

Review of:
Internet Quarantine: Requirements for Containing
Self-Propagating Code

- Paper by:
 - David Moore, Colleen Shannon, Geoff Voelker, Stefan Savage (UCSD)

- Published in:
 - IEEE INFOCOM
 - March 2003, San Francisco

- Review by:
 - Bharath Madhusudan

Introduction

- Motivation for the work
 - Problem: Worms are arguably today's biggest Internet security issue
 - Reason: cause system downtime (=economic loss) and Data loss
 - Contribution of the paper
 - Give lower bounds on requirements for worm containment systems
 - Reaction Time
 - Containment Strategy
 - Deployment Scenario

How do Worms Spread?

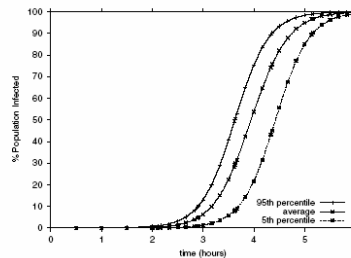
- Random
- Warhol Worms
- Surreptitious Worms

How can We Fight Them?

- Defenses
 - End System – Per host throttling
 - Router Based – Cisco NBAR, Snort, etc
- Prevention
- Treatment
- Containment
 - Hope for Automation
 - Incremental Deployment

Modeling Worms

- Roots in Epidemiology
- Incidence = Infectives X Suceptibles X Avg Contact Rate
- Properties of the function



CS6814: Fall 2003

 Washington University in St. Louis

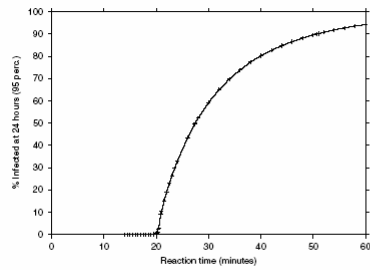
Modeling Containment Systems

- Reaction Time
- Containment Strategy
 - Address Blacklisting
 - Content Filtering
- Deployment Scenario
 - Likely non-universal deployment at the edge

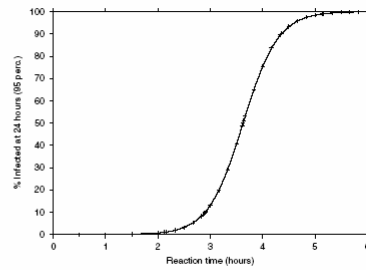
CS6814: Fall 2003

 Washington University in St. Louis

Idealized Deployment



(a) Address Blacklisting

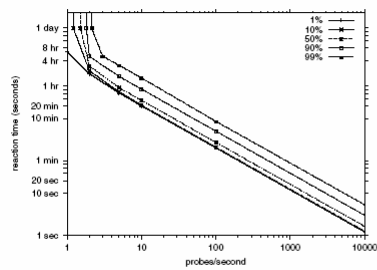


(b) Content Filtering

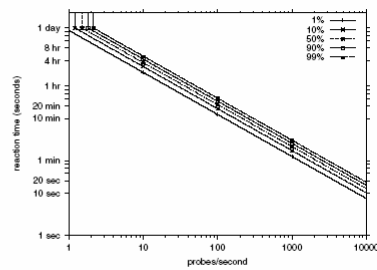
CS6814: Fall 2003



Generalized Worm Containment



(a) Address Blacklisting



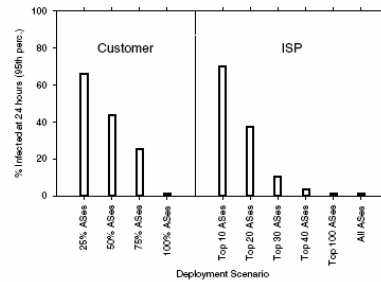
(b) Content Filtering

CS6814: Fall 2003



Practical Deployment

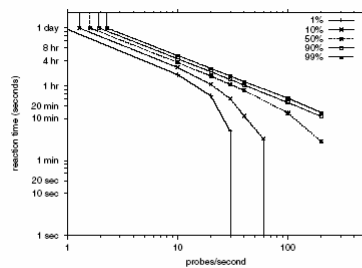
- Network Model
 - Develop an AS graph
 - Identify Vulnerable hosts and their ASes
- Deployment Scenario
 - Assign ASes or Customer Networks to containment system
 - Shortest paths also calculated



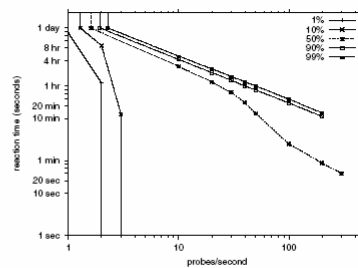
CS6814: Fall 2003



Generalized Containment



(a) Top 100 ISPs



(b) 50% Customers

CS6814: Fall 2003



Conclusions

- Reaction Time
 - Automated
- Containment Strategy
 - Content Filtering
- Blocking Location
 - Widespread