Modeling, Analysis, and Mitigation of Internet Worm Attacks

Abstract:

In recent years, worms have become one of the major threats to the security of the Internet. In this talk, I will present our research on modeling, analysis, and mitigation of Internet worm attacks, which includes:

(1) We present a “two-factor worm model”, which considers the impact of human counteractions and network congestion on a worm's propagation.
(2) To detect the presence of an Internet worm at its early stage (to ensure us to have enough time for defense), we present a non-threshold based detection methodology, “trend detection”, to detect the exponential growth trend, not the traffic burst, of worm monitored data.
(3) For defense against fast spreading worms, we present a “feedback dynamic quarantine system”. It implements two principles that have been used in the epidemic disease control in the real world: “preemptive quarantine” and “feedback adjustment”.
(4) We find that a “routing worm”, which scans the IP space defined by BGP routing prefixes, propagates several times faster than a traditional worm. A routing worm could also conduct selective attacks to a specific AS, ISP, or country; and, unfortunately, it can be easily implemented by attackers.
(5) We systematically model and analyze worm propagation under different scanning strategies such as local preference scan and sequential scan, and derive several interesting conclusions.