ISSN 1847-3938

mipro 2014

organizer upro

37th international convention

May 26-30, 2014, Opatija – Adriatic Coast, Croatia

Lampadem tradere

mipro - path to knowledge and innovation

mipro proceedings

MIPRO 2014

37th International Convention

May 26 - 30, 2014
Opatija, Croatia

Proceedings

Conferences:

Microelectronics, Electronics and Electronic Technology /MEET

Distributed Computing, Visualization and Biomedical Engineering /DC VIS

Telecommunications & Information /CTI

Computers in Education /CE

Computers in Technical Systems /CTS

Intelligent Systems /CIS

Information Systems Security /ISS

Business Intelligence Systems /miproBIS

Digital Economy and Government, Local Government, Public Services / DE-GLGPS

MIPRO Junior - Student Papers /SP

Edited by:
Petar Biljanović

All papers are published in their original form

For Publisher:

Petar Biljanović

Publisher:

Croatian Society for Information and Communication Technology,
Electronics and Microelectronics - **MIPRO**
Office: Kružna 8/II, P. O. Box 303, HR-51001 Rijeka, Croatia
Phone/Fax: (+385) 51 423 984

Printed by:

GRAFIK, Rijeka

ISBN 978-953-233-078-6

Computer Classroom Operating System Security (Windows)

Mario Zovkić*, Tedo Vrbanec**
*Primary school Barilović, Barilović & Primary school Katarine Zrinski Krnjak, Krnjak, Croatia
**Faculty of Teacher Education, University of Zagreb, Zagreb, Croatia
*mario.zovkic1@skole.hr, **tedo.vrbanec@gmail.com

Abstract - Computer security, school security policy and school computers usability should be important for all school computers and network resources users. But instead of implementing security policy, users often unintentionally compromise computer functionality and security out of ignorance or negligence. Since Windows is the default operating system in the majority of Croatian schools, students often have to use computers in the role of administrator. Bearing in mind the multitude of new technological solutions and continual changes which happen in this industry, this paper tries to provide an overview of software solutions for IT administrators of school computers, which are also applicable in libraries, colleges, universities and other public places which use computers with Windows OS.

Keywords: Classroom, Security, Windows, Policy.

I. INTRODUCTION

Windows is the *de facto* standard operating system for desktop computers in Croatian schools. It is in IT teacher's best interest to keep the maintainance of computers as simple as possible and to require as little interventions as necesarry during classes. Because of that, and due to ignorance or negligence, the configurations in computer classrooms are mostly intended for the users in the administrator role, regardless of who is logged in: a teacher or a student. When students are logged in as administrators, they have the freedom to do whatever they want. As they are curious by nature, they like to explore on their own to see what they can change on the computer or what they can access and make all sorts of mischief: change the desktop backgrounds and screen savers, delete files from the computer, install programs and games and use the installations to add different toolbars in the web browser. For children who have an advanced knowledge of computers, possible limitations and restrictions represent a kind of challenge. In this context, we will show some guidelines for increasing the operational security in computer classrooms where Windows OS is installed, but these guidelines are partially applicable to other operating systems as well.

II. OPERATIONAL AND PROGRAM SECURITY

"Operational security includes two aspects of computer security; the first represents the ways of increasing the awareness of possible actions among the potential victims, while the second represents the ways in which computer criminals can be prevented from committing these acts". [1] It should be made clear to the employees that security is threatened and that everyone shares the risk and the responsibility. "The only way in which operational security can function completely is by implementing operational security in the programs of physical insurance as well as the personnel security and communications within an organization. In fact, the operational security is primarily used as an aid in making those security programs as productive as possible." [1]. This could be argued. Namely, the authors of this paper believes that operational security, apart from the education of users, is the most important element of the security system of an organization, as well as of a person as an individual or as a part of an organizational structure. However, it is perfectly obvious that an organization can never stop searching for vulnerable spots, breaches of security and methods of prevention, and can never stop discovering successful breach attempts, all this along with continual training of employees and users. [1]

"There are two types of systems: open and closed ones. If you use open source software you can analyze and inspect the code of security mechanisms and practically be sure that it will do what it is designed to do and nothing more. That means that you can check it for existence of trapdoors and backdoors, and in the end be sure that it will not send any data to manufacturer's servers (it is really not important what it sends, it is important whether it sends the data without your permission – this is how your privacy gets violated). If you use closed source software, the only thing that can help are patches and service packs, but you will not have a guarantee of the data leek (except for the manufacturer's promise)."[2] A recent discovery in the computer industry is the "cloud computing", which is [3] "a technology that keeps up data and its application by using the internet and central remote servers". According to Harauz and Kaufman [4] "we have the ability to utilize scalable, distributed computing environments within the confines of the Internet." Regarding data, i.e. data security, the safety of these systems is questionable: "So let's pause to consider the alter ego of the cloud as panacea: the cloud as a platform for malice. How bad could it get? [5]" If we look at the system administrator's side, it is an excellent solution, because the other side takes care of the security, integrity and maintenance of the computer. There are global players, and in Croatia a local ISP, "Croatian Telecom", started offering their Cloud computing service at the end of May 2013, where the user is given the right to use their computer. The user is shown a desktop with the applications that the ISP offers and the user immediately has a functional computer without the necessity to maintain it or worry about its security. [6]

One of the fundamental postulates of operational security is to create a user account that doesn't have administrative authorities (limited user). In Unix-like operating systems that is the only possibility, and completely normal, but in Windows OS it is an option that makes the daily use very complicated. Very often, the users change the settings of the operating system without even being aware of it. Any need for intervention or

repairing from the administrator, usually an IT teacher, is a waste of valuable time during classes or leads to unpaid working hours of the IT teacher in the role of system administrator. Considering the installed OS – Windows, the computers in Croatian schools often have inadequate hardware capacity. Apart from that, it is a fact that Windows OS works more and more slowly as more time passes from the day of the installation (problem with Windows Registry). Altogether, computers are slow, and become slower with time, which increases the amount of time that needs to be spent on them. In the modern world, which is turbulent and accelerated, it is important to minimize the amount of time necessary for computer maintenance, i.e. to strive towards minimizing that time by automatization. There are on average 19 computers in Croatian computer classrooms [7]. Based on that, we can approximately calculate the necessary time for their minimal maintenance, providing that there are no unforeseen situations. It is necessary to update the OS monthly, which takes at least ten minutes, depending on the speed of the computer, speed of the administrator and the internet connection. It equals a total of four classes a month, if we don't count the updating of user programs, control programs and additional programs; such as Java, Flash, Shockwave, programs for pdf files, video and audio files, etc., and sometimes the updating of the latest versions of antivirus programs. Web browsers are the favorite targets of attack on computers. Therefore it is important that they, as well as their add-ons and plugins, are independently updated. Web browsers such as Firefox, Google Chrome and Opera can be independently updated, but they require administrative authorities. Internet Explorer usually requires an intervention from the administrator during the installation of a newer version.

Servers should be equipped with smart UPS in case of an unexpected electricity loss and voltage stabilization, in order to keep the public services alive, and in order to protect the hardware from damage with controlled shutdown, in case the power supply loss lasts longer. It is desirable to protect the BIOS of personal computers with a password, because although the password is easy to cancel, it is necessary to open the PC case, which slows down and discourages the potential attacker. Safety copies of the data which is important for the school should be kept on a dislocated medium. The likelihood of a flood in schools is minimal, but the likelihood of a fire is greater. Permanent copies should be made at least once a year at the end of every school year. Safety copies of the data should be made depending on the importance and the amount of the generated information, and for critical data, safety copies should be made automatically, in real time.

III. Access to Operational Security

There are two basic types of computer classrooms in Croatian schools: thin client with or without multiseat technology and PC/laptop based classrooms. In a thin client approach, one or more powerful servers provide the central intelligence and control center for the security system. The end-user terminals display the graphical interface and process input from the mouse and keyboard. Most of the intensive processing happens on the server(s). It is also possible to start up the OS of the computer through the network using the Open Thin Client OS (http://openthinclient.org/).

Multiseat systems resemble thin-client systems with client interfaces (mouse, keyboard and monitor) attached directly to the computer that does the processing. That computer runs a program or operating system capable of managing multiple user sessions at the same time. Userful Multiplier and Windows Multipoint Server 2012 are two programs that fall into this category. PCs are computers that only one user can work on at a certain point – the one that is logged in to the operating system at that point. Locking the computers (which we will explain below) has its advantages:

a) there is less likelihood that a computer will pick up a virus or some other malware,
b) the administration of the computers is easier, (which leaves more time for other things),
c) there is less disk fragmentation due to constant installation/uninstallation of applications,
d) there are fewer (non-standard) applications which represent a safety hazard.

We will suggest several ways in which a satisfactory level of OS computer security can be achieved.

A. Group Policies for Various User Groups

These group policies reinforced with passwords make a good start. For example, administrators have all the rights (installation/uninstallation of programs; adjusting, adding and removing hardware), while regular users have the right to start an internet browser, office applications, etc. This approach has its limitations, because it is necessary to create several user groups and more access levels (for example, student, teacher, administrator), and these groups need to be administrated. Nevertheless, using group policies is much more efficient if the computers are cloned, or even better, if a domain group policy is used so it can be easily controlled by the domain controller.

B. Lockdown Software

This type of program enables the administrator to determine which devices users can access, which programs they can start, which folders they can see and access (for example, hiding the control panel and certain programs). These programs are not demanding, i.e., they don't require a large amount of knowledge or a centralized server. Depending on the computer classroom configuration and the program options, the administrator can control all these setting from one central computer. Disk protection programs that automatically delete all changes on the disk upon the next computer start up, user log out, or some other setting of the program, also fall into this group. Using this approach, a lot of people will think, "Why bother using antivirus protection?" But bearing in mind the increasing ingenuity of malware programmers and the fact that viruses keep getting more and more complicated and hard to discover, installing an AV solution for a greater computer safety is still recommended. Also, by updating, you don't only install patches, but also newer versions of programs (for example, Internet Explorer), as well as various improvements. Although the installation of an antivirus solution decreases the total available performance of the computer (which is sometimes extremely important), it is recommended to have an active and updated antivirus software. Each computer should be adjusted so that it

automatically downloads virus definitions. These are some software solutions for locking the settings: Fortres Grand Fortres 101, Deepfreze, Faraonics WINselect, KioWare, Rollback RX, Faraonics DeepFreeze and Centaurion Technologies DriveShield.

Deskman program [8] has one button to lock down workstations. It has the kiosk mode which tightly secures desktops and locks computers and it also has the ability to set up custom restrictions. It can freeze an application to create a safe environment and stop unwanted applications.

Deep Freeze [9] allows you to restore a PC on every restart. It has a virtual drive, an on/off protection switch so if administrators need to make any updates on a deepfreeze workstation, they have to turn off the deep freeze protection which requires a system restart.

When compared to above programs, Drive Vaccine [10] does not need to be turned off in order for any updates or software installations to be made, and protects the Master Boot record. Below we present a table with an overview of possibilities of particular programs:

TABLE 1. COMPARISON OF COMPUTER LOCK DOWN AND SYSTEM RESTORE PROGRAMS

Type of program	Name	License	Limitations / requirements	Publisher(URL)
System restore or disk protection	Deep Freeze	Commercial	Linux version only supports the SuSE Linux Enterprise Desktop, 10% free hard drive space	Faronics(1)
	Fortres Grand Clean Slate	Commercial	There is no version for Windows 8 and Linux	Fortres Grand(2)
	RollBack Rx	Commercial	There is no Linux version	Horizon DataSys(3)
	Drive Vaccine	Commercial	There is no Linux version	Horizon DataSys(4)
	Returnil System Safe 2011	Free for non-commercial, personal home use	Does not work on Windows 8, does not have Linux version	Returnil Virtual System(5)
Lockdown PC	Toolwiz Time Freeze	Freeware	Does not support Linux	Toolwiz(6)
	HDGuard	Commercial	Does not support Linux	RDT – Global(7)
	Faraonics WINselect	Commercial	Does not support Linux	Faraonics(8)
	SiteKiosk 8	Commercial	Does not support Linux	Provisio(9)
Application Launch Restriction	Windows 7 UAC	Commercial	Requires Windows 7	Microsoft

Table legend
(1) http://www.faronics.com/en-uk/products/deep-freeze/standard/
(2) http://www.fortresgrand.com/products/cls/cls.htm
(3) http://www.horizondatasys.com/products_and_solutions.aspx?ProductId=1
(4) http://www.drivevaccine.com/
(5) http://www.returnilvirtualsystem.com/returnil-system-safe
(6) http://www.toolwiz.com/products/toolwiz-time-freeze/
(7) http://www.hdguard.com/
(8) http://www.faronics.com/en-uk/products/winselect/
(9) http://www.sitekiosk.com/SiteKiosk/Default.aspx

If a school has a "server-client" logical network configuration, the administrators can control permissions from one computer. In case of a peer-to-peer network, the best solution is to clone the adjusted computer. When you clone the Windows OS (with the exception of the sysprep option for Windows 7), it is almost always necessary to have the same or quite similar (chipset) configurations of the cloned computers because of HAL, which is considered to be the driver for the motherboard and allows instructions from higher level computer languages to communicate with lower level components, but prevents direct access to the hardware. [11]

C. VHD (Virtual Hard Disk)

A virtual hard disk is a file that encapsulates a hard disk image. [12] It may contain what is found on a physical HDD, such as disk partitions and a file system, which in turn can contain files and folders. It is typically used as the hard disk of a virtual machine (VMware, Oracle VM VirtualBox, Windows Virtual PC, Microsoft Hyper-V Server). VHD contains the disk image which is loaded into the memory of the computer and all changes can later reflect on the OS itself (or not, depending on the options), so a layer is created between the computer resources and the program itself and there is no danger of compromising the security and integrity of the OS which is installed on the physical disk. It is recommended to use the native Windows 7 boot because the virtualization program still puts a burden on the computer.

D. Live CD/DVD

A live CD or a live DVD is a completely bootable computer operating system which boots from a CD, DVD or a USB and runs in the computer's memory. Live USB flash drives have the ability to write changes back to their bootable medium.

IV. WINDOWS SPECIFIC ISSUES

Windows XP is an incredibly resilient OS and is used by the majority of teachers in schools, but for which the support expired on April 8, 2014. Usually, the computers have a version of Windows already pre-installed on them, so the installation of a newer version would either be a license violation, or the right to an OS upgrade would need to be bought. **This is where the responsible government department comes in and mostly makes (pays for) an agreement with Microsoft that allows "a free" OS upgrade for the computers that already have a license, which is renewed every 3 years.** However, the Windows OS upgrade often does not end adequately, and it is necessary to reinstall the entire OS and all the required program support. But using outdated computers [7] that aren't capable of **running** newer OS versions eliminates any possibility for change within the Windows domain, which is notoriously demanding regarding hardware. Also, OS upgrade is a rather time-consuming job for an IT teacher, even if it is just for one computer, so it's normal that they are usually not thrilled about doing it. Alternatively, a version of Linux OS could be installed, but that brings many other problems (mostly subjective, due to user habits, and to a smaller extent objective), that could all be summed up as lack of time and/or desire to change.

As a result of the agreement that was signed between the Department of Science, Education and Sports and the Microsoft Company in June 2011, about licensing Microsoft software for primary and secondary schools, as well as for higher education institutions and public science institutes - „Microsoft Campus and School/Academic Agreement", all primary and secondary schools encompassed by the agreement have acquired the right to use licensed Microsoft software that can be downloaded from the web page: https://msdc.skole.hr/. Also, in November 2013, the Minister of Science, Education and Sports Željko Jovanović, Ph.D. and the Chief Executive

Officer of Microsoft, Steve Ballmer, signed the "Education Transformation Agreement" (ETA) with the aim to improve the Croatian education system [13] which, among other things, includes free use of Office 365 system for about 550 thousand students, college students, teachers and professors. There is also an interesting possibility for the IT teachers who have started using Windows 7 (but available and limited only for the Enterprise and Ultimate versions [14]): creating VHD disks and starting the computers from those disks. VHD is a format in which the disk is virtual. It contains everything that is on the hard disk of the computer (partitions and files) and it is used as the physical disk of a virtual computer. It enables the computer to set it up and to boot from the OS that is stored on it. This technically demanding principle is made simpler for teachers by selfless enthusiasts: Mark Minasi and his "Steadier State" [15], and the Finnish programmer Sami Laiho and his tool "Wioski" [16]. Wioski is a "self-healing kiosk-computer running Windows 7/8". It is a "wrapper that surrounds your own WIM-file of Windows 7/8 OS installing it on a VHD-file and using a differencing disk for writing incremental data." [16] Steadier State "freezes the computer as an image and creates a snapshot of the current activity as a virtual C:\. Restarting gives the option to roll back or keep the new snapshot." [15]

Windows 8 shows great functionality in the form of "refresh" and "reset" functions. [17] "Refresh" preserves user settings, user data, and applications bought through the Windows store. Everything else is removed and restored to defaults. Reset purges all applications and data, and reinstalls the operating system reverting it to a brand new fresh installation which requires reentering a license key and performing initial setup when completed. Programs that check whether a particular program has a newer version (such as Secunia PSI) can be helpful with computer maintenance. Another interesting possibility is using one program to start the installation of many others, such as InstallPad (http://installpad.philisoft.com/), where we first need to enter the URL addresses from which the instalation will be downloaded, and then the program downloads and installs them on the computer on its own. It is even better to visit Ninite.com (http://ninite.com/) and choose all the programs that need to be installed from the web page, and then they are downloaded and installed through one installer on their own.

Legal aspect of Windows licenses

When it comes to creating images, bear in mind that Microsoft Volume Licensing programs are not a source of full license for the Windows operating system. These programs offer only upgrade licenses for the Windows desktop PC. [18] Volume License media can be used to deploy software only to licensed desktop PCs. A customer cannot acquire an initial or “full” Windows desktop PC license through any Microsoft Volume Licensing program. The Windows desktop PC operating system upgrade license is for upgrades only. [18]

Reimaging is permitted if the copies made from the Volume Licensing media are identical to the originally licensed product. Windows Enterprise is not available outside the Volume Licensing programs and, therefore, is not eligible for reimaging. [19] Customers can use these copies from Microsoft media only if they are the same product and version, contain the same components, and are in the same language. [19] Reimaging using Volume Licensing full version media requires that customers have licensed the Windows desktop operating system either preinstalled through the OEM or as an FPP retail product. [19] A licensed version of Windows 7 OS is also required for the Windows upgrade license through Volume Licensing, where "customers must first acquire a full license for a qualifying operating system preinstalled by an OEM". [18] Bear in mind that one cannot actually upgrade from Windows XP to Windows 7. [20]

Windows Deployment

The most popular open source deployment solutions nowadays are Clonezilla and FOG. Clonezillla has an archaic text-based interface and it is not recommended for novice users while FOG provides a web-based interface accessible from any computer on the network. It also has the ability to deploy images from mobile devices. [21] If an administrator has to deploy images across the network, setting up a dedicated cloning server is required. "For Clonezilla SE, this means setting up a Diskless Remote Boot in Linux (DRBL) server by installing it on top of a Debian or CentOS server." [21] Another option (for small networks) is to use the DRBL live CD to convert the machine into a temporary server. If all of the machines for imaging are not on the network, Clonezilla is a must, because FOG can clone only from an imaging server. FOG, by default, requires hosts to be registered (recording a unique MAC address) before imaging and before deployment (it can be overridden with an enabled Capone plug-in [22]). Clonezilla doesn’t require registering a host.

When it comes to installation, FOG "installation script creates the components required for an imaging server on top of a standard LAMP server." [21] The "FOG server is designed to integrate with existing network infrastructure such as DHCP and DNS servers, although it can also set these up on its own." [21] If an existing DHCP server is used, PXE traffic must be forwarded to the FOG server and the firewall must be configured to pass traffic to the server. The FOG service has additional features and can "schedule tasks, such as deploying images, installing and managing printers, tracking access to cloned machines, powering up a computer remotely using Wake-On-LAN, and installing applications remotely via a feature called snap-ins." [21] "With snap-ins you can directly push the executable installer for a simple application to a Windows computer." [21] Snap-ins can also be used for pushing software updates to client computers. FOG's menu has additional features and "offers options to wipe a disk, restore deleted files, scan a disk for bad blocks, and run a virus scan using ClamAV." [21]

If the person in charge of computer maintenance decides to use the Windows server, they have the technology called WDS (Windows Deployment Service) at their disposal. WDS is included as a Server Role in all 32-bit and 64-bit versions of Windows Server 2008. Deployment must be performed with the "sysprep tool" which is included in every instance of Windows 7 and Windows 8. The machine must be sysprepped (all system-specific information from an installed Windows image is removed; including the computer security identifier (SID)) and then the image can be deployed using WDS. There is no limit to the number of times that the Sysprep command can run on a computer, but the clock for Windows Product Activation begins its countdown the first time Windows starts. Sysprep/generalize command can be used to reset the Windows Product Activation a maximum of three

times. If the Sysprep command needs to be run multiple times on a single computer you have to use the SkipRearm setting in the Microsoft-Windows-Security-Licensing-SPP component to postpone resetting the activation clock. [23] There is probably no need to have outside experts perform the deployment in schools (as far as students are concerned), because according to article 12, paragraph 11 [24], students' documents are only kept until the end of each school year. Below we present a table with some solutions for Windows deployment.

TABLE 2. POSSIBLE SOLUTIONS FOR WINDOWS DEPLOYMENT

Name(URL)	License	Specific requirements
Smart Deploy(1)	Commercial	It has a platform pack (PC drivers for different vendors)
Fog project(2)	Free	**A**pache, **M**ySQL, **P**HP but they are automatically downloaded by the software
Clonezilla(3)	Free	-
System Center 2012 R2 Configuration Manager(4)	Commercial	Active Directory schema must be extended, SQL Server is required, and multiple site server roles have to be configured.
Symantec Altiris Deployment Solution(5)	Commercial	-

Table Legend
(1) http://www.smartdeploy.com/
(2) http://www.fogproject.org/
(3) http://clonezilla.org/
(4) http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2-configuration-manager/default.aspx
(5) http://www.symantec.com/deployment-solution

V. RECOMMENDATIONS FOR THE IMPROVEMENT OF SCHOOL COMPUTERS SECURITY

Administrators should lock the rooms where computers are stored, and also set up authorized video surveillance. If, despite the fact that all deadlines have expired, security policy still doesn't exist, it should be imposed on schools by the responsible government department. It must be introduced to all school employees who should be given a test to make sure they are familiarized with the security policy, under the threat of having their salary reduced until they have successfully passed it. After that, all other users such as outside collaborators and students should be familiarized with the policy. Users of public computers should sign an agreement stating they will use the computers in conformity with the security policy. This could be achieved by having a simple application appear when the computer starts, with the following message: "By using this computer you accept the terms of use that are in accordance with the institution's regulations and the ISP." The application could be more complex so that before using the computer, the user must answer correctly three randomly picked questions about the security policy of the institution and the ISP. Apart from the digital message on the computers, detailed regulations should be displayed in the classroom so that everyone could read them. Regulations should include the ways the equipment and resources can be used, as well as the proper behavior. A few guidelines that should be listed:

1) Who has the right to use the computers? (for example, the age limit for using the computers, chat rooms and social networks as well as a list of web pages allowed for persons under 18)
2) Strictly forbidden actions, i.e., a ban against disrupting the physical integrity (against slamming, hitting and breaking the computers, equipment and the cables), as well as a ban against moving the equipment (mouse, keyboard, printer…)
3) For what purposes the computers can be used and a ban against sharing files and illegal distribution of copyright protected material.
4) A ban against changing the settings of the computer's OS (downloading illegal programs and malware, using BitTorrents, visiting and downloading pedophile and porn material), the possibility or impossibility to print, save files to various media, run external programs or download programs.
5) Disciplinary actions for those who don't abide by the previously stated rules (the possibility of charging for damage, reporting to authorities, banning against further access and use of the computers and equipment). Public computer labs should "protect themselves from possible lawsuits by educating their staff, clients, and students about copyright law." "Users need to be educated that installing unlicensed software is a prohibited activity." [25]

As more and more devices (PDAs, mobile phones, tablets) are connected to the internet, communication security becomes more important. It is necessary to design and configure a network according to the rules of the trade – it is not a layman's job and it should be given over to an outside company or CARNet, in case the IT teacher is not competent enough. Within the domain of operational security, if Windows are used, then XP should be abandoned and upgraded at least to Windows 7 and also a functional solution should be implemented for locking the settings and/or restoring the computer to a desired state. We recommend the VHD technology and its possibilities, since it is available within Windows, but a live CD/USB of a Linux version is not a restrictive solution since the school curriculum doesn't mandate the platform/software, but only the topics that have to be covered. If it is financially possible, the cloud, i.e. a virtual desktop is an even simpler solution. If the computers are too weak/old and the Windows 7 or newer versions cannot be installed on them, then the options of replacing the computers with newer ones or installing a newer version of Linux distribution should be considered, or the PC computers should be converted into clients with the acquisition of a strong Windows server. Concerning the Windows deployment, it is necessary to keep in mind the Windows licenses, and in practice we recommend a version of Windows server and Windows deployment service, considering that their use in schools is free of charge, or perhaps open source programs such as FOG and/or Clonezilla. "Clonezilla SE makes the most sense for networks with clients that don't require much administration after being imaged, such as those in Internet cafes, libraries, and school labs." [21] If the machines aren't connected to a network, Clonezilla must be used. Taking care of computer security also means creating a set of rules for using the computer equipment, and taking care of all aspects of security must never stop.

VI. CONCLUSION

Nowadays, the concern for security on the internet, on the computer, on social networks and in everyday life is

becoming more and more important. Since more and more devices are being connected to networks, and technology and mobile devices are becoming more available and have become a constituent part of everyday life, we should think hard about introducing the topic of IT security and computer security into our curriculums. In the primary school practices, there is very little regard for computer security. In the authors' opinion, this will not change until a very serious incident occurs in an institution; until then, very little attention and time will be spent on it. It appears that it all comes down to the IT teacher, i.e., to how much will and knowledge he/she can invest in the students' education and the computer classroom. Investing time in some solutions for locking the settings, deleting the changes made on the computer, live distribution, or a cloud solution are some viable options for every person, but it all greatly depends on financial capacity, responsibility and concern for the confidentiality of information, and on personal attitude, knowledge and skills. Regardless of the path, there are two crucial choices: a) whether to use Windows or not and b) whether to lock the settings or give complete freedom (all users as administrators)? Things are well as long as the responsible government department is making agreements with Microsoft and gives Windows products for teachers to use "free of charge", but what can be done once there is no more money or once the politics instruct all state institutions to switch to open code for some reason? In that case, the only legal and correct solution is to switch to an "alternative", free of charge and much safer OS (for example Linux). This way every line of the code would be under control and we would be sure that a certain part of the code is working the way it was meant to. Concerning the question of whether or not to lock the settings or give complete freedom to users, the authors believe that it is more productive to give almost complete freedom to users, i.e., to use some sort of technology for deleting the changes, i.e., for restoring all the settings, even if that means that computers should often be cloned. Further research is necessary in the field of computer security, such as: what is the level of computer security in Croatian institutions, and how much do the IT teachers in schools (especially the ones who play the role of system administrators) know about computer security and maintenance which include broad topics such as security, hardware, software, networks and application of IT technology in class, HCI and creating digital educational material. Finally, how much do the students, whom the schools and teachers are here for, know about IT and computer security and do the perceived shortcomings in the system significantly influence the knowledge they acquire through informal channels?

REFERENCES

[1] Miroslav Bača, Uvod u računalnu sigurnost. Narodne novine, 2004.

[2] Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić, "'Security of Computer Systems and Networks' Book Preview," ComSIS, vol. 4, no. 1, 2007.

[3] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Analysis of performance by using security algorithm on cloud network," international conference on Emerging trends in engineering and management (ICETM2012), pp. 23–24, 2012.

[4] John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing," IEEE Security and Privacy, vol. 7, no. Issue 4, pp. 61–64, Aug. 2009.

[5] Blumenthal, M.S., "Hide and Seek in the Cloud," IEEE Security Privacy Magazine, vol. 8, no. 2, pp. 57–58, 2010.

[6] Hrvatski telekom, "T-com cloud computer," 2013. [Online]. Available: https://www.hrvatskitelekom.hr/poslovni/ict/cloud/racunalo. [Accessed: 01-Jul-2013].

[7] K. Pavlina, A. Pongrac, B. Latas, "Hardware equipment of computer classrooms in Croatian elementary schools," MIPRO, 2012 Proceedings of the 35th International Convention, pp. 1325 – 1327, 25.05 2012.

[8] Anfibia, "Deskman," 2013. [Online]. Available: http://www.anfibia-soft.com/products/deskman/. [Accessed: 30-Jun-2013].

[9] Faraonics, "Deep Freeze," 2013. [Online]. Available: http://www.faronics.com/products/deep-freeze/. [Accessed: 30-Jun-2013].

[10] Horizon Data Sys, "Drive Vaccine," 2013. [Online]. Available: http://www.drivevaccine.com/. [Accessed: 30-Jun-2013].

[11] Wikipedia, "Hardware abstraction," 18-Oct-2013. [Online]. Available: http://en.wikipedia.org/wiki/Hardware_abstraction. [Accessed: 28-Jun-2013].

[12] Liang Yang, Anthony F. Voellm, "Hyper-V Virtual Hard Disk (VHD) Performance White Paper," A Microsoft White Paper, Mar. 2010.

[13] The Government of the Republic of Croatia, "The Government President Milanović and the Minister with the Chief Executive Officer of Microsoft," November 2013. [Online]. Available: http://public.mzos.hr/Default.aspx?art=12804. [Accessed: 23-Dec-2013].

[14] "VHD limitation," technet.microsoft.com, 22-Oct-2009. [Online]. Available: http://technet.microsoft.com/en-us/library/dd799282%28WS.10%29.aspx#BKMK_limitations.

[15] Mark Minasi, "Stadier State," 2012. [Online]. Available: http://www.steadierstate.com/.

[16] Sami Laiho, "Wioski," 2013. [Online]. Available: http://www.wioski.com/.

[17] Microsoft, "windows refresh, restore," 2013. [Online]. Available: http://windows.microsoft.com/en-US/windows-8/restore-refresh-reset-pc. [Accessed: 19-Feb-2013].

[18] Microsoft, "Operating System License Requirements: Initial Operating System and Transfer of License." 2013.

[19] Microsoft, "Reimaging Rights," 2013. [Online]. Available: http://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Reimaging.pdf. [Accessed: 13-Mar-2013].

[20] Mirosoft technet, "Windows 7 Upgrade Paths," 17-Jun-2009. [Online]. Available: http://technet.microsoft.com/library/dd772579.aspx. [Accessed: 13-Mar-2013].

[21] Mayank Sharma, "Clonezilla vs. FOG: The clone wars," 18-Mar-2013. [Online]. Available: http://www.openlogic.com/wazi/bid/275172/Clonezilla-vs-FOG-The-clone-wars. [Accessed: 01-Aug-2013].

[22] FOG, "Fog project Wiki," 02-Oct-2011. [Online]. Available: http://fogproject.org/wiki/index.php?title=Plugins:_Capone. [Accessed: 05-Aug-2013].

[23] Microsoft technet, "How Sysprerp Works," 07-Aug-2010. [Online]. Available: http://technet.microsoft.com/en-us/library/dd744512%28WS.10%29.aspx. [Accessed: 13-Mar-2013].

[24] MZOŠ, "Pravilnik o načinima i postupcima i elementima vrednovanja učenika u osnovnoj i srednjoj školi," 2010. [Online]. Available: http://dokumenti.ncvvo.hr/Dokumenti/pravilnik_vrjednovanje_os_ss.pdf. [Accessed: 30-May-2013].

[25] Hilary Naylor, "Securing Your Computers for a Public Computing Environment," 10-Jul-2007.