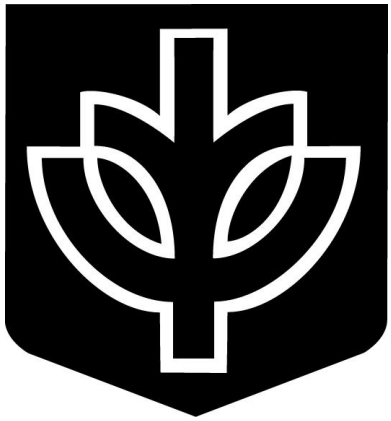
NETWORK CONNECTIVITY SUSPENSION POLICIES AND PROCEDURES



Information Security Team
DePaul University
1 East Jackson Boulevard
Chicago, Illinois 60604 US
https://infosec.depaul.edu/

13th December 2002

Copyright Notice

Contents

1 Summary

Network connectivity is provided to students, faculty and staff at DePaul University to perform a large variety of tasks ranging from academic research to business communication. This connectivity is generally provided through connections to networks which, in turn, are connected to the Internet. Such connectivity makes any host connected vulnerable to attack from many vectors.

Limiting the spread of compromised systems often involves removing a host from the network for analysis and reloading. This process works well for a central computing center with adequate system personnel, but does not scale well to a distributed campus environment. Making the matter more difficult is the lack of updated contact information for the responsible party of each host on the network.

The Information Security Team has developed the policies and procedures in this document to assist in maintaining the integrity and survivability of the DePaul University network, in part and whole. These means will be used to establish contact with the responsible party of a compromised end-host and assist in incident response and recovery when required.

2 Triggers for Suspension

The DePaul University Information Security Team maintains a philosophy that end-user privacy is paramount to monitoring and compliance regulations. Because of this philosophy, we rely heavily on the reports from external sources regarding copyright infringement or illegal content. Our analysis of communications focuses on anomalies and known attack signatures. These types of triggers for network suspension are detailed in the following sections.

2.1 Limiting the Spread of Network Attacks

If a host is acting as an agent in the distribution or spread of a computer virus, worm, denial of service attack or other distributed remote atttacks, the host will be subject to the suspension procedures in this policy. An owner of the host may be liable for the actions of this host and any damages incurred as a result.

2.2 Copyright Infringement

INFOSEC does not actively attempt to discover materials violating either the "Copyright Act of 1976" or the "Digital Millenium Copyright Act." INFOSEC does not scan networks, nor analyze end-hosts or communication, looking for violations. When a report is made regarding the violation of copyrighted material, we will act according to United States Code Title 17, Chapter 5, Section 512 [1] which states (in regards to violating material) that a service provider will "upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material." As a service provider to the Internet the University must fully support this, and other, applicable laws of usage.

2.3 Misuse

2.3.1 Unauthorized Access or Attempted Access

The attempts to knowingly or unknowingly use a computer, network or any components thereof on the DePaul University network to gain further unauthorized use of University or external systems will be subject to the suspension procedures outlined in this policy, *regardless of intent*. Unauthorized access or attempted access may further be subject to investigation and procecution under various elements of United States Code 18, including Chapter 47 Section 1030 titled "Fraud and related activity in connection with computers." [2]

To promote research and development of new security technologies, INFOSEC *strongly recommends* that controlled test networks and computer systems be developed for student, faculty and staff use. Test environments should be built under specific permission from the University, and in no means should be connected to the DePaul University network or Internet.

2.3.2 Illegal Material, Including Child Pornography

Network connectivity will be immediately suspended upon the report that an end-user is transmitting, storing or caching illegal material, including child pornography. All applicable local, state, federal and international laws will be honored by INFOSEC in protection of the University.

2.3.3 Other Violations and Misuse

Any other violations not directly listed in this document are subject to suspension based on the violation of applicable University policies and local, state, federal and international law.

3 Network Suspension Procedures

The following procedures will be implemented at the recommendation of the Information Security Team when discovering new threats or vulnerabilities that have been introduced to the network. These procedures are intended to contain any immediate threat to the network or surrounding hosts and should be followed by a proper chain of incident response.

3.1 Students

Any incident involving a student owned or University leased personal computer may involve the following procedures.

1. The incident will be verified by the Information Security Team, and all steps will be taken to identify the host, user and vulnerability that is present.

2. The information regarding the incident will be logged into a database strictly for use by INFOSEC.

3. In the event that the incident involves copyright violations or inappropriate use, INFOSEC will contact the Dean of Students office through the use of a digitally signed email. All information regarding the incident shall be submitted to the Dean of Students. The Dean of Students office should verify the message is valid through the use of digital verification of the signature. This message *should* only be honored if it is signed by the Information Security Team, or by a trusted key signed by the Information Security Team's signing key.

4. The Networks and Telecom group will be contacted via a digitally signed email requesting suspension of network connectivity and services. The Networks and Telecom group *should* verify the digital signature to be from the Information Security Team, or a trusted key signed by the Information Security Team's signing key.

5. An appropriate entry will be made into a database accessible to Customer Technology Services (CTS). This database will include the IP address, MAC address, user information and reason for suspension.

6. The host should be cleaned up in the following manner.

   (a) If the host is leased by DePaul University, CTS will contact the DePaul Depot to reinstall the operating system. We strongly recommend that a bit-stream backup be made of the hard drive prior to reinstalling. This backup should be submitted to INFOSEC for further analysis.

   (b) If the host is owned by the student, CTS will contact the student to inform them of the situation and outline any steps required to recover. INFOSEC strongly recommends that a bit-stream backup be made of the hard drive for further analysis by INFOSEC. The student *should* be advised on this course of action.

7. The Dean of Students office, CTS or DePaul Depot will contact INFOSEC advising that the host has been properly secured.

8. INFOSEC will contact Networks and Telecom to restore network connectivity.

3.2 Faculty and Staff

Incidents involving a University owned *or* a personal computer owned by an individual faculty or staff member shall be subject to the following suspension procedures.

1. The incident will be verified by the Information Security Team, and all steps will be taken to identify the host, user and vulnerability that is present.

2. The information regarding the incident will be logged into a database strictly for use by INFOSEC.

3. In the event that the incident involves copyright infringement or other inappropriate use:

   (a) INFOSEC will send a digitally signed email to notify the area manager or faculty member of the violation or inappropriate use. If these entities are not available or do not respond in a timely manner, INFOSEC will contact the department Director or Academic Dean responsible for overseeing the respective area. A grace period of forty-eight (48) hours will be allowed for the individual to respond and outline an action compliant with INFOSEC requirements for mitigating the problem.

   (b) If the timeline is not met, Networks and Telecom will be notified through a digitally signed electronic mail message requesting suspension of connectivity. The Networks and Telecom group *should* verify the digital signature to be from the Information Security Team, or a trusted key signed by the Information Security Team's signing key.

4. An appropriate entry will be made into a database accessible to Customer Technology Services (CTS). This database will include the IP address, MAC address, user information and reason for suspension.

5. Copyright infringement and inappropriate use manners should follow normal inter-department disciplinary actions. Once the matter has been addressed, the manager, faculty or staff member should notify INFOSEC.

6. The host should be cleaned up in the following manner.

   (a) If the host is leased by DePaul University, CTS will contact the DePaul Depot to reinstall the operating system. We strongly recommend that a bitstream backup be made of the hard drive prior to reinstalling. This backup should be submitted to INFOSEC for further analysis.

(b) If the host is owned by the faculty or staff member, CTS will contact them appropriately regarding the situation and outline any steps required to recover. INFOSEC strongly recommends that a bit-stream backup be made of the hard drive for further analysis by INFOSEC. The individual *should* be advised on this course of action.

7. CTS, or the DePaul Depot, will contact INFOSEC when the host has been properly rebuilt and secured.

8. INFOSEC will contact Networks and Telecom to restore network connectivity.

4 Report Archiving

The information pertaining to network suspension is archived by the Information Security Team. Upon written request by University executives or INFOSEC management, this information will be fully disclosed to those individuals. The following information may be archived by INFOSEC.

1. Summary and technical analysis of the behavior leading to network suspension.
2. Victim name, email address and telephone number.
3. Offenders name, email address and telephone number.
4. IP address, MAC address and location of host requiring suspension.

INFOSEC reserves the right to use the information regarding network suspensions, *and the pertinent behavior leading to such suspension*, to document incident trends related to computer and information security. Neither victims nor offending parties shall be named directly *or* indirectly when performing trend analysis and generating reports.

References

[1] Title 17, Chapter 5, Section 512, *United States Code*
United States House of Representatives, 1947, (rev. 1998)

[2] Title 18, Part I, Chapter 47, Section 1030, *United States Code*
United States House of Representatives, 1948, (rev. 1970)