Desktop operating systems market share and their conformity with the international IT security standard ISO 15408

Predrag Oreški
Teacher's College in Čakovec
poreski@vus-ck.hr

Dragutin Kermek
University of Zagreb
Faculty of Organization and Informatics Varaždin
dkermek@foi.hr

Abstract: In this paper authors present the research method they use to determine the desktop operating systems market share in Croatia. The method includes the analysis of web access log data of some of the most frequently visited Croatian web sites.
For operating systems that make the market share, authors quote their evaluated assurance level according to *ISO 15408 – Information technology – Security techniques – Evaluation criteria for IT Security (The Common Criteria for Information Technology Security Evaluation* - *CCITSE).*

Keywords: operating system, market share, security, ISO 15408.

1. Introduction

Almost all contemporary desktop computers have Internet access and use its services. The Internet is used as a way of transportation of service packs, patches for operating systems such as Windows or Linux and updates for various anti-virus software.
Bearing in mind that Internet services are intensively used, operating system security becomes even more important. Safety-critical and similar applications in various organizations require the highest level of operating system security. The operating system manufacturers are improving its products to match the requirements and criteria of existing IT security standards to become eligible for use in these organizations.

Operating systems are not perfect products. According to [9] there are the following top 10 vulnerabilities for Windows and Unix systems:

a) Windows systems:
- Internet Information Server,
- Microsoft Data Access Components,
- Microsoft SQL Server,
- NetBIOS shares,
- Anonymous logins – null sessions,
- LAN Manager authentication,
- General Windows authentication,
- Internet Explorer,
- Remote registry access,
- Windows Scripting Host,

b) Unix systems:
- Remote procedure calls (RPC),
- Apache web server,
- Secure shell (SSH),
- Simple Network Management Protocol (SNMP),
- File Transport Protocol,
- R-services – Trust relationships,

- Line Printer daemon,
- Sendmail,
- BIND/DNS,
- General Unix authentication.

The software manufacturers are establishing the procedures for continuous delivery of their products updates, typically using Internet. Therefore, almost every desktop computer today needs and accesses the Internet and leaves its trails in it[1]. This feature is used in the method to determine what operating systems are parts of the desktop operating systems market share.

2. The research method

Every visit to a web site is logged in its access log and this data contains information that can be used to determine the operating systems market share. The most suitable sources of data for operating systems market share analysis are sites with general contents that have a large number of unique visitors.
The authors use the method of questionnaire to acquire such access data for 30 most frequently visited sites in Croatia.

The web site access log record can be configured to have its contents as in the following examples:

1. visit using Microsoft Internet Explorer 6.0 and Microsoft Windows XP (NT 5.1):

```
193.198.134.40 - - [23/May/2004:10:39:46 +0200] "GET /logo.htm HTTP/1.1"
200 474 "http://www.vus-ck.hr/" "Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1)"
```

2. visit using Konqueror and Linux:

```
66.194.6.74 - - [23/May/2004:22:27:35 +0200] "GET /logo.htm HTTP/1.1" 200
474 "http://www.vus-ck.hr/" "Mozilla/5.0 (compatible; Konqueror/3.1-rc4;
i686 Linux; 20020507)"
```

The access log record structure in previous examples is as follows:

```
%h %l %u %t \"%r\" %>s %U \"%{User-agent}i\"

%h - remote computer IP address,
%l - remote login name (if delivered - otherwise '-'),
%u - remote user (if delivered - otherwise '-'),
%t - date/time,
%r - first row of query,
%>s - query status,
%U - requested URL without query string,
"%{User-agent}i\" - browser and operating system data,
\ - space.
```

[1] Authors of this paper understand that if a desktop computer accessing the Internet is in LAN that is behind a firewall and/or uses proxy, in that case the data in access logs can be those of its firewall or proxy.

The research is performed using these steps:

1. ranking of Croatian web sites is performed according to number of visits during May 2004 using data from http://www.trafficranking.com,

2. according to results achieved in previous step, the questionnaire is sent to the 30 most visited sites in Croatia, asking them to provide their web access log data.

   The requested data could be:
   - the result of processing using software such as *Webalizer*, *Awstats*, etc.,
   - not processed raw data from web site access log for a given month and year,

3. the gathered data is processed as needed to achieve mutual comparability,

4. operating systems are ranked on the basis of their market share and related to their achieved ISO 15408 standard EAL (Evaluation Assurance Level).

The site *trafficranking.com* provides statistical data that are commercially available from providers *Alexa*, *AC Nielsen* and *Media Metrix*. Every unique visitor is counted only once, so if someone does 50 visits during May 2004, only one visit is counted. This is actually number of different users of a site. Today this is an industrial standard in measuring the importance of some web site. This property has an important value in the process of determining the operating systems market share - multiple visits of a specific user (who uses the specific operating system and specific browser) are represented as one specific operating system and one specific browser.

2.1. Research results

Web access log data (partly processed or raw) is provided for domains *vip.hr, ht.hr, iskon.hr, besplatne-stvari.hr* and *carnet.hr.*

Only a small number of domains participated in the questionnaire process:

- 8 out of 30 domains replayed (26,67%),
- 5 out of 30 domains provided their data (16,67%).

However, domains that provided data are ranked 1st (*iskon.hr*), 4th (*vip.hr*), 9th (*ht.hr*), 23rd (*carnet.hr*) and 26th (*besplatne-stvari.com*) out of 30, according to number of unique visitors.

The operating systems market share according to web access log data in analysed domains in Croatia in May 2004 is as follows:

Rank	Operating system	Range	Average
1	Microsoft Windows XP (NT 5.1)	44,46 – 57,60	53,70
2	Microsoft Windows 98	17,36 – 25,96	20,43
3	Microsoft Windows 2000 (NT 5.0)	11,00 – 18,46	14,86
4	Microsoft Windows ME	4,10 – 5,40	4,87
5	Microsoft Windows NT 4.0	0,50 – 3,50	1,52
6	Linux	0,13 – 1,50	0,64
7	Microsoft Windows 95	0,30 – 0,86	0,55
8	Macintosh PPC	0,34 – 0,78	0,37
9	Mac OS	0,20 – 0,20	0,20

Table 1. The operating systems market share according to web access log data in analysed domains in Croatia in May 2004.

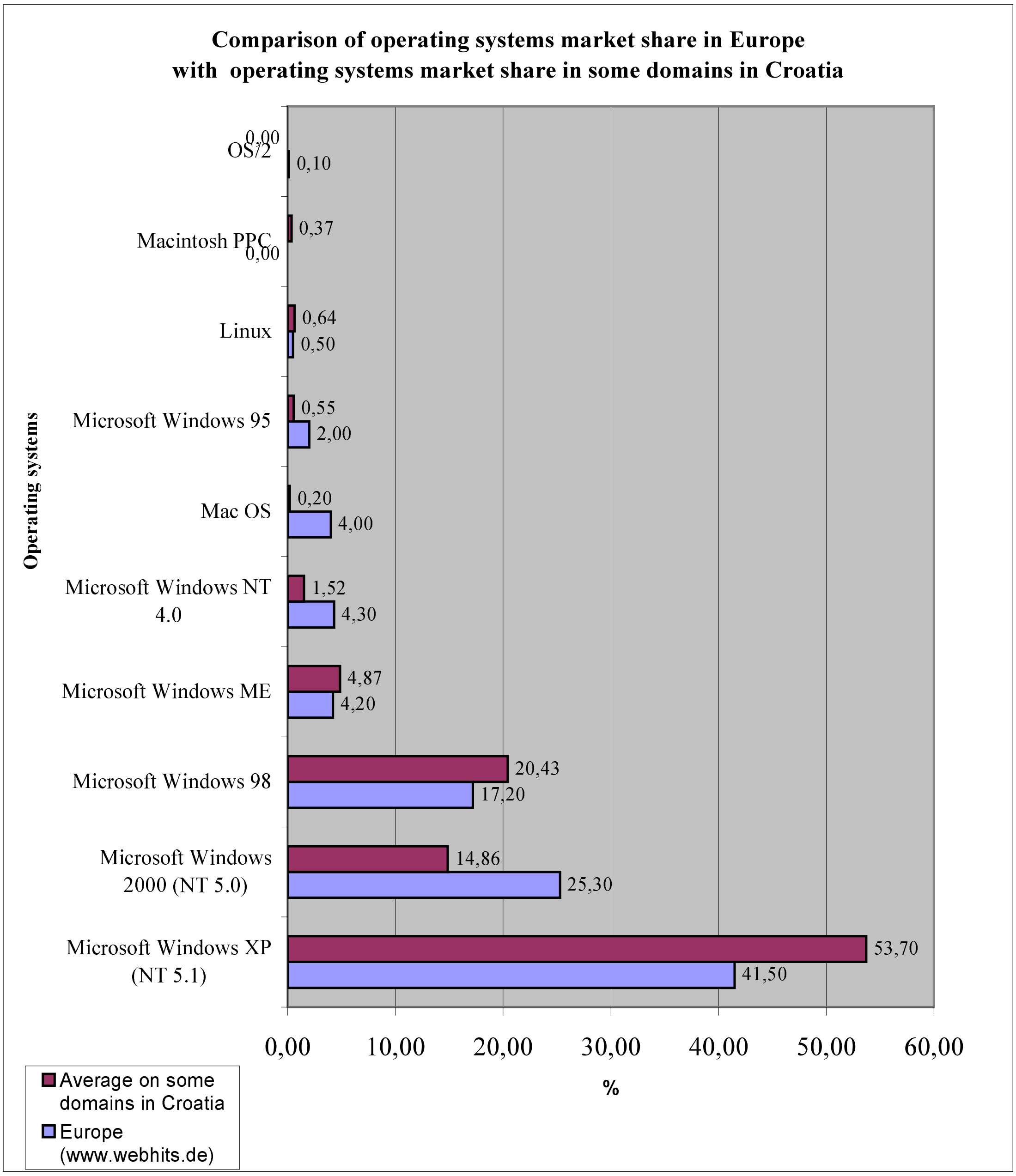


Chart 1. Comparison of operating systems market share in Europe and operating systems market share according to web access log data in some domains in Croatia

The pondered average could also be calculated, but it's not performed in this paper because the number of unique visitors for each of 30 domains is in very close range (4.973 to 4.767 unique visitors).

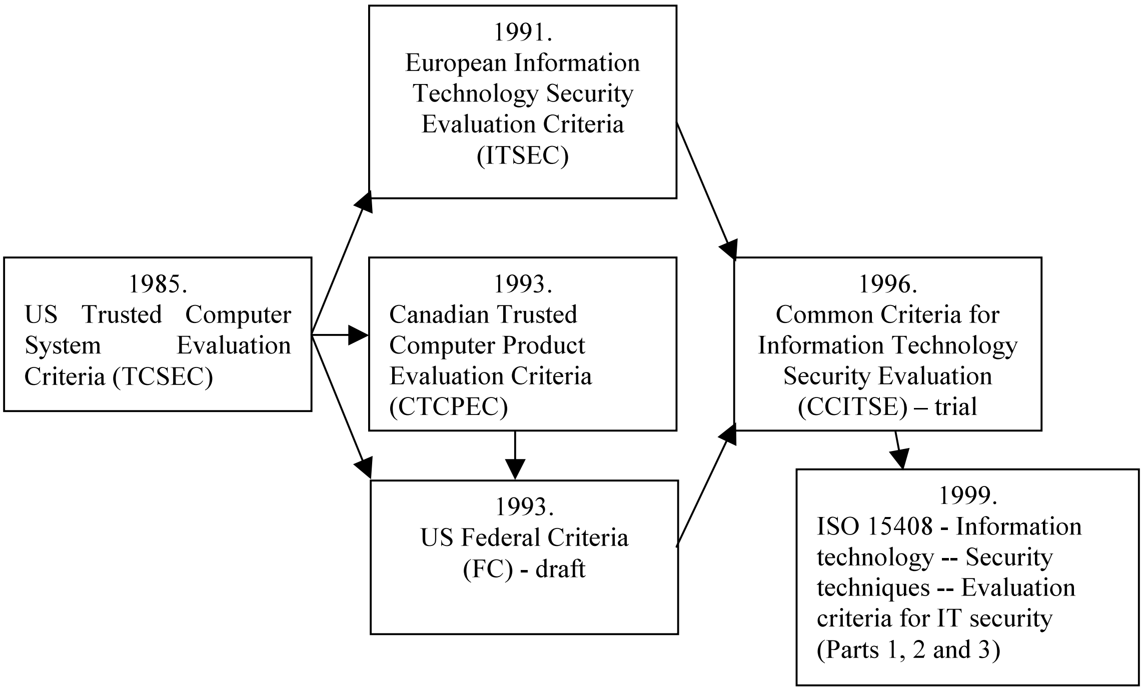
The data from www.webhits.de and the data from some domains in Croatia show the common property: the sites ranked 1 – 3 are Microsoft Windows XP, Microsoft Windows 2000 and Microsoft Windows 98.

Mac OS has significantly larger operating systems market share in Europe than in Croatia.

Microsoft Windows 95 has only a small portion of operating systems market share.

The average usage of Linux is similar and it's very low (www.webhits.de 0,50% - some domains in Croatia 0,64%).

3. The conformity of the desktop operating systems with the international standard ISO 15408


1991.
European Information Technology Security Evaluation Criteria (ITSEC)
1985.
US Trusted Computer System Evaluation Criteria (TCSEC)
1993.
Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
1996.
Common Criteria for Information Technology Security Evaluation (CCITSE) – trial
1993.
US Federal Criteria (FC) - draft
1999.
ISO 15408 - Information technology -- Security techniques -- Evaluation criteria for IT security (Parts 1, 2 and 3)

Scheme 1. IT Security standards development scheme

The Common Criteria for Information Technology Security Evaluation (CCITSE) represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. In the early 1980's the Trusted Computer System Evaluation Criteria (TCSEC) was developed in the United States. In the succeeding decade, various countries began initiatives to develop evaluation criteria that built upon the concepts of the TCSEC but were more flexible and adaptable to the evolving nature of IT in general.

In Europe, the Information Technology Security Evaluation Criteria (ITSEC) version 1.2 was published in 1991 by the European Commission after joint development by the nations of France, Germany, the Netherlands, and the United Kingdom. In Canada, the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) version 3.1 was published in 1993 as a combination of the ITSEC and TCSEC approaches. In the United States, the draft Federal Criteria for Information Technology Security (FC) version 1 was also published in 1993, as a second approach to combining North American and European concepts for evaluation criteria.

Work began in 1990 in the International Organization for Standardization (ISO) to develop international standard evaluation criteria for general use. The new criteria were intended to be responsive to the need for mutual recognition of standardized security evaluation results in a global IT market. This task was assigned to Working Group 3 (WG3) of subcommittee 27 (SC27).

In June 1993, the authors of the CTCPEC, FC, TCSEC, and ITSEC pooled their efforts and began a project to align their criteria and create a single draft CC document. The intent of the project was to resolve the conceptual and technical differences found in the source criteria and then, to deliver the results to ISO as a contribution toward its work in building the international standard. [1], [10]
In 1999 the final result is presented – the new international standard ISO 15408.

ISO 15408 consists of 3 mayor parts [1]:

- *Part 1: Introduction and general model,*
- *Part 2: Security functional requirements,*
- *Part 3: Security assurance requirements.*

The purpose of this standard is to provide:

- a security standard for manufacturers,
- a basis for specifying security requirements in product specification,
- additional criteria and metrics for selection of secure operating system.

The evaluated operating systems can achieve one of the following ISO 15408 *Evaluated Assurance Level (EAL)* [1]:

- Evaluation assurance level 1 (EAL1) - functionally tested,
- Evaluation assurance level 2 (EAL2) - structurally tested,
- Evaluation assurance level 3 (EAL3) - methodically tested and checked,
- Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed,
- Evaluation assurance level 5 (EAL5) - semi-formally designed and tested,
- Evaluation assurance level 6 (EAL6) - semi-formally verified design and tested,
- Evaluation assurance level 7 (EAL7) - formally verified design and tested.

Operating system are ranked on the basis of their market share and related to their achieved ISO 15408 standard EAL (Evaluation Assurance Level), as follows:

Rank	**Operating system**	**%** (average)	**ISO 15408** **EAL**
1	Microsoft Windows XP (NT 5.1)	53,70	-
2	Microsoft Windows 98	20,43	-
3	Microsoft Windows 2000 (NT 5.0)	14,86	**EAL 4** (Professional, Server)
4	Microsoft Windows ME	4,87	-
5	Microsoft Windows NT 4.0	1,52	- [2]
6	Linux	0,64	**EAL 3** (Red Hat Enterprise Linux WS, Version 3 Update 2) **EAL 3+** (SuSE Linux Enterprise Server V8, Service Pack 3, RC4)
7	Microsoft Windows 95	0,55	-
8	Macintosh PPC	0,37	-
9	Mac OS	0,20	**EAL 3** (Apple Computer Mac OS X v10.3.6 and Apple Computer Mac OS X Server v10.3.6, both with Common Criteria Tools Package)

Table 2. The operating systems market share according to web access log data in analysed domains in Croatia in May 2004
with associated *ISO 15408 Evaluated Assurance Level (EAL)*. [2], [5], [6], [7], [8]

[2] The first Microsoft Windows operating system evaluated by an IT security standard was Windows NT 4.0. It was evaluated in order to be used in the offices of one of Microsoft's most significant user - USA Department of Defense. NT was evaluated against an oldest IT security standard – *1985. US Trusted Computer System Evaluation Criteria (TCSEC).* This operating system achieved level of C2 – *Controlled Access Protection.*

Table 2. shows that only one operating system, among first three ranked in some domains in Croatia, is evaluated according to ISO 15408 (Microsoft Windows 2000).
For the first time there are also two Linux operating systems evaluated. However, they are both enterprise (server) editions, not desktop. Also, contrary to number of other Linux editions that are Open source and GNU licensed, they are not free of charge.

4. Conclusion

According to the results of data analysis of web access logs of some domains in Croatia, the most frequently used operating systems in Croatia are those of Microsoft Windows family.

The analysis of operating systems market share and their conformity with standard CCITSE / ISO 15408 shows that Microsoft's latest and most frequently used operating system Microsoft Windows XP is still not evaluated. However, its ancestor Microsoft Windows 2000 achieved EAL 4. It took Microsoft three years to perform this. [5], [6]

This information should help the IT decision makers when deciding what operating system they should use in their organization, especially in the safety-critical environments (e.g. hospitals, airports, power plants, military, police, government agencies). When considering Microsoft as a desktop operating system provider they might consider using an older and successfully evaluated Microsoft Windows 2000 rather than newest Microsoft Windows XP.

Popular Linux distributions, like *Knoppix* (based on *Debian* Linux), which are easy to install and which include a lot of applicable software, influence the market share of Linux operating system. However, the analysis performed in this paper shows that the present market share of desktop Linux operating system is very low: average 0,64% in some domains in Croatia and 0,50% in Europe.

For the first time enterprise editions of Linux operating systems – Red Hat and SuSE - are successfully evaluated according to CCITSE / ISO 15408.

References:

[1] *CCITSE v2.1 – Common Criteria for Information Technology Security Evaluation (ISO 15408 - Information technology -- Security techniques -- Evaluation criteria for IT security),* http://www.radium.ncsc.mil/tpep/library/ccitse/ccitse.html, May 2004,

[2] *Validated product list*, http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#operatingsystem, July 2005,

[3] Online statistical data from http://www.webhits.de, May 2004,

[4] Online statistical data from http://www.trafficranking.com, May 2004,

[5] *Microsoft Windows 2000 Awarded Common Criteria Certification,* http://www.microsoft.com/presspass/press/2002/Oct02/10-29CommonCriteriaPR.asp, Microsoft Corpomarket sharen, 02.10.2002,

[6] *Windows 2000 Common Criteria Certification – Frequently Asked Questions,* http://www.microsoft.com/presspass/press/2002/Oct02/1029CommonCriteriaFAQ.asp, Microsoft Corpomarket sharen, May 2004,

[7] *Certification Report – SuSE Linux Enterprise Server V8 Service Pack 4, RC4, sponsored by IBM Corpomarket sharen*, http://www.bsi.bund.de/zertifiz/zert/reporte/0234a.pdf, 14.01.2004,

[8] *Common Criteria Certification Report No. P200 – Red Hat Enterprise Linux,* http://www.cesg.gov.uk/site/iacs/itsec/media/certreps/CRP200.pdf, 02.2000,

[9] *Cyber security,* Richard A. Kemmerer, Department of Computer Science, University of California Santa Barbara, Proceedings of the 25th International Conference on Software Engineering (ICSE.03) IEEE 2003,

[10] *Building an International Security Standard*, Kimberly Caplan, James L. Sanders, IT Pro, IEEE 1999.