LSA IT Security Policy
Minimum Version for Operating Systems and applications/services
TABLE OF CONTENTS

INTRODUCTION ............................................................................................................... 3

PATCHING OF COMPUTERS .......................................................................................... 4

MINIMUM VERSIONS OF OPERATING SYSTEM (OS) AND APPLICATIONS ...... 5

  Minimum Operating System List .................................................................................... 6
  Minimum Versions of Services, Applications, or Daemons ........................................... 7

Services and Applications that will be identified
and reviewed by the Security Administrator ................................................................. 8

MITIGATION TECHNIQUES ........................................................................................... 9

  Removal from Network ................................................................................................... 9
  Hardware Firewall ......................................................................................................... 9
  Software Firewall ......................................................................................................... 9
  Non-Routable VLAN ...................................................................................................... 9

APPEALS PROCESS ....................................................................................................... 10

APPENDIX A: ANNOUNCEMENT OF THE SECURITY INITIATIVE FOR LSA .... 11
Introduction

This document sets forth the LSA security policy for all computer systems connected to the College’s network. It is LSA’s intent to secure and protect college computers before they are compromised by attackers attempting to gain unauthorized or illegal access.

The College implemented a mandatory patching requirement for all college computer systems that went into effect on October 31, 2005 (See the Deans’ letter announcing the security initiative for LSA in Appendix A.). LSA will continue to strengthen the security of its networked computers by requiring a minimum version for the operating systems (OS) and services/applications for all college computer systems connected to the network. These security enhancements must be in place by January 1, 2007.

Because a single insecure computer on the network poses a potential threat to all other computers, users and their data, the procedures and requirements listed in this document must apply to all computers in the college that connect to the College’s network.

If a computer cannot meet the minimum requirements as described in this document, the user can make use of one or more of the mitigation techniques described in this document. These mitigation techniques are provided as alternatives to patching/upgrading an insecure computer that cannot meet the minimums. These mitigation techniques can help to secure systems that fall into this category.

Threats to the security of our networked computers continue to grow in number and to evolve in form. Therefore, the LSA security policies will continue to be updated as new threats are identified and as superior countermeasures are developed. The most recent version of the LSA Security Policies will be available on the LSAIT Security Web page at: http://www.lsa.umich.edu/lsait/admin/security.asp.
Patching of Computers

LSA’s intent in the first iteration of our computer security effort has been to identify vulnerable computers and patch them before they are compromised by a malicious program. Monthly vulnerability scans are conducted by the LSAIT Security Administrators using eEye Retina scanners. The scans are run against all computers (about 7,500 systems) located in LSA. These scans search for vulnerabilities across multiple operating systems.

These scans start on the 1st calendar day of each month and conclude approximately on the 10th. It is important to note that this scanner is not 100% accurate and false positives occasionally occur. The final decision to identify a system as vulnerable requires careful review by a LSA Security Administrator.

Upon reviewing the “scan reports”, a Security Administrator will notify IT staff within the units of vulnerable computers. The Security Administrators will work directly with the unit IT staff or the LSA Computer Service Group (CSG) to provide one grace request for the patching of the computer. When a system is verified as patched by the unit IT staff or LSA CSG, the computer will be removed from the list of vulnerable computers.

LSAIT will block network access to any system that shows the same vulnerability for two successive scans. If the computer is not patched, the Security Administrator has the authority to have the computer disconnected from the campus network.

Any computer that appears to be manipulating the scanning process to gain intermittent, insecure access to the network or avoid upgrade/patch installation will be removed from the network by the Security Administrator.

Some computers may not be capable of being patched due to specialized equipment or application software that may become inoperable due to the patching procedure. In these cases, an alternate remedy should be used to protect the computer and the department network to which it is connected. The Security Administrator will assist to determine an alternate solution. To date, alternative working solutions have been found for most of these unique circumstances. See the “Mitigation Techniques” and “Appeals” section for additional information.
Minimum Versions of Operating System (OS) and Applications

The purpose of minimum (OS) versions is to establish a baseline for computer security across the college. With the increasing threat of computer attacks across the Internet, only the most recent versions of computer operating systems and applications are robust enough to provide protection for user account credentials and institutional data.

All computers in the college that connect to the network are scanned for the version level of their operating systems (OS) and those services/applications running on them. If a computer is not upgraded to the minimum version level after being identified as below minimum in two successive scans, then it becomes a candidate for removal from the campus network. The minimum versions listed here will be evaluated yearly and revised as necessary. **Units and users will have a minimum of 6 months of notification before a new minimum version level is changed.**

LSAIT will block network access to any system that shows the same vulnerability for two successive scans. If the computer is not upgraded, the Security Administrator has the authority to have the computer disconnected from the campus network.

Any computer that appears to be manipulating the scanning process to gain intermittent, insecure access to the network or avoid upgrade/patch installation will be removed from the network by the Security Administrator.

Some computers may not be able to be upgraded to the minimum version levels due to specialized equipment or application software that may become inoperable if upgraded. In these cases, an alternate remedy should be deployed to protect the computer. The Security Administrator will assist to determine an alternate solution. To date, an alternate working solution was found for most of these unique circumstances. See the “Mitigation Techniques” and “Appeals” section for additional information.
Minimum Operating System List

The table below outlines the minimum Operating System levels for the most popular computing platforms used by the College of LSA as of May 1st, 2006.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Minimum Client Level</th>
<th>Minimum Server Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>XP SP2 (w/current patches)</td>
<td>2003 SP1 (w/current patches)</td>
</tr>
<tr>
<td>Macintosh</td>
<td>OSX 10.4.11 “Tiger” (w/current patches)</td>
<td>OSX 10.4.11 “Tiger” (w/current patches)</td>
</tr>
<tr>
<td>Linux – Red Hat</td>
<td>RHEL 3 (w/ current patches)</td>
<td>RHEL 3 (w/ current patches)</td>
</tr>
<tr>
<td>Linux – SuSe</td>
<td>10.0 (w/current patches)</td>
<td>10.0 (w/current patches)</td>
</tr>
<tr>
<td>Solaris (Sun systems)</td>
<td>8.0 (w/current patches)</td>
<td>8.0 (w/current patches)</td>
</tr>
<tr>
<td>Unsupported Operating</td>
<td>One of the two most recent releases (w/current patches)</td>
<td>One of the two most recent releases (w/current patches)</td>
</tr>
<tr>
<td>Systems**</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* These systems are not directly supported by LSA Information Technology
** Operating Systems that are not supported by LSA Information Technology are not exempt from LSAIT security policy. Users of these systems should contact the LSAIT Security Administrators.
Minimum Versions of Services, Applications, or Daemons

The table below outlines the minimum version level for the most troublesome services/applications that are deployed on college computers as of May 1st, 2006.

<table>
<thead>
<tr>
<th>Application/Service Software</th>
<th>Minimum Version/Patch Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>Version 2.0 (w/current patches)(^1)</td>
</tr>
<tr>
<td>MaxDB</td>
<td>7.3.0 Build 25</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>Version 6.0 (w/current patches)</td>
</tr>
<tr>
<td>Microsoft SQL</td>
<td>Version 2000 SP3a (w/current patches)</td>
</tr>
<tr>
<td>MySQL</td>
<td>Version 3.23 OR 4.0</td>
</tr>
<tr>
<td>Oracle (Database)</td>
<td>9.2.0.x or 10.1.0.x (w/current patches)</td>
</tr>
<tr>
<td>Postfix</td>
<td>2.x</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Version 8.0.3.x/7.02003.x</td>
</tr>
<tr>
<td>Samba</td>
<td>Version 2.2.12 or 3.0.14a (w/current patches)</td>
</tr>
<tr>
<td>Sendmail (Mail Server/Daemon)</td>
<td>Version 8.12.10 for Solaris 8</td>
</tr>
<tr>
<td>SSH</td>
<td>Version 2.0 Protocol or better</td>
</tr>
<tr>
<td>Veritas Backup Exec</td>
<td>Version 9.1 or 10.0.5484 with Hotfix 24 (w/current patches)</td>
</tr>
</tbody>
</table>

\(^1\) 1.3.x if required for certain web applications but the Systems Administrator should review the configuration for known vulnerabilities.
Services and Applications that will be identified and reviewed by the Security Administrator(s)

The following list of applications and services pose a high level of security risk to the college if installed incorrectly, or if protective measures (e.g. firewalls) are not implemented as part of the installation.

- Cleartext FTP
- Cleartext Telnet
- Sendmail (as a Mail Server or Daemon)
- Samba
- Apache
- Microsoft IIS
- Microsoft SQL
- Oracle
- MaxDB
- PostgresSQL
- Any service that uses the SunRPC protocol
- Peer-to-Peer file sharing software (e.g. Napster, Kazaa, BitTorrent, emule, etc.)
- Google Desktop Search (Engine)

LSAIT will scan for computers running these services or applications. If a system is identified as running one of these high risk applications, a Security Administrator in collaboration with the local unit IT staff will conduct a risk analysis on that computer. The risk analysis will look at the technical configuration and threat level to the college network. The security administrator will approve these high risk applications provided the system is properly configured, managed, and secured. Alternatively, the Security Administrator can stipulate that the high risk application be disabled entirely or be moved to a production server in LSAIT or ITCS.

The mitigation techniques and appeals process described in this document also applies to these applications on LSA computers.
Mitigation Techniques

If a computer cannot be patched or upgraded due to special circumstances then one or more of the following mitigation techniques should be employed by the computer owner or department computer support person in conjunction with the LSAIT Security Administrators to secure the computer. The goal of these mitigation techniques is to achieve compliance and secure the computer thru alternative means to patching or upgrading the computer. LSAIT’s Security Administrators can be reached at lsa.it.security.admins@umich.edu.

Removal from Network
The quickest way to secure a computer is to simply remove it from the network by disconnecting the network cable. This prevents any attacker who does not have physical access to the computer from being able to access and/or compromise it. This may actually be a good choice for users who are working with extremely sensitive data and are concerned with confidentiality.

Hardware Firewall
Hardware firewalls work by allowing only specified communications to reach the computer(s) behind the firewall. This option is fairly easy to implement and can protect multiple computers. Hardware firewall devices (e.g. Linksys) must be purchased. The cost is generally less than $100 per firewall. Departments are expected to cover the cost of the hardware firewalls. Funds from the Faculty Computing Upgrade Program (FCUP) or other departmental resources can be used to cover this expense. In any case, LSAIT will work collaboratively with the local unit to purchase firewall devices.

Software Firewall
Software firewalls work in a similar way to hardware firewalls but only work for a single machine. They have the advantage of being (generally) free but they may not be available for all operating systems. There may also be a significant amount of overhead in configuring and maintaining the software for the computer professional supporting the machine. A software firewall may require installing 3rd party software or configuring technologies included in the OS.

Non-Routable VLAN
A VLAN (Virtual Local Area Network) is a segregated section of the network. The machine remains on the network but is not immediately visible to outside network traffic. Machines on the same VLAN are free to communicate to each other but all communication emanating from the VLAN must pass through a gateway machine. If the computers that need mitigation and need to communicate with one another are also in the same room, a small switch that is not connected to the LSA network can provide this service in lieu of a full-service VLAN. If it is determined that a non-routable VLAN is the best mitigation technique, LSAIT will have to be involved in evaluation, design and deployment of the VLAN to ensure compliance with the College network.
Appeals Process

Given our experience with the first iteration of our computer security effort and the mandatory patching of computers across the college, we anticipate very few circumstances that will require use of the appeals process. To date, the LSA Security Administrators (through collaboration with the unit) have been very successful at finding workarounds to unusual computer configurations where patching or upgrading may not be possible. The Security Administrators are sensitive to the functionality of specific research, scientific and instructional computer configurations in the college. Every effort is always made to accommodate instruction and research computing while balancing the need for safe computing and sound security practices.

However, if a workaround such as the mitigation techniques listed in this document are not found suitable for a specific technical reason (e.g. instrumentation connected to a computer that cannot meet the minimum requirements) then the user and their local IT representative should contact the LSAIT Security Administrators for assistance. The Security Administrators can be reached at lsa.it.security.admins@umich.edu.

If the Security Administrator, local IT professional and user are unable to agree upon a proper mitigation technique or workaround, then these individuals should present the specifics about the situation to the LSAIT Security Committee (lsa.it.security.committee@umich.edu). This advisory committee includes faculty members, Key Administrators, and college IT staff. The committee will review the needs of the user and all of the technical details of the situation and make a recommendation to the Dean. The Dean will make the final decision on exceptions to the LSA security policy.

In its review, the LSA IT Security Committee will assess the security risk to the University and will involve the U-M Information Technology Security Services (ITSS) group when necessary. The goal of the committee is to ensure that computer systems meet requirements set forth in the Standard Practice Guide (SPG 601.07) and any applicable legal requirements. The committee is also expected to keep the business, academic and research needs of the College in mind when making a recommendation to the Dean.

Any exceptions to the security minimums must be approved by the Dean and will require written documentation to ensure complete understanding and compliance by all parties. This “exemption agreement” will ask that the user accept full responsibility for supporting the machine(s) in question and acknowledging the risk(s) inherent in going outside these compliance guidelines.
Appendix A: Announcement of the Security Initiative for LSA

From: Francis, Anthony [mailto:afrancis@umich.edu]
Sent: Friday, July 29, 2005 11:18 PM
To: lsa.dept.chairs@umich.edu
Subject: LSA computer security concerns

To: Faculty and staff in the College of LSA
From: Rick Francis, Bob Johnston

As we all know, computers and information technology equipment have become integral components of our personal and professional lives. The security of these systems is of vital importance to all of us. The interconnection of modern high speed networks and the internet brings great benefits in collaboration and work efficiency. Unfortunately, these same computers and networks, if unsecured, pose a risk to all of us. Almost every day the news reports cases of malicious computer viruses, worms, denial of service attacks, stolen identities, etc. One unsecured machine, if attacked and compromised, can cause catastrophic problems to our networks, our individual computers, and the valuable work that is stored on them all.

This summer, the College has asked LSAIT to scan the College network to identify insecure, or outdated, systems that increase the vulnerability of our network. This action is in compliance with the University’s Standard Practice Guide which reads, in part, “To ensure the existence of this information resource environment, members of the University community will take actions, in concert with State and Federal agencies and other interested parties, to identify and set up technical and procedural mechanisms to make the information technology environment at the University of Michigan and its internal and external networks resistant to disruption.” (SPG 601.07)

The monthly LSAIT security scan of the entire college network identifies machines that are running old operating systems with inherent vulnerabilities, or newer operating systems that have not been kept current with their security updates or configurations. If compromised, these machines can pose a serious security risk to their users and, potentially, all of the other computers on our networks. Over the course of the summer and into the early fall, LSAIT will use the scan data to identify potentially vulnerable computers and to work with local computer support staff to correct the vulnerabilities. In the majority of cases the changes are relatively minor and involve upgrading or patching the operating system of the computer. Funds that are provided to units through the Faculty Computer Upgrade Program should be used to replace or upgrade any faculty computers that may be too old to run the operating system that meets our security standards. Staff computers will be centrally covered by the Staff Computer Upgrade Program.
Machines that are not or cannot be made compliant with the security standards by October 31, 2005, will be prevented from connecting to the College network. LSAIT will work with the units’ local computer support (either departmental or provided centrally by LSAIT Computer Support Group (CSG)) to meet these standards.

Our computer security posture will have to evolve as systems and threats develop. To ensure that our computer security posture stays current, we are planning to institute standards that will specify the minimum level of the various operating systems (OS) that the College supports for all computers that are connected to the College network. IT staff across the college are currently discussing these minimum standards with your staff and faculty. We welcome your input on this next step of the development of our computer security policy.

We ask that you assist your computer support staff, and LSAIT, as they assess the vulnerabilities of our network and work to ensure that all of your computer systems are protected. We trust that you understand that this undertaking is necessary to protect the computing and network resources of the College and the University.

Anthony H. Francis  
Professor of Chemistry &  
Associate Dean for Budget, LSA

email: afrancis@umich.edu
chemistry - fax: (734) 936-9463
chemistry - tel: (734) 663-1125
Dean's Office - fax: (734) 764-2697
Dean's Office - tel: (734) 647-2224