Trusted Network and Host Security Management in the Context of the MSU Statement of Acceptable Use

11 April 2005 -- Draft endorsed by Network Communications Advisory Commmittee
Draft revised 19 April 2005 (changes only to 4th paragraph of the Purpose section)

Purpose of this document

New forms of security tools that operate in an "embedded" fashion, either on the network (e.g., at the router level) or within network-connected host computers, have become essential to the implementation of efficient and thorough network and host security. In the context of this document, "security" is used in its broadest sense, to include technologies intended to detect and control malicious network activity and running at the network router level, at the level of and in the form of network firewalls, and in host-based forms resident on servers and other equipment connected to the network. Because embedded security typically involves inspection of network data packets, packet-stream activity, or patterns of "user" activity on webservers, it could be interpreted to violate the user privacy protection provisions of the MSU Statement of Acceptable Use (SAU; http://www.msu.edu/au/). Because it is an effective tool in protecting the security of the network, and of systems and data connected to the network, it also is a key means for privacy protection itself.

Section V.1.4 of the SAU states:

> "The content of User files is not to be surreptitiously or otherwise examined, nor is the User-generated message content of User network transactions to be monitored, without the prior written permission of either the User involved or the Vice Provost for [Libraries,] Computing and Technology."

It is the intent of the Vice Provost for Libraries, Computing and Technology (VPLCT), as sanctioned by this provision of the SAU, to grant permission to University units to implement these forms of network and host security if they follow the guidelines described in this document. Security techniques should be implemented in ways that minimize the risks and potential for infringement of privacy or infringement of unimpeded information flows that are desired by users. This document describes measures for doing this, as well as the background principles involved.

This document has been reviewed and endorsed by the Network Communications Advisory Committee to the VPLCT on 11 April 2005, which also aided greatly in its development. It is being shared broadly in Spring 2005 to seek additional commentary from the broader MSU community. Any comments, questions or concerns regarding this document or any specific security implementation on a campus network, subnet or host computer should be directed to David Gift, VPLCT (353-0722; gift@msu.edu).

Foundational principles

MSU's data communication networks, at the institutional "backbone" level and at local "subnet" levels (collectively referred to here as "the network"), are institutional resources provided to facilitate the work and scholarship of MSU's students, faculty and staff (including extramural collaborations), and to facilitate appropriate public access to University information resources. The principles for operating data networks and host services connected to the networks at Michigan State University are embodied in the University's SAU. There are four fundamental principles in this regard:

1. **Honoring personal privacy.** Users should expect the highest possible level of personal privacy regarding their use of the network and connected services, and the content of the data they move across or store within the network and those services.

2. **Facilitating the unimpeded flow of information.** The core work of the University community is scholarship in its many forms -- research, creative endeavors, study, teaching, outreach and engagement -- and effective scholarship depends vitally on the unimpeded flow of ideas and information.

3. **Optimizing the utility of the network and its connected resources.** The network and its connected computing resources should work effectively for users. Users have come to rely on the network as a basic utility essential to their work and study, as fundamental as electrical power, lighting, telephones or clean water. At the same time, the network is a *shared, limited resource*. As with any shared, limited resource, the overall performance of the network can be seriously compromised by circumstances such as very large bandwidth consumption, or inappropriate (malicious) use by users or by machines connected to the network.

4. **Optimizing the security of data and systems on the network.** Data (much of which is confidential or sensitive) and systems connected to the network should be as secure and safe as possible from unintentional and intentional harm that might present across the network. One aspect of protecting personal privacy on the network (Principle #1) is that data, the systems on which it is stored and processed, and the network on which it is moved, are secure from unauthorized or inappropriate access and use. One aspect of protecting the utility of the network (Principle #3) is that the machines that operate the network itself or that are connected to the network are secure from unauthorized access, tampering or inappropriate use.

Growing importance of security to the other principles

Security measures implemented on the network and on host computers connected to the network are becoming increasingly important, even essential, to the protection of personal privacy, the protection of unimpeded data flows, and the protection of network and host utility. Members of the MSU community, and of the general public who use MSU data resources, have come to depend very heavily on the reliable performance of these systems to support their daily work and scholarship. At the same time, the

number, frequency and variety of malicious attacks that are occurring across networks, on campus and around the world, have increased to the point where they have now become absolutely common and routine. Malicious code is frequently designed to be self-replicating, spreading very efficiently across networks to infect multiple computers. Inappropriate network or host use behavior is no longer under the total control of human users. The user of an infected machine may be quite unaware that their machine is infected, and they need to take no action of their own to cause or permit the computer infection to spread to other machines or to cause their own machine to behave inappropriately. The network is now a critical production worktool, but simultaneously has become a quite treacherous environment, and the costs of network or host failure have become very material.

The challenge: balancing security implementation with privacy and unimpeded data flows

At the time of this writing, the most effective tools to use to better secure the network and the data and machines connected to it, and to best assure the utility of the network and its connected resources, use methods that also may infringe or be perceived to infringe, to some degree, privacy and the unimpeded flow of data. An example of this familiar to most computer users is virus-scanning of email. This involves a computer program that searches through every email message and attachment file looking for any of a large number of "signatures", or data bit patterns, of malicious code; when such patterns are found in the email content, the email message is "filtered" in some way: discarded, or quarantined to a separate storage location, or "sanitized" to remove the offensive code. Strictly speaking, the inspection of email and attachment content for malicious code signatures is an invasion of privacy, involving, as it does, "deep packet inspection" or the inspection of the contents of network data packets or transferred data files. Filtering of email also may impede the flow of information, especially if the detected malicious code signature is a false-positive (i.e., non-malicious code that just happens to have the same bit string that constitutes a malicious-code signature, causing a legitimate piece of email to be destroyed, redirected or altered).

To make matters more challenging, some network attacks involve code that is not inherently malicious, but rather may be recognized by the pattern of network activity at the packet level (packets carry data on networks) or at the level of "typical user behavior" of a network or host service. An example of this type of attack is a "denial-of-service" attack where a network server is intentionally swamped by a deluge of packets aimed at it simultaneously from other machines. Another example is a "dictionary" attack in which a hacker attempts multiple unauthorized log-ins to a system by repetitively guessing at user identities and passwords by systematically working through permutations of alphanumeric patterns. Today, effective control of these forms of malicious activity must be done inside the network, usually inside of or at the location of routers and switches ("network-embedded" techniques), or at the level of machines that host network-connected services (web servers, for example). Embedded techniques at the network and host levels affect very broad classes and numbers of users, making deployment of these security measures a weighty matter.

Because of the proliferation and prevalence of malicious activity, most users today have indicated a willingness to be subject to a certain degree of potential privacy or information flow infringement in exchange for the enhancement of security and utility of the network and of their own data and computing resources attached to it. The means by which security management is implemented are important; for example, email users probably are comforted knowing that virus scanning is being done by an algorithm running on a machine ("robotic inspection") and not by a person, and that the machine is using a set of rules from a trusted third party for identifying known viruses and malicious code.

Implementing "trusted" security

Security should be implemented in a way that is trusted by users, striking the best balance between security, privacy and unimpeded information flows. There are no technical means by which to define "trusted security", so perhaps the best way to describe it is to say what it is not, and to do that in human terms: **The purposes of security management are to make the network more secure and more reliable while respecting the personal privacy of users as well as their ability to access and move information in desired ways. Thus, no "security" measures should be taken that would cause an informed user to doubt or distrust the motives or intentions of the security managers.**

Network or host security may be implemented on MSU networks pursuant to the following guidelines, intended to enhance the level of user trust while allowing for effective security implementation:

1. **Address only malicious activity; do not use security technology for inappropriate control or manipulation of communications.**

    1.1. **Prefer robotic inspection**. Screening and processing of network data flows or of user activity data on host computers should be done principally by machines executing strict security algorithms. User data should only be subject to human inspection to determine when a pattern of malicious activity that machines have flagged as malicious requires human intervention to manage, or represents safe network traffic or host user activity that should be allowed. Every reasonable means should be taken to avoid opportunities or attempts to ascribe meaning to filtered communications, other than to identify and manage malicious intent activity.

    1.2. **Prefer use of security rules from trusted third-party sources**, for example, vendors that specialize in security tools, or organizations such as SANS (www.sans.org) and US-CERT (www.cert.org). Circumstances can arise in which the security rules needed to control an outbreak of malicious activity are not available from 3rd-party sources, in a timely manner or perhaps at all. In these circumstances, locally-generated rules or locally-controlled actions, which may include non-robotic actions (i.e.,

"hand work" by network managers), may be necessary to secure the network or a host machine.

1.3. **Deploy any extraordinary security means only for the limited time necessary to control the malicious outbreak.** From time to time an outbreak of malicious activity may require particularly aggressive security management techniques (i.e., measures not usually in place and which go beyond what would normally be done to protect the network or host machine). Any such technique should be employed judiciously and for as short a time as possible. Once the security threat intended to be managed by such extraordinary means abates, the means also should be terminated if no further material threat is anticipated.

1.4. **Consider configuring security management mechanisms so that malicious activity from user machines is blocked, but authorized users may continue to conduct appropriate uses, as an alternative to blocking access to machines originating malicious activity.** Authorized users may operate machines that become unintentionally infected. If the malicious activity generated by these machines can be controlled without disconnecting the machines from the network or from host services, disconnection may be avoided so that the users may continue to conduct normal, authorized network or host use while measures are taken to correct the problems with their machines. Network or host administrators retain the right to block access of an offending machine as a means of implementing security and utility management. (This item provides an updated interpretation of SAU section 1.3, but only in the context of this exception for security implementation.)

2. Avoid or minimize logging or storage of user content or activity data, and minimize any potential risk of exposure of such data.

2.1. If logging or storage is necessary, appropriate controls should be placed on access to any stored data to minimize the number of people who have access to it and to limit access to only those who have a need to know in regard to the stored data.

2.2. Every reasonable means should be taken to minimize and restrict the:

- number of people who may have opportunity to review user data for these purposes;
- amount of data so exposed;
- number of places such data may be stored;
- time interval over which the data may be stored or exposed;
- use of data which provide or imply personal identities.

3. **Notify users in advance and in an easy-to-access manner if/that their network or host system use is subject to security protocols.**

    3.1. Document in general terms the purposes and likely effects (both the intended good effects and the potential adverse effects on users) of the security protocols, and how user privacy will be protected. Inform users in advance if materially new and different techniques are to be implemented that may affect their use of the network or systems.

    3.2. Provide a mechanism for hearing and dealing with user complaints or concerns when a user feels that their expectations for privacy or unimpeded flow of information have been improperly infringed.

        3.2.1. If any user feels that their complaint has not been appropriately addressed at the level of network or local host system management or administration at which it initially applied, they may make an appeal to the Vice Provost for Libraries, Computing and Technology, who will act as the final arbiter in the matter.

    3.3. Give due consideration to feasible alternatives for users who find the security protocols to unduly restrict their work

4. **Mitigate false-positive decisions or overly-restrictive limitations of the security protocol.** If it is found that a particular security rule or technique causes unacceptably high false-positive rates or limitations on network or host activity which overly constrain the ability of users to do their work, give due consideration to elimination of use of that rule or technique.