Changing Trends in Vulnerability Discovery

S.W.Tope[1], S.M.Furnell[1], M.Papadaki[2] and G.Pinkney[2]

[1] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[2] Symantec, Hines Meadow, St Cloud Way, Maidenhead, Berkshire, United Kingdom
e-mail: info@network-research-group.org

Abstract

There is an increasing awareness of vulnerabilities in computer software. Vulnerabilities have to be found before an exploit can take place. Thus it is up to those wishing to seek exploits and those seeking defences or remedies to find these vulnerabilities. This research presents the results into changing trends and focus on the different operating systems towards the most widely used ones. It also examines the shift towards exploitation of vulnerabilities in other software, such as applications, as well as revealing how some of the types of vulnerabilities are declining whilst others are as frequent as ever.

Keywords

Vulnerabilities, Operating Systems, Applications, Exploits

1. Introduction

Vulnerabilities and exposures to exploits in software have become more widely known and there is an increasing awareness as to how they can be exploited. A vulnerability is considered to be a "security flaw found in a certain technology. The technology may be an operating system, an application program, a network protocol, a mathematical algorithm, or sometimes a hardware component" (The Honeynet Project, 2004). It is known that vulnerabilities exist and the growth in awareness has led to much more comprehensive recording and sharing of information of such vulnerabilities.

An exploit is where there is an attempt to take advantage of the vulnerability. This may be by use of a program or by manual methods, although it is not always easy to achieve. The rewards to some have now become apparent and increasingly popular. The view of Kaspersky is that "the use of system exploits to get a foothold in the corporate network and spread rapidly has now become commonplace as writers of malicious code have woken to the potential 'helping hand' provided by vulnerabilities in common applications and operating systems" (Kaspersky et al, 2004).

Thus the fact that the vulnerabilities exist is not in itself very useful in designing or preparing defences. It is the types of vulnerabilities that exist and their exploitation that is of additional use. This does not mean that vulnerability trends and the knowledge of where they are being found are not of importance. If we do not know the types of software that are vulnerable and open to exploits, then there is a lack of direction as to where to place defences or how to correct the problems.

The aim of the investigation presented in this paper was to ascertain whether certain operating systems were the focus of attention more than others, and whether this focus has remained the same. Additionally, it aims to determine whether the focus of attention is on operating systems or whether it has shifted to other software such as applications. If there is such a change in focus, either between operating systems, then why has this taken place? If a change in focus for vulnerability seekers is taking place, how are the software developers coping, so as to develop more secure code, or are the same vulnerabilities still being discovered?

2. Reporting standards and databases

There are variations in the figures given by different sites and reporting authorities as to the number of vulnerabilities. In the early days, there may well have been a lack of understanding of the vulnerabilities and their importance. There was also a lack of cooperation, collection of statistics, and reporting or sharing of information. Additionally, there was not the knowledge or publicity of the ways and methods of utilising such vulnerabilities for malevolent or other purposes. Thus some databases show a more dramatic increase in the number of vulnerabilities as they have fewer recorded in the past and are more ready to accept reported vulnerabilitities now without checking on the actual vulnerability.

The de facto standard in the security industry is the Common Vulnerabilities and Exposures (CVE) started by MITRE in 1999 (Rhose, 2003). The idea came from work done by Mann & Christey (1999) where they found different names for the same vulnerabilities being used by different sites. They realised that there was a need for a common and standardised approach. This involved consistency in naming as well as free and complete sharing of information (Rhose, 2003). Prior to being recognised as CVEs vulnerabilities are referred to as CANs (Candidates). The numbering method to date has given different prefixes of ‘CVE’ and ‘CAN’, though from 19th October 2005, they will all have a CVE prefix with a status line.

Such is the importance and recognition now placed on vulnerability discovery and recording that the Department of Homeland Security in the USA has revealed that the National Vulnerability Database (NVD) will be maintained by the National Institute of Standards and Technology (NIST). There are a number of databases maintained by companies such as Secunia (secunia.com) and SecurityFocus (securityfocus.com) and these can be of equal importance. Rhose (2003) considered that an advantage of Bugtraq was the speed that information was updated and with less formality. One problem is that many reported vulnerabilities fail to be actual vulnerabilities or exposures.

3. Utilisation of data

The primary sources that was utilised for extrapolating data in this study were the CVE project and the National Vulnerability Database maintained by NIST. Additional utilisation of databases included those maintained by Secunia and SecurityFocus. The investigation also looked at other research carried out by companies such as the technology research firm Yankee Group. This information is more easily extrapolated and can be used as a basis for comparisons.

The decision to concentrate on the information provided by the CVE project is in part due to the consistency of the information provided, its history and not least the high regard with which it is held. In addition, the information provided in the National Vulnerability Database was utilised not so much for absolutes and the overall trend but rather as a means of comparing different operating systems. This was useful when comparing like for like software.

Other databases, such as Bugtraq, were not used due to the length of time they have been operating and the consistency of their data for comparison over any length of time. Initially, there were few reports but this has risen rapidly so that almost any flaw or bug is reported, including many that are not vulnerabilities. Other research and work was still examined in order to compare with the extrapolated data for comparison. The SecurityFocus newsletters were included in the research. This was in order to discover the changing focus that has taken place on Microsoft and Linux distributions as well as how the vulnerabilities were reported.

4. Results

The figures for the MITRE list show a fairly constant rate of vulnerability reports and recording since 1999. It should be remembered that some of the CANs may still be rejected, especially for the more recent years. The figures for the National Vulnerability Database show a constant rise though there was a fall in 2003. Where they both agree is the sudden and rapid rise in reports in 2005. It should be noted that the number for 2005 had already passed the figure for 2004, even though only the first six months were included (see Table 1 below). The daily average is rising and for example, on 12.7.2005 there were 35 new CANs and on 26-27.7.2005 there were 45 new CANs. These are not unusual figures and certainly reflect the trend at the time of the study.

Year	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005** (to 1.7.2005)
CVEs & CANs	1562	1202	1396	1580	1085	1704	2104
NVD (NIST)	914	1013	1672	1858	1189	2161	2222

Table 1: Vulnerabilities Recorded

Source: http://www.cve.mitre.org/ and http://nvd.nist.gov/

Whilst there are still vulnerabilities being discovered in the Windows operating systems as can be seen in Table 2, they are not as dramatic as they once were. The figures for XP Professional actually declined and though rising once again are doing so at a similar rate to the rest of vulnerabilities being discovered.

Year	**2000**	**2001**	**2002**	**2003**	**2004**	**2005** (to 1.7.2005)
Number of Vulnerabilities	1	-	22	19	17	28
As % of Total Vulnerabilities	0%	-	1%	2%	1%	1%

Table 2: Windows XP Pro

Source: http://nvd.nist.gov/

The results for Red Hat Linux (the most common distribution of Linux) are similar for 2002 to 2004. Prior to that, Windows XP had not been released and as such cannot be compared. Whilst the figures are similar, they are for Red Hat Linux 6, 7, 8 and 9. Thus they are actually different versions, but often a user will upgrade.

Year	**2000**	**2001**	**2002**	**2003**	**2004**	**2005** (to 1.7.2005)
Number of Vulnerabilities	47	49	17	22	10	12
As % of Total Vulnerabilities	5%	3%	1%	2%	0%	0%

Table 3: Red Hat Linux

Source: http://nvd.nist.gov/

These figures do not include vulnerabilities in all kernel revisions. This is a difficulty in comparison and Microsoft will keep their operating system going for longer (with the possible exception of the Millennium Edition) with service packs being added. Additionally, there is some conflict with the figures for the Linux Kernel as well as other Red Hat systems. Red Hat Desktop had 19 vulnerabilities in 2004 and 48 in the first six months of 2005, whilst the figures for Fedora were 20 and 47 (source: http://nvd.nist.gov/). Prior to 2004, the recorded vulnerabilities for the Linux Kernel never exceeded 21, and in 2003 they stood at 16 for the entire year. The past two years has seen a dramatic rise to 45 in 2004 and 58 in the first six months of 2005. This is continuing with 71 being reported in 2005 as at the end of August.

In examining a number of minor or more obscure operating systems, there were often no vulnerabilities recorded. Whilst much publicity has been made of mobile malware, there is only a single recorded vulnerability (CAN-2005-0681) on the Symbian operating system, four affecting specific handsets and four others relating to areas such as Nokia Electronic Documentation. Apart from the very obscure operating systems, the research did examine others such as the different forms of BSD. It was only Free BSD that has a significant number of vulnerabilities to date with some attention paid to Net BSD and Open BSD. The remainder such as 386 BSD, BSD I, BSD/OS and Eclipse BSD barely register (see Table 4).

BSD Variant	**Number of Vulnerabilities** (up to 19.5.2005)
Free BSD	265
Net BSD	88
Open BSD	77
386 BSD	0
BSD I	7
BSD / OS	9
Eclipse BSD	0

Table 4: BSD Vulnerabilities

Source: http://www.cve.mitre.org/

The same can be said for Unix variants. Whilst HP-UX, IRIX, SCO and Solaris have a significant number of vulnerabilities, others such as Sun OS, System V and TRU64 barely register (see Table 5).

Unix Variant	**Number of Vulnerabilities** (up to 19.5.2005)
HP-UX	127
IRIX	127
SCO	131
Solaris	226
SUN OS	34
System V	33
TRU64	32

Table 5: Unix Vulnerabilities

Source: http://www.cve.mitre.org/

Year	**1999**	**2000**	**2001**	**2002**	**2003**	**2004**	**2005** (to 1.7.2005)
Number of Vulnerabilities	169	142	160	227	91	134	93
As % of Total Vulnerabilities	18%	14%	10%	12%	8%	6%	3%
Total number of Vulnerabilities	914	1013	1672	1858	1189	2159	2223

Table 6: Microsoft Products

Source: http://nvd.nist.gov/

All of the Unix variants show a decline in the number of vulnerabilities being discovered and reported. SCO had 27 Candidates in 2004 and to date (19.5.2005) has not had a single reported vulnerability in 2005. Solaris is down to 10 from 26 in 2004, IRIX to 3 compared with 11 in 2004, and HP-UX has 4 compared with 10 in 2004. This is at a time when the overall numbers are going up elsewhere. Thus attention is certainly moving away from the Unix operating systems. This may well be in part due to the maturity of the systems and the lack of new kernels, versions etc. It was observed in the statistics maintained by Secunia that the number of vulnerabilities for Red Hat Linux began with a surge and then fell away. The problem in interpreting these figures is that as a new version of the distribution was released, so the focus of attention shifted. Still, the trend was a downward one, even prior to the release of newer versions of the ‘distribution’.

The downward trend of Microsoft products in the number of vulnerabilities that are being found is supported by recent research by the Yankee Group. They found that “Microsoft flaws continue to flow – but at a significantly reduced rate” (Jaquith, 2005). Their view using NIST ICAT data (now NVD) was that the focus has shifted towards security products. This may in part be due to security companies seeking to discredit each others’ products. Their study revealed that they were responsible for 26% of vulnerability discoveries involving rival security products. Another view is that the growing focus and danger is with drivers. There is a view that device drivers are the most dangerous as they are part of the kernel and the quality of software developer is not as high as that of the operating systems. In an audit of the Linux 2.6.9 kernel by the security firm Coverity, over half of the flaws were in device drivers. (Lemos, 2005). Thus it may not just be a general switch of attention to other software, but in particular types of software such drivers, networking and security software that have more access to the system as well as potential for damage. In 2004 Cisco had 75 vulnerabilities recorded (NVD) compared to 29 in 2003. The actual figures for ‘drivers’ do not as yet support the above theory. Mitre had only 45 entries (as at 1.7.2005), and although there was a jump in 2004, the figures are not large enough to have any marked impact on the overall statistics. Certainly, within Linux applications there are few vulnerabilities in the ‘Administration’ category (172 in 505 applications- of which 71 were for ‘ethereal’), in the System category (233 in 1013) but alters noticeably in Networking Applications. In the DNS section of Networking there were 54 vulnerabilities in 40 applications, ‘e-mail’ had 201 in 163 applications, and ‘firewalls’ had 108 in 102 applications.

Instead of looking at the attention paid to the operating system in isolation, the operating system as a whole, with applications and drivers installed was investigated. SecurityFocus (www.securityfocus.com) has been publishing weekly newsletters since September / October 2000 for vulnerabilities in Linux and Windows (as well as a general newsletter). In June / July 2001 (a period of 9 weeks – see Figure 1) there were 129 Microsoft Vulnerabilities reported and only 28 for Linux (including applications, drivers etc.). From the beginning, the Linux newsletters included vulnerabilities in applications and other software that affected Linux. Initially the Microsoft Newsletters comprised Microsoft products only. The method of compiling the Microsoft newsletters began to change towards the end of 2001 depending upon the editor (#60, dated 12.11.2001, was the first), though the last to include only Microsoft products was #111 dated 4.11.2002 (6 vulnerabilities in Microsoft products).

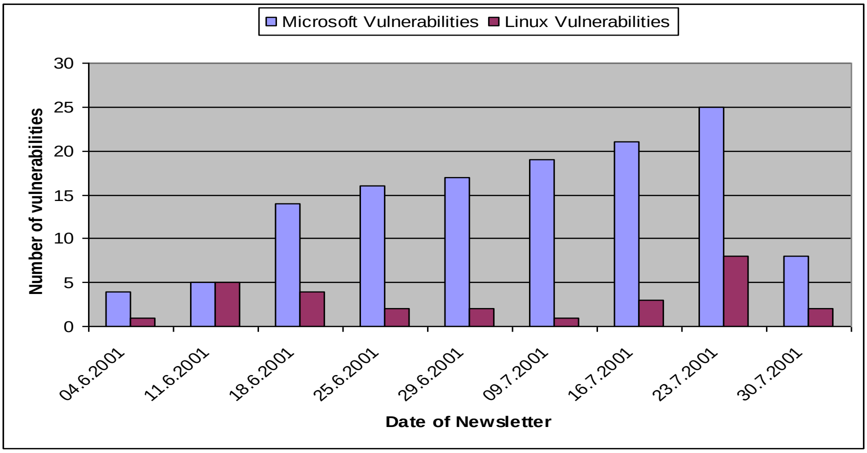

Figure 1: SecurityFocus Newsletters

Source: http://www.securityfocus.com/newsletters

After these were included in the Microsoft Newsletter, the relative difference between the two systems has significantly altered (see extrapolated quarterly figures in Figure 2). Apart from a fall in 2003 / 2004 that matches the general trend, the numbers are once again rising. This significant rise began in the last quarter of 2004 and is being sustained.

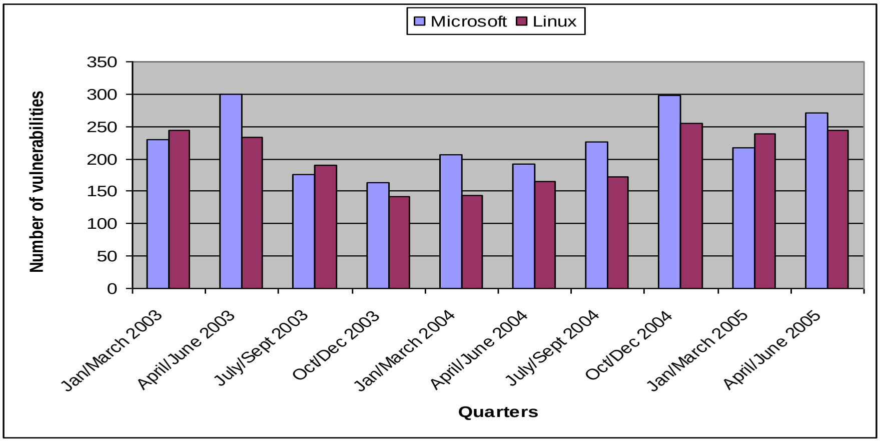

Figure 2: SecurityFocus Newsletters

Source: http://www.securityfocus.com/newsletters

It is certainly clear that there is less emphasis on Microsoft products per se and as the figures are similar from one Operating System to the other, the implication is that more emphasis is being paid to software other than the operating systems themselves. It is not so much of a question as to trends in operating systems now but rather as an overall platform and how they are affected by other interacting pieces of software. Thus the attention may well be shifting away from operating systems.

The trend of increases in applications relating to operating systems and the changes in the variety of software and operating systems available has led to SecurityFocus now reviewing their ‘security mailing lists’. It is felt that the present lists are too confining as so much is contained within a finite number of lists. They now expect to have more mailing lists in the near future.

NIST lists different vulnerability types in its National Vulnerability Database. These are:

- Design Error
- Race Condition
- Configuration Error
- Environmental Error
- Exceptional Condition Error
- Access Validation Error
- Input Validation Error – (a) Buffer Overflow & (b) Boundary Condition Error

Most of the errors have remained fairly constant as a proportion to the overall numbers of vulnerabilities. This is not so for Design Error that has fallen from a peak of 29% in 2002 to 14% in the first six months of 2005. Configuration Error has fallen from 6% to 2% over the same period of time, and Buffer Overflows have fallen from 23% in 2003 to 12% in the first six months of 2005 (even though the overall percentage for ‘Input Validation Errors’ has remained constant). As different software usage becomes more popular so does the emphasis in different types of attack. Vulnerabilities involving SQL Injection have risen from 7 in 2001, to 42 in 2003, 108 in 2004, and 209 in the first six months of 2005. Vulnerabilities involving PHP have risen from 35 in 2003 to 120 in 2004, and 165 in the first 6 months of 2005.

5. Discussion

The figures when comparing different operating systems indicate that vulnerabilities tend to be discovered and reported principally in those operating systems that are more commonly used. When an operating system has reached a certain point then the number of vulnerabilities that are discovered and reported becomes somewhat similar. Operating systems have been the focal point in the past and the numbers of vulnerabilities in the principal operating systems has generally remained at the same numeric level though rising in 2005. Figures for minor or rarely used operating systems are certainly not rising. There has certainly been a shift away from Microsoft products as the source of vulnerabilities, possibly due to increased attention to security as well as the diminishing returns offered to vulnerability seekers. They are still a major focus of attention due to their market presence, as well as certain hostile views that are commonly held by some in the computing fraternity.

There is some evidence of a shift towards applications and other software, though specific to certain types such as networking and security products. This does not mean that there is less emphasis upon the principal operating systems as these are maintaining their share of vulnerabilities being discovered. Rather, software other than operating systems is coming under increasing scrutiny. The evidence shows that there is convergence between Microsoft and other vendor applications. This convergence may alter, as rising trends that other vendor applications have shown may continue. The rate of vulnerabilities being discovered is rising rapidly since the end of 2004, and this rate would appear to be similar for the principal operating systems as it is for non-operating system software.

The rise and shift in focus for those seeking vulnerabilities is still developing. Some products are more mature than others and thus may be written with different levels of attention to security. The larger companies are aware of the attention that the media and public now pay to security and the discovery of vulnerabilities. Certain types of vulnerabilities have received considerable publicity in the past, principally ‘buffer overflows or overruns’ and these have declined considerably along with ‘design errors’. Certainly the larger companies are more aware of how to ensure that code is written in a manner that to avoid these types of vulnerabilities and security audit tools are better at locating these vulnerabilities before being released. Despite this, the problem has not been eradicated and even the most well known software still suffers from these types of vulnerability. Certainly, as software such as PHP becomes more popular, so the attention of those seeking vulnerabilities becomes focused. This is not only due to the popularity of the software, but also the increase in awareness by the vulnerability hunters.

6. Conclusions

The focus of attention remains upon the software that is more commonly used. Whilst Microsoft has taken steps to produce more robust and safer software, those seeking vulnerabilities have started to look elsewhere. They will still concentrate on the most commonly used operating systems or software in which a vulnerability will possibly impact the most. It is not so much that Microsoft does not remain the focus of attention, but rather there is an increased awareness of vulnerabilities elsewhere, and as Linux distributions become more user friendly and increase in popularity so there is more attention being paid to their flaws. The focus of attention is still directed towards specific areas and is not arbitrary.

7. References

Jaquith A, (2004) “*Fear and Loathing in Las Vegas: The Hackers Turn Pro*” http://www.yankeegroup.com/ public/products/decision_note.jsp?ID=13157 Accessed 29.6.2005

Kaspersky E, Emm D, Gostev A, and Blanchard M (2004), “*Malware Trends in 2004*”, http://www.viruslist.com/en/trends Accessed 15.02.2005

Lemos, R (2005) “*Device Drivers filled with Flaws, threaten security*” http://www.securityfocus.com/ print/news/11189 Accessed 29.6.2005

Mann D & Christey S (1999) "*Towards a Common Enumeration of Vulnerabilities*" http://www.cve.mitre.org/ docs/cerias.html Accessed 12.2.2005

Rhose M, (2003) "*Vulnerability naming schemes and description languages: CVE, Bugtraq, AVDL and VulnXML– A SANS GSEC practical*", http://www.sans.org/rr/whitepapers/threats/ 1058.php Accessed 12.12.2004

The Honeynet Project (various) (2004) *Know Your Enemy* 2nd Edition Addison-Wesley Professional ISBN: 0321166469