Computer Worms, Detection, and Defense

Robert J. Cole
The Pennsylvania State University, USA

Chao-Hsien Chu
The Pennsylvania State University, USA

INTRODUCTION

Since the first widespread Internet worm incident in 1988, computer worms have become a major Internet threat and a subject of increasing academic research. This worm, known as the *Morris Worm,* was written by Cornell University student Robert Morris. Morris's worm infected Sun Microsystems Sun 3 and VAX hosts running versions of 4 BSD UNIX by exploiting flaws in several standard services. Although there is no strong consensus as to the definition of a worm (Kienzle & Elder, 2003), the general notion of a worm can be understood by way of contrast with viruses. A virus is a program that can 'infect' another program through modification to include a copy of itself (Cohen, 1984). Worms, in contrast, are often characterized as not requiring another program for execution or another agent for activation—that is, a worm can execute and propagate itself autonomously (Spafford, 1988). This characterization of worms as malcode that does not require human intervention for propagation is, however, not universally accepted. For example, Kienzle and Elder (2003) define worms as malicious code that propagates over a network, either with or without human intervention. Such a definition includes e-mail-based mass-mailer viruses, a category that would be largely excluded if the need for human intervention is excluded from the definition of a worm.

In the years following the Morris Worm, many new worms have been observed. From a network security perspective, worms represent a special category of threat due to the fact that worms attack on large spatial and short temporal scales. For example, on July 19, 2001, more than 359,000 computers were infected by the Code Red worm in less than 14 hours (Moore, Shannon, & Brown, 2002). As rapid as this infection was, attacks on shorter temporal scales are possible, a point made theoretically by Staniford, Paxson, and Weaver (2002) and later demonstrated by the Slammer worm, which in 2003 infected 90% of vulnerable hosts within 10 minutes (Moore, Shannon, Voelker, & Savage, 2003). Such rapid attacks are too fast for human-mediated countermeasures, and thus have motivated the development of automated detection and defense systems.

This article presents a worm overview focused on detection and defense. For the reader with little background knowledge of worms, this article will be useful as a short survey of this important topic. Below, background material is presented, followed by a discussion of detection and defense methods, and future trends.

BACKGROUND

An understanding of worm behavioral characteristics is an essential prerequisite to understanding worm detection and defense. This section presents an overview of worm target discovery and epidemic modeling.

Worms use various technical means such as buffer overflow attacks to exploit vulnerabilities in victim machines, victims that are first discovered in a target discovery phase. Target discovery can occur in two forms: with or without a priori knowledge of vulnerable hosts. A worm instance with a priori knowledge of victims must possess a pre-established list of such victims, a list possibly prepared by an attacker well in advance of the start of the attack. Such a list of initial vulnerable hosts is termed a *hitlist.* Absent a hitlist, or following the exhaustion of the hitlist, the worm attack must transition to target discovery methods that use no a priori knowledge of vulnerable hosts. Such methods often use random scanning, in which a potential victim network address is selected randomly using one of several methods and the host is subsequently attacked through the transmission of the exploit payload to the target address. Below, target discovery methods are discussed in greater detail.

Due to the indiscriminate nature of random scanning, observation of attack traffic is readily accomplished using monitors called *network telescopes* (Moore, Shannon, Voelker, & Savage, 2004). Network telescopes monitor *dark address space,* sections of the current Internet IPv4 address space that are routable but contain no production hosts. Thus, traffic observed by network telescopes is anomalous by definition. Network telescopes are characterized by their size, which is denoted using /n notation, where n refers to the number of bits in the network portion of the 32-bit address. Large '/8' network telescopes can monitor 1/256th of the IPv4 address space.

Worm Behavior Modeling

Various models borrowed from epidemiology have been applied to model worm dynamics. The simple epidemic model (SEM) (Frauenthal, 1980), also known as the susceptible infectious (SI) model, characterizes hosts as transitioning from the susceptible to the infectious state. The SEM has been extended to include hosts recovering from infection and returning to the infectious state (SIS model) or being permanently removed from the vulnerable population (SIR). Both the SI and SIS models have nonzero equilibrium infected populations, whereas in the SIR model, the infected population can eventually reach zero. These models assume the *homogeneous mixing* condition, where every infected individual is assumed to be equally likely to infect any susceptible individual. Below, the SEM is explained in greater detail.

In the SEM, rate of change of the number of infected hosts I(t) is given by:

$$\frac{dI(t)}{dt} = \beta S(t)I(t) \tag{1}$$

where S(t) is the number of susceptible hosts at time t, and β is the pairwise infection rate given by the average number of contacts leading to a new infection per unit of time per infective per susceptible in the population (Frauenthal, 1980).

For a worm attack, a susceptible host is one that exhibits the particular vulnerability exploited by the worm. Under the assumption that the number of vulnerable hosts N is constant throughout the attack, the number of infected and susceptible hosts are related by I(t) + S(t) = N. In this case, (1) can be written as:

$$\frac{dI(t)}{dt} = AI(t) - BI^2(t) \tag{2}$$

where A = βN and B = β. For a worm attack using uniform random scan (see Target Discovery Methods section below), the pairwise infection rate β is given by the ratio of average individual targeting rate η and the IPv4 address space (Zou, Gong, Towsley, & Gao, 2005); thus $\beta = \eta/2^{32}$. Equation (2) is a special form of Bernoulli equation known as the Verhulst equation, which has the following solution (Kreyszig, 1999):

$$I(t) = \frac{I_0 A}{BI_0 + (A - BI_0)e^{-At}} \tag{3}$$

The solution to the Verhulst equation is known as the logistic law of population growth. The steady-state value of I, I_∞, can be found by setting dI(t)/dt to zero, which gives the solution $I_\infty = A/B$. Thus this type of growth is characterized by populations that monotonically increase or decrease to the limit A/B for any initial population size. In the case of the SEM, A/B = N; thus the limit of the number of infections is the vulnerable population size. Figure 1 shows I(t) for N = 360,000, I_0 = 1, and η = 6, 12, and 18. The parameters for the η = 6 curve are representative of the Code Red (Moore et al., 2002) attack; the η = 12 and η = 18 curves illustrate the impact of increasing the targeting rate.

Target Discovery Methods

A worm's method of target discovery is an important characteristic because it affects the virulence of the resulting epidemic and has associated behavioral invariants that may be exploited for detection purposes. Several important target discovery methods are described below.

Uniform Random Scan

Scanning refers to the process of attempting communication with a potential victim, using either TCP or UDP transport protocols. A worm without a priori knowledge of the location of vulnerable hosts can simply scan the entire IPv4 address space in a uniformly random