The Taming of the Academic Freedom

T. Vellemaa[1], R. Nahkur[2], L. Kadajane[3], M. Fisch[4]

[1]Department of IT Services, University of Tartu, Ülikooli 18a Tartu 50090, Estonia, terje.vellemaa@ut.ee. [2] Department of IT Services, University of Tartu, Ülikooli 18a Tartu 50090, Estonia, rain.nahkur@ut.ee. [3] Department of IT Services, University of Tartu, Ülikooli 18a Tartu 50090, Estonia, lauri.kadajane@ut.ee. [4]Department of IT Services, University of Tartu, Ülikooli 18a Tartu 50090, Estonia, mark.fisch@ut.ee.

Keywords
Standardization, workstation management, software distribution, computer management, infrastructure integration.

1. EXECUTIVE SUMMARY

In order to meet evolving academic and business needs, IT infrastructure must continuously adapt to support new applications and capabilities. As systems become more sophisticated, management costs and security risks can increase and affect the ability to maintain service levels.

In today's world there are many different practices for more efficient IT management through standardization. One of the most acknowledged and most common of these best practices is ITIL. Based on ITIL and COBIT standards, Microsoft has developed its own Core Infrastructure Optimization model (CIO).

1.1. Situation background

At the University of Tartu, a heterogeneous system has been established: approximately 200 SUN Solaris/Linux servers, approximately 30 Windows-based servers and a great number of Windows workstations. The system consists of UNIX Open LDAP, Oracle Internet Directory and Microsoft Active Directory. Most of our information systems have been built to be compatible with Open LDAP.

The objective of the article is to show the progress of standardization at the University of Tartu, based on our experiences. In 2004, Microsoft Systems Management Server 2003 was implemented to manage and configure Windows-based client workstations.

1.2. Central management meets the Academic Freedom

In the atmosphere of academic freedom at the University, the project is making some good progress. So far the University's centralized environment consists of approximately 700 workstations (1/5 of all workstations) and this number is growing steadily. This experience gives us a good basis for comparing managing standardized and unstandardized environments. In our work process we rely on Microsoft Core Infrastructure Optimization model.

As a result of our centralization efforts, the former atmosphere of academic permissiveness has been replaced by a reasonably regulated, reliable and safe environment, with restrictions mainly aimed at preventing users from inadvertently putting their computers and data at risk, while at the same time taking into account their specific needs.

1.3. Conclusions

Relying on our experiences we may say that there are many benefits in having standardized desktop environment. The four main ones would be: more secure infrastructure; more efficient software management; lower total cost of ownership; more efficient use of human resources.

2. STANDARDIZATION IN THE ATMOSPHERE OF ACADEMIC FREEDOM

2.1. Academic Freedom

In a classical sense, academic freedom can be understood as the freedom of scientists and students to pursue scientific research and proclaiming uncomfortable truths without fear of sanction on the part of the government. From history we know many examples of scientists who have lost their lives, because their discoveries conflicted sharply with the then prevailing religious world view. Although the situation today is less dramatic, researchers nevertheless need a principal consensus regarding their freedom of enquiry regardless of the results of their work.

Unfortunately, some academic workers tend to expand the notion of academic freedom and perceive as its violation also all kinds of regulations concerning their work environment, including restriction of user permissions both in information systems as well as in their workstations. However, due to its complexity, IT requires regulating and restricting user rights in order to maintain the functionality and capacity to operate.

Although the constraints on the freedom of academic staff are unpopular, they are nevertheless accepted, since in the end positive aspects greatly outweigh the inconveniences caused by the restrictions.

2.2. Why Microsoft?

The debate Linux vs. Microsoft has gone on for a long time and still continues in the IT world. In our case this dispute was solved by the spontaneous development of the environment already years ago. The initial solution used UNIX-like operation systems as servers, while workstations were predominantly equipped with Windows. The management of workstations was done “manually”, one at a time at each respective subunit to the best of their resources. Attempts to find UNIX-based management tools were unsuccessful, i.e. we were unable to identify an Active Directory comparable with SMS in terms of functionality and reliability for the maintenance of Windows-based workstations.

The broader reason for preferring Microsoft’s products is the scope, quality and availability of know-how. In other words, Microsoft offers a very broad range of services and products which as a rule are compatible with one another. In our experience the solutions offered by Microsoft are increasingly reliable and they are free from the tendency to stay for a long time without security update and version upgrades which is a common problem with Linux. Very important is also the availability of professional know-how – if the solution cannot found on the web, we know we can count on the assistance of either Microsoft itself or their partners, which enables us to solve problems rapidly or to avoid them by timely reaction.

A good example of Microsoft’s broad range in the IT field is Core Infrastructure Model – a test which we passed through for units managed by us. The test taken by us comprised a series of questionnaires, divided into five groups, which established the general level of our organisation’s IT-infrastructure. While “basic” is the level of any IT-infrastructure, the standardized level can be attained through efficient and carefully planned work and the last two already require a serious, focused effort. Microsoft has developed manuals to provide guidance on how to advance from one level to the next. The majority of institutions fall somewhere between the first and second level.

Our test results are shown in Figure 1. Since we don’t yet manage mobile devices, owing to their small number and heterogeneity, our result in the ”Desktop, Device, & Server Management” section of the test remained in the basic-level. Our result in this section was also affected by the fact that we have only a small number of Windows-based servers which at the same time perform very diverse tasks (which is why their management is still largely unautomated). In the ”IT & Security Process” category we are on the basic level, as our University-wide security policy is currently under revision and the process documentation has not been regulated.

Core Infrastructure Optimization	Basic	Standardized	Rationalized	Dynamic
Identity & Access Management		✓		
Desktop, Device, & Server Management	✓			
Security & Networking		✓		
Data Protection & Recovery		✓		
IT & Security Process	✓			

Figure 1 Core Infrastructure Optimization Assessment results

Our experience has not confirmed Microsoft's much-talked-about monopolist tendencies. They have been very obliging with our UNIX-based solutions. Microsoft has offered practical advice, products and cooperation partners, who have been able to assist us. Moreover, Microsoft offers considerable discounts for educational institutions.

The above encomium is not to say that Microsoft products are absolutely flawless; from our viewpoint they simply offer the best price/quality ratio.

3. THE SITUATION BEFORE SMS

Before 2004, UNIX was dominant in the area of servers and Windows could be encountered only in workstations. In 2004, the first Windows-based servers arrived – two domain controllers and a System Management Server (hereafter SMS). SMS was then still largely in the testing phase: there were many unsolved problems and many software installations still had to be done manually. The test group consisted of 60 computers, but an actually working and reliable solution could not be reached yet.

The installation of operation systems and software in workstations was done manually. Installation via RIS (Remote Installation Services) was also tried, but due to anomalies it was later abandoned. The security updates were usually installed via Windows Automatic Updates. At the same time the situation was rather confused: there was no exact overview of software situation and versions. The actual situation could only be established by an on-site audit.

The situation with user rights was no less chaotic. Experiments with Policy gave anomalous results and the decision was made then to abandon it. Administrator rights were granted to users far too easily, sometimes with drastic result. More humorous cases include one over-enthusiastic user who had installed several antivirus programmes on his/her desktop which then endlessly moved contaminated items from one quarantine folder to another. However, the situation in regard to virus attack statistics was far from funny – 4–5 times a year it was necessary to isolate a study building or an entire faculty by a network interruption in order to fend off a virus attack. The security situation was further aggravated by the widespread of the insecure Windows 98 and undoubtedly also by the low level of awareness among the end-users.

4. SITUATION AT THE UNIVERSITY CENTRALLY MANAGED DEPARTMENTS

Since 2005, a number of developments have occurred in our desktop lifecycle management. The environment has become more secure and reliable; the number of centrally managed desktops is growing rapidly.

The most important change is the new user authentication schema – as described in the paper published in 2005, one of the open issues was the situation where the users authenticated themselves in our central Active Directory as trusted Windows NT 4.0 domain users. A one-way trust relationship was established between UNIX-based Samba NT 4.0 emulating domain and our Active Directory. That was rather unfortunate solution, since it was not possible to centrally manage any user-based computer settings. In 2006, we redesigned our Windows-based infrastructure. A software solution has been developed, to synchronize all user accounts and group membership information from UNIX-based Open LDAP and Samba environment to the central Active Directory. We also

redesigned the Active Directory basic organizational unit structure, making it more logical and more administrator-friendly. At this point we could speak of the version 2.0 as the University's Active Directory.

4.1. Group policies

Based on new AD structure, an altogether new group policy structure has been developed. The fact that the desktop users authenticate themselves as Active Directory user objects made it possible to centrally apply user-based group policy objects. In terms of security, the most urgent step was to deny ordinary desktop users any administrative permissions over their local workstation. This move has cut massive department-wide computer virus epidemics about five times (see Figure 2). At first that step was not very popular – a number of users protested and claimed the permissions they were familiar with, mostly the permission to install their own software. After some time and some explanative work the majority of that group realized, that it is necessary not to allow users to install any software independently and that it enables them to work more efficiently as there is less downtime due to defectively installed software or malware attacks.

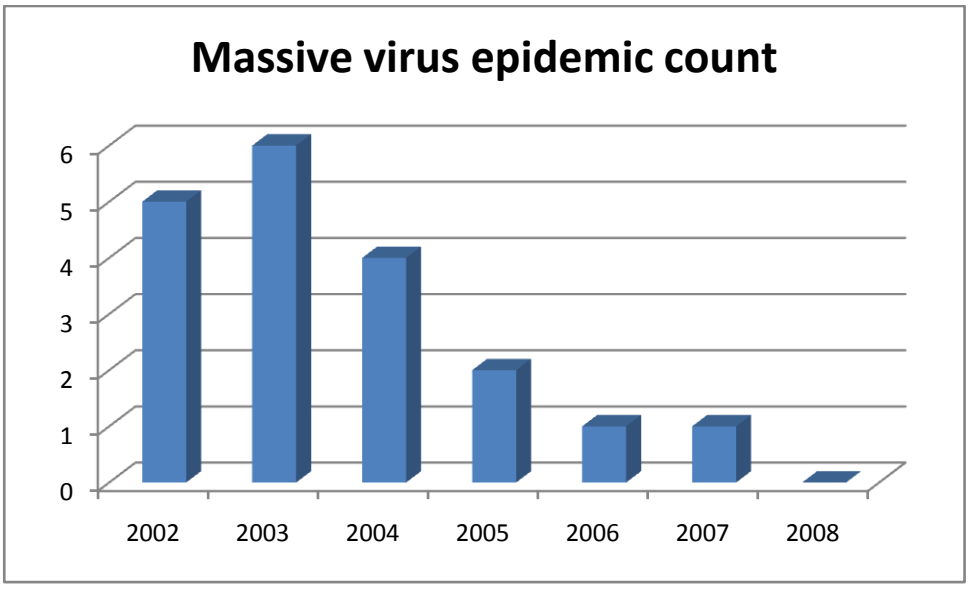

Figure 2 **Massive virus epidemic count per year**

New and simplified group policy structure basically involves only two different policies that change client computer's settings centrally – the managed computers' options policy and managed computers' restrictions policy. The first one contains a number of security changes in the computer configuration (for example local administrator and guest accounts disabling and renaming, disabling the showing of the last logged in username in the login window, changing default event log access permissions, changing the settings of Windows Firewall, removing any unassigned accounts from desktop's local administrators group, etc.) and user-based desktop environment configuration (for example redirects user's My Documents folder to the network share, removes permission to change user's My Documents folder path, removes permission to access Windows Update). The other one contains computer-based restrictions on the use of PKI and a number of user-based restrictions (for example fixates Internet Explorer settings, hides all unnecessary Control Panel applets, fixates desktop resolution, removes access to the operating system's registry modifying utilities, prevents user access to system partitions, prohibits unpermitted file execution, etc.).

Some changes have also occurred in the standardized desktop management. Today, as the departments managed by us have joined Microsoft's Campus Agreement, we are allowed to install the most recent operating system upgrade and office software on our workstations. So, the basic operating system level that we support in our central desktop management environment is Microsoft Windows XP with Service Pack 2. As desktop hardware we buy one major brand enterprise level

workstations only, all other configurations are not supported. The operating system installation process is fully automated – to this end we use Microsoft Remote Installation Services. In the process of software distribution there is no revolutionary progress – the same Microsoft Systems Management server is used as in 2004. The only major change is in software updates distribution which is now centrally managed and most of Microsoft patches undergo a testing phase.

For testing purposes, we have recently implemented a virtual environment based on Microsoft Virtual Server 2005 Release 2. All new software packages and updates are tested in that environment against virtual machines and afterwards some of these are also tested against real computers, as some software just does not work properly in a virtualized infrastructure (for example, CheckPoint VPN client is unable to run in a virtual machine).

5. SITUATION IN THE PERIPHERY

The situation at the University departments who manage their IT independently is very diverse. At one extreme is an extremely detailed management where users are granted only minimal permissions, to the point that they are not even allowed to choose the location of programme icons on their desktops. As a rule, these University units have their own isolated subnet where the network management is extremely safe and which enables a detailed overview of the situation. The renewal of computer fleet, as well as the maintenance of the network infrastructure is tightly controlled by the management team. Such units usually have their own local domain, software management system and even its own mail server, although the University provides central e-mail service to all students and staff anyway. On one hand, this approach guarantees a greater reliability and security; on the other, the users are not very happy with their limited permissions which don't enable them to customize their workstation to suit their specific needs. In our case, such system is dependent on a single administrator in whose system no one else has any permissions or knowledge about its design.

The other extreme, which in its pure form is fortunately rare, would be a totally unregulated infrastructure, where the computers are purchased by the users who have full administrative rights to their workstations and can install the necessary software independently. The network infrastructure is the only service provided by the local IT support. The users' computer knowledge in these units is usually above average, but unfortunately not always sufficient to avoid unpleasant situations. Computers plagued by spyware and viruses, low-quality hardware and faulty set-up are a common phenomenon. Usually the IT support is provided by a competent local user for whom it means extra job. Unfortunately, we lack an overview of licensed software in these units.

The representatives of both groups also collaborate with us to some extent – those of the first group mainly in problems regarding infrastructure and the others owing to their IT ignorance. The cooperation could be far more active, but it is hindered due to historical reasons – the IT Department at the University of Tartu is more recent than local IT supports at faculties and institutes; therefore the competence reached us later than periphery. However, the confidence in us seems to be growing and many of these "islands of resistance" have expressed their willingness to join us in the near future.

6. LESSONS LEARNED AND FUTURE GOALS

What did we learn and where would we like to go tomorrow?

As a result of the last three years work we may say that there are many benefits in having standardized desktop environment. The four main ones would be:

1. More secure infrastructure as well as planned software distribution schema provides more stable security level as all software updates and patches applied are tested and approved by administrators.
2. More efficient software management as having standardized and centrally automatically distributed software saves time spent to the process itself.
3. Lower total cost of ownership. Having one or two standardized hardware platforms and buying the computers with wholesale prices is more cost effective. Also owning computers pieced out by competent specialists is more reliable and warranty terms are more favourable.

4. More efficient use of human resources. Automatic software distribution saves workers time spent on installation actions. Having standardized and well proved software environment reduces the amount of work spent on providing support in solving unpredictable problems.

In the near future some tasks still need to be completed. Presently, no central printer management has been implemented, but we plan to standardize the printing systems and to implement a centrally managed print spooler service. In the summer of 2008, we plan to upgrade our System Management Server to the Microsoft System Center Configuration Manager 2007 (former project name SMS 4.0). If the escalation process needs more active directory domain controllers, we will upgrade our AD to the Windows Server 2008 domain level which will give us many new security and management features.

In a longer perspective we are planning to implement the full Microsoft System Center product family.

In software standardization process we would like to improve our testing capacities and in the future to use as little as possible freeware of suspect origin and without proper manufacturer support. For example, some problems with freeware are related to unattended installation; there is a number of adware included to the installation packages, for which it is impossible to get any support if some errors occur.

In the work process, there are a few loose ends as well. One major problem is the lack of good web-based helpdesk information system. We have tried different freeware and commercial applications, but almost all of them fail to meet our requirements. The most promising is Microsoft System Center Service Manager, but it is in beta stage at the moment and no concrete release date has been announced yet.

Another open issue is mobile device management – more and more users need to access University's infrastructure from everywhere and they are using more and more mobile devices (PDAs, smartphones). There are some problems with patching and distributing software updates, as Microsoft has officially declared that they will disable that functionality by default because there is no common hardware platform and they just cannot guarantee that the device will work properly after upgrade.

7. REFERENCES

Vellemaa, T., Jalakas, A., Tiidumaa, A. (2005). What do you want to manage today? *Proceedings of the 11th International Conference of European University Information Systems*.

Microsoft Core Infrastructure Optimization: http://www.microsoft.com/business/peopleready/coreinfra/default.mspx.

Microsoft Core Infrastructure Optimization test:

https://roianalyst.alinean.com/calculators/microsoft/core_io/Microsoft_Core_IO.html

Microsoft Systems Management Server home: http://www.microsoft.com/smserver/default.mspx