threats and vulnerabilities described in this book. The key points raised in this chapter are these:

- Peer-to-peer sharing is a system with no central control. As such, the architecture is promising for widely distributed applications of largely autonomous agents. As a research area, peer to peer is interesting for military applications, distributed, large-scale problem solving, and serverless client-to-client interaction. These uses of peer-to-peer architectures are not widely implemented, however.
- Current peer-to-peer use centers on sharing of music, photos, video, and similar data types. In this context, the two significant problems of peer-to-peer networking are unacceptable data disclosure and improper code installation. The data disclosure tends to occur when access permissions are set too loosely or the sharing region is set too broadly. Code installation occurs in conjunction with downloading, installing, and updating the peer-to-peer system software.

TABLE 17-1 Threat–Vulnerability–Countermeasure Chart for Peer-to-Peer Sharing Systems

Threat	Consequence	Severity	Ease of Exploitation
Unauthorized disclosure	Loss of data confidentiality	Serious	Easy
Introduction of malicious code	Compromise of confidentiality, integrity, or availability	Serious	Easy

Vulnerability	Exploitability	Prevalence
Unsafe defaults	Easy	Widespread
Poor system administration	Easy	Widespread
Download of malicious software	Moderately easy	Moderate

Countermeasure	Issues Addressed	Mitigation Type	Mitigation Effect	Effort
User education	All	Prevention	Strong	Low
Secure software	All	Prevention	Strong, but limited by unlikely occurrence	Moderately low, but unlikely to occur
Legal protections (copyright)	Inappropriate sharing	Prevention	Weak	Low
Outbound guard	Inappropriate data transfer	Prevention	Fairly strong	Moderate

- Much P2P exchange involves relatively new, and therefore less sophisticated computer users. Perception and appreciation of risk and harm can be lower with this group.
- Education, secure defaults, and export filters are primary controls although, for several reasons, these countermeasures are infrequently employed.

In the next chapter we consider another current area of security concern, which also relates to a technology popular with younger people: social media, such as Facebook. In that chapter user awareness of threats is also a major issue, as is transmission of malicious code. However, the primary concern in that chapter involves privacy: situations in which the user unwittingly shares too much information.

Before we consider social media, however, we explore how laws and the courts can protect computers and data.

RECURRING THREAD: LEGAL—PROTECTING COMPUTER OBJECTS

Suppose Martha wrote a computer program to play a video game. She invited some friends over to play the game and gave them copies so that they could play at home. Steve took a copy and rewrote parts of Martha's program to improve the quality of the screen display. After Steve shared the changes with her, Martha incorporated them into her program. Now Martha's friends have convinced her that the program is good enough to sell, so she wants to advertise and offer the game for sale by mail. She wants to know what legal protection she can apply to protect her software.

Copyrights, patents, and trade secrets are legal devices that can protect computers, programs, and data. However, in some cases, precise steps must be taken to protect the work before anyone else is allowed access to it. In this section, we explain how each of these forms of protection was originally designed to be used and how each is currently used in computing. We focus primarily on U.S. law, to provide examples of intent and consequence. Readers from other countries or doing business in other countries should consult lawyers in those countries to determine the specific differences and similarities.

Copyrights

In the United States, the basis of copyright protection is presented in the U.S. Constitution. The body of legislation supporting constitutional provisions contains laws that elaborate on or expand the constitutional protections. Relevant statutes include the U.S. copyright law of 1976, which was updated in 1998 as the Digital Millennium Copyright Act (DMCA) specifically to deal with computers and other electronic media such as digital video and music. The 1998 changes brought U.S. copyright law into general conformance with the World Intellectual Property Organization treaty of 1996, an international copyright standard to which 95 countries adhere.

Copyrights are designed to protect the expression of ideas. Thus, a copyright applies to a creative work, such as a story, photograph, song, or pencil sketch. The right to copy an *expression* of an idea is protected by a copyright. Ideas themselves, the law alleges, are free; anyone with a bright mind can think up anything anyone else can, at least in theory. The intention of a copyright is to promote regular and free exchange of ideas.