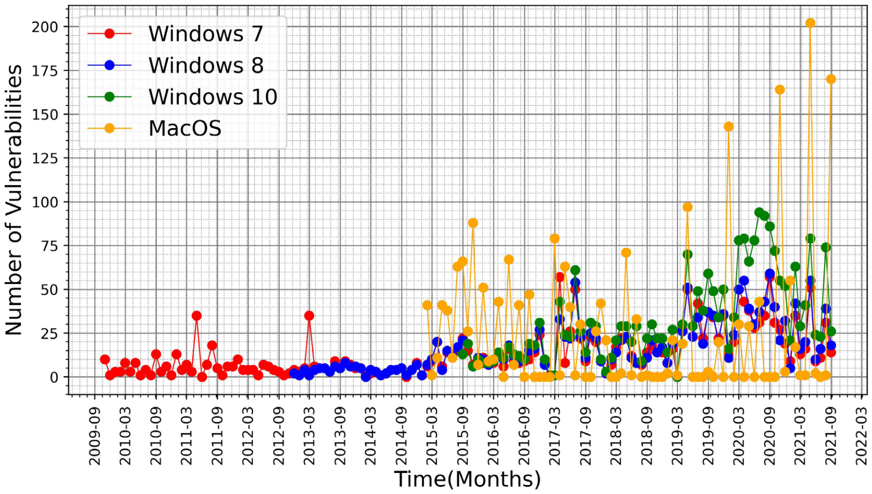

Figure 3. Time series patterns of Windows 7, Windows 8, Windows 10, and MacOS.

Table 1. Descriptive statistics of vulnerability datasets: Windows 7, Windows 8, Windows 10, and MacOS.

OS Name	Time	Total	Mean	Median	Stan.dev
Windows 7	Oct. 2009-Aug. 2021	1922	13.44	9	13.02
Windows 8	Nov. 2012-Aug. 2021	1756	16.57	11.5	14.32
Windows 10	Aug. 2015-Aug. 2021	2368	32.43	26	24.54
Mac OS X/MacOS	Jan. 2015-Aug. 2021	2103	26.29	5	41.48

additional security features compared to others but vulnerability data does not support the claim. It is known that Windows 10 has numerous amounts of additional features and functionality than Windows 7, and Windows 8, and having so many features in one software means there are many possible ways to have flaws. These additional features may cause an increase in the number of vulnerabilities in Windows 10.

This graph shows that MacOS has more vulnerabilities than other software. Windows 10 seems to be the least secure desktop OS among other Microsoft OS. Sometimes visual representation might not be enough to explain the actual characteristic of data. Even though the number of vulnerabilities of the MacOS seems to be higher, the rate at which vulnerabilities change could be less. This will imply that MacOS is a secure Desktop OS.

2.2. The Stochastic Process

As can be seen from Figure 3, the number of vulnerabilities as a function of time results as a non-stationary signal/time series. We let $N(T)$ be the number of vulnerabilities as a function of time and our objective is to develop or identify a stochastic process that drives $N(T)$ so that we can characterize probabilistically the behavior of the number of vulnerabilities as a function of time. Let $N(T_i), i = 1, 2, \cdots, n$ be the stochastic variables of $N(T)$, we proceed to rank the stochastic variables, that is, the number of vulnerabilities as a function of time from the smallest to the largest, that is, $N(T_1)$ is the smallest number of vulnerabilities occurs at T_1 and the largest at T_n. Such an arrangement of the stochastic variables represents the growth of the number of vulnerabilities of the OS. Figure 4 displays the behavior of the growth pattern of the number of vulnerabilities for Windows 7, 8, 10, and MacOS.

The stochastic process that characterizes the growth behavior of the stochastic variables is similar to the Power Law Process [10] [16]. Thus, the probability of observing a specific number of vulnerabilities, $N(T)$ in a given interval $(0, T]$ is given by

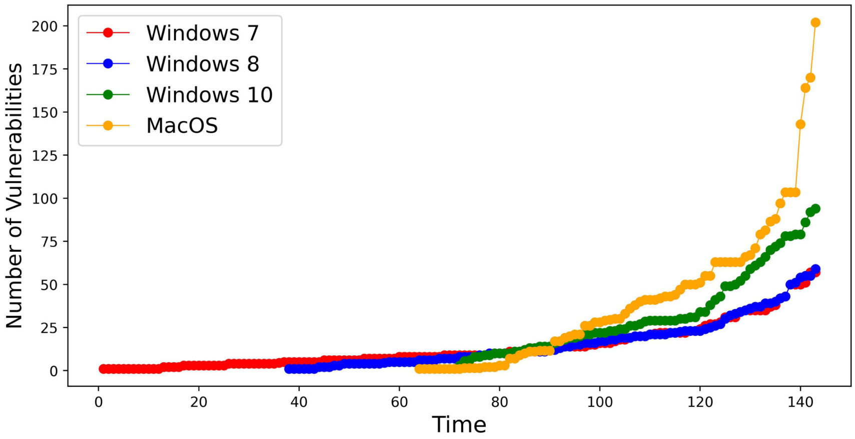

Figure 4. The vulnerabilities growth pattern of Windows 7, Windows 8, Windows 10, and MacOS.

$$\begin{aligned}&\left[V\left(N\left(T\right)\right)=N\left(T\right);T\right]\\&=\frac{1}{N\left(T\right)!}\exp\left\{-\int_0^T VIF\left(V\left(N\left(T\right)\right)\right)\mathrm{d}V\left(N\left(T\right)\right)\right\}\\&\times\left(\int_0^T VIF\left(V\left\{N\left(T\right)\right\}\right)\mathrm{d}V\left(N\left(T\right)\right)\right)^{N(T)},\ T>0.\end{aligned}\tag{1}$$

The $VIF\left(N\left(T\right)\right)$ is the **Vulnerability Intensity Function** of the operating system as a function of time *T*, which measures the rate at which the number of vulnerabilities changes with respect to time. The actual value of $VIF\left(N\left(T\right)\right)$ is defined as follows:

$$VIF\left(N\left(t\right)\right)=\frac{VII}{\gamma}\left(\frac{T}{\gamma}\right)^{VII-1},\quad T>0,\quad VII>0,\quad \gamma>0,\tag{2}$$

where VII is the **Vulnerability Index Indicator** and γ is a scale parameter [7] [8]. The above stochastic process (1) after substitution of $VIF\left(N\left(T\right)\right)$, reduces to,

$$P\left[V\left(N\left(T\right)\right)=N\left(T\right);T\right]=\frac{1}{N\left(T\right)!}\exp\left\{-\frac{T^{VII}}{\gamma^{VII}}\right\}\left(\frac{T}{\gamma}\right)^{N(T)\times VII},\tag{3}$$

which parallels the Power Law Process.

Thus, given the number of vulnerabilities at times $T_1,T_2,\cdots,T_n$, where $T_1<T_2<\cdots<T_n$, then the truncated conditional probability distribution function, $f_i\left(T\mid T_1,\cdots,T_{i-1}\right)$, is given by

$$f_i\left(T\mid T_1,\cdots,T_{i-1}\right)=\frac{VII}{\gamma}\left(\frac{T}{\gamma}\right)^{VII-1}\exp\left\{-\left(\frac{T}{\gamma}\right)+\left(\frac{T_{i-1}}{\gamma}\right)^{VII}\right\},\quad T>T_{i-1}.\tag{4}$$

Hence, the likelihood function of Equation (4) is given by

$$\begin{aligned}L\left(VII,\gamma\right)&=\prod_{i=1}^{N(T_i)}f_i\left(T\mid T_1,\cdots,T_{i-1}\right)\\&=\left(\frac{VII}{\gamma}\right)^{N(T)}\exp\left\{-\left(\frac{T_{N(t)}}{\gamma}\right)^{VII}\right\}\prod_{i=1}^{N(T)}\left(\frac{T_i}{\gamma}\right)^{VII-1}.\end{aligned}$$

Now, we can proceed to obtain maximum likelihood estimates of ***VII*** and γ, that is,

$$\widehat{VII}=\frac{N\left(T\right)}{\sum_{i=1}^{N(T_n)}\ln\left(\frac{T_n}{T_i}\right)},\tag{5}$$

and the parameter γ,

$$\hat{\gamma}=\frac{T_n}{N\left(T\right)^{1/\widehat{VII}}}.\tag{6}$$

3. Results

3.1. The Vulnerability Intensity Function (*VIF*)

Assume the number of vulnerabilities of computer operating system at time *T* is denoted by NV_T. The probability of observing a specific number of vulnerabilities, $NV(T)$ in a given interval $(0,T]$ is given by:

$$P\left[V\left(NV(T)\right)=NV(T);T\right]$$
$$=\frac{1}{NV(T)!}\exp\left\{-\int_0^T VIF\left(V\left(NV(T)\right)\right)\mathrm{d}V\left(NV(T)\right)\right\}$$
$$\times\left(\int_0^T VIF\left(V\left\{NV(T)\right\}\right)\mathrm{d}V\left(NV(T)\right)\right)^{NV(T)},\quad T>0.$$

The part of the entities in the above stochastic process, $VIF\left(NV(T)\right)$, is the **Vulnerability Intensity Function (*VIF*)** that drives the number of vulnerabilities of the computer operating system at time *T*. The general form of ***VIF*** is given below:

$$VIF\left(NV(T),VII,\gamma\right)=\frac{VII}{\gamma}\left(\frac{T}{\gamma}\right)^{VII-1},\quad T>0,\quad VII>0,\quad \gamma>0. \tag{7}$$

The usefulness of ***VIF*** is that it gives us the rate at which the number of vulnerabilities changes as the function of time of the computer operating systems.

We obtained the maximum likelihood estimates of the parameters within the **Vulnerability Intensity Function (*VIF*)**, ***VII***, and γ. The estimates are given below:

$$\widehat{VII}_n=\frac{N(T_n)}{\sum_{i=1}^{N(T_n)}\ln\left(\frac{\widehat{NV}_n}{\widehat{NV}_i}\right)},$$

and

$$\hat{\gamma}_n=\frac{\widehat{NV}_n}{N(T)^{1/\widehat{VII}}}.$$

Now, we proceed to obtain the ***VIF*** of the Microsoft operating systems Windows 7, Windows 8, Windows 10, and Apple operating system MacOS.

3.1.1. The *VIF* of Windows 7

There is a total of 143 months of vulnerabilities data set for Windows 7 from October 2009 to August 2021. Assume the number of vulnerabilities at time *T* is denoted by VS_T. We rank VS_T such that $VS_1<VS_2<VS_3<\cdots<VS_T$ from the smallest value of VS_1 to the largest value VS_{143} as a function of time T. Then, the analytical estimate form of the ***VIF*** of Windows 7 is given below and gives us the rate at which the number of vulnerabilities changes as a function of time of Windows 7:

$$\widehat{VIF}_{win7}=\frac{\widehat{VII}_{win7}}{\gamma_{win7}}\left(\frac{T_n}{\gamma_{win7}}\right)^{\widehat{VII}_{win7}-1},\quad T_n>0,\widehat{VII}_{win7}>0,\gamma_{win7}>0.$$
$$=\frac{0.530}{0.005}\left(\frac{T_n}{0.005}\right)^{0.530-1}.$$

The rate of change of the number of vulnerabilities of Windows 7 is illustrated graphically in **Figure 5**.

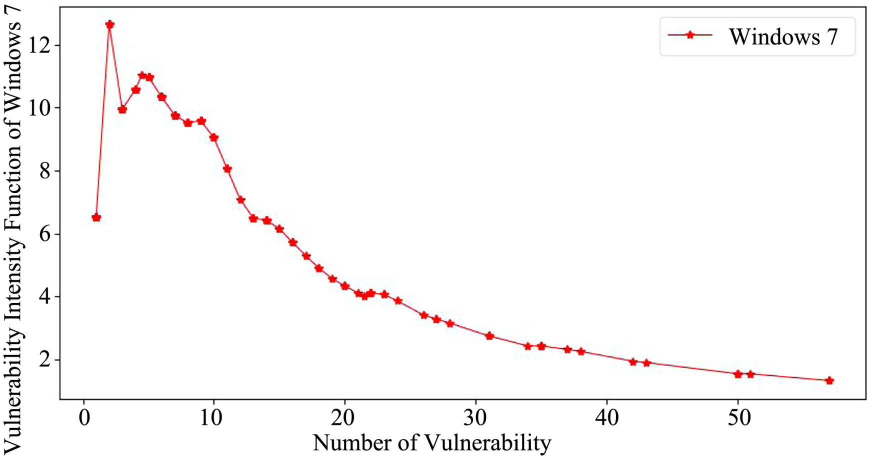

Figure 5. The **Vulnerability Intensity Function** (*VIF*) of Windows 7.

We can observe from the graphs that except for a few points, the **Vulnerability Intensity Function** of Windows 7 decreases when the number of vulnerabilities increases. The smallest value of the number of vulnerabilities of Windows 7 is 1 and the corresponding value of ***VIF*** is 6.5. When vulnerabilities change from 1 to 2, the ***VIF*** changes to 12.64. Then, ***VIF*** decreases to 9.93 for vulnerabilities equal to 3. Similarly, we can find ***VIF*** for each month depending on the number of vulnerabilities that change from previous months. The highest value of the number of vulnerabilities found in the Windows 7 is 57. The ***VIF*** changes from 1.54 to 1.32 when the number of vulnerabilities increases from 51 to 57.

3.1.2. The *VIF* of Windows 8

There is a total of 106 months (approximately 9 years) of vulnerabilities data set for Windows 8, starting from November 2012 to August 2021. Assume the number of vulnerabilities at time T is denoted by VE_T. We rank VE_T such that $VE_1 < VE_2 < VE_3 < \cdots < VE_T$ from the smallest value of VE_1 to the largest value VE_{106} as a function of time T. Then, the analytical estimate form of the ***VIF*** of Windows 8 is given below and gives us the rate at which the number of vulnerabilities changes as a function of time of Windows 8:

$$\widehat{VIF}_{win8} = \frac{\widehat{VII}_{win8}}{\gamma_{win8}}\left(\frac{T_n}{\gamma_{win8}}\right)^{\widehat{VII}_{win8}-1}, \quad T_n > 0, \widehat{VII}_{win8} > 0, \gamma_{win8} > 0.$$

$$= \frac{0.601}{0.025}\left(\frac{T_n}{0.025}\right)^{0.601-1}.$$

The rate of change of the number of vulnerabilities of Windows 8 is shown in Figure 6.

We can observe from the graphs with the exception of a few fluctuations, the **Vulnerability Intensity Function** (*VIF*) of Windows 8 has a decreasing pattern when the number of vulnerabilities increases. The smallest value of the number of vulnerabilities of Windows 8 is 1 and the corresponding value of ***VIF*** is 3.5. When vulnerabilities change from 1 to 2, the ***VIF*** changes to 7.69. Then, ***VIF***

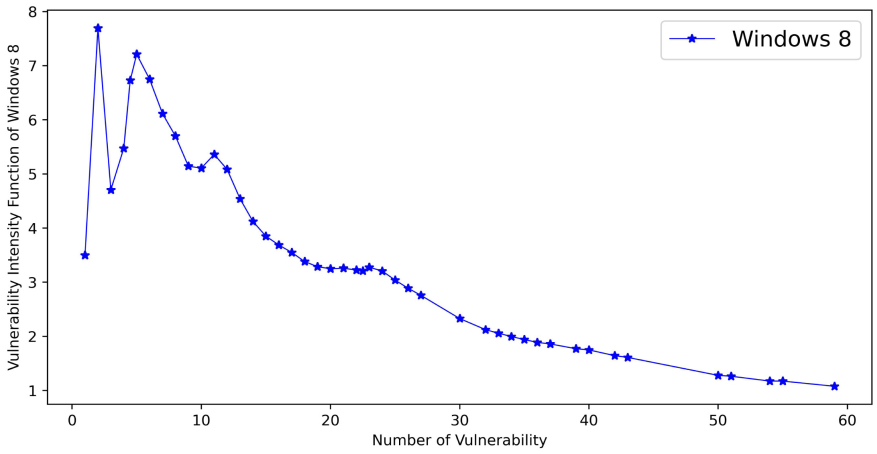

Figure 6. The **Vulnerability Intensity Function (** ***VIF*** **)** of Windows 8.

decreases to 4.71 for vulnerabilities equal to 3. After that ***VIF*** starts increasing and reaches 6.11 for a number of vulnerabilities equal to 5. This kind of pattern can be seen throughout the graphs of ***VIF*** when the number of vulnerabilities changes from previous months. At last, the highest value of the number of vulnerabilities found in the Windows 8 is 59. The ***VIF*** changes from 1.17 to 1.08 when the number of vulnerabilities increases from 55 to 59.

3.1.3. The *VIF* of Windows 10

There are 73 months of vulnerabilities data set for Windows 10. Assume the number of vulnerabilities at time T is denoted by VT_T. The ascending order of vulnerabilities of Windows 10 is $VT_1 < VT_2 < VT_3 < \cdots < VT_{73}$ from August 2015 to August 2021. Then, the analytical estimate form of the ***VIF*** of Windows 10 is given below and gives us the rate at which the number of vulnerabilities changes as a function of time of Windows 10:

$$\begin{aligned}\widehat{VIF}_{win10} &= \frac{\widehat{VII}_{win10}}{\gamma_{win10}}\left(\frac{T_n}{\gamma_{win10}}\right)^{\widehat{VII}_{win10}-1}, \quad T_n > 0, \widehat{VII}_{win10} > 0, \gamma_{win10} > 0. \\ &= \frac{0.742}{0.289}\left(\frac{T_n}{0.289}\right)^{0.742-1}.\end{aligned}$$

The rate of change of the number of vulnerabilities of Windows 10 is displayed by Figure 7.

We can observe from the graphs that there are many fluctuations in the ***VIF*** of Windows 10 than in Windows 7 and Windows 8. The **Vulnerability Intensity Function** of Windows 10 has a decreasing pattern when the number of vulnerabilities reaches 30. The smallest value of the number of vulnerabilities of Windows 10 is 3 and the corresponding value of ***VIF*** is 1.25. When vulnerabilities change from 3 to 6, the ***VIF*** changes to 0.71 and increases to 1.03. After that ***VIF*** starts increasing and reaches 2.55 for a number of vulnerabilities equal to 12 which is the highest value of ***VIF*** in 73 months. At least, the highest value of the number of vulnerabilities found in the Windows 10 is 94. The ***VIF*** changed from 0.582 to 0.576 when the number of vulnerabilities increases from 92 to 94.

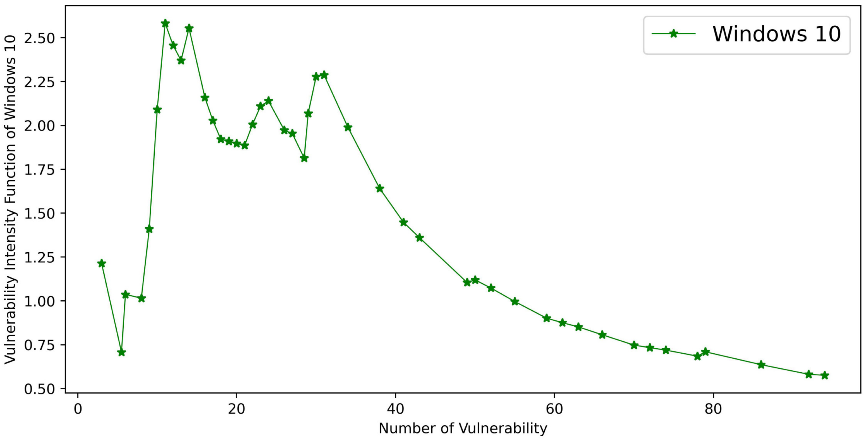

Figure 7. The **Vulnerability Intensity Function (** ***VIF*****)** of Windows 10.

3.1.4. The *VIF* of MacOS

There are 80 months of vulnerabilities data set for MacOS. Let $VM(T)$ be the number of vulnerabilities as a function of time T of MacOS. The ascending order of vulnerabilities of MacOS is $VM_1 < VM_2 < VM_3 < \cdots < VM_{80}$ from January 2015 to August 2021. Then, the analytical estimate forms of the ***VIF*** given below, and gives us the rate at which the number of vulnerabilities changes as a function of time of MacOS:

$$\widehat{VIF}_{mac} = \frac{\widehat{VII}_{mac}}{\gamma_{mac}}\left(\frac{T_n}{\gamma_{mac}}\right)^{\widehat{VII}_{mac}-1}, \quad T_n > 0, \widehat{VII}_{mac} > 0, \gamma_{mac} > 0.$$

$$= \frac{0.418}{0.006}\left(\frac{T_n}{0.006}\right)^{0.418-1}.$$

The rate of change of the number of vulnerabilities of MacOS is displayed by Figure 8.

We can observe from the graph that the **Vulnerability Intensity Function** of the MacOS has decreasing pattern when the number of vulnerabilities increases. The smallest value of the number of vulnerabilities of MacOS is 1 and the corresponding value of ***VIF*** is 5. When vulnerabilities change from 1 to 2, the ***VIF*** changes to 24.16. This is the only increasing pattern for MacOS after that we have gradually decreasing patterns of ***VIF***. The value of ***VIF*** decreases when the number of vulnerabilities changes from the previous months. At last, the largest value of the number of vulnerabilities found in MacOS is 202. The ***VIF*** changes from 0.21 to 0.17 when the number of vulnerabilities increases from 170 to 202.

3.1.5. Comparison of *VIF* of Windows 7, Windows 8, and Windows 10

The **Vulnerability Intensity Function (** ***VIF*****)** identifies analytically and graphically the rate at which the number of vulnerabilities changes as a function of time for a MOS. We can use the estimated value of the **Vulnerability Intensity Function,** $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ to compare the rate of changes in vulnerabilities of different operating systems. In this section, we have used the $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ to compare three Windows operating systems: Windows 7, Windows 8, and Windows 10.

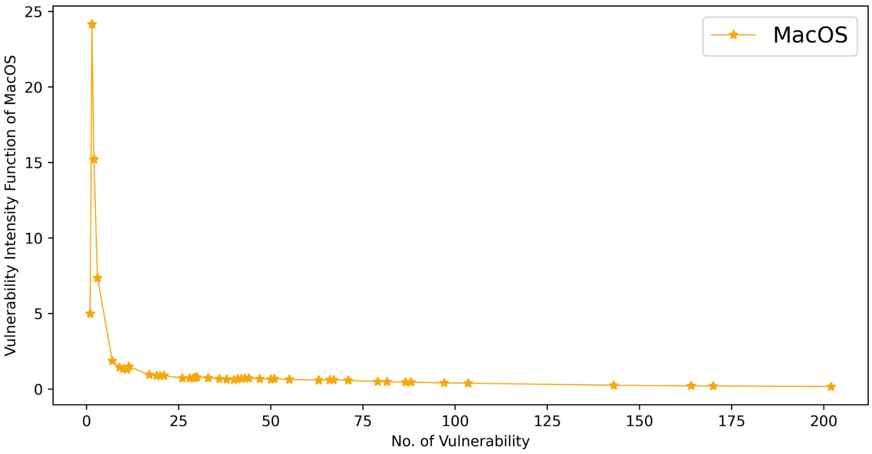

Figure 8. The **Vulnerability Intensity Function (*VIF*)** of MacOS.

The lowest values of $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ implies that the rate at which the number of vulnerabilities changes each month of Windows OS is low. The highest value $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ implies that the rate at which the number of vulnerabilities changes each month of respective Windows OS is high. Thus, the Windows operating systems with the lowest values of ***VIF***, $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ will be the safest Windows OS.

Figure 9 shows us the comparison of the **Vulnerability Intensity Function** of Windows 7 ($\widehat{VIF_{win7}}$), Windows 8 ($\widehat{VIF_{win8}}$), and Windows 10 ($\widehat{VIF_{win10}}$), respectively. The vulnerabilities data set collected for Windows 7, Windows 8, and Windows 10 are from October 2009 to August 2021, November 2012 to August 2021, and August 2015 and August 2021. The median value of the ***VIF*** of Windows 7, Windows 8, and Windows 10 are 8.06, 3.77, and 1.92 respectively. Based on this result we can conclude that the rate at which the number of vulnerabilities changes in Windows 10 is less than in Windows 8 and Windows 7. From the plot, we can also see that the distribution of ***VIF*** of Windows 10 and 7 is negatively skewed whereas the distribution of ***VIF*** of Windows 8 is positively skewed. This means that the vulnerability discovery rates of Windows 7, and widows 10 are decreasing, and Windows 8 is increasing.

Figure 10 shows the **Vulnerability Intensity Function (*VIF*)** of three Microsoft Windows operating systems as the function of time. The data available to us are in different time periods because the updates are published in different time frames by Microsoft Corporation. Hence, for transparency, the times taken for the comparison of these three operating systems are from August 2020 to August 2021.

Figure 10 illustrates that the ***VIF*** of Windows 10 is the lowest, Windows 8 is in the middle and Windows 7 is the highest as one would expect. Thus, we can describe the rate at which the number of vulnerabilities changes with respect to time (months) as lowest for Windows 10 and highest for Windows 7. Microsoft cooperation has added many security features to Windows 10. They claimed that Windows 10 is supposed to be the best and most secure operating system.

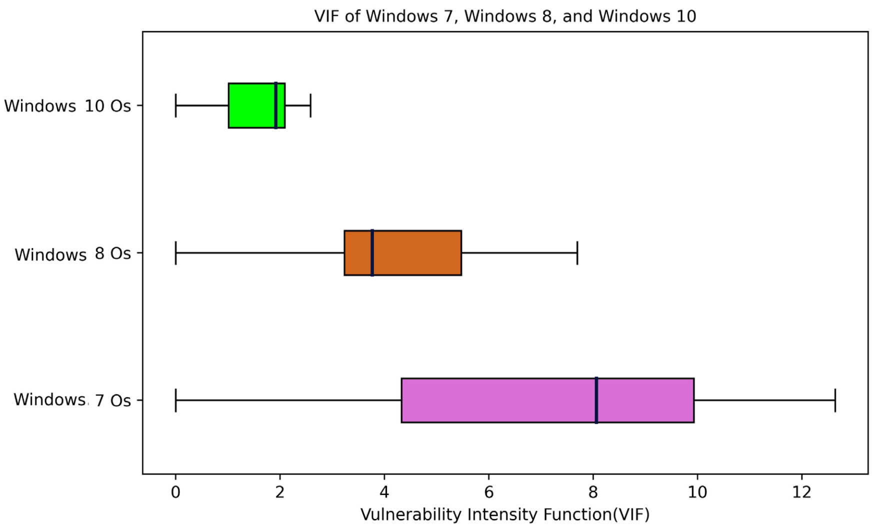

Figure 9. The **Vulnerability Intensity Function (** ***VIF*****)** of Windows 7, 8, and 10.

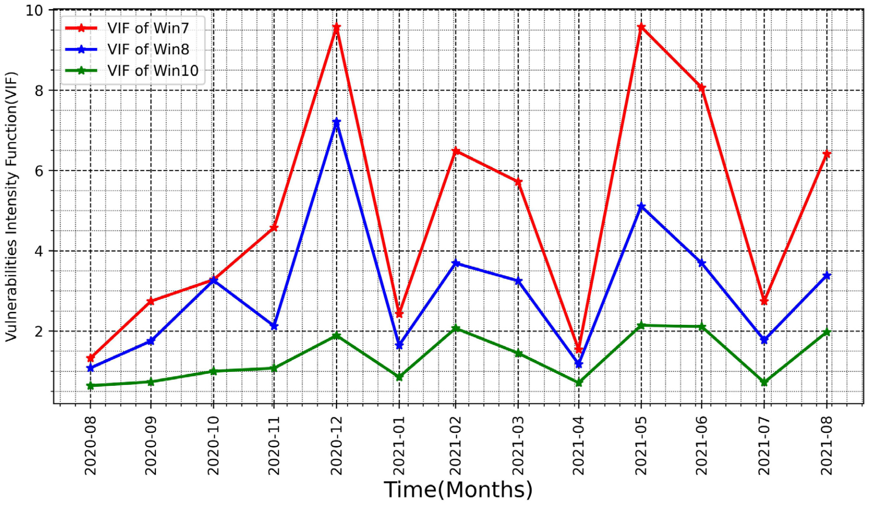

Figure 10. The comparison of *VIF* of Windows 7, Windows 8, and Windows 10 from August 2020 to August 2021.

Our study support that Microsoft 10 is the secure Windows OS among the three.

In addition from **Figure 10**, we can see a similar time series pattern among Windows 7, Windows 8, and Windows 10. There are many common types of vulnerabilities that can affect more than one Windows operating system at the same period of time. For example, vulnerability CVE-2018-8641 had affected Windows 10, Windows 8.1, and many Windows servers. These common types of vulnerability have influenced the number of vulnerabilities found in Windows 7, Windows 8, and Windows 10 (monthly).

3.1.6. The Comparison of *VIF* of MacOS with Windows 10

The **Vulnerability Intensity Function (** ***VIF*****)** identifies analytically and graphically the rate at which the number of vulnerabilities changes as a function of time for any OS. In this section, we have used the $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ to compare the best Windows operating systems: Windows 10 with Apple's operating systems MacOS. By comparing the ***VIF*** of MacOS with Windows 10, we can identify which software has a higher rate of vulnerability change as a function of time. The lowest values of $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ will imply that the rate at which the number of vulnerabilities changes each month of OS is low. Thus, the operating systems with the lowest values of ***VIF***, $\widehat{VIF}\left(NV(T);\widehat{VII},\hat{\gamma}\right)$ will be the safest OS.

We have estimated the **Vulnerability Intensity Function** of MacOS ($\widehat{VIF_{mac}}$) as a function of time (monthly) with parameter $\widehat{VII}$ and $\hat{\gamma}$. We proceed to study the behavior of the number of vulnerabilities of MacOS by deriving the rate of changes in ($\widehat{VIF_{mac}}$). The **Vulnerability Intensity Function** of the number of vulnerabilities for 80 months (approximately 7 years) of MacOS is shown in Figure 11. Additionally, the **Vulnerability Intensity Function** of the number of vulnerabilities for 73 months (approximately 6 years) of Windows 10 is also shown in Figure 11.

We observe the fluctuations of the ***VIF*** of MacOS are sequentially higher and not uniform as a function of time whereas the ***VIF*** of Windows 10 fluctuations are smaller and quite uniform. Furthermore, from 2015 to 2017, the VIF_{win10} was higher than VIF_{mac}. After that ***VIF*** of MacOS has considered the amount of higher fluctuations between 2018 to 2019 and from starting of 2021 to at end of august 2021. There are many fluctuations in the number of vulnerabilities of the MacOS. For example, In October, November, and December, the numbers of vulnerabilities were 164, 3, and 55, respectively. At the same time, the number of vulnerabilities of Windows 10 was 55, 52, and 21 respectively. Another major change occurred from April 2021 to May 2021 when vulnerabilities changed

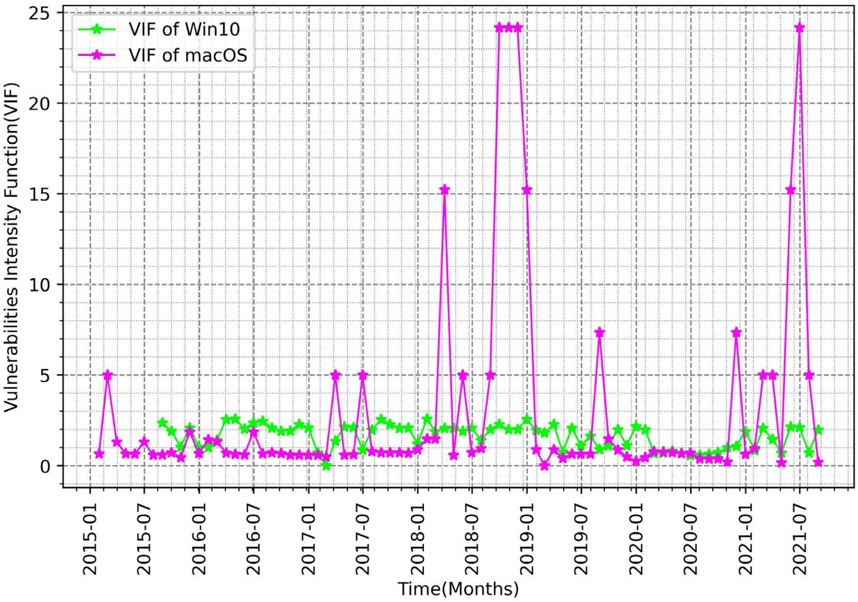

Figure 11. The **Vulnerability Intensity Function** (***VIF***) of Windows 10 and MacOS.

from 202 to 2. At the same time, the number of vulnerabilities of Windows 10 was changed from 79 to 24. The ***VIF*** explains the rate at which the number of vulnerabilities changes with respect to time, so it will be higher if the difference between the numbers of vulnerabilities each month is higher. Thus, the ***VIF*** of MacOS was higher. Hence, there is a high-security risk in MacOS than in Windows 10 in terms of vulnerabilities found in the software.

3.2. The Vulnerability Index Indicator (*VII*)

Within the definition of ***VIF*** in the previous section, we introduce the term the **Vulnerability Index Indicator (** ***VII*****)**. This Index Indicator gives us very useful information about the behavior of the number of vulnerabilities at a specific time. The general form and estimate of ***VII*** are defined as:

$$\widehat{VII}_n = \frac{N(T_n)}{\sum_{i=1}^{N(T_n)} \ln\left(\frac{\widehat{NV}_n}{\widehat{NV}_i}\right)},$$

where we assume the number of vulnerabilities of a computer operating system at time T is denoted by NV_T and $N(T_n)$ rank of NV_T.

The **Vulnerability Index Indicator (** ***VII*****)** monitors the behavior of the number of vulnerabilities of each operating system at a specific time. The ***VII*** value may be greater than 1, approximately equal to 1, and less than 1. The interpretation of $\widehat{VII}$ is as follows: if $\widehat{VII} < 1$ means that the number of vulnerabilities is decreasing, if $\widehat{VII} > 1$, then the number of vulnerabilities is increasing and if $\widehat{VII} \approx 1$ then the number of vulnerabilities remains unchanged.

Now, we proceed to present the ***VII*** of the Microsoft operating systems Windows 7, Windows 8, Windows 10, and Apple operating system MacOS.

3.2.1. The *VII* of Windows 7

There is a total of 143 months of vulnerabilities data set for Windows 7 from October 2009 to August 2021. Assume the number of vulnerabilities at time T is denoted by VS_T. We rank VS_T such that $VS_1 < VS_2 < VS_3 < \cdots < VS_{143}$ from the smallest value of VS_1 to the largest value VS_{143} as a function of time T. Then, the analytical form of the ***VII*** and its estimate of Windows 7 is given by

$$\widehat{VII}_{win7} = \frac{N(T_n)}{\sum_{i=1}^{N(T_n)} \ln\left(\frac{\widehat{VS}_n}{\widehat{VS}_i}\right)},$$

with the numerical estimates it is given by

$$\widehat{VII}_{win7} = \frac{142.5}{\sum_{i=1}^{143} \ln\left(\frac{57}{\widehat{VS}_i}\right)}.$$

We have monitored the number of vulnerabilities of Windows 7 by assessing the behavior or changes in $\widehat{VII}$. The estimated parameter of the **Vulnerability**

Index Indicator ($\widehat{VII}$) of the number of vulnerabilities of 143 months from October 2009 to August 2021 of Windows 7 is 0.53. The **Vulnerability Index Indicator** of Windows 7 is less than 1. It indicates the rate at which the vulnerabilities of Windows 7 are decreasing. Hence, the number of vulnerabilities found in Windows 7 is also decreasing. This might due to the user of Windows 7 is gradually decreasing. The estimated value of the **Vulnerability Index Indicator** ($\widehat{VII}$) of the number of vulnerabilities of Windows 7 from Aug. 2020 to Aug. 2021 are shown by **Figure 12**.

Thus, from **Figure 12** that number of vulnerabilities of Windows 7 from 2009 to Aug., 2020 with $\widehat{VII} = 0.53 < 1$. The **Vulnerability Index Indicator** ($\widehat{VII}$) rose from 0.53 to 0.67. Thus, the number of vulnerabilities decreases from 57 to 31 from 2020-08 to 2020-09. When $\widehat{VII}$ approaches one or more than 1, the vulnerabilities of the operating system increase. When $\widehat{VII}$ approaches to less than 1, the vulnerabilities of the operating system keeps decreasing. The $\widehat{VII}$ close to one and more than 1 for October, November, and December 2020, that is, 0.72, 0.82, and 1.18. Hence, the vulnerability decreases gradually from 31 to 27,19, and 9, respectively. For 2021-01, number of vulnerability decreases from 35 to 13 with $VII = 0.65 < 1$. If there are small changes that happen in the number of vulnerabilities of Windows 7 each month, we can see these changes by the **Vulnerability Index Indicator** ($\widehat{VII}$).

3.2.2. The *VII* of Windows 8

There is a total of 106 months (approximately 9 years) of vulnerability data for Windows 8 from November 2012 to August 2021. We assume that the number of vulnerabilities at time *T* is denoted by VE_T. We rank VE_T such that $VE_1 < VE_2 < VE_3 < \cdots < VE_{106}$ from the smallest value of VE_1 to the largest value VE_{106} as a function of time *T*. Then, the analytical form of the ***VII*** and its

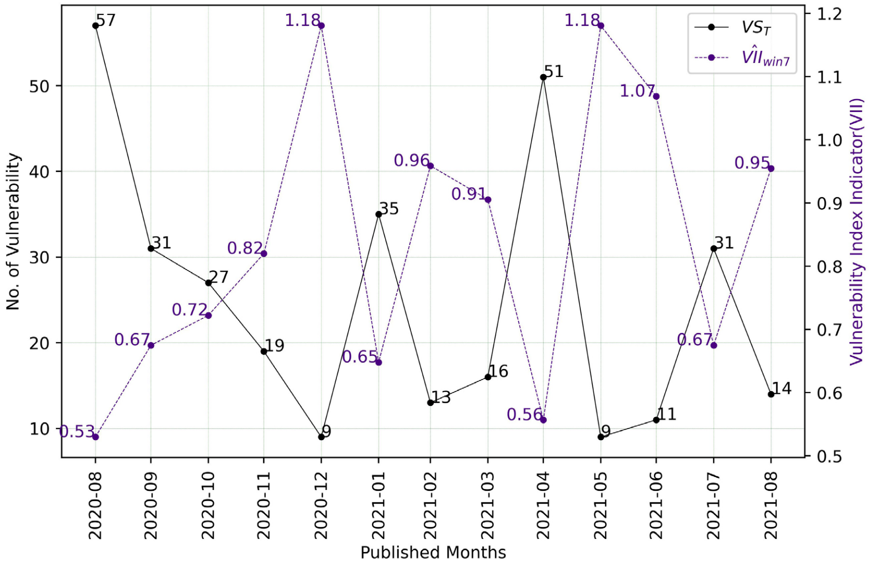

Figure 12. The **Vulnerability Index Indicator** (*VII*) of Windows 7 from August 2020 to August 2021.

estimates of Windows 8 is given below and it gives us the behavior of the number of vulnerabilities at a specific time of Windows 8:

$$\widehat{VII}_{win8} = \frac{N(T_n)}{\sum_{i=1}^{N(T_n)} \ln\left(\frac{\widehat{VE}_n}{\widehat{VE}_i}\right)}.$$

Thus, with the approximate maximum likelihood estimates of Windows 8 is

$$\widehat{VII}_{win8} = \frac{106}{\sum_{i=1}^{106} \ln\left(\frac{59}{\widehat{VE}_i}\right)}.$$

The number of vulnerabilities of Windows 8 by assessing the behavior or changes in $\widehat{VII}$. The estimated parameter of the **Vulnerability Index Indicator** ($\widehat{VII}$) of the number of vulnerabilities of 106 months (approximately 9 years) from November 2012 to August 2021 of Windows 8 is 0.601. The **Vulnerability Index Indicator** of Windows 8 is less than 1. It indicates the rate at which the vulnerability of Windows 8 is decreasing. Hence, the number of vulnerabilities found in Windows 8 is also decreasing. The estimated value of the **Vulnerability Index Indicator** ($\widehat{VII}$) of the number of vulnerabilities of Windows 8 from Aug. 2020 to Aug. 2021 is shown by **Figure 13**.

We can observe from **Figure 13** that number of vulnerabilities of Windows 8 were descending from November 2012 to August 2020 with $\widehat{VII} = 0.60 < 1$, so the number of vulnerabilities decrease from 59 to 40 in Nov. 2020. For 2020-09 and 2020-10, $\widehat{VII}$ gradually move toward one, that is, $\widehat{VII} = 0.71$ and $\widehat{VII} = 0.92$ respectively. Hence the number of vulnerabilities decreases from 59 to 40 and 21, respectively. The $\widehat{VII}$ decreases from 0.92 to 0.76 for November 2020, and the number of vulnerabilities increased from 21 to 32. The **Vulnerability Index**

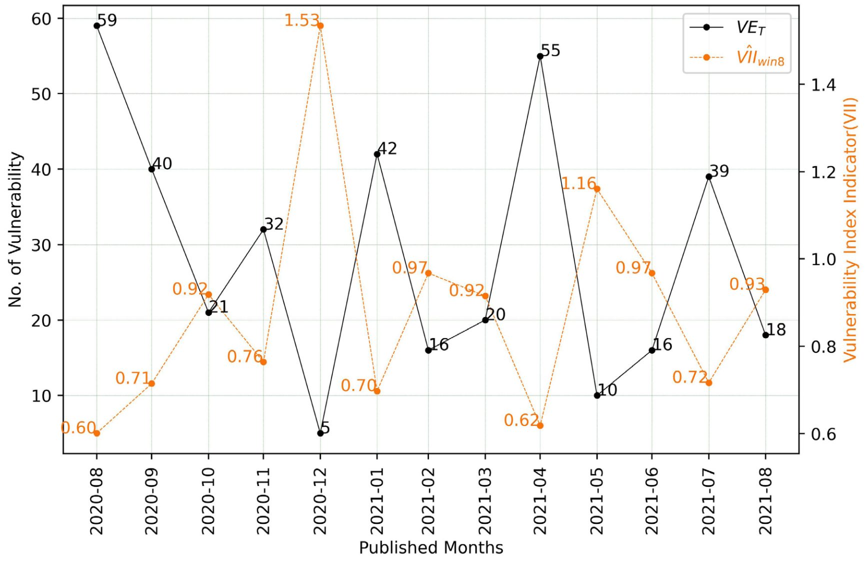

Figure 13. The **Vulnerability Index Indicator** (*VII*) of Windows 8 from August 2020 to August 2021.

Indicator ($\widehat{VII}$) sharply rises from 0.76 to 1.53. Thus, the number of vulnerabilities also sharply decreases from 32 to 5 from 2020-11 to 2020-12. The **Vulnerability Index Indicator** ($\widehat{VII}$) sharply decreases from 1.53 to 0.70. This implies that the number of vulnerabilities highly increased from 5 to 42 for the months 2020-12 to 2021-01. Similarly, we can observe the behavior of vulnerability of Windows 8 for remaining months by estimating the value of ***VII***.

3.2.3. The *VII* of Windows 10

There are 73 months of vulnerabilities data set for Windows 10 from August 2015 to August 2021. We assume the number of vulnerabilities at time T is denoted by VT_T. The ascending order of vulnerabilities of Windows 10 is $VT_1 < VT_2 < VT_3 < \cdots < VT_{73}$. Then, the analytical form of the ***VII*** of Windows 10 is given below and gives us the behavior of the number of vulnerabilities at a specific time of Windows 10:

$$\widehat{VII}_{win10} = \frac{N(T_n)}{\sum_{i=1}^{N(T_n)} \ln\left(\frac{\widehat{VT}_n}{\widehat{VT}_i}\right)},$$

with the numerical estimates it is given by

$$\widehat{VII}_{win10} = \frac{73}{\sum_{i=1}^{73} \ln\left(\frac{94}{\widehat{VT}_i}\right)}.$$

We can monitor the number of vulnerabilities of Windows 10 by assessing the behavior or changes in $\widehat{VII}$. The estimated parameter of the **Vulnerability Index Indicator** ($\widehat{VII}$) of the number of vulnerabilities of 73 months (approximately 6 years) from August 2015 to August 2021 of Windows 10 is 0.74. The **Vulnerability Index Indicator** ($\widehat{VII}$) of Windows 10 is less than 1. It indicates the failure rate of the vulnerability of the operating system is also decreasing. The estimated value of the **Vulnerability Index Indicator** ($\widehat{VII}$) of the number of vulnerabilities of Windows 10 from Aug. 2020 to Aug. 2021 is shown by **Figure 14**.

We can observe from **Figure 14** that number of vulnerabilities of Windows 10 was descending from August 2015 to August 2020 with $\widehat{VII} = 0.77 < 1$ so the number of vulnerabilities decreased from 86 to 72 in September 2020. The $\widehat{VII}$ gets close to one and more than 1 for September, October, November, and December 2020, that is, 0.81, 0.93, 0.96, and 1.44 respectively. Hence the vulnerability decreases gradually from 86 to 72, 55, 52, and 21, respectively. The **Vulnerability Index Indicator** ($\widehat{VII}$) sharply decreases from 1.44 to 0.87. This implies the number of vulnerabilities decreases from 63 to 29 for the month 2021-01 to 2021-02. Similarly, we can interpret the behavior of Windows 10 for the remaining months. We are able to predict the behavior of vulnerability of Windows 10 for the given time by estimating the value of $\widehat{VII}$ of the previous month for the year correctly.

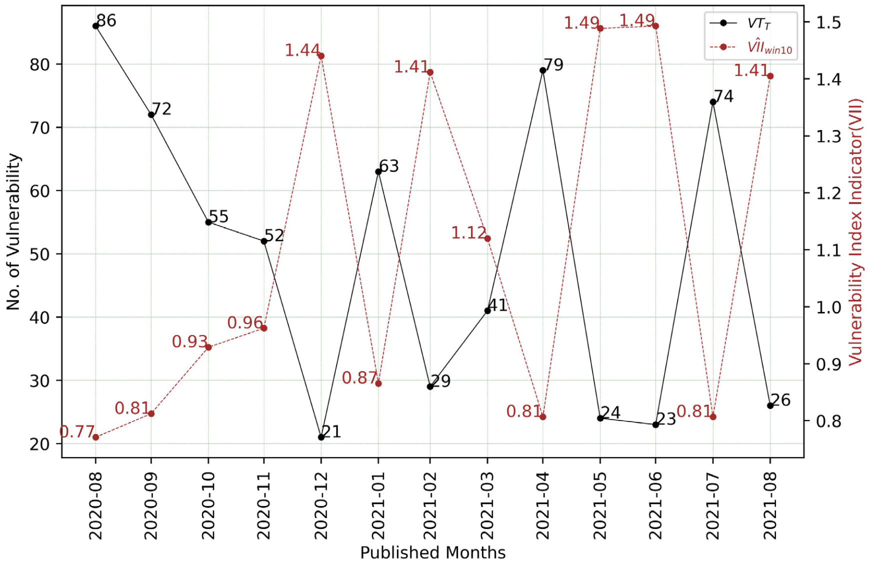

Figure 14. The **Vulnerability Index Indicator (*VII*)** of Windows 10 from Aug. 2020 to Aug. 2021.

3.3. The *VII* of MacOS

We are using 80 months of vulnerabilities data set for MacOS. Let $VM(T)$ be the number of vulnerabilities as a function of time T of MacOS. The ascending order of vulnerabilities of MacOS is $VM_1 < VM_2 < VM_3 < \cdots < VM_{80}$ from January 2015 to August 2021. Then, the analytical form of the ***VII*** and its estimate $\widehat{VII}_{mac}$ of MacOS is given below and gives us the behavior of the number of vulnerabilities at a specific time of the MacOS:

$$\widehat{VII}_{mac} = \frac{N(T_n)}{\sum_{i=1}^{N(T_n)} \ln\left(\frac{\widehat{VM}_n}{\widehat{VM}_i}\right)},$$

with the maximum likelihood estimates it is given by

$$\widehat{VII}_{mac} = \frac{80}{\sum_{i=1}^{80} \ln\left(\frac{202}{\widehat{VM}_i}\right)}.$$

The estimated parameter of the **Vulnerability Index Indicator** $\widehat{VII}_{mac}$ of the number of vulnerabilities of 80 months (approximately 7 years) from January 2015 to August 2021 of MacOS is 0.42. The $\widehat{VII}_{mac}$ of MacOS is less than 1. It indicates the failure rate of the vulnerability of this operating system is also decreasing. The number of vulnerabilities found in MacOS is also decreasing. **Figure 15** shows the number of vulnerabilities and ***VII*** of the MacOS from August 2020 to August 2021.

The number of vulnerabilities of MacOS increased when the ***VII*** of MacOS decreased. The number of vulnerabilities of MacOS was ascending from January 2015 to August 2020 with $\widehat{VII} = 0.54 < 1$ and stays the same on September with zero vulnerability. The $\widehat{VII}$ is equal to 0.45, 1.26, 0.60, and 0.57 for October,

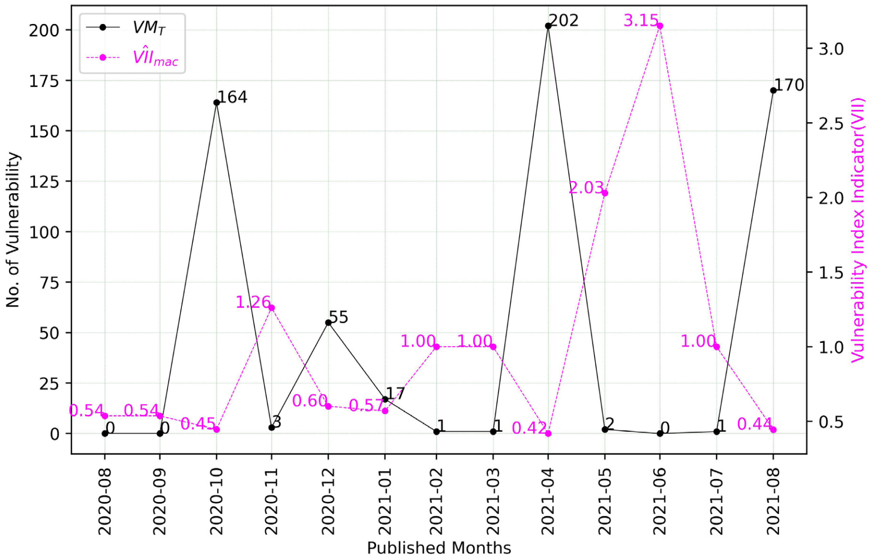

Figure 15. The **Vulnerability Index Indicator** of MacOS from August 2020 to August 2021.

November, December 2020, and January 2021, respectively. Hence, the vulnerability changes from 164 to 5, 55, 17, and 1, respectively. On 2021-02 and 2021-03, the number of vulnerabilities stays equal to 1 when the **Vulnerability Index Indicator** ($\widehat{VII}$) was approximately equal to 1. The **Vulnerability Index Indicator** ($\widehat{VII}$) decreases from ≈1 to 0.42. This implies the number of vulnerabilities sharply decreases from 202 to 1 for the month 2021-04 to 2021-05. Similarly, we can interpret the behavior of MacOS for remaining months.

3.4. Comparison of *VII* of Windows 7, Windows 8, Windows 10, and MacOS

The **Vulnerability Index Indicator** ($\widehat{VII}$) monitors the behavior of the number of vulnerabilities of the operating systems at a specific time. Table 2 gives the estimated values of $\widehat{VII}$ for Windows 7, Windows 8, Windows 10, and MacOS from August 2020 to August 2021. Three behaviors of the operating systems are possible. The behavior of $\widehat{VII}$ is greater than 1, approximately equal to 1, and less than 1. We interpret the changes in $\widehat{VII}$ as follows: If $\widehat{VII} < 1$ means that the number of vulnerabilities is decreasing. It will be secure software for that specific time. If $\widehat{VII} > 1$, then the number of vulnerabilities are increasing . That means there will be a high-security risk for that software. If $\widehat{VII} \approx 1$, then the number of vulnerabilities remains the same.

From Table 2, the $\widehat{VII}$ of all four software were less than 1 on August 2020, September 2020, October 2020, January 2021, and April 2021. That means the number of vulnerabilities decreases. On Nov. 2020 the $\widehat{VII}$ of all three Windows OS were less than 1 and for MacOS, it was greater than 1. Thus, the number of vulnerabilities of all three OS is decreasing, and MacOS are increasing. On Dec. 2020 the $\widehat{VII}$ of all three Windows OS were greater than 1 and for MacOS, it was less than 1. Thus, the number of vulnerabilities of all three OS is

Table 2. Behavior of vulnerability of Windows 7, Windows 8, Windows 10, and MacOS.

Date	$\widehat{VII}_{win7}$	beh_7	$\widehat{VII}_{win8}$	beh_8	$\widehat{VII}_{win10}$	beh_{10}	$\widehat{VII}_{mac}$	beh_{mac}
8/31/2020	0.53	<1	0.60	<1	0.77	<1	0.54	<1
9/30/2020	0.68	<1	0.71	<1	0.81	<1	0.54	<1
10/31/2020	0.72	<1	0.92	<1	0.93	<1	0.45	<1
11/30/2020	0.82	<1	0.76	<1	0.96	<1	1.26	>1
12/31/2020	1.18	>1	1.53	>1	1.44	>1	0.60	<1
1/31/2021	0.65	<1	0.70	<1	0.87	<1	0.57	<1
2/28/2021	0.96	<1	0.97	<1	1.41	>1	$1\pm\varepsilon$	$1\pm\varepsilon$
3/31/2021	0.91	<1	0.92	<1	1.12	>1	$1\pm\varepsilon$	$1\pm\varepsilon$
4/30/2021	0.56	<1	0.62	<1	0.81	<1	0.42	<1
5/31/2021	1.18	>1	1.16	<1	1.49	>1	2.03	>1
6/30/2021	1.07	>1	0.97	<1	1.49	>1	3.15	>1
7/31/2021	0.68	<1	0.72	<1	0.81	<1	$1\pm\varepsilon$	$1\pm\varepsilon$
8/31/2021	0.96	<1	0.92	<1	1.41	>1	0.44	<1

increasing, and MacOS are decreasing. In Feb. 2021 and Mar. 2021, in Windows 7 and Windows 8, the $\widehat{VII}$ were less than 1. Thus, the number of vulnerabilities is decreasing. Whereas the $\widehat{VII}$ of Windows 10 was greater than 1 so the number of vulnerabilities increases. At the same months, the $\widehat{VII}$ of the MacOS were equal to $1\pm\varepsilon$, which means the number of vulnerabilities of MacOS were approximately equal to 1 and it is the smallest possible value of vulnerability occurrence. On May 2021 and June 2021, the $\widehat{VII}$ of all three software were greater than 1 and for Windows 8, it was less than 1. Thus, the number of vulnerabilities of all three OS is increasing, and Windows 8 are decreasing. The number of vulnerabilities in all three OS decreased because the $\widehat{VII}$ was less than 1 except for MacOS in July 2021.

The $\widehat{VII}$ of the MacOS was equal to $1\pm\varepsilon$, which means the number of vulnerabilities of MacOS was approximately equal to 1. Finally, on Aug. 2021 the $\widehat{VII}$ of all three Windows OS were less than 1 whereas, for Windows 10, it was greater than 1. Thus, the number of vulnerabilities of all three OS is decreasing, and Windows 10 are increasing.

3.5. Relation between *VIF* and *VII*

The part of the entities in the stochastic process given in Equation (1), $VIF\left(N\left(T\right)\right)$, is the **Vulnerability Intensity Function (** ***VIF*****)** that gives us the rate at which the number of vulnerabilities changes as a function of time T of the computer operating systems. The general form of ***VIF*** is given below:

$$VIF\left(NV\left(T\right),VII,\gamma\right)=\frac{VII}{\gamma}\left(\frac{T}{\gamma}\right)^{VII-1},\ T>0,\ VII>0,\ \gamma>0.$$

The **Vulnerability Index Indicator** (*VII*) is the parameter within the **vulnerability intensity function** (*VIF*). The maximum likelihood estimate of *VII* is given below:

$$\widehat{VII}_n = \frac{N(T_n)}{\sum_{i=1}^{N(T_n)} \ln\left(\frac{\widehat{NV}_n}{\widehat{NV}_i}\right)}.$$

The relation between *VIF* and *VII* is directly proportional to each other. When the value of $\widehat{VII}$ increases by small value, we will see some increase in the value of $\widehat{VIF}$ and vice versa. Table 3 shows the estimated values of $\widehat{VII}$ and $\widehat{VIF}$ for Windows 7, Windows 8, Windows 10, and MacOS from August 2020 to August 2021. In Table 3, we can observe three different kinds of relationship between $\widehat{VII}$ and $\widehat{VIF}$.

That is, if the value of $\widehat{VII}$ increases, then $\widehat{VIF}$ also increases. That means the number of vulnerabilities of the respective OS will increase at a specific time. If the value of $\widehat{VII}$ decreases, then $\widehat{VIF}$ is also decrease. That means the number of vulnerabilities of the respective OS will decrease at a given time. Lastly, if the value of $\widehat{VII}$ stays the same, then $\widehat{VIF}$ also stays the same. In this case, there will be no changes in the number of vulnerabilities at that specific time. When the $\widehat{VII}$ is equal to $1 \pm \varepsilon$, which means the number of vulnerabilities is approximately equal to 1 and it is the smallest possible value of vulnerability occurrence while ranking the number of vulnerabilities of the OS.

Table 3. The list of estimates of Windows 7, Windows 8, Windows 10, and MacOS.

VII_{win7}	VIF_{win7}	VII_{win8}	VIF_{win7}	VII_{win10}	VIF_{win10}	VII_{mac}	VIF_{mac}
0.53	1.33	0.60	1.08	0.77	0.64	0.54	0.39
0.68	2.74	0.71	1.75	0.81	0.73	0.54	0.39
0.72	3.28	0.92	3.26	0.93	0.10	0.45	0.21
0.82	4.57	0.76	2.13	0.96	1.07	1.26	7.36
1.18	9.58	1.53	7.21	1.44	1.89	0.60	0.64
0.65	2.43	0.70	1.64	0.87	0.85	0.57	0.95
0.96	6.49	0.97	3.69	1.41	2.07	$1 \pm \varepsilon$	$5 \pm \varepsilon$
0.91	5.72	0.92	3.25	1.12	1.45	$1 \pm \varepsilon$	$5 \pm \varepsilon$
0.56	1.54	0.62	1.17	0.81	0.71	0.42	0.17
1.18	9.58	1.16	5.12	1.49	2.14	2.03	15.23
1.07	8.06	0.97	3.69	1.49	2.11	3.15	24.16
0.68	2.74	0.72	1.77	0.81	0.72	$1 \pm \varepsilon$	$5 \pm \varepsilon$
0.96	6.41	0.92	3.38	1.41	1.97	0.44	0.21

4. Conclusions

We have identified the stochastic process that characterizes the probabilistic behavior of the number of vulnerabilities of a computer operating system. This stochastic process is similar to the Non-Homogeneous Poison Process or the Power Law Process. We introduce two very important and useful concepts that will play an integral part in cybersecurity problems. We introduce the concept of **Vulnerability Intensity Function (** VIF) which identifies the behavior of the rate of change of the number of vulnerabilities of a computer operating system as a function of time. Secondly, we introduce the concept of the **Vulnerability Index Indicator (** VII) which monitors the behavior of the number of vulnerabilities at a specific time. The VII conveys the following very important information. If $VII \approx 1$, the number of vulnerabilities of the OS remains the same is prior to the testing time. If $VII < 1$, the number of vulnerabilities of the OS decreases at the specific time of testing. If $VII > 1$, the number of vulnerabilities of the OS increases at the specific time of testing.

The VIF and VII were obtained using real data for Microsoft's Operating System and Apple's OS, more specifically, we studied Windows 7, Windows 8, Windows 10, and MacOS. A comparison of the VIF and VII of all the OS was given. Also, the relationship between the estimated value of VIF and VII of the four operating systems has been shown to be directly proportional to each other.

Funding

This research is protected by University of South Florida TTO.

Conflicts of Interest

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

References

[1] Desktop Operating System Market Share Worldwide. https://gs.statcounter.com/os-market-share/desktop/worldwide

[2] Kaluarachchi, P.K., Tsokos, C.P. and Rajasooriya, S.M. (2016) Cybersecurity: A Statistical Predictive Model for the Expected Path Length. *Journal of Information Security*, **7**, 112-128. https://doi.org/10.4236/jis.2016.73008

[3] Rajasooriya, S.M., Tsokos, C.P. and Kaluarachchi, P.K. (2017) Cyber Security: Nonlinear Stochastic Models for Predicting the Exploitability. *Journal of Information Security*, **8**, 125-140. https://doi.org/10.4236/jis.2017.82009

[4] Kaluarachchi, P., Tsokos, C. and Rajasooriya, S. (2018) Non-Homogeneous Stochastic Model for Cyber Security Predictions. *Journal of Information Security*, **9**, 12-24. https://doi.org/10.4236/jis.2018.91002

[5] Pokhrel, N. and Tsokos, C. (2017) Cybersecurity: A Stochastic Predictive Model to Determine Overall Network Security Risk Using Markovian Process. *Journal of Information Security*, **8**, 91-105. https://doi.org/10.4236/jis.2017.82007

[6] Alenezi, F. and Tsokos, C.P. (2020) Machine Learning Approach to Predict Com-

puter Operating Systems Vulnerabilities. 2020 3*rd International Conference on Computer Applications & Information Security* (*ICCAIS*), Riyadh, 19-21 March 2020, 1-6. https://doi.org/10.1109/ICCAIS48893.2020.9096731

[7] Bain, L.J. and Engelhardt, M. (1991) Statistical Analysis of Reliability and Life-Testing Models. Marcel-Dekker, New York.

[8] Bassin, W.M. (1969) Increasing Hazard Functions and Overhaul Policy. *Proceedings of the* 1969 *Annual Symposium on Reliability*, Vol. 8, 173-178.

[9] Bozorgi, M., Saul, L.K., Savage, S. and Voelker, G.M. (2010) Beyond Heuristics: Learning to Classify Vulnerabilities and Predict Exploits. *Proceedings of the* 16*th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Washington DC, 24-28 July 2010, 105-114. https://doi.org/10.1145/1835804.1835821

[10] Crow, L. (1974) Reliability Analysis for Complex Repairable Systems. In: Proschan, F. and Serfling, R.J., Eds., *Reliability and Biometry*, SIAM, Philadelphia, 379-410.

[11] Edkrantz, M. and Said, A. (2015) Predicting Cyber Vulnerability Exploits with Machine Learning. 13*th Scandinavian Conference on Artificial Intelligence*, Vol. 278, 48-57.

[12] Movahedi, Y., Cukier, M. and Gashi, I. (2019) Vulnerability Prediction Capability: A Comparison between Vulnerability Discovery Models and Neural Network Models. *Computers & Security*, **87**, Article ID: 101596. https://doi.org/10.1016/j.cose.2019.101596

[13] Pokhrel, N., Rodrigo, H. and Tsokos, C. (2017) Cybersecurity: Time Series Predictive Modeling of Vulnerabilities of Desktop Operating System Using Linear and Non-Linear Approach. *Journal of Information Security*, **8**, 362-382. https://doi.org/10.4236/jis.2017.84023

[14] Zhang, S., Caragea, D. and Ou, X. (2011) An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities. *International Conference on Database and Expert Systems Applications*, Bilbao, 29 August-2 September 2011, 217-231. https://doi.org/10.1007/978-3-642-23088-2_15

[15] National Vulnerability Database. https://nvd.nist.gov

[16] Tsokos, C.P. (1995) Reliability Growth: Nonhomogeneous Poisson. In: Balakrishnan, N., Leon Harter, H. and Anderson, J.E., Eds., *Recent Advances in Life-Testing and Reliability*, CRC Press, Boca Raton, 319.