Reactive Zero-day Worm Protection

Kihong Park (PI), Bhagya Bethala, Ikyun Kim

Network Systems Lab, Department of Computer Sciences, Purdue University

Spread of Slammer worm

< 10 mins to infect the vulnerable population

Global Protection

- Early detection at transit points
  - Earlybird, Polygraph etc.
- Dissemination of information to content-based filters to contain the spread

Zero-day worms

- SQL server buffer-overflow vulnerability
  - Jan 25, 2003
- LSASS buffer-overflow vulnerability
  - Apr 11, 2004
- Vulnerability disclosure
  - Apr 30, 2004
- 0-day attack
  - July 24, 2002
- 185-day attack
  - 0-day attack
- Sasser Worm released
  - Apr 11, 2004
- Future worm released
  - Apr 30, 2004

Time gap between vulnerability disclosure and release of a worm that exploits it is decreasing

Approach: Cooperative Filtering

Deployment

power-law nature of Internet enables small deployment

Performance Evaluation

Simulation setup:
- 2004 AS topology with 16921 ASes and $2^{32}$ hosts
- Live Earlybird-like detection

Key parameters
- Uniform random scanning
- Filter deployment: 3%
- Detector deployment: 3%
- Scan rate: 10K scans/sec
- Initial infections: 10 (random)