

A Model of the Spread of Randomly Scanning Internet Worms that Saturate Access Links

Prof. George Kesidis

Penn State

ABSTRACT:

This talk will begin with a brief introduction to scanning worms and a survey of ideas proposed to defend against them. We present a simple, deterministic mathematical model for the spread of randomly scanning and bandwidth-saturating Internet worms. Such worms include Slammer and Witty, both of which spread extremely rapidly. Our model, consisting of coupled SIR (Kermack-McKendrick) equations, captures both the measured scanning activity of the worm and the network limitation of its spread, i.e., the effective scan-rate per worm/ infective. The Internet is modeled as an ideal core network to which each peripheral (e.g., enterprise) network is connected via a single access link. It is further assumed in this note that as soon as there is a single end-system in the peripheral network is infected by the worm, the subsequent scanning to the rest of the Internet saturates the access link, i.e., "instant" saturation. We fit our model to available data for the Slammer worm (actual scans captured by U.Wisc.'s /8 tarpit and associated routeview information) and demonstrate its ability to accurately represent Slammer's total scan-rate to the core.