CPSC156a, Fall 2003
Solution Set for HW4

Question 1:

The basic decentralized system architecture of Kazaa addresses the goal of avoiding Napster-like liability. Because there is no central server that plays the role of matching up peers, as there was in the original Napster system architecture, there is no central, important target to sue for contributory copyright infringement. There are many supernodes that match up peers (indeed, any node with a good Internet connection can become a supernode), and even if some of these were shut down by copyright-infringement suits, the Kazaa network could continue to operate with the remaining supernodes (and new supernodes would arise). Liability is also affected by the fact that Sharman Networks, Ltd., the company that distributes the Kazaa software, is based in Australia and has offices in Europe; it is less straightforward for US copyright holders to sue an Australian company than it was for them to sue Napster, which was based in the US.

To achieve Napster-like efficiency, Kazaa has many "supernodes," each of which can play a role similar to that of the Napster server (*i.e.*, matching a peer that wants to receive a file with one that can send it). Furthermore, it is only when a supernode cannot satisfy a request for a file that it sends that request to another supernode. So Gnutella-style "query flooding" is avoided.

Correct answers to the efficiency part and the liability part were worth 8 points each.

Question 2:

Copyright infringement is an unauthorized use of a copyright work that is not covered by the Fair-Use doctrine. DMCA violation is either (1) circumvention of an effective technological measure whose purpose is protection of a work's owner's rights or (2) distribution of circumvention tools. Thus copyright law governs the use of copyright works, and the DMCA (or at least the provisions of it that are relevant to Question 2) governs the technical systems designed to manage copyright works. It is possible to be guilty of DMCA violation but not of copyright infringement; for example, a circumventor could "hack around" a technical-protection system, thus gaining the ability to distribute a copyright work without the owner's permission, but not actually distribute it.

Correct explanations of the difference between DMCA violation and copyright infringement were worth 12 points. Answering that it is possible to violate the DMCA but not infringe copyright was worth 4 points.

Question 3:

The following quote from Bruce Schneier (in C. Mann's "The Heavenly Jukebox") answers this question very well: "At the moment, [circumvention is] hard to do. You always

have two kinds of attackers, Joe Average and Jane Hacker. Many systems in the real world only have to be secure against Joe Average. But if I am Jane Hacker, the best online, I can write a program that does what I do and put it up on the Web -- click here to defeat the system. Suddenly Joe Average is just as good as Jane Hacker."

The DMCA provision that addresses this threat is the prohibition on distribution of circumvention tools.

Correctly stating that experts can distribute easy-to-use circumvention tools via the Internet was worth 12 points. Naming the correct DMCA provision was worth 4 points.

Question 4:

IP packets are the basic unit of information exchange on the Internet, and they lend themselves very well to the distinction between content and control information. A network-monitoring system could be programmed to read and/or save the *header* fields of each packet and ignore the *payload* field. The former is control information and, in particular, contains source and destination IP-addresses. The latter is "content of communication."

Correctly identifying the IP packet as the relevant data structure was worth 4 points. A correct explanation of how control and content information may be separated was worth 12 points.

Question 5:

Confidentiality has been achieved when information cannot be read by someone not authorized to read it.

Integrity has been achieved when information cannot be modified by someone not authorized to modify it.

Availability has been achieved when everyone who is legitimately entitled to access a piece of information or a network service can in fact do so.

As we have read in the CERT posting on "Security of the Internet," it is not always necessary for an attacker to break into a networked machine in order to compromise one of these properties. For example, suppose that machine A is sending unencrypted traffic to machine B. A rogue router on the path from A to B could compromise both confidentiality and integrity. It could read and save the payload fields of the IP packets (even though it only needs to use the header fields in order to accomplish its routing task) and subsequently pass them along to an adversary of A and B; this would compromise confidentiality. It could also modify the payload fields before sending the packets along to the next hop in the path to B, thus compromising integrity. Availability of a machine M can be compromised by an attacker who mounts a "denial-of-service" attack without breaking into M; the attacker sends such a high volume of traffic to M that it consumes all of the bandwidth of M's network connection, and legitimate users cannot get through.

Each correct definition was worth 8/3 points. Each correct explanation of how to compromise one of these security properties without breaking in was worth 8/3 points.

Question 6:

Unsolicited commercial email is trespass to chattel only if it harms the condition, quality, or value of the recipient's computer system. For example, CompuServe won a trespass-to-chattel lawsuit against Cyber Promotions, because the tens of millions of messages that Cyber Promotions sent to CompuServe customers used up a huge amount of processing power, disk space, and bandwidth, thus seriously harming the quality of the service that CompuServe was able to provide. Intel, however, lost its suit against Hamidi, because his email did not harm the functionality of Intel's corporate network (although the content of these messages did upset people). As the California Supreme Court wrote in its *Hamidi* decision, making all unsolicited commercial email trespass to chattel might "create substantial new costs, to email and e-commerce users and to society generally in lost ease and openness of communications and in lost network benefits."

Correctly making the distinction between unsolicited email that is trespass to chattel and unsolicited email that is not was worth 8 points. A correct argument that society would not necessarily be better off if all unsolicited commercial email were considered trespass to chattel was worth 8 points.