Testimony of Gregory Marchwinski

CEO

Red Lambda, Inc.

A V2R Company

2180 West State Road 434

Suite 6140

Longwood, FL 32779

407-682-4940 x4280

before the

Committee on the Judiciary

Subcommittee on Courts, the Internet and Intellectual Property

Hearing on:

"An Update – Piracy on University Networks"

March 8, 2007

Chairman Berman, Ranking Member Coble, and members of the Subcommittee, on behalf of my Florida based software company, Red Lambda, and its employees, I thank you for the opportunity to speak with you today about digital piracy on campuses, a problem that we as a company have been working very hard to help solve.

As you are probably aware, Red Lambda's technology was originally developed at the University of Florida, specifically to combat illegal file-sharing on its campus housing network. At the University of Florida, a huge amount of bandwidth was being consumed by the illegal downloading of both music and movie files. Additionally, the University was being overwhelmed with large numbers of

complaints associated with violations of the Digital Millennium Copyright Act. Two of the University's network engineers embarked on a mission to find a workable solution to these problems and wound up developing technology in-house to combat the illegal-file trading. After the solution was installed on the University's networks, massive amounts of bandwidth were conserved and complaints associated with the Digital Millennium Copyright Act dropped to zero, proving the effectiveness of the technology. The key to the strength of the solution was its architecture. The engineers used a peer-to-peer architecture, similar to the ones used by file-sharing technologies, to combat peer-to-peer downloading – fighting fire with fire if you will. Those two network engineers, along with myself, are Red Lambda's founders. We have since licensed the technology from the University of Florida, re-branded it using the name, cGRID::Integrity, have launched a full commercialization effort and expect to reach forty employees in the next year. Because of this history and close tie to the university space, I am especially pleased to be able to share with you our knowledge and experience as it relates to digital piracy and technology.

First though, let me be clear about the nature of the problem. Peer-to-peer file sharing is not just about a few blatant abusers. A significant proportion of the user population shares files. Peer-to-peer file sharing is a disruptive technology enabled by the phenomenal growth in broadband – and this is even truer on university campuses where students have access to a far faster network than the general population. A UK based company, Cache Logic, estimated that 60% of Internet traffic was consumed by the usage of peer-to-peer protocols in 2004.

In order to properly convey the risks associated with the usage of peer-to-peer protocols, I would like to spend the beginning of my presentation discussing certain technological trends in peer-to-peer protocols that lend themselves to further investigation on the part of universities and colleges.

ENCRYPTION

The first item that I would like to discuss is the trend toward encryption. In the past, people would almost always share music and movie files in the clear, that is to say, the files they traded were transparent on the network. Standard packet inspection technologies could tell what was being sent over the network. Recently however, in an attempt to avoid detection, file-sharers have begun to encrypt their files before they send them. The file-sharers' goal is that if packet inspection technologies cannot tell what is being sent, the chance of getting caught sharing files is lessened. Fortunately, Red Lambda anticipated this trend, and developed technology that is not dependent upon packet inspection. Red Lambda's product, cGRID::Integrity is still effective even when packets are encrypted. Red Lambda's approach is focused on the behavior of the peer-to-peer protocol, not the particular movie or song that is being transferred

The great irony of Red Lambda's focus on the protocol vs. the content is that Red Lambda is at once both enemy number one to illegal file-sharers and best friend to privacy rights advocates. This is because Red Lambda does not even make an effort to ascertain the exact content of the file – we only care about the method in which it was sent – the protocol. Additionally, in an effort to support academic freedom ideals, cGRID::Integrity also gives network administrators, at their discretion, the ability to allow peer-to-peer protocols to run on their network. This could be important, for example, to a professor who would like to use a particular protocol to share research files with students and not be hampered by a technology that blocks the usage of all peer-to-peer protocols on the school's network. We feel that this mix of capability represents the best possible balance in a technology solution. cGRID::Integrity stops illegal file-sharing in its tracks, even encrypted file-sharing, and also honors values held high in the university space – privacy rights and academic freedom.

DARKNETS

In addition to the trend toward encryption, I believe it is important to touch upon a more technologically subtle issue: file-sharing on Darknets. In the university setting, Darknets operate at a local area network level, typically for a building or dorm. You could think of a local area network as an exclusive miniature network for a particular building, area or department. When two or more users on the same local area network communicate with each other, the data from their network activity never leaves the local area network. In essence, the packets do not pass through security mechanisms that are typically placed between the local area network and the main network. Under a typical Darknet scenario, users on the same local area network intentionally seek each other out with the express purpose of illegal-file sharing.

Prior to Red Lambda's technology, this activity could remain undetected, as long as the file-sharers traded with others in the same local area network. cGRID::Integrity's underlying architecture automatically blankets a virtual network on top of an existing network, including all its local area networks, rendering Darknet file-sharing ineffective. The primary alternative solution to cover all Darknets is for universities to place a detection appliance inside every local area network. However, this solution is impractical and cost prohibitive, and we have yet to see this in practice.

MALWARE

In closing the technological discussion, I would like to briefly mention another underlying problem associated with the usage of peer-to-peer protocols on university networks. Increasingly, peer-to-peer protocols are being used as carriers of malware, like spam, viruses, and worms. A 2006 study titled, "Malware Prevalence in the KaZaA File-Sharing Network" by Shin, Jung, and Balakrishnan

found that 15% of the sampled executable files contained a viral code and that 52 different viruses were active in the KaZaA network in May 2006. This is just one example of many, easily found using basic Internet searches. Given the virus content rate, the blocking of peer-to-peer protocols on networks is an important consideration for network security. Some technologically astute individuals had an early sense of all the potential issues surrounding peer-to-peer protocols and effectively wound up being ahead of the curve with their warnings about malware. A few years ago, anyone voicing these warnings would have probably been accused of a self-serving activity. Those early concerns about malware are categorically being displayed right now on networks, with malware over peer-to-peer protocols proliferating rapidly.

All of these issues, encryption, Darknets, and malware deserve the attention of university network administrators. I hope that my overview has been helpful to the Subcommittee. This concludes my technical overview of issues associated with peer-to-peer protocols and I would now like to move to a discussion of the financial and non-pecuniary benefits of using a technology like Red Lambda's cGRID::Integrity.

BENEFITS

First and foremost, I would like to stress to the Subcommittee and to the educational community at large that Red Lambda is absolutely committed to making the technology available to educational institutions at a price that is affordable and easily sustainable for university budgets. We offer substantial discount for universities off of the retail price, even for small schools. We are also willing to offer group pricing for associations wanting to purchase the technology for its member schools. Additionally, Red Lambda has already invested heavily in development areas that are important to schools. We have found that schools find the most value in solutions that install easily to existing network environments without necessitating hardware purchases. It has also been our experience that technologies that can interface with a

variety of existing identity management and registration mechanisms are favored over those that do not. Red Lambda has created an interface that universities can use to easily track and identify offenders. It is no longer a burden to track down file-sharers and identify them.

Schools implementing the technology will benefit on several fronts, the most important of which has to do with consistency of principal and the promotion and forwarding of ethical behavior. Our universities are one of the country's most influential and prolific sources of intellectual property. Universities care a great deal about protecting their own intellectual property which is easily demonstrated through the vast array of carefully crafted patents and licensing agreements authored by universities' legal teams. It only stands to reason that a similar degree of care and consideration should be paid to others' intellectual property. Implementing a technology like Red Lambda's ensures that schools are spared the embarrassment and ill opinion associated with the careless disregard for digital intellectual property rights on their networks. The United States Trade Representative spends vast resources policing piracy issues abroad and naming names, especially in developing countries and rapidly developing economies. However, within our own borders, untold theft is taking place on the government funded university networks including the Internet2 backbone. Protecting intellectual property is without argument one of the most important pillars of our economy and it is paramount that we treat digital intellectual property rights with the same level of care and concern as other intellectual property rights, like those associated with scientific research and literary works.

Universities using a technology solution to stem piracy on its networks will benefit immediately and tangibly from the absence of pre-litigation notices and complaints. Adjudication costs associated with these types of issues are high and should drop to zero when a solution like Red Lambda's is used on the network. Before cGRID::Integrity was adopted at the University of Florida, the school was

processing a large number complaints per month associated with Digital Millennium Copyright Act (DMCA) compliance. Since the cGRID::Integrity installation four years ago, the University of Florida Housing and Residence team has received one DMCA complaint. The University of Florida estimated that it saved 3000 man hours in the 12 month period after the cGRID::Integrity installation in judicial processing time alone, reducing the average case lifecycle from 16 days to 45 minutes**.**

In addition to adjudication expenses, universities and colleges can also expect their bandwidth consumption and its associated costs to drop dramatically once a technology like cGRID::Integrity has been installed. This will help universities defer hardware upgrades often necessitated by bandwidth expansion. The University of Florida managed to defer a $2 million upgrade for several years as a result of cGRID::Integrity bringing the universities bandwidth usage back into check for legitimate purposes.

Chairman Berman, Ranking Member Coble, and members of the Subcommittee, I would like to thank you for holding this hearing today and for inviting me to speak on Red Lambda's behalf. I encourage you to exercise your influence to stem the digital piracy issue on campuses. I have provided in my written testimony a Red Lambda created Policy Guide that can be used by schools to develop effective peer-to-peer policies. The Policy Guide also gives examples of ways that schools can use Red Lambda's cGRID::Integrity to deliver educational content to students and other network users.

In closing, I would like to stress four important areas.

1) Red Lambda's technology respects privacy rights by focusing on the protocol, not the content. We don't care about what students may be sharing…only that they are sharing using a particular protocol.

2) cGRID:: Integrity ensures that violators are easy to track down and identify, eliminating concerns that some have about the time and energy it takes to find file-sharers
3) We know of no other technology that is as practical and effective to use for file-sharing on Darknets as our own.
4) Finally, with cGRID::Integrity, network administrators can permit the usage of particular peer-to-peer protocols at their discretion, ensuring a network environment that thwarts file sharers and allows academic freedom to thrive.

Thank you for your time.

Red Lambda, Inc. – Policy Guide

Blending technology and traditional tools in a comprehensive set of policies to combat illegal file sharing in the university setting.

This guidebook outlines a battery of policy ideas rooted in technology that can be implemented in tandem with each other to achieve maximum effectiveness in the area of digital intellectual property rights protection.

Step 1: Establish Policy, and Educate the Population

In practice, Universities have found that advance education, and active, consistent feedback are essential to the success of an Anti-Piracy campaign. cGRID::Integrity is capable of automating many of these steps, including the dynamic generation of training materials based on historical data, and performing mass communications with staff, faculty and students. The following table outlines some ideas that have been successful in practice:

Adopt Official Education Policy about Anti-Piracy	Inform University Population	Send anti-piracy policy memorandum to university staff, faculty, and management Introduce anti-piracy policy, examples of misuse, and the scope of possible university sanctions in printed and online registration materials. State that civil and criminal penalties could additionally apply. Post anti-policy literature/posters in all housing units and in student gathering areas of university

		Post anti-piracy policy on university website for easy look-up Require completion of dynamic web training module before network user access is granted Develop residence life programming for housing
	Staff Education	Require housing residence life staff to attend training session detailing the anti-piracy policy, media consumption alternatives, and the discipline cycle for infractions Provide frontline staff & faculty with quick-fact reference sheet to address questions Provide appropriate staff with reference documents for each violation type, describing the implications of the violations in a non-technical way – this may include judicial advisors, a disciplinary council, or Office of the General Counsel
	Student Education	Repeat of dynamic training module at the beginning of each new semester as a way to further reduce incidences, especially first time offenders. The dynamic content will be based on user's history and changes in the web's technical landscape.

Step 2: Adopt Codified Remediation Steps to Stem Piracy

There are a number of different remediation processes that are effective in combating piracy. All of these processes share in common the following elements:

- Detection
- Intervention
- Communication
- Sanctioning
- Restoration

In practice, the Restoration conditions define those items that need to happen before a case is considered "closed". While there are many different options, a three level remediation process remains the most popular option for universities within residential housing. Different strategies may be employed in combination to factor-in severity and historical information, such as:

Fixed Time Window: Violation severity is based on a fixed period, such as every academic year, or for the entire period of residency. A forgiveness policy may be instituted to "wipe the slate clean" periodically.

Sliding Time Window: Violation severity is based on the last time a violation occurred. For example, if the user's last violation was a week ago, it would be more severe than if the user's last violation was a year ago.

Volume-based: Violation severity at each stage is based on the volume or rate that pirated content is being exchanged, with fixed minimum and maximum sanctions. This distinguishes between aggressive, intentional use, and accidental use, while still enforcing the University's policy.

Content-specific: Violation severity is regulated by the type of content being transferred.

Method-specific: Violation severity is regulated by the specific way the content was being exchanged. This is designed to provide extra sanctioning for those methods that may also be disruptive to network operation, while maintaining strong remediation for regular violations

Included below is a sample of a typical three-stage process.

First Offense

1	Restrict internet access for 15 minutes; do not restrict on-campus access
2	Enter offense into database including user ID and traffic detail
3	Populate help desk with incident and user ID and traffic detail in case user calls
4	Notify user by email with description of the offense and highlight section of the Acceptable Use Policy that was violated
5	Notify Judicial Affairs; copy offender in email

Restoration Conditions:

1	Complete web training, sign with University ID
2	Complete 15 minute network timeout
3	Close related help desk ticket (automatic)

Second Offense

1 Restrict internet access for 5 days; do not restrict on-campus access

2 Repeat notification and evidentiary steps from First Offense

Restoration Conditions:

1 Complete advanced web training, sign with University ID

2 Complete 5 day network timeout

3 Close related help desk ticket (automatic)

Third Offense

1 Refer student to judicial affairs for processing, forward evidentiary record of first and second time violations

2 Restrict internet access “indefinitely” pending decision by the judicial staff who shall enter the sentence into the judicial interface

3 Repeat notification and evidentiary steps from First Offense

Restoration Conditions:

1 Complete Judicial Affairs specified network timeout

2 Complete additional sanctions; clearance to restore service may be given by judicial affairs manually or automatically

3 Close related help desk ticket (automatic)

Sample Sanctions for a 3-Step Process

The following "Sanctions" content highlights additional options that can be incorporated into the remediation lifecycle. Sanctions should be enumerated in the body of the University's judicial policy.

Reprimand - The student is sent formal written notice and official recognition that the behavior has violated the Student Code of Conduct

Conduct Probation - Conduct probation is assigned for a specified period of time and is intended to foster reflection, responsibility, and improved decision-making. The student is deemed not in good standing. Other conditions of probation are specific to the individual case and may include loss of eligibility to serve as a student organization officer, participate on any athletic team, or to participate in other specified student activities. Future established misconduct or failure to comply with any conditions or to complete any assignments might lead to more severe sanctions

Loss of University Privileges - Denial of specific University privileges including but not limited to attendance at athletic functions, unrestricted library use, parking privileges, university computer usage, and residence hall visitation for a designated period of time

Suspension - The student is required to leave the University for a given or indefinite period of time, the termination of which shall depend upon specified acts of the student's own volition related to mitigation of the offense committed. The student must comply with all sanctions prior to re-admission

Expulsion - The student is permanently deprived of his/her opportunity to continue at the University in any status.

Restitution - The student and/or the student's parents shall be responsible for the payment of costs or damages incurred by university to adjudicate a complaint or lawsuit associated with copyright violations, or for Help Desk time spent.

Community/University Service - A student is required to complete a specified number of hours of service to the campus or general community

Education Requirements - A student is required to complete a specified educational sanction related to anti-piracy