

CSE331: Introduction to Networks and Security

Lecture 16

Fall 2006



Announcements

- Project 2 is due next Weds.
 - If you haven't started, you should start soon...

Analysis: Random Constant Spread Model

- IP address space = 2^{32}
- N = size of the total vulnerable population
- $S(t)$ = susceptible/non-infected hosts at time t
- $I(t)$ = infective/infected hosts at time t
- β = Contact likelihood
- $s(t) = S(t)/N$ proportion of susceptible population
- $i(t) = I(t)/N$ proportion of infected population

- Note: $S(t) + I(t) = N$

Infection rate over time

- Change in infection rate is expressed as:

$$\frac{di}{dt} = I(t) * \beta * s(t)$$

of infected hosts

rate of contact

likelihood that
contacted hosts
is susceptible

Rewrite to obtain:

$$\frac{di}{dt} = \beta * i(t) * (1-i(t))$$

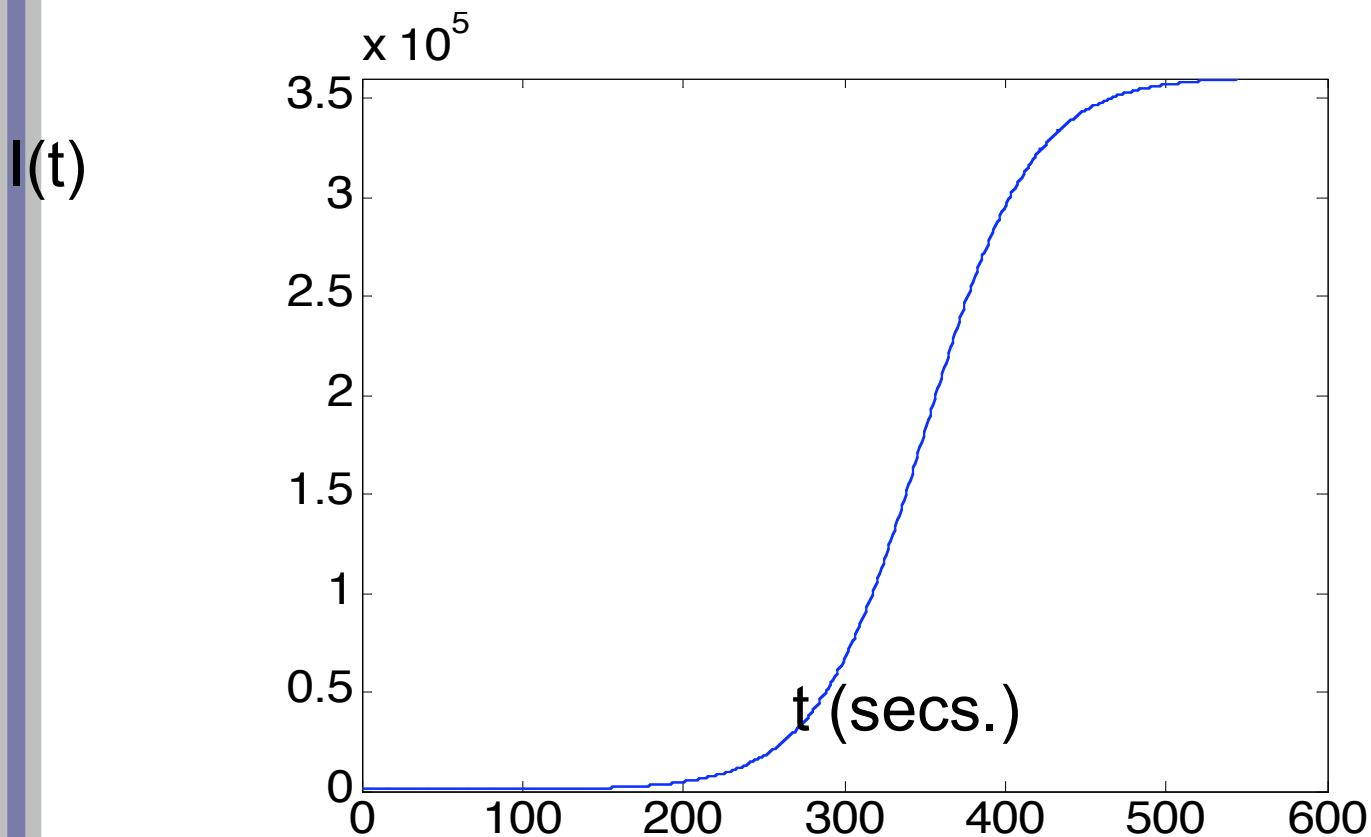
Integrate to get this closed
form:

$$i(t) = \frac{e^{\beta(t-T)}}{1 + e^{\beta(t-T)}}$$

T = integration constant

Exponential growth, tapers off

- Example curve of $I(t)$ (which is $i(t) * N$)
- Here, $N = 3.5 \times 10^5$ (β affects steepness of slope)



What can be done?

- Reduce the number of infected hosts
 - **Treatment**, reduce $I(t)$ while $I(t)$ is still small
 - e.g. shut down/repair infected hosts
 - Reduce the contact rate
 - **Containment**, reduce β while $I(t)$ is still small
 - e.g. filter traffic
- Reactive
- Reduce the number of susceptible hosts
 - **Prevention**, reduce $S(0)$
 - e.g. use type-safe languages
- Proactive

Treatment

- Reduce # of infected hosts
- Disinfect infected hosts
 - Detect infection in real-time
 - Develop specialized “vaccine” in real-time
 - Distribute “patch” more quickly than worm can spread
 - Anti-worm? (CRClean written)
 - Bandwidth interference...

Effects of "patching" infected hosts

- Kermack-McKendrick Model
- State transition:

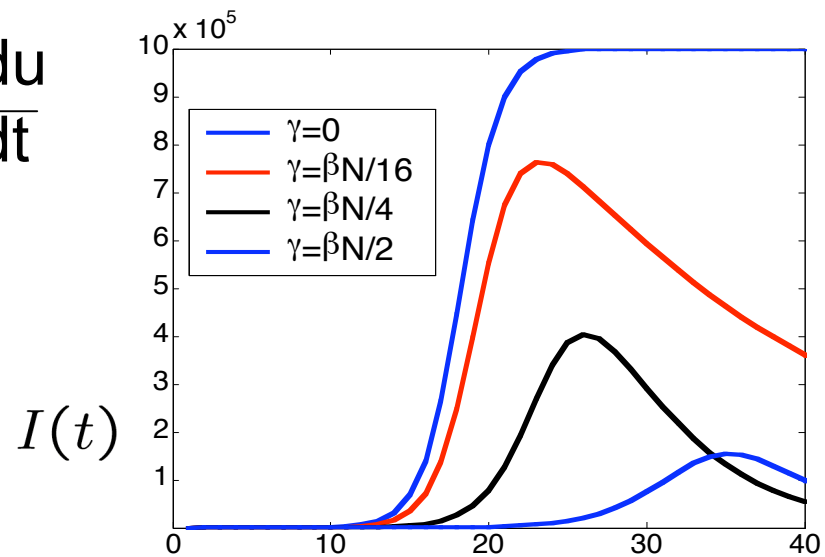


$U(t)$ = # of removed from infectious population

γ = removal rate

$$\frac{di}{dt} = \beta * i(t) * (1-i(t)) - \frac{du}{dt}$$

$$\frac{du}{dt} = \gamma * i(t)$$



Containment

- Reduce contact rate β
- **Oblivious defense**
 - Consume limited worm resources
 - Throttle traffic to slow spread
 - Possibly important capability, but worm still spreads...
- **Targeted defense**
 - Detect and block worm

Design Space

- Design Issues for Reactive Defense
[Moore et al 03]
- Any reactive defense is defined by:
 - **Reaction time** – **how long** to detect, propagate information, and activate response
 - **Containment strategy** – **how** malicious behavior is identified and stopped
 - **Deployment scenario** - **who** participates in the system
- Evaluate the requirements for these parameters to build **any** effective system for worm propagation.

Methodology

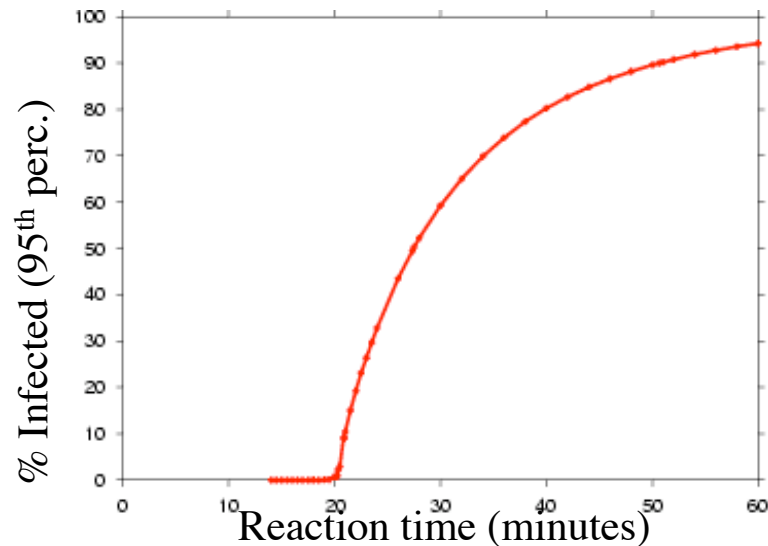
- **Moore et al., "Internet Quarantine:..." paper**
- **Simulate spread of worm across Internet topology:**
 - infected hosts *attempt* to spread at a fixed rate (probes/sec)
 - target selection is uniformly random over IPv4 space
- **Simulation of defense:**
 - system detects infection within reaction time
 - subset of network nodes employ a containment strategy
- **Evaluation metric:**
 - % of vulnerable hosts infected in 24 hours
 - 100 runs of each set of parameters (95th percentile taken)
 - Systems must plan for reasonable situations, **not** the average case
- **Source data:**
 - vulnerable hosts: 359,000 IP addresses of CodeRed v2 *victims*
 - Internet topology: routing topology derived from RouteViews

Initial Approach: Universal Deployment

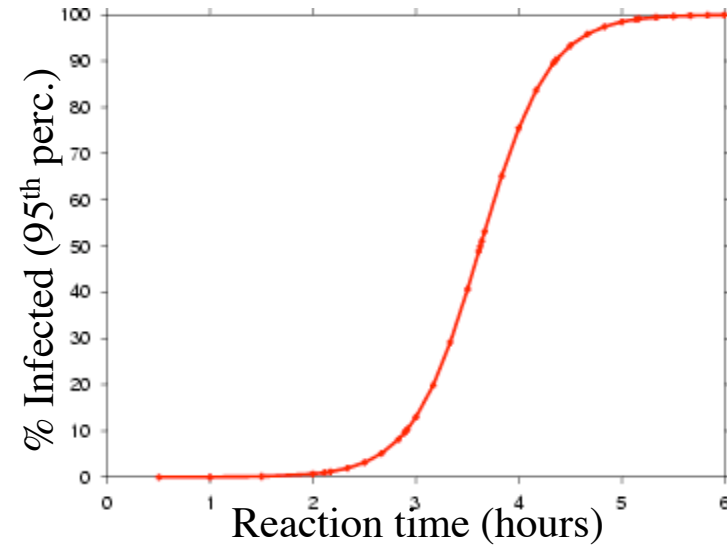
- Assume **every host** employs the containment strategy
- Two containment strategies they tested:
 - **Address blacklisting:**
 - block traffic from malicious source IP addresses
 - reaction time is relative to each infected host
 - **Content filtering:**
 - block traffic based on signature of content
 - reaction time is from first infection
- How quickly does each strategy need to react?
- How sensitive is reaction time to worm probe rate?

Reaction times?

Address Blacklisting:



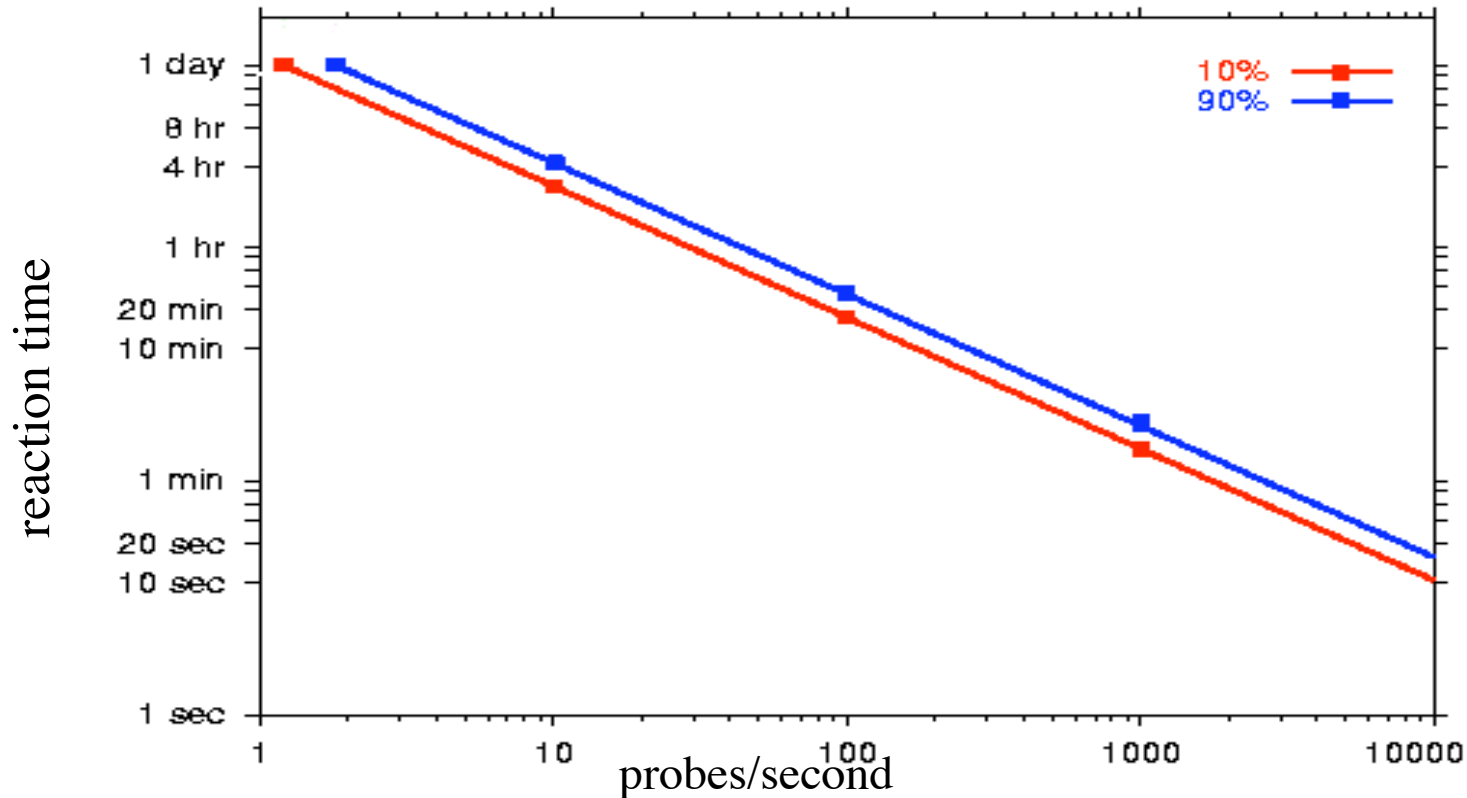
Content Filtering:



- To contain worms to 10% of vulnerable hosts after 24 hours of spreading at 10 probes/sec (CodeRed):
 - Address blacklisting: reaction time must be < 25 minutes.
 - Content filtering: reaction time must be < 3 hours

Probe rate vs. Reaction Time

Content Filtering:



- Reaction times must be fast when probe rates get high:
 - 10 probes/sec: reaction time must be < 3 hours
 - 1000 probes/sec: reaction time must be < 2 minutes

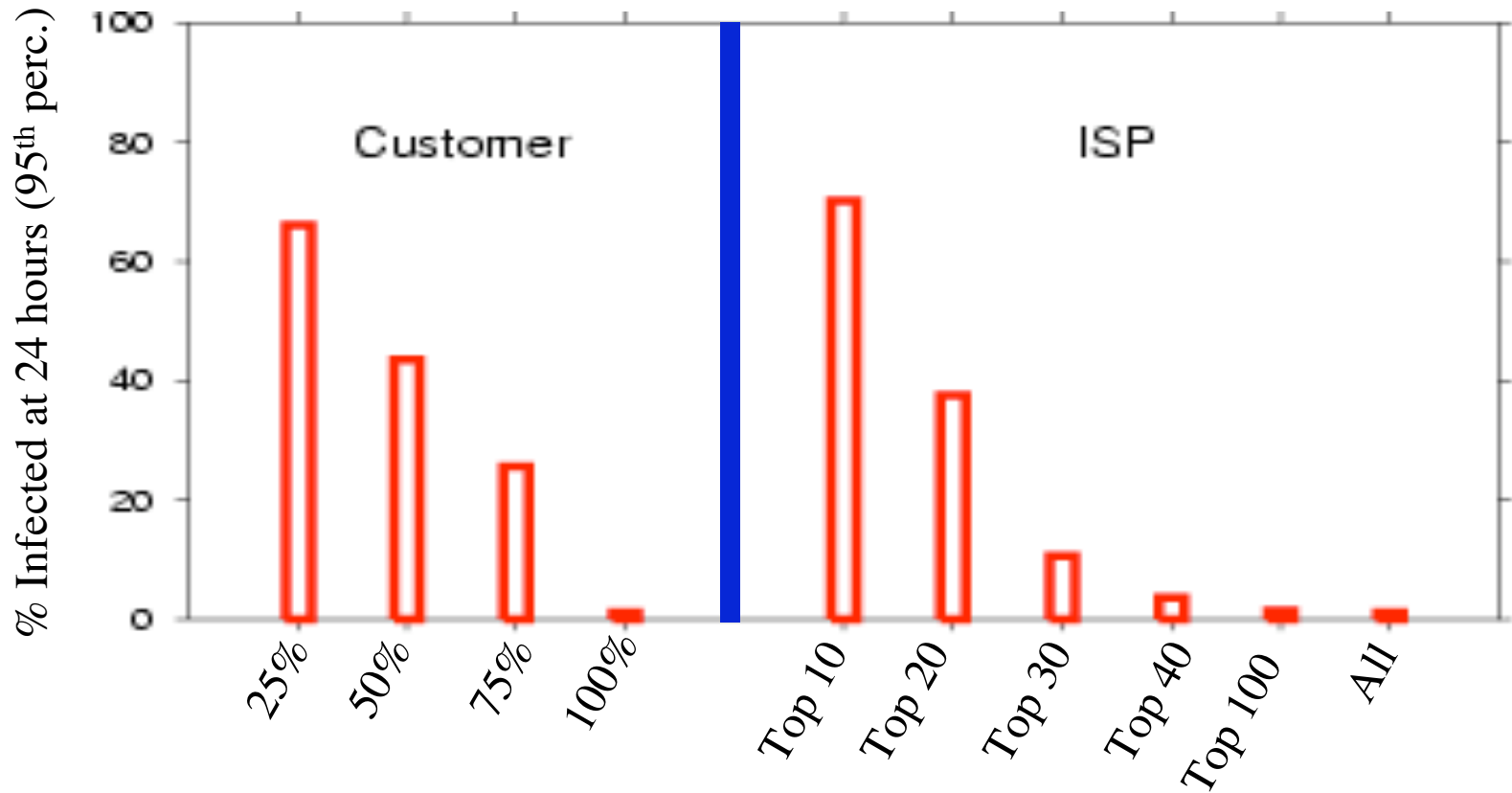
Limited Network Deployment

- Depending on every **host** to implement containment is not feasible:
 - installation and administration costs
 - system communication overhead
- A more realistic scenario is limited deployment in the **network**:
 - Customer Network: firewall-like inbound filtering of traffic
 - ISP Network: traffic through border routers of large transit ISPs
- How effective are the deployment scenarios?
- How sensitive is reaction time to worm probe rate under limited network deployment?

Deployment Scenario Effectiveness?

Reaction time = 2 hours

CodeRed-like Worm:

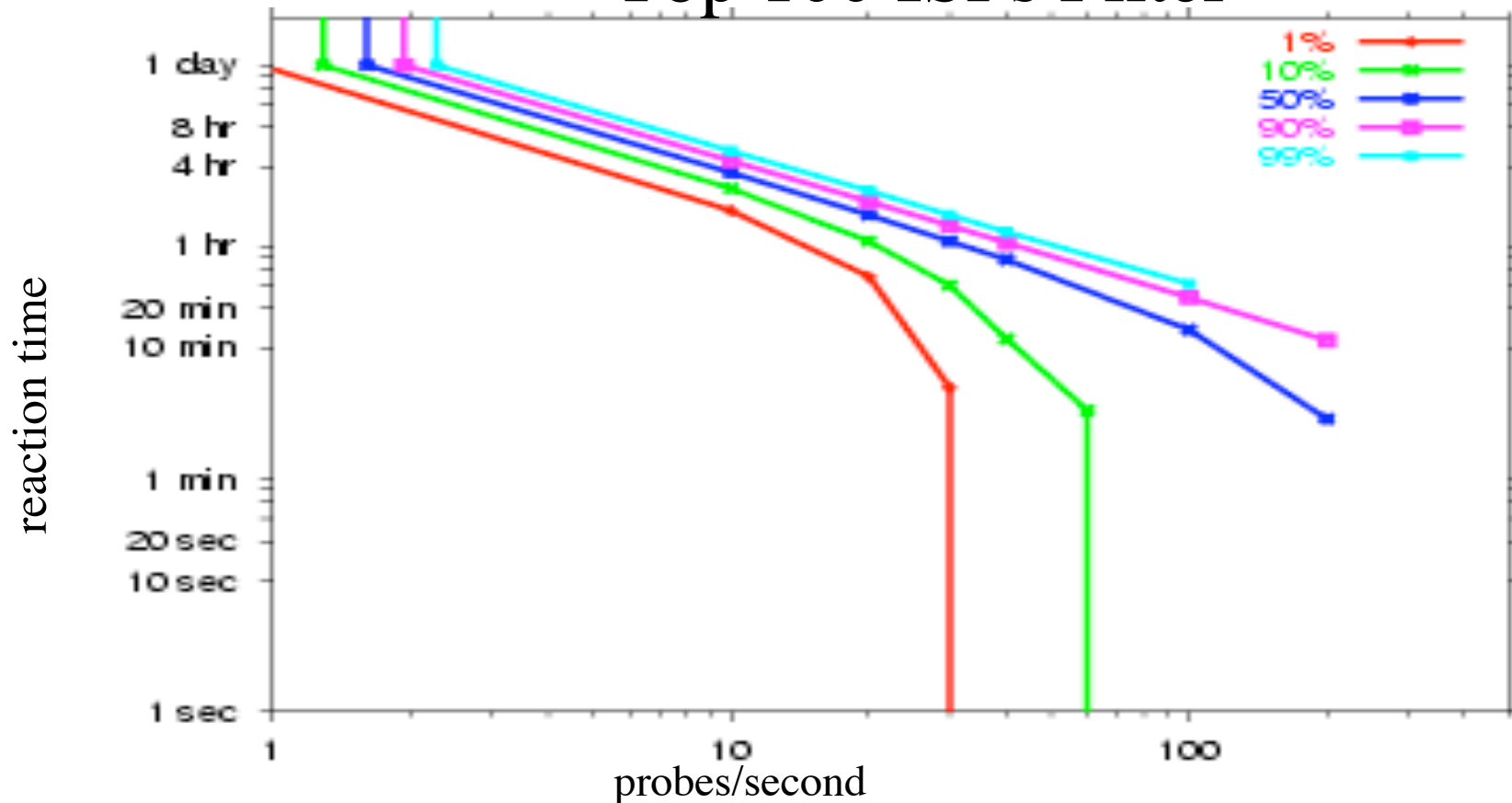


Content filtering firewalls
at edge of customer nets.

Content filtering at exchange
points in major ISPs.

Reaction Time vs. Probe Rate (II)

Top 100 ISPs Filter



- Above 60 probes/sec, containment to 10% hosts within 24 hours is impossible even with *instantaneous* reaction.



Summary: Reactive Defense

- Reaction time:
 - required reaction times are a couple minutes or less (far less for bandwidth-limited scanners)
- Containment strategy:
 - content filtering is more effective than address blacklisting
- Deployment scenarios:
 - need nearly all customer networks to provide containment
 - need at least top 40 ISPs provide containment