Peer to Peer File Sharing Facts

Document Number: ITS-0005 **Date Published(sys):** 7/8/2021

General Description

Purpose:

This information covers some commonly asked questions concerning P2P applications and their use at Trinity University.

Policy Content

Please be aware that the only types of servers that are allowed on the TUNetwork are web servers. P2P programs that allow others to connect to your machine are acting as file servers, and are therefore not allowed. If you use file sharing on the TUNetwork, Trinity University, as your Internet Service Provider (or ISP), is obligated to forward you any copyright complaints we receive about your activity on your computer.

What is a peer-to-peer application?

Peer-to-peer (P2P) file sharing applications are used to connect you to directly to another person's computer (and, frequently, to give them the ability to connect to your machine) in order to transfer files between the two computers. There are three key characteristics that define a P2P application:

- The ability to discover other peers
- The ability to query other peers
- The ability to share content with other peers

What programs fall into this category?

The programs that fall into this category are programs like KaZaA, AIM (if you have file sharing enabled), iMesh, Morpheus, Limewire, Gnutella, BitTorrent, and others.

Why are peer-to-peer applications an issue at Trinity?

There are a number of problems. In the process of sharing files back and forth with other peers, you put yourself in the position of possibly infecting or damaging your own computer. Not everyone is as trustworthy as you are; there are those out there who will disguise a malicious program as something harmless, like a music file. The intent is either to infect your machine or to install a remote control program on your machine in an effort to use your machine for nefarious purposes. For example, there is a specific worm that is transmitted through KaZaA that actually has the ability to overwrite files on your hard drive.

Because these programs attempt to discover and query other peers, they generate network traffic which is sometimes interpreted as hostile. When another network administrator sees this type of traffic targeted towards their networks, it can be misinterpreted as a probe for vulnerabilities or an attack.

Many files being shared on peer-to-peer networks are distributed without the permission of the person or company who owns the copyright on that work. Downloading, or making available for download, these copyrighted works can be a violation of federal law. Many copyright owners monitor P2P networks to find infringers, and large industry organizations have stated that they will file lawsuits against individual sharers. If you are sued, the damages can be significant—in the thousands of dollars.

Finally, TUNetwork policy states:

- The Network is to be used in accordance with Trinity University's academic mission by enhancing the educational experience and value for those who study and work at the university. The network is not available for unrestricted use for any other purpose.
- Due to potential competing enterprise services, Trinity University does not allow network users to run SMTP or DHCP servers on the wired or wireless networks.
- Registration of a domain to a Trinity University IP address is prohibited. This includes, but is not limited to, direct DNS resolution and DNS aliasing.

How does the use of peer-to-peer application affect TU?

This affects the security and stability of Trinity's network. We care about the security of our students' machines. We also have a duty to all users to provide adequate access and a stable network. Peer-to-peer applications affect both of these missions.

In tests done by IT staff at another institution, one song was downloaded and within half an hour, three

people had connected to the machine to upload that same file. So, that one 5MB download quickly became 20MB. At the same rate, that one song would result in 720MB of outbound file transfers in one day. Multiply this by more than 2000 TigerNet connections and an even larger number of office connections, and you will begin to understand our concern. This means that our network would be used to serve others outside of the university to the detriment of our own users here at Trinity. After all, the primary purpose for our network is to assist in academic research and to provide facilities for the Trinity community.

Some of these programs allow remote control of your computer, either as part of their design or by allowing new ways for your computer to be compromised. This is significant because if this were to happen and your computer were then used to attack another institution or corporation, there would be serious security and legal consequences. Your machine would also then be vulnerable to catching a virus and then potentially spreading it to others.

These programs do a lot more than you might be aware of. Some can automatically upgrade themselves. This would be a huge problem if the request for the upgrade were redirected to another site that would install a program such as a Trojan horse. KaZaA, for example, has the ability to create a separate P2P network without your knowledge through additional software that is installed when you load its software. c|net wrote about this "stealth network" in an article published in 2002. This "stealth network" would then have the ability to use University resources and run distributed computing applications over this new network—all without your knowledge or consent. To add insult to injury, this network could then be used to distribute and store advertisements on local machines.

Why have you started to get concerned about this now?

Actually, we have always been concerned about this. We have had a system for handling these inquiries in place for some time now and have not changed anything in the way we handle these incidents. However, owners of copyrighted material have become more sophisticated about the trading of their material. In addition, copyright owners have expressed an intention to take formal legal action against people who share files. Trinity wants to keep its students informed, so that they do not become of the recipient of such a lawsuit. We believe that it is appropriate for us to take further steps to inform our students about the potential risks in P2P.

Who is contacting Trinity about these issues?

We are being contacted by the legal organizations representing the artists who own the copyrighted material.

Infringement Notice - Gaming
Infringement Notice - Music
Infringement Notice - Movie

How does this affect the downloading of music files?

Most music files are copyright protected, which means that they can only be distributed with the permission of the people who own that copyright. The copyright holders contact an ISP when its members violate these copyrights. One violation of the copyright is to distribute the copyrighted material via peer-to-peer applications or networks. Trinity University and ITS have to follow up on any complaints of this type that we receive. Because we are your ISP, we have a duty to pass complaints we receive on to you if you are the owner of the computer referenced in the complaint. As the owner of the "server", you could be liable if the copyright owner chose to sue (see Copyright Law, Title 17. We feel it best to contact our users and give them a chance to fix the issue before it gets to that stage.

What are Trinity's policies on peer-to-peer applications, and how do they compare to other university's policies?

At Trinity University, a violation of these policies for students will result in the temporary disabling of the offender's port for up to a one week period, depending on the severity of the offense. If a second violation occurs for the same offense the user's port will be disabled for up to a three week period. In the event a port has to be disabled for a third time during the same semester for the same offense, the port will be disabled for up to an eight week period. Also, if the offense occurs at the end of one semester, i.e. December, the port will remain disabled for the specified time period during the spring semester to fulfill the obligation of that restriction. Winter and Spring breaks are excluded from the penalty period. Any service performed on an individually owned computer because of a violation of these policies is subject to the fee associated with that service. Disabling of one's network access automatically incurs a Deactivation Fee that will be charged to their student account. For current fees, see the Student Computer Service Center.

At Trinity, we review our policies and standards on a regular basis to evaluate their currency and relevancy. We have specific policies in place regarding the use of the TUNetwork. These policies are available on this website and already cover most issues brought up by peer-to-peer applications. Other schools choose to handle this issue in various ways. Many schools are evaluating their policies to address peer-to-peer application usage specifically. Some have installed software that blocks all peer-to-peer transactions from the network. Many others operate as we do, with a tiered set of consequences for repeat violations.

How do I prevent my machine from being accessed as a file server?

You need to make sure that your peer-to-peer applications are configured correctly. Make sure that they are not set up to perform "auto-discovery" type network searches and that they are not set up to act like a file server. You do not want to have your machine accessible to the world because then everyone will have the ability to download files from your machine.

Is this all necessary?

Trinity University has a commitment to academic freedom; however, we are still bound by the law. If you do not like the direction in which copyright law is heading, let your voice be heard by contacting your state and local representatives.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v1.0	8/14/2019 1:40 PM	Courtney Cunningham

Vice President Approval:

Enter Vice President(s) that are responsible for approving this document

Name:	Title:
Gary Logan	Vice President for Finance & Administration