

Network Security Task Force
New threats to campus technology
and
Recommendations for immediate action
1-Oct-2001

NSTF Members:

Dan deBeaubien, Director, IT/Distributed Computing Services

George Fox, Director, IT/Administrative Computing

Brenda Helminen, Director, IT/Telecommunications Engineering

Amy Hughes, Internal Auditor

Shawn Laemmrich, System Administrator, TTTC

Robert Landsparger, Sr. System Administrator/Manager, Civil and Env. Eng.

Section I: Executive Summary

It is imperative that Michigan Tech respond to the current national crisis and the recent dramatic increase in Internet attacks. To address these issues, IT has formed the Network Security Task Force (NSTF). IT asked the Security Subcommittee of the CAC and the MTU System Administration Council to participate by appointing representatives to the NSTF. This document is the result of this group's work.

The Network Security Task Force (NSTF) recommends that MTU take the following actions as soon as possible to reduce its vulnerability to major Internet threats.

MTU Information Technology should:

- 1) Screen all campus computers for security vulnerabilities and assist departmental staff with the removal of these vulnerabilities. Remove computers from the campus network that become threats to network stability.
- 2) Scan all campus email for viruses as recommended in the CAC security committee's newly drafted policy.
- 3) Install passive network monitors and access control systems to detect and prevent unauthorized access to campus computers.
- 4) Install a small number of central web servers for departments who cannot meet network security minimums.
- 5) Establish a computer and network security web site to disseminate security information, patches, etc.
- 6) Increase physical security of the EERC network operations center and the administrative computer center.
- 7) Review and/or tighten security on centralized campus systems such as Banner.

The implementation costs for these seven items are:

FY 2001-2002 Costs:	\$184,050
FY 2002-2003 Costs:	\$94,100
FY 2003-2004 (ongoing) Costs:	\$131,700

A detailed breakdown of these costs is in Appendix A.

This document consists of five sections: the executive summary, physical security, protection from Internet attacks, security of central campus resources, and the

appendices. It outlines a practical and prudent course to lessen MTU's exposure to vandalism, hackers, viruses and other Internet disruptions.

All of these steps act to reduce the security risks to campus technology, but they do not eliminate them. We can deter attacks by being prepared, but we cannot rely on deterrents to work exclusively. We need to be prepared for recovery.

To maintain a stable computing environment, it is becoming necessary to divert more resources to address security issues than in the past.

Raising the level of security on campus systems and the campus network will cause some temporary disruption in day-to-day activities.

All computers and network systems on campus will be affected by these technology and policy changes.

Section II: Physical Security

The primary concern with computer center physical access is the risk of vandalism or other damage to campus computer and network equipment. Damage to this equipment could cost millions of dollars and cause campus-wide technology service outages lasting weeks.

Physical access to the EERC network operations center (NOC) and to the Administration Building computer center has been restricted. New policies requiring ID badges and visitor registration have been written and distributed. A copy of the new access policies is in Appendix B.

Motion-detector-based alarm systems have been installed in the EERC NOC and will be armed, according to procedures posted in the NOC. Alarm response procedures are being reviewed with Public Safety.

Section III: Protection from Internet attacks, viruses, and hackers.

In recent months there has been a dramatic increase in the frequency and the virulence of email and network viruses. Computer and network security experts are predicting that this is a permanent change and are recommending that institutions upgrade their security practices in response. Michigan Tech has experienced several major outages and long periods of degraded network performance during such incidents.

There are three major components to addressing these types of security incidents:

- a) Centralized security scanning and review
- b) Centralized email virus scanning
- c) Passive network monitoring and intrusion detection

All three components are necessary to adequately lower MTU's vulnerability to common forms of attack and to provide for earlier detection and response to hackers. The implementation of these measures will require many procedural changes, new policies as well as significant personnel and financial resources.

Centralized security scanning is the act of giving every computer on our network a daily security "checkup", and giving some computers, such as our public web servers, special attention. IT will help department system administrators increase security, as needed, and will act to protect campus technology by restricting access to computers with security issues. IT will install a network access control system to control and monitor traffic to and from campus. IT will assist departments in resolving security vulnerabilities by providing web resources to patch vulnerable systems and by hosting web sites for departments that cannot meet minimal security standards.

Included in Appendix C is an interim procedure for security response measures.

The primary risks of continuing without central security scanning are:

- 1) Increasing number of major network and computer outages due to Internet attacks such as "Code Red", "Code Red II", and "Nimda". These outages have caused several 2-4 hour outages, during business hours. They have also caused major disruption to servers in many academic and administrative areas.
- 2) Loss, corruption and/or theft of campus computer data. Many of these viruses act not only to disrupt services, but also to remove or erase data and allow unauthorized access to the computers they infect. Once this access is gained, attackers have the ability to do with the infected system and its data as they wish.

Email virus scanning is a process where all email sent through a central 'hub' is scanned for email viruses. The major issues involved are:

- 1) All mail isn't sent through a central point today.
- 2) There will be some delay added to the campus mail delivery system due to the virus scanning process.
- 3) What to do with infected mail.

The Security Committee of the CAC, in conjunction with IT staff, has spent considerable time developing a document addressing these concerns. The draft document is included in Appendix D. It is the recommendation of the NSTF that the recommendations set forth in that document be implemented as soon as possible.

The risks of not scanning for email viruses are similar to those for not centrally scanning for other security vulnerabilities. They are:

- 1) Continued outages caused by email viruses such as “I Love You”, “Anna Kournikova”, “Sircam”, “World Trade Center” and many others.
- 2) Loss, corruption or theft of data (see above).

Passive network monitoring and intrusion detection is installing and operating a system designed to detect in-progress network and computer attacks such as hacker intrusions, denial of service attacks (DoS), ICMP storms, and other network anomalies. It also includes installing computer tripwires that set off alarms when would-be hackers attempt to gain access.

The primary risks of not deploying a monitoring and detection system are:

- 1) Delayed reaction to a new security event. Systems that can aid in detecting and responding to these events reduce the duration of the outage and limit the damage caused by the security breach. Michigan university campuses that were ill prepared for the Nimda virus suffered complete failure of their campus networks because they could not detect and clean up quickly.
- 2) Inability to detect highly destructive or brand new virus threats. These systems are the only effective means of handling viruses that exploit as-yet-unknown system vulnerabilities, or viruses that propagate slowly and do not cause noticeable network disruption during the infection phase.
- 3) Inability to detect attacks by more skilled hackers, directed at single computers on campus.

The implementation of these three systems replaces our current practice of each department establishing its own standards for security in favor of a uniform standard for all of campus. As such, it is important to address a few philosophies needed to guide this change. The overall security and stability of campus computers and networks need to come before the needs of a particular unit. When security issues arise, IT staff will contact department system administrators and their managers and/or department heads to discuss needed security measures in an attempt to balance campus security with departmental resource availability and priorities. Negotiations between central security staff and departmental administrators will work well while taking proactive security measures. However, IT will continue to act to preserve the stability of the core campus technology services as per the campus computer use policy and other telecommunications policies. During an active network incident, it is often necessary to take reactive measures first to contain a problem, followed by an explanation.

Section IV: Security of central campus resources

Securing the access to central campus resources such as administrative computing systems, centralized or large servers, and telecommunications equipment is a long-standing, well-known practice at our University. The reason that we have included it in

this document is that this area of security has the largest impact on the behavior and habits of the large numbers of users of these systems. Activities in this area include verifying who has access to the system, reviewing the access privileges each user has, and validating that access mechanisms, such as passwords, are secure.

Also, a secure campus password system should be implemented for use in web applications requiring authentication. These measures will increase the protection given to individuals' private data.

Section V: Appendices

Included in this section are:

Appendix A: Resource Requirements Breakdown

Appendix B: Physical Security Policy

Appendix C: Interim Security Response Procedure

Appendix D: Draft Five of MTU Email Virus Scanning Policy

Appendix A: Resource Requirements Breakdown

Security Area	FY01-02	FY02-03	FY03-04
Centralized Computer Security Screening	\$13,100	-	\$7,200
Central Email Virus Scanning	\$76,600	\$13,200	\$20,700
Passive Network Monitoring, Intrusion Detection, and Access Control	\$22,800	-	\$11,600
Web Hosting	\$26,600	-	\$9,700
Web Based Security Center	\$7,000	\$5,000	\$6,600
Staff Salary Support	\$27,500*	\$55,000	\$55,000
Staff Benefits	\$10,450*	\$20,900	\$20,900
Total	\$184,050	\$94,100	\$131,700

*These numbers are based on ½ salary and benefit costs for a FTE beginning in January, 2002.

Appendix B: Physical Security Policy

This policy is effective 24-Sep-2001.

Section 1: Physical Access to the EERC NOC.

All doors to the EERC NOC are to be kept closed and locked at all times, except when the following procedure is being followed:

If it is absolutely necessary to prop open the north door of the EERC NOC, then

- 1) CLOSE and LOCK the two doors near ETS between the main corridor and the rear hallway. Insert the 'Go to customer service signs' on the doors.
- 2) CLOSE and LOCK the door near Customer Service between the main corridor and the rear hallway. Insert the 'Go to customer service signs' on the door.
- 3) The rear (north) door to the NOC may now be temporarily propped open.

When finished, please re-open the doors, and remove the signs.

Customer service staff is expected to escort people into the back hallway during these times.

In emergency situations such as power or cooling failure, the Director(s) of Telcom Engineering, Distributed Computer Services, or their named designees may override these policies.

Section 2: Identification of EERC NOC staff and visitors.

Everyone in the EERC NOC must wear a badge.

All employees with EERC NOC access will be issued badges and are expected to wear these badges at all times in the NOC.

Guest badges are available. See Customer Service for information on obtaining a guest badge.

Customer service staff is expected to direct guests to either the Director(s) of Telcom Engineering, Distributed Computer Services, or their named designees.

Appendix C: Interim Security Response Procedure

Step 1: Establish security-scanning schedule.

It was established that every computer should be checked minimally once per day. Administrators of computers that are registered but unreachable for more than 2 weeks will be contacted.

Step 2: Establish severity of known security holes.

All security problems detected by the central scanning software will be broken into four categories.

Step 3: Respond to security vulnerabilities.

The following table was developed.

Severity Level	Severity Definition	Response
Low	Low level risk	Post info, ignore.
Medium	Somewhat obscure, exploitable but not common	Post info, notify*, limit access after one week if uncorrected.
High	Easy to exploit, highly visible, vulnerability is prone to attack.	Post info, notify*, limit access after 3 days (at 3:00 pm of third day).
Critical	Current security breach.	Limit access, notify*.

*Notification. Each department can designate up to three levels for notification. For example: Primary system administrator, entire system departmental computer support group, and department head. They would be notified as follows.

Severity Level	Primary Contact	Secondary Contact	Final Contact
Medium	+0 days warning of 1 week disconnection + all other messages	+2 days if not acknowledged, +4 days if not resolved	+6 days if not resolved
High	+0 days warning of 3 day disconnection + all other messages	+1 day if not acknowledged +2 day if not resolved	+2 day if not resolved
Critical	+0 day notice of disconnection	+0 day notice of disconnection	+0 day notice of disconnection

Appendix D: DRAFT FIVE of MTU Email Virus Scanning Policy

Use of email at Michigan Tech is one of the main forms of communication used by faculty, staff, and students. Protection of the email system from virus attacks is an integral part of helping to ensure that Michigan Tech keeps its email system productive and efficient. Components of effective virus protection include central and local scanning as well as user awareness.

Central Virus Scanning

All email originating from or destined for a Michigan Tech owned or operated server must go through the central Michigan Tech email system.

Any email message that is sent from or delivered to Michigan Tech's email system will automatically be scanned electronically for viruses.

An email message or its attachment(s) suspected of having a virus will have the following occur:

1. If the virus can be removed from the message: remove the virus, add a note to the message stating the action that was taken, and forward the message to the recipient.
2. If an attachment to the email has a virus which cannot be removed/cleaned: delete the attachment, add a note to the message stating the action that was taken, and forward the message to the recipient.
3. If the message still contains a virus: delete all but the message headers, add a note to the message stating the action that was taken, and forward the message to the recipient.
4. If the sender of the message is an @mtu.edu address: a note stating the action that was taken on the message is also sent to the sender. No notice will be sent to any other senders of email messages found to be carrying a suspected virus.

A virus scanning program will be used to scan for viruses contained in email messages. In addition to using a virus scanning program, other mechanisms may be used in an emergency to protect Michigan Tech systems from viruses.

Local Virus Scanning

It is highly recommended that virus scanning also be used at the department and desktop level.

User Awareness

Users play a role in virus protection by being aware of other avenues of contracting viruses, such as web pages and file sharing. Virus scanning cannot detect all viruses contained in email messages.

RECOMMENDATIONS

(NOTE: these are recommendations in support of the virus scanning policy, but are not part of the policy)

Virus scanning should commence immediately after final approval of this policy.

Scan incoming email messages once which will then be distributed via a listserv discussion list. Once the message has been scanned and found to be virus-free, all the copies of the same message going out will not need to be re-scanned. This is seen as a reduction in the overall time necessary to perform the scanning.

The time delay in delivery of the message created by the scanning process should be limited to several minutes.