# Chapter LI
# Ethics of "Parasitic Computing": Fair Use or Abuse of TCP/IP Over the Internet?

**Robert N. Barger**
*University of Notre Dame, USA*

**Charles R. Crowell**
*University of Notre Dame, USA*

## ABSTRACT

*This chapter discusses the ethics of a proof-of-concept demonstration of "parasitic computing." A "parasite" computer attempts to solve a complex task by breaking it up into many small components and distributing the processing of these components to remote computers that perform this processing without the knowledge or consent of those owning the remote computing resources. This is achieved through the use of the TCP/IP Internet protocol and, in particular, the checksum function of this protocol. After a discussion of similar exploits, the ethical issues involved in this demonstration are analyzed. The authors argue that harm should be the standard for determining if parasitic computing is unethical. They conclude that a revised notion of the rights of ownership is needed when dealing with the shared nature of the Internet. Suggestions for future research are offered.*

## INTRODUCTION

This chapter will examine some of the issues raised by a proof-of-concept demonstration of "parasitic computing" reported in the journal, *Nature* (Barabasi, Freeh, Jeong, & Brockman, 2001). In this type of computing, a "parasite" computer attempts to solve a complex task by breaking it up into many small components and distributing the processing related to those components over a number of separate remote computers. While the parasitic procedure represents a form of distributed computing, it differs importantly from other well-known examples such as the

Search for Extraterrestrial Intelligence (SETI) Project (SETI@home, 2003). The distributed computing utilized in SETI involves volunteers from around the world who allow their local computers to be used for ongoing analysis of vast amounts of data obtained from a radio telescope constantly scanning the heavens. SETI allows anyone with a computer and Internet connection to download software that will read and analyze small portions of the accumulated data (SETI@home, 2003). In effect, SETI has created a super computer from millions of individual computers working in concert.

Like SETI, parasitic computing takes advantage of the power of distributed computing to solve complex problems, but the parasite computer induces “participating” computers, already connected to the Internet, to perform computations without the awareness or consent of their owners. By their own admission, Barabasi et al. (2001) were aware of the ethical issues involved in their demonstration of parasitic computing. On the project Web site they state: “Parasitic computing raises important questions about the ownership of the resources connected to the Internet and challenges current computing paradigms. The purpose of our work is to raise awareness of the existence of these issues, before they could be exploited” (Parasitic Computing, 2001). In this chapter, we will begin to explore these “important questions” by focusing on the type of exploitation inherent in parasitic computing and by considering some of the ethical issues to which this new form of computing gives rise.

## BACKGROUND

The proof-of-concept demonstration reported by Barabasi et al. (2001) involved a single “parasite” computer networked to multiple “host” Web servers by means of the Internet. The underlying communication between the parasite and hosts followed the standard TCP/IP protocol. Within this context, the parasite exercised a form of *covert exploitation* of host computing resources, *covert* because it was accomplished without knowledge or consent of host owners, and *exploitation* because the targeted resources were used for purposes of interest to the parasite, not necessarily the host owners. Covert exploitation of networked computing resources is not a new phenomenon (Smith, 2000; Velasco, 2000). In this section, we will review a few common examples of covert exploitation including some that take advantage of known vulnerabilities in the Internet communication process.

### Internet Communication Protocols

The Internet evolved as a way for many smaller networks to become interconnected to form a much larger network. To facilitate this interconnection, it was necessary to establish standards of communication to insure uniformity and consistency in the ways by which a computer attached to one part of the Internet could locate and exchange information with other computers located elsewhere. These standards, known as “protocols,” emerged through the influence of the Internet Society, the closest thing the Internet has to a governing authority. The de facto standard that has emerged for Internet communication is a family of protocols known as the Transmission Control Protocol/Internet Protocol (TCP/IP) suite (Stevens, 1994). This TCP/IP standard helps to insure certain levels of cooperation and trust between all parties employing the Internet.

As shown in Figure 1, the TCP/IP protocol suite usually is represented as a layered stack where the different layers correspond to separate aspects of the network communication process (Stevens, 1994). The bottommost *link* layer in the stack corresponds to the physical hardware (i.e., cables, network cards, etc.) and low-level software (i.e., device drivers) necessary to maintain network connectivity. The middle two layers represent the *network* and *transport* layers, respectively.