Understanding the Behavior of Internet Worm PArallel Worm Simulator (PAWS)

Tiffany Tachibana
California State University, Montetey Bay

Background

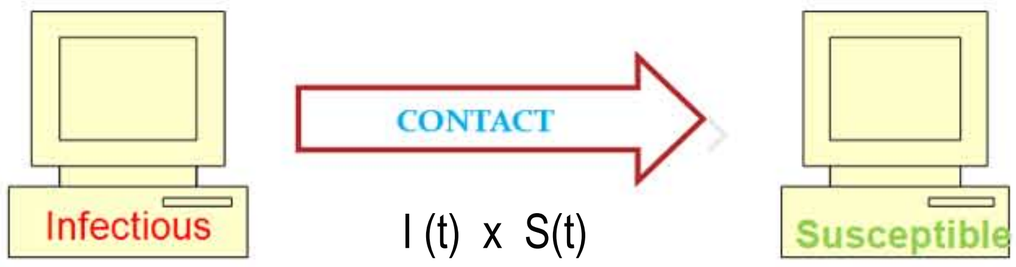
- The intention on this research is to study the Internet worm's propagation behavior. This study is adopted from S. Wei and J. Mircovic's worm modeling who developed PAWS.
- Contained and isolated yet realistic environment is required to accomplish the goal.
- DETER and PAWS are the simulation tools used in the research experiment to replicate the Slammer worm's propagation.

How Worms Spread?

- Simple Epidemic Model

State Transition:

Each host stays in one of the two states either susceptible or infectious.



I (t) x S(t)

No. of Contacts is proportional

Susceptle host = hosts vulnerable to infection

Infectious host = have been infected and can infect others

I(t) = number of infectious host at time t

S(t) = number of susceptible host at time t

What is an Internet Worm?

- a self-replicating program that propagates itself across the network..

Once it discovers the target, the worm sends out a probe to exploit the security flaw of that target machine and transfer a copy of itself, then it will activate a new cycle of propagation.

The DETER Testbed

- The cyber-DEfense Technology Experimental Research (DETER) testbed provides publicly available infrastructure for conducting computer security experiments.
- Designed for isolation and containment yet realistic network environment.
- A Web-based interface user-friendly Java GUI for setting up network toplogy and remotely access machines.

PAWS: Internet worm spread simulator

- Models the Internet at Autonomous System level and obtain its global connectivity from Route Views project.
- PAWS worms' features are customizable and configurable, depending on what particular Internet worm propagation an experimenter wishes to study.
- PAWS simulation and scanning techniques are distributed and discrete.

Experiment

- PAWS's Slammer worm configuration:
  Default Internet Model = IPv4 address space
  Scanning_rate = 4000 per second
  Vulnerable_population = 75,000
  Determine_vulnerable_host () = Randomly mark 10 vulnerable hosts as infected
  Simulation Interval = 0.05 per second
  Port of Exploit = 49162
  Transport Protocol = UDP
  Scanning strategy: random
  Life cycle = 10 minutes

- PAWS' Distributed and discrete scanning
  Each physical node simulates a portion of the Internet. Machines synchronize with each other at discrete time intervals.
  Nodes use stream socket to exchange information.
  Every time unit, each infected host produces a list of target IP addresses to scan. Worm scans sent to non-vulnerable hosts are dropped.