Policy for the Techmasters Server

The 2008-09 Techmaster Board

January 10, 2009 (v2.0)

The Techmasters Club exists to provide technological support for the Phillips Academy community and to encourage technological understanding and facility on campus. The Techmasters Server is a wonderful asset that can help us to accomplish both of these goals. For the Techmasters Server to be a valuable educational resource for the community and for the club, the server needs to be open to student use and experimentation. Historically, however, this principle of openness has been in tension with security concerns that have arisen from the server's important role as a support service and from its trusted place in the academy network. The following usage policy attempts to maximize openness while mitigating potential for abuse.

Technological Overview

The Techmasters Server is a Dell Poweredge 2900. Instead of running a single operating system like most computers, the server uses something called virtualization technology (Xen hypervisor with a CentOS Dom0 and paravirtualized machines). In effect, the server has split personalities. It thinks that it is multiple different servers, each of which can behave as if it's a real physical machine. These multiple personalities, called guests, are unwittingly controlled by a master personality: Dom0. None of the guests knows that it is the same computer as Dom0, and only Dom0 can manipulate the other guests. This allows the Techmasters board and members of Technology Office, who are the only individuals with access to Dom0, to totally control each guest and to prevent use of one guest from interfering with the functions of another.

Risks to be Mitigated

There are various risks that the school takes in allowing Techmasters to run a server. These risks can be put into three broad categories: damage to mission critical services run by Techmasters, "bad" content (more on this later), and security risks to the wider network.

Techmasters currently runs services "mission critical" to the school, namely the work order system. In the past, the server has also been used for the Grasshopper Night ticketing system and electronic voting, among other Student Council projects. Obviously, these services are a priority to the school, and every effort must be made to keep these services running smoothly.

A second risk is that of the server being used to traffic in "bad" content such as illegally obtained copyrighted material, slanderous material, hate speech, pornography, etc. Downloading and hosting "bad" content on the server has been a problem in the past, and for obvious reasons presents a risk to the school.

The third risk is that the server, which has a unique position in the school network, could present a risk to that wider network as a whole. Prevention of this risk is largely beyond the scope of this document because it has much more to do with network policy than with server policy. Nevertheless there are certain steps that Techmasters can take to prevent the server becoming a security risk. These will be discussed below.

A Policy that Mitigates these Risks

This policy is a series of guidelines to be interpreted by the Techmasters board and by the PA Technology Office. The latter is the final authority regarding use of the server, and agents of the Technology Office will have access to all aspects of the server for purposes of enforcing proper use as necessary.

1. Techmasters with access to the server must sign an agreement in which they accept the necessary terms and take personal responsibility for their use or misuse of the server. Techmasters who abuse the server will stand to have their access privileges indefinitely revoked, may have their standing within the club revoked, and could be further disciplined under the AUP.

2. Dom0 and any guests running mission critical functions will be accessible only to the Techmasters board and will run no processes unrelated to their primary functions. Additionally, all other use of the server will be secondary to these functions (for instance, if there is a resource shortage, other virtual machines will be shut down). Mission-critical functions are considered to be those that benefit the entire school community, such as the Work Order system, student council projects, etc.

3. Access to non-mission critical guests will be granted on a case-by-case basis to Techmasters who have signed the above-mentioned agreement. Individual use of the server must be secondary to the mission-critical services mentioned above, and an individual's computational resources will be capped if they exceed a reasonable level. Individuals with access to the server are required to keep their authentication credentials private and secure. They may not grant other individuals access to their account(s) for any reason whatsoever.

4. The Techmasters board is to exercise all due diligence in maintaining the security of the server. For instance, the board must ensure that all services running on the server remain up-to-date and must move quickly to address any known vulnerabilities. Additionally, the server should not have unnecessary open ports and should not run unnecessary services.

5. In order for it to serve its designated purposes, the server requires incoming and outgoing internet access on certain ports (as documented elsewhere). This may be provided by the Technology Office as long as the Techmasters board can demonstrate a need and as long as this internet access is not abused.

6. Outgoing internet access exists primarily for maintenance purposes. It will be made available to non-board members on a case-by-case basis, if a demonstrated need exists, and may be severely throttled.

7. Publicly available web services (such as the Techmasters web page, the Work Order System, the web pages of individual Techmasters, and web applications written for the Student Council) must be pre-approved by the Technology Office before they are made accessible. Web services should not solicit unnecessary personal information from users and must not solicit private information (anything from home address to credentials for another website). Any personal data stored on the server should be deleted after it is no longer being actively utilized.

8. All applications written by Techmasters and run on the server must be open source and freely licensed. The source code should be stored offsite in an accessible fashion. Third-party software is not subject to these restrictions but must meet the criteria in the next point.

9. In addition to the above restrictions, Techmasters may only store two types of content on the server: content the copyright to which they hold, and content that they have been authorized by the copyright holder to distribute (not just to possess, but to distribute). Exceptions may be granted by the Technology Office. For example, Techmaster Bob can store on the server a document that that he wrote himself, or that its author, Alice, personally authorized him to distribute. He could not store a copy of Microsoft Internet Explorer, even if legally downloaded from the Microsoft website, because he is licensed only to use it, not to distribute it. He could, however, store a copy of Mozilla Firefox because the Mozilla Public License authorizes redistribution of their software.

10. The Techmasters Server must at no point masquerade as representing Phillips Academy or the Phillips Academy Technology Office.

11. In addition to the above, Techmasters use of the server must be permissible under the AUP.

Conclusion

This policy both addresses the risks outlined above and maintains a spirit of openness in line with our role as an educational club.

The 2008-09 Techmasters Board