Internet Quarantine: Moore, Shannon, Voelker, Savage [Moore03a]

CSci551: Computer Networks
SP2006 Thursday Section

John Heidemann

Context

- DoS: external attacks on a host
- what about *worms?*
  - automated programs that exploit known vulnerabilities
- (compare to viruses:)
  - programs that require users to run them, then the exploit the user's account

Key ideas

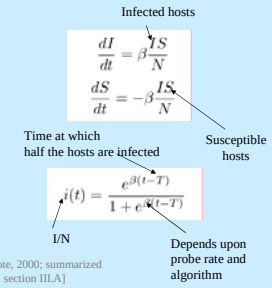
- what's needed to stop worm spread
- alternatives:
  - prevention, treatment, **containtment**
- automated defenses
  - blacklists
    - find who's infected
    - cut that host off
    - (like IDS anomoly detection)
  - content filtering
    - find a signature for the worm
    - shut that signature off everywhere
    - (like IDS signature-based detection)
- how do they compare?

Containment

- *containment* of automated (self-propagating) code (*worms*)
  - how can you contain worms?
  - ***can*** you contain worms?
- … we need to understand how fast worms can propagate

Epidemic Models

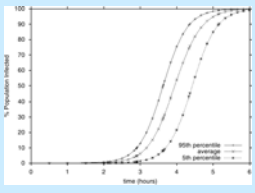
- Studied in the medical literature for many years
- SIR model
  - Susceptible, Infected, Removed individuals
  - simple differential equation



from Hethcote, 2000; summarized [Moore03a, section IIIA]

Predictions

- Code-Red v2
  - randomly probes full 32-bit address space
  - 360k vulnerable hosts
  - probe rate O(100 probes/s)



prediction is roughly consistent with what was observed (although data is not in paper)

Containment Strategies

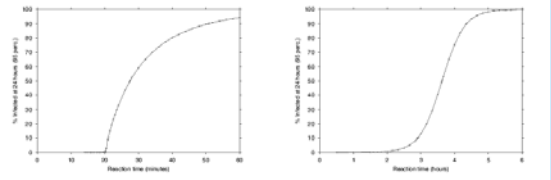
- Address blacklisting
  - detect individual infected hosts, block them
- Content filtering
  - figure out signatures, block that traffic everywhere

How to Evaluate?

- time to stop spread?
  - not really, without intervention, even tiny infection rate eventually gets everyone
- percent infected after fixed time
  - idea: enough time and humans can plan a custom defense
  - automated tools just need to slow things down
- and look at how quickly tools must react

Filtering Code-Red-like Worms

[Moore03a figure 2]



Address Blacklisting Content Filtering

observations: content filtering can be slower (slower is better because same number of hosts compomised in longer time)

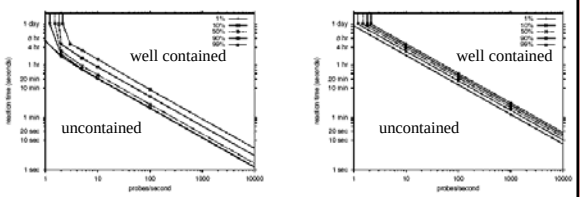
content filtering is better (the worm can run free longer and we still contain it)

blacklisting gets *hosts*, but content filtering gets the *worm*

limit of blacklisting is that it must identify each new problem individually

More Aggressive Worms

[Moore03a figure 3]



(a) Address Blacklisting (b) Content Filtering

higher probe rates are *much* harder to contain

how can a worm probe smarter? probe local address spaces…partly because network is closer, but mostly because localization gives simple distributed coordination

Who Needs to Filter?

- clients or ISPs?
- either way, we'll never get everyone, but what about partial coverage?
- conclusions:
  - getting a few top ISPs helps a lot
    - why? you get the core of the network and all the transit paths
  - getting end-networks is much less effective

What's New Since This Work?

- invited talk last years by Don Towsley (U. Mass.)
  - careful mathematical foundations to this problem
  - studied more recent (faster) worms
- "Warholl Worm": the Internet in 15 minutes
- SQL-Slammer worm: 4000 scans/s (!)
- does topology matter?
  - worms become *network* limited

Other questions/observations?

- xxx