University of California, Riverside
Computing and Communications

Digital Millennium Copyright Act (DMCA) and Higher Education Opportunity Act (HEOA)

Proposed Tools to Ensure Campus Compliance, Protect Student Access to Systems, and Provide Automated Management and Remediation
February 27th 2012

Introduction and Background

UCR provides ultra-high speed bandwidth and virtually ubiquitous network access to campus faculty, staff, and students. Per privacy and confidentially policy (UC's Electronic Communications Policy, ECP), Computing and Communications (C&C) does not, in general, investigate and/or monitor network traffic and in no way attempts to serve as an arbiter of electronic content.

Given the speed of UCR's network and the paramount concern for privacy and confidentially, misuse of the network can and does occur. One common form of misuse is illegal file sharing of copyrighted materials, most often music, movies, software, and games (illegal file sharing is most commonly enabled via the Peer-to-Peer (P2P) software protocol). There are two important statutes relating to illegal file sharing that impact universities and their network management practices:

- *Digital Millennium Copyright Act (DMCA).* The DMCA includes specific penalties for illegal file sharing, but also provides "safe harbor" provisions that protect universities if they stop offenders when appropriately notified. For example, when the Recording Industry Association of America (RIAA) notifies UCR of an alleged violation, the campus must actively stop the file sharing to retain its "safe harbor" and avoid prosecution and penalties.

  Current Status. C&C supports various technologies that associate a DMCA complaint with an individual network user (typically a student). These technologies "shut down" network access until the student meets with Student Conduct Programs and remedies the situation.

- *Higher Education Opportunity Act (HEOA).* The HEOA places three general requirements on Universities as follows:

  1. An *annual disclosure* to students describing copyright law and campus policies related to violating copyright law.

     Current Status. UCR has a broad communications program in place to educate faculty, staff, and students about illegal file sharing (this includes e-mails throughout the year, posters in labs, handouts in the residence halls, ads in the Highlander, etc.).

  2. A *plan to "effectively combat the unauthorized distribution of copyrighted materials"* by users of its network, including "the use of one or more technology-based deterrents".

     Current Status. UCR employs "packet shaping" technologies that GREATLY LIMIT the bandwidth available to students who use protocols that are most closely associated with illegal file sharing; please note that C&C doesn't eliminate / ban these protocols since they can be used for legal purposes.

3. A *plan to "offer alternatives* to illegal downloading".

   Current Status. UCR has promoted (via web sites, e-mails, posters, etc.) legal file sharing alternatives, some for cost, others completely free.

A summary UCR's activities in this regard can be found at http://dmca.ucr.edu/

Proposed Modifications to UCR's DMCA and HEOA Technologies / Systems

The number of DMCA violations is overwhelming UCR's ability to meet with students, inform them of complaints, discuss remediation, and restore network access. Importantly, when a student loses wireless network access, it can have a negative impact on academic performance. Additionally, when students are presented with a DMCA violation notice, the most common reaction is to assert that they did not know the software was on their computer.

In response to these issues (overwhelming number of complaints, negative impact of lost network access, and students claims relating to a lack of P2P software knowledge), C&C is proposing two system deployments as follows:

1. *Automated Notification that P2P traffic has been Observed*. A new UCR tool will monitor student network utilization and attempt to identify P2P traffic. If this traffic is encountered, the student will be notified via e-mail that P2P activity has been observed, and if this traffic involves non-copyrighted material (or appropriate sharing of copyrighted material), no action needs to be taken.

   However, if the student is not aware this traffic exists, steps for remediation and removing the P2P software are presented. Importantly, no effort is made by C&C to determine the destination of the traffic, the nature of the network content, etc., so UC policies relating to privacy and confidentiality are not violated. This technique has been successfully deployed and utilized across the United States (for example, at the University of Michigan, Northwestern, University of Oregon, Iowa State, etc.).

2. *Self-Remediation of First Offence*. A second tool will enable UCR students to engage in a self-remediation process when UCR receives DMCA violation notices. Using this system, students will be presented a web page outlining the complaint, their responsibilities to remove the copyrighted material and P2P software, and penalties for a second offence (loss of wireless access through the end of the academic year). This new electronic approach will DRAMATICALY lessen the workload for Student Conduct Programs and C&C, and it will also enable students to regain access to the network in the shortest time possible.

   These two new technologies are complete, tested, and ready to deploy. Moreover, the systems have been presented to the AVC of Enrollment Management and to the Director of Student Conduct Programs who have both endorsed deployment. C&C is therefore seeking final approval from the Provost to deploy the two aforementioned systems / technologies.