

# KEEPING AN EDUCATIONAL NETWORK HEALTHY: DIFFERENTIATING MALICIOUS AND NAÏVE STUDENTS ON AN EDUCATIONAL NETWORK ENVIRONMENT

Cesar A. Monroy  
Computer Science and Engineering  
Mississippi State University  
Mississippi State, MS 39762

Dr. Ray Vaughn  
Computer Science and Engineering  
Mississippi State University  
Mississippi State, MS 39762

*Abstract - Many information security officers or network system administrators at universities and colleges face the problem of not knowing when students are utilizing the campus network in ways that can affect the image of the university or even cause monetary losses. Improper use of the network could either be willful and maliciously done or perhaps just naïve students unaware of viruses on their computers or the dangers posed by P2P networking software. The quick identification of these students is of great benefit for both the university and the students. The author will focus this paper on a Quarantine method implemented by at Mississippi State University to reduce or eliminate the stated problem.*

**Keywords: Quarantine, network security, security policy, security management.**

## 1.0 Introduction

The use of a university's computer network has changed dramatically over time. According to V. E. Rezmierski, M. R. Seese, and N. St. Clair II, within the past few years, colleges and universities have moved from dependency on mainframes, where data protection and management tasks were managed centrally, to distributed computing network systems [13]. W. Klein lists areas of network management that are of concern to campus network administrators. Two that are within the scope of this paper are: Operational status-What is the current state of the network's "health"? and Problem Handling- What process is followed when a problem is detected? [14].

College and university computer networks went from being used mainly for educational purposes to exchanging copyrighted materials such as music, games and movies, playing networked games, and performing illegal activities such as stealing personal data by hacking into university servers. Sometimes it is necessary to isolate a computer from a campus network in order to protect the health of the network and at times protect the integrity of the university or even the students.

Maintaining a healthy network should not only be a concern of a network administrator or information security officer but also of the students. According to G. Spafford most people are not too concerned with Information Security [5]. Students using the network improperly can be categorized as Malicious Students or Naïve Students.

Malicious students are students that use their technical knowledge to setup servers to share copyrighted material, hack in university servers, or intentionally affect the health of the campus computer network by spreading viruses, worms, spyware and other types of malware.

Naïve Students are students that are not aware of the problems that a computer infected with a virus may have on the health of the campus network, have antivirus software with old virus definitions, play network games on the campus network, or download pirated software, music, movies without an understanding of the consequences of the law.

## **2.0 Background**

### **2.1 Cases**

Since the early 80's university and college network systems have been affected adversely by students. In 1983, Kevin Mitnick was arrested at University of Southern California for trying to use a university computer to gain illegal access to the ARPAnet. He was discovered sitting at a computer in a campus terminal room, breaking into a Pentagon computer over the ARPAnet, and was sentenced to six months in a juvenile prison [3]. One of the first major cases was in 1988, the Morris Worm. It was created by Robert T. Morris, Jr., a graduate student at Cornell University. He launched a self-replicating worm that got out of hand and spread to networked computers, clogging government and university systems [8].

In a study performed by C. Wong, C. Wang, D. Song, S. Bielski, and G. R. Ganger of real network traces from a campus computing network, they discovered that there exist reasonable rate limits for an enterprise network that would severely restrict the spread of a worm but would have negligible impact on almost all legitimate traffic. Their study shows the effect that a quarantine process has on Internet worms and the health of the campus network [1].

Christopher Andrew Phillips a former University of Texas student was sentenced for hacking the computer system at the University of Texas [4]. At George Mason University, network administrators anxious to protect the school's computer network from a raft of viruses and worms plaguing the Internet, unplugged thousands of students from the network [15]. Many other network security cases that occurred on a campus network can be found at <http://www.crime-research.org>.

### **2.2 The law**

An important issue that should be addressed when implementing the quarantine process in an educational network environment is the Family Educational Rights and Privacy Act (FERPA) [12]. It is very important to differentiate the use of the quarantine process from monitoring the network for health purposes and monitoring the network for the content being transmitted (what the students are viewing). According to V. E. Rezmierski, M. R. Seese, and N. St. Clair II researchers at the University of Michigan designed and implemented a study entitled: The Logging and Monitoring Privacy Project (LAMP) to understand the nature of system administrators' security-related activities, the data being collected, the systems on which logging is being done, and the nature of training these administrators have received [13].

The student awareness of The Copyright Act (17 U.S.C. § 106) [2] is a very important factor in the health of a campus network. According to the Software and Information Industry Association (SIIA), Internet piracy is growing at an exponential rate. SIIA's investigations have

revealed a large portion of this activity is attributable to college students. Hiding behind the presumed veil of their campus network, students log on to unlawfully reproduce and distribute copyrighted material valued at millions of dollars. However, as the students are often using a university-owned network or computers, they are placing the university in a position of liability as well [10].

SIIA has resolved numerous cases of this form of piracy in cooperation with college officials. For example, in the matter of Andrews University in Berrien Springs, Michigan, university network administrators noticed unusual activity on the campus network. Upon tracing the source activity, two students were identified and implicated in the piracy [10].

### **3.0 Addressing the problem**

#### **3.1 Quarantine**

The quarantine process is being implemented across many different organizations in varying ways using hardware and or software. New technologies are being developed that perform similar to the quarantine process implementation at this University. Microsoft Corporation provides a tool with Microsoft Server 2003 called Network Access Quarantine control that delays normal remote access to a private network until the configuration of the remote access computer has been examined and validated by an administrator-provided script.

Microsoft is also developing a software tool that is called Network Access Protection that will be part of Windows Longhorn and Windows Vista. According to the developers, it is designed to help administrators maintain the health of the computers on the network, which in turns helps maintain the network's overall integrity [7].

Alcatel is another vendor that is jumping into the quarantine revolution and joining Microsoft Corporation. Alcatel's technology works in conjunction with Network access Protection by controlling network access and automatically quarantining intruders through its new Access Guardian feature set and the Alcatel OmniVista 2770 Quarantine Manager[6].

#### **3.2 Campus Quarantine**

A process called Network Quarantine has been implemented at the Mississippi State University to maintain the health of the campus network by isolating problematic computers and identifying their users until the problems have been fixed. This could be when a networked computer is used to conduct activities that violate University policy; or when a computer is generating high network traffic that may affect the performance of the campus network.

According to Mr. Thomas Ritter, the University's Information Security Officer, the quarantine process uses a software "Captive Portal" application that randomly scans the campus network for different types of network packets and anomalous amount of network traffic generated. When specified packets are detected, a log file is created and sent to the network administrator or information security officer for further investigation and possible placement in quarantine.

According to Wikipedia, a captive portal technique forces an HTTP client on a network to see a special web page (usually for authentication purposes) before surfing the Internet normally. This is done by intercepting all HTTP traffic, regardless of address, until the user is

allowed to exit the portal [16]. This happens when the computer is placed in quarantine so that information can be gathered on the user of the computer.

When the quarantine software evaluates the Cisco Netflow data logs, a log file is created that looks as follows:

```
Scanner report – Day Month year time
Last seen: Date Time
Port #
IP Address:          DNS Name          Flows  MBytes  Packets
130.18.163.194      ws194-163.hathorn.dynamic    419   0.06   1257
Port 0
IP Address          DNS Name          Flows  MBytes  Packets
130.18.41.142      ws142-41.Butler.dynamic    1197  0.15   1571
```

The network administrator or network security officer analyses the log file and decides whether or not the computer should be placed in quarantine, sometimes this is done automatically depending on the situation. Some of the reasons to place a computer in quarantine are detrimental network activity, infection with a worm or virus, unauthorized distribution of copyright material/ computer programs, games, motion pictures, and/or music recordings.

When a computer is put in quarantine the user will be redirected to a webpage stating that the computer has been placed in a specified level of quarantine with a message that says, “Your machine is likely infected with a worm or virus (or other reason). During a recent period this machine probed/scanned thousands of systems (or other activity).” They will be directed to the Policy that states the proper use of the campus network and given guidance to remediate the problem and get the computer out of quarantine.

The University has set up three levels of Network Quarantine with each level being more restrictive and each having more stringent requirements for removal from quarantine [17]. In the first and second level the user of the computer must identify themselves with their unique credentials, in this case their NetId and NetPassword.

At level 1, the DHCP parameters are modified so that web access to DNS-based URLs is redirected to a quarantine web page. The web page provides information about the possible problem along with suggested corrective actions. It also provides a link for the user to remove the computer from quarantine, and hopefully after the problem has been corrected.

Level 2 is similar to level one but in order to remove the computer from quarantine, they must contact the network administrator. Usually a computer gets to this level after being in level 1 and no action was taken to resolve the problem that initially put the computer in quarantine.

In level 3, the DHCP parameters are modified so that all DHCP-based network communication is disabled. Additionally, the network port to which the offending computer is connected may be disabled. No network communication is possible. The user must contact the network administrator to remove the computer from quarantine.

### **3.3 Facts and Figures**

Since the implementation of the quarantine process, the health of the campus network has dramatically improved. The spread of viruses and worms has been reduced and the distribution of copyrighted material has been minimized. The following figures provided by Mr. Thomas

Ritter show how the quarantine process has played a big role in maintaining a healthy network and differentiating naïve students from malicious students.

Figure 3.1 shows the total number of computers that have been quarantine since August 2005.

Total				
Number Disabled	Percent Disabled	Number Enabled	Percent Enabled	Total
78	10.5%	663	89.5%	741

Figure 3.1

Figure 3.2 shows the number of computers that have been at specific quarantine levels.

Breakdown by Quarantine Level						
Level	Enabled Count	Enabled Percent	Disabled Count	Disabled Percent	Total Count	Total Percent
1	604	81.5%	48	6.5%	<b>652</b>	<b>88.0%</b>
2	43	5.8%	23	3.1%	<b>66</b>	<b>8.9%</b>
3	16	2.2%	7	0.9%	<b>23</b>	<b>3.1%</b>
TOTAL	<b>663</b>	<b>89.5%</b>	<b>78</b>	<b>10.5%</b>	<b>741</b>	<b>100%</b>

Figure 3.2

Figure 3.3 shows the total count of computers quarantine by reason.

Totals by reason		
Reason	Count	Percent
Detrimental Network Activity	247	33.3%
Infected with a worm or virus	449	60.6%
Unauthorized distribution of copyrighted material-music recordings	25	3.4%
Unauthorized distribution of copyrighted material-motion pictures	4	0.5%
Unauthorized distribution of copyrighted material-games	6	0.8%
Unauthorized distribution of copyrighted material-computer programs	8	1.1%
Automatic Quarantine	2	0.3%
TOTAL	<b>741</b>	

Figure 3.3

### 3.0 Summary

The quarantine process is a great tool for a system administrator or information security officer to maintain a healthy network and prevent problems related to copyright violations. The numbers show that the system has been working well for Mississippi State University and has significantly maintained a healthy network, aided in the discovery of illegal sharing of copyrighted material and increased students awareness of information security related issues.

As an Educational Institution, Universities and Colleges are expected to provide a safe environment which allows a variety of different educational experiences. Network technology allows students to broaden their repertoire of educational tools like WebCT, Pod Casting, etc., while the Internet provides students ready access to many different, high quality resources at minimal or no cost. A campus computer network can be used inappropriately, and a university should model appropriate behaviors and be vigilant when involving students in working with computer networks.

The Software and Information Industry Association has provided a recommended University Internet Usage Policy [11] that addresses some of the concerns with privacy issues and University internet monitoring. It is intended to serve as both a deterrent against wrongdoing as well as an educational tool detailing what is permissible. The level of privacy users (faculty, students, staff) may expect from their computer usage may be curtailed in an effective policy. Having a clearly designed policy will enable the school to protect against wrongdoing and associated liabilities as well as minimize technological threats to the system [9].

### 4.0 References

- [1] C. Wong, C. Wang, D. Song, S. Bielski, and G. R. Ganger, "Dynamic Quarantine of Internet Worms," *Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN'04)*, Carnegie Mellon University, 2004.
- [2] Copyright Law of the United States of America and Related Laws Contained in Title 17 of the *United States Code*, <http://www.copyright.gov/title17/92chap1.html> (Current 2006)
- [3] D. Meriwether, "Kevin Mitnick, An excerpt from Takedown", <http://www.takedown.com/bio/mitnick.html> (Current 1995).
- [4] Department of Justice, "Jury convicts former student of hacking into U.T. computer System", <https://www.utexas.edu/datatheft/usao-6-10-2005.pdf> (Current 10 Jun. 2005)
- [5] G. Spafford, "Blaming the victim" *Computers & Security*, Vol. 15, Issue 5, 1996, pp. 418.
- [6] M. Burnworth, "Alcatel strengthens network infrastructure security with support for Microsoft's Network Access Protection technology" WebWire, <http://www.webwire.com/ViewPressRel.asp?SESSIONID=&aId=11820> (Current 29 March 2006).

- [7] Microsoft TechNet, “Network Access Protection”,  
<http://www.microsoft.com/technet/itsolutions/network/nap/default.msp> (Current 2006).
- [8] PCWorld.com staff, “Timeline: A 40-year history of hacking”, *CNN*,  
<http://archives.cnn.com/2001/TECH/internet/11/19/hack.history.idg/index.html>  
(Current 19 Nov. 2001).
- [9] Software and Information Industry Association, “Privacy Issues & University Internet Monitoring”, <http://www.spa.org/piracy/pubs/privacyissues.pdf> (Current 2006).
- [10] Software and Information Industry Association, “Higher Education and Software Use”, <http://www.spa.org/piracy/pubs/highereduse.pdf> (Current 2006).
- [11] Software and Information Industry Association, “SIIA Anti-Piracy's Recommended University Internet Usage Policy”,  
<http://www.siaa.net/piracy/pubs/UnivInternetUsagePolicy.pdf> (Current 2006).
- [12] U.S. Department of Education, “Family Educational Rights and Privacy Act (FERPA).” <http://www.ed.gov/policy/gen/reg/ferpa/index.html> (Current 22 Nov 2004).
- [13] V. E. Rezmierski, M. R. Seese Jr. and N. St. Clair II, “University systems security logging: who is doing it and how far can they go?” *Computers & Security*, Vol. 21, Issue 6, October 2002, pp. 557-564.
- [14] W. Klein, “Operations and management of a campus packet network” *Network, IEEE*, Vol 5, Issue 2, March 1991, pp.16 – 22.
- [15] Washington Post, “Universities Rush to Protect Networks,”  
<http://www.crime-research.org/news/2003/09/Mess0501.html> (Current 5 Sept. 2003).
- [16] Wikipedia, “Captive Portal”, [http://en.wikipedia.org/wiki/Captive\\_portal](http://en.wikipedia.org/wiki/Captive_portal) (Current 24 March 2006).
- [17] Interview with Mr. Thomas Ritter and review of ITS Policy PP-ITS-0014.