THE ENFORCERS – THE UNIVERSITY OF FLORIDA'S ICARUS P2P-BLOCKING SOFTWARE HAS CLIPPED STUDENTS' FILE-SHARING WINGS. DO ITS POLICY-ENFORCING CAPABILITIES GO TOO FAR?

By David Joachim:
Network Computing
February 19, 2004

Campus residents can no longer use Kazaa, Morpheus or any other P2P (peer-to-peer) file-sharing software to download music, movies or software applications at the University of Florida. The free lunch ended abruptly at the beginning of the 2003-04 school year, when network administrators working in the campus housing unit turned on software they developed that not only detects illicit network activity but also dynamically enforces acceptable-use policies without IT intervention.

The software-called Icarus, for Integrated Computer Application for Recognizing User Services-is mostly a collection of PERL scripts. It pulls information from commercial and open-source tools used to monitor the network and spots traffic patterns that look like P2P transfers. Icarus then tracks down the user's IP address, flashes a pop-up warning and limits access to the internal campus network. An e-mail alert is sent to the student, who must agree to suspend use of the offending P2P desktop software to regain full Internet access.

News of the crackdown spread across college campuses like a new Eminem MP3, sparking an outcry from civil libertarians that UF, a public university, was violating students' privacy and suppressing open expression. It also raised questions about which priority was paramount for college administrators-protecting copyrights on behalf of the entertainment industry or cultivating innovation among computer science students and other researchers who want to run advanced applications on the campus network.

For IT practitioners everywhere, UF's story is sure to touch off a debate that is as timely as it is timeless: How much network policing is too much?

Overnight Success

There's no debate about Icarus' effectiveness. Before it was turned on, there were as many as 3,500 simultaneous violators at any given time on the Gainesville campus, school officials say. On the day the switch was flipped, 1,500 violators were caught. There were only 19 second-time violators and no third-time violators. Purged of the digital cholesterol of media files, the network saw an 85 percent drop in uplink data volume.

Since then, violations have slowed to a trickle. Another 500 or so have been caught for the first time, 150 for the second time and four for the third time. Only third-timers are formally charged with violating the terms of use, and their cases are sent to the campus judiciary.

The inventors of the software say it can be applied to any number of network threats and annoyances, including spam, worms, viruses, Trojan horses and denial-of-service attacks. In fact, even before it was applied to P2P traffic, Icarus controlled the Welchia worm by automatically quarantining infected computers, university IT officials say. The software is so good that a campus

committee on licensing decided last month to apply for a patent and explore ways to commercialize Icarus.

Icarus was born just as the recording and film industries started turning up the heat on college administrators to do something about the rampant copyright infringement occurring under their roofs. Nobody knows for sure what percentage of all P2P file swapping occurs on college campuses, but demographics and high-speed connections-often hundreds of times faster than home broadband service-make campuses a hotbed of P2P activity, experts say. UF students will soon get gigabit connections to the desktop, upgraded from 10- to 100-Mbps connections.

Contractors monitoring P2P networks on behalf of the RIAA (Recording Industry Association of America) and the MPAA (Motion Picture Association of America) are hunting down the most flagrant traders of copyrighted works on college campuses. In turn, the trade groups are sending thousands of complaints to college administrators every month.

College campuses have come up with a mix of technical and non-technical answers. Most have simply throttled down the bandwidth devoted to file-swapping programs, using traffic-shaping tools from Packeteer and other network monitoring vendors. A straightforward and inexpensive approach, this method has other advantages over blocking P2P traffic completely: It's less likely to anger students, and it keeps campus administrators out of the copyright debate.

Some universities, including the Massachusetts Institute of Technology, have established no technical safeguards, only strengthening the wording of their policies on piracy. But most schools, even MIT, are complying with entertainment industry requests to identify users snagged by the RIAA and MPAA dragnets.

Still others have found creative ways to manage the flood of traffic generated by music and movie swapping. Stanford University caught heat two years ago when it set up a server to manage requests for music files on the popular Gnutella file-sharing service. The IT department's goal was to cut down on requests leaving the campus by directing queries internally, to PCs in the dorms, thus easing the strain that music files were placing on external links to the Internet. But the MPAA complained that the server effectively handed students a tool to violate copyright laws, and the university shut it down after six months, recalls Richard Holeton, Stanford's head of residential computing.

Now Stanford relies on traffic shaping alone; the university has no plans to impose additional restrictions. There's "nothing illegal" about using the protocols associated with P2P file sharing, says Holeton, who calls UF's policy draconian.

"To me, to use any kind of network-management tool to identify somebody who might potentially be doing something is kind of Big Brotherish," Holeston adds. "It's like pulling over everybody on the highway who is driving a certain kind of car that could potentially be breaking the law, and giving them a ticket."

Says Fred von Lohmann, a senior staff attorney at the Electronic Frontier Foundation: "If John Ashcroft asked us to do this, we'd be crying foul, but the recording industry does it and we roll over."

A spokesman for the RIAA wouldn't disclose how many universities have been subpoenaed for names of students, but he did say, "Virtually every university has complied."

No Servers, Please

Robert Bird, coordinator of network services in UF's housing division and the lead developer of Icarus, counters that the program was not developed to enforce copyrights. Rather, it was conceived as a way to enforce a ban on servers operated out of dorm rooms. The IT staff was already monitoring such activity manually, by examining log files, but the process was laborious and reactive. Icarus automates the collection and analysis of log files contained in the university's routers, switches, firewalls, port scanners and intrusion-detection systems. It also dynamically enforces the no-server policy by issuing a pop-up warning on the user's desktop and shutting down Internet access until the user complies with campus policy, Bird says.

UF's no-server policy has been in place for six years. School officials were concerned that some students would use their high-speed connections to run commercial Web sites. The policy is not uncommon for campuses that run separate network operations for housing, as UF does, Bird says. Many Internet service providers also prohibit the use of personal broadband connections for Web serving and other applications that demand high-speed uplinks.

Since Icarus went live last September, only three of the 7,500 students living on campus, most of them freshmen, have asked to be exempted from the no-server rule, and those requests were granted, Bird says. In all, there are fewer than a dozen exceptions to the rule campus-wide. (No exceptions have been granted for P2P software use, but users can still activate P2P-sharing sessions on the academic and wireless networks, because Icarus isn't used there.) The low number of exemption requests shows that while there are clearly legitimate uses for on-campus servers and maybe even P2P file-sharing applications, those instances are rare. Bird contends that the policy is not as heavy-handed as critics suggest.

But some network administrators at other schools say it's contrary to a research university's mission to prohibit servers. One admin points out that when David Filo and Jerry Yang set up a Web server in a Stanford dorm room a decade ago, it became Yahoo. Bird sees it differently. "If 85 percent of your bandwidth is wasted on trivial activity, you can't get legitimate research done," he says. "We simply don't have the spare bandwidth." Before the launch of Icarus, Bird says he often received complaints from dorm residents who couldn't download video of their classes because of network congestion.

Others object to Icarus on the grounds that it doles out punishment without due process. "If your computer starts a file-sharing event, there is an automatic punishment levied against you in that your connection is terminated," says Chris Hoofnagle, associate director of EPIC (Electronic Privacy Information Center).

In a way, that's exactly what UF's administrators were hoping for. Before Icarus, Bird was sending about 1,000 cases of copyright violations to the campus judiciary every semester. Since Icarus went live, the campus judiciary has had to process cases against only the four third-time violators. Bird says he actually protects students from lawsuits, because he stops their illegal activity before the RIAA or MPAA discovers they are active P2P users.

UF campus officials say Icarus helps them educate students about copyright infringement and their responsibility as network citizens. Weeks before the software was turned on, school officials blanketed the campus with warning flyers. "This is better than just turning them over to the authorities or disciplining them outright because there is still a lot of misunderstanding about it," says J. Michael Rollo, vice president for student affairs.

Icarus has the added benefit of keeping network costs-and, by extension, student fees-low, Rollo says. "We've got to keep in perspective what it costs to run this network, and make sure we can get video of the next economics lecture to the desktop," he says.

Outside Pressure

Copyright infringement may not have been the reason Bird and his co-worker, Will Saxon, developed Icarus, but to some administrators, stopping piracy was as much of a goal as freeing up bandwidth.

Pressure from outside the campus was clearly mounting last spring as the software was being developed. At that time, Norbert Dunkel, the director of housing and residence education and Bird's boss, was appointed to a committee investigating the impact of P2P file sharing for the ACUOI (Association of College and University Housing Officers International). Also, in April, Kathy Bergsma, the university's information security manager, received a record 73 complaints from the entertainment industry that UF students were illegally distributing copyrighted works. Those complaints would be handed off to Bird to investigate, and Bird would then turn over his findings to the campus judiciary.

Most college campuses appoint someone like Bergsma, usually a data security administrator, to field complaints under the Digital Millennium Copyright Act. The DMCA, passed by Congress in 1998, updated U.S. copyright laws to address issues such as fair use, service-provider liability and the circumvention of digital copyright protections.

"We love Icarus because it reduced our workload tremendously," Bergsma says. She has received no DMCA complaints about dorm residents from the entertainment industry since Icarus was turned on, though she still receives some complaints about users on the academic and wireless networks, where Icarus is not in use.

Sandy Senti, Bergsma's DMCA counterpart at Stanford, stops short of endorsing Icarus, even though it would ease her workload. "There's a very fine line we walk between fostering innovation and ensuring that people are doing the right thing," she says.

Only a handful of students came in to UF's campus housing office to complain after Icarus was turned on, Dunkel says. He thinks the outcry wasn't louder because most users recognized that what they were doing was indefensible. Those who did complain were mostly concerned that campus administrators were looking at the content of downloads. But Bird assured those students that he didn't need to see the content to identify the traffic as P2P.

Privacy isn't the only beef among critics. Hoofnagle of EPIC is concerned that UF is inhibiting student expression simply by demonstrating an ability-and willingness-to tie computer activity to end-user identities. "It's important that students not feel like they're being monitored," he says, "so that they're willing to explore ideas that might be controversial."

The New Napster

UF's student newspaper, the Independent Alligator, has called Icarus "invasive," "annoying" and "evil." The paper advocates a policy more like the one at Penn State University, where students can listen to all the music they want, using the relaunched (and now commercial) Napster service. Penn State pays Napster an undisclosed sum on behalf of students for a so-called tethered music service, and those fees are passed along to students as part of a $160 annual technology fee, says Russell Vaught, Penn State's associate vice provost for information technology.

Users of tethered music services download recordings and pay a kind of rental fee for the copyright. In order to keep the music when they are no longer Penn State students, users can choose to take over the monthly payments for the tethered service or convert to perpetual rights by paying either 99 cents per song or $9.99 per album.

Penn State operates a local cache for Napster downloads, so only about 10 percent of them come from outside the campus, Vaught says. And because the service uses commercial-grade servers and compression, Napster downloads are far leaner than those using Kazaa. Tracks that can take as long as 20 minutes to download over Kazaa take less than a minute on the campus service, Vaught says. In the end, while Penn State isn't eliminating music downloads as UF is, the activity places only a light burden on the network, he says.

As for Icarus, more than 100 universities have quietly expressed interest in the software. The University of Arizona has agreed to beta test the software when UF releases the code in the spring, says Ted Frohling, UA's principal network systems analyst. Until that time, the university is relying on traffic shaping. IT gives P2P traffic a low priority rating between 7 a.m. and 5 p.m. but places no restrictions at other times.

Still, the UA campus attorney's office has decided that the university will not chase down students for suspected copyright violations, though it will act on complaints from the RIAA and MPAA. Campuses with this type of policy generally believe that if they routinely police their networks, they will subject themselves to legal action under the DMCA, which states that campuses must stop any infringement they know about.

P2P Off-Campus

It's unclear how many commercial Internet service providers will want to follow UF's lead and restrict the use of their networks for P2P file exchanges. Several big and small ISPs contacted for this story say most of their services provide dedicated bandwidth that isn't affected by the loads other customers place on the network, so they have no reason to regulate use.

But that's not the case for cable operators, whose share of the broadband market is growing rapidly. Users of Internet-over-cable share their bandwidth with their neighbors, and the commodity pricing, usually under $50 per month, is based on the assumption that users won't hog bandwidth. Data-transfer rates explode as more subscribers set Kazaa and other P2P file-sharing programs to download large media files all day in the background. As transfer rates increase, cable providers have a choice: Increase capacity to accommodate the growth, or set limits on the total transfer rates allowed per month or on the use of specific protocols such as those inherent to P2P file-sharing services.

"It's like electricity: If one person is melting down the power grid, shut that person down," says John Pescatore, a data security analyst at Gartner.

Cable operators can cite other reasons to closely monitor user activity. Some experts estimate that as much as 70 percent of the traffic on cable data networks is generated by spam and viruses. As much as they would love to rely on Microsoft and other software vendors to fix these problems, cable providers can't afford to wait.

At least one cable operator has begun to crack down. Comcast measures the amount of bandwidth each subscriber consumes; those who use "excessive" bandwidth are warned that they are violating the terms of service and abusing their user privileges. Comcast is also one of the

providers that agreed to divulge the identities of users suspected by the entertainment industry of copyright infringement. Other such providers include BellSouth, EarthLink, Time Warner Cable and Verizon.

Experts agree that Icarus and programs like it will have to adapt as the architecture of Web applications evolves. In fact, Fred Cohen, an analyst at the Burton Group, calls Icarus unexceptional as a new technology. By relying on unique traffic patterns to identify types of data traffic, it will always be susceptible to illicit network activity designed to look like legitimate traffic, true to the fundamentals of computer science.

Even Tom Temple, the MPAA's director of Internet enforcement, agrees that the ability to monitor file transfers will get harder as more Web applications take on P2P characteristics. The latest Apple operating system makes a Macintosh a Web server right out of the box. "You can open it up as an FTP server and share your hard drive; that is a form of P2P," he says. Also, the latest version of AOL Instant Messenger permits direct, PC-to-PC transfers of files, including copyrighted works.

Whether Icarus and similar programs endure as a solution to the P2P problem or any number of other network nuisances, it will be up to network administrators and their employers to determine where the line should be drawn between innovation and automated network enforcement. That debate has only just begun.