Past Well-known Worm

- Code Red (Jul. 2001)：360,000 infected in 14 hours
- Slammer (Jan. 2003)：75,000 infected in 10 minutes
  Congested parts of Internet (ATMs down…)
- Blaster (Aug. 2003)： 150,000 ~ 8 million infected
  DDOS attack (shut down domain windowsupdate.com)
- Witty (Mar. 2004)：12,000 infected in half an hour
  Attack vulnerability in ISS security products
- Sasser (May 2004)：500,000 infected within two days

- Recent large-scale infections are mostly “Botnets”.

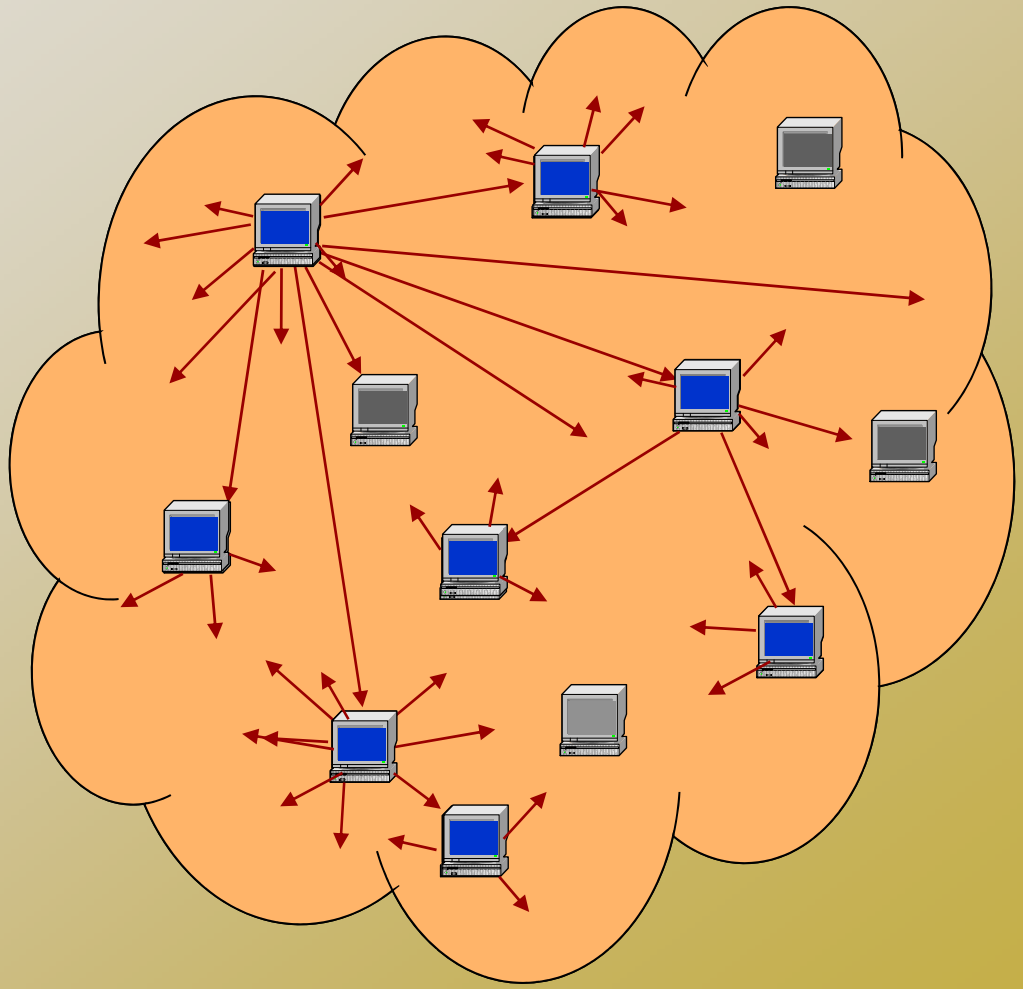
Worm propagation process

- Find new targets
  - IP random scanning

Compromise targets

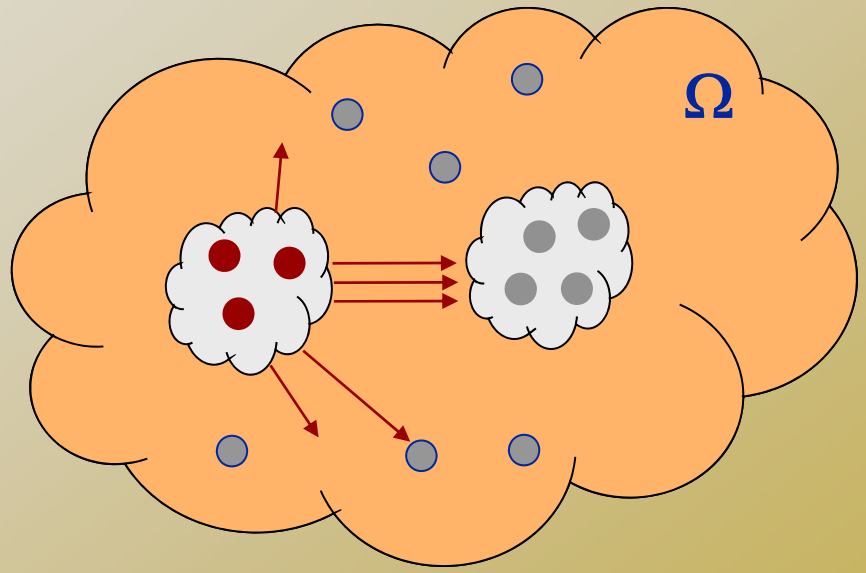
- **Exploit vulnerability**

Newly infected join infection army



Simple worm propagation model

- address space, size Ω
- N : total vulnerable
- I_t : infected by time t
  - N-I_t vulnerable at time t
- scan rate (per host), η



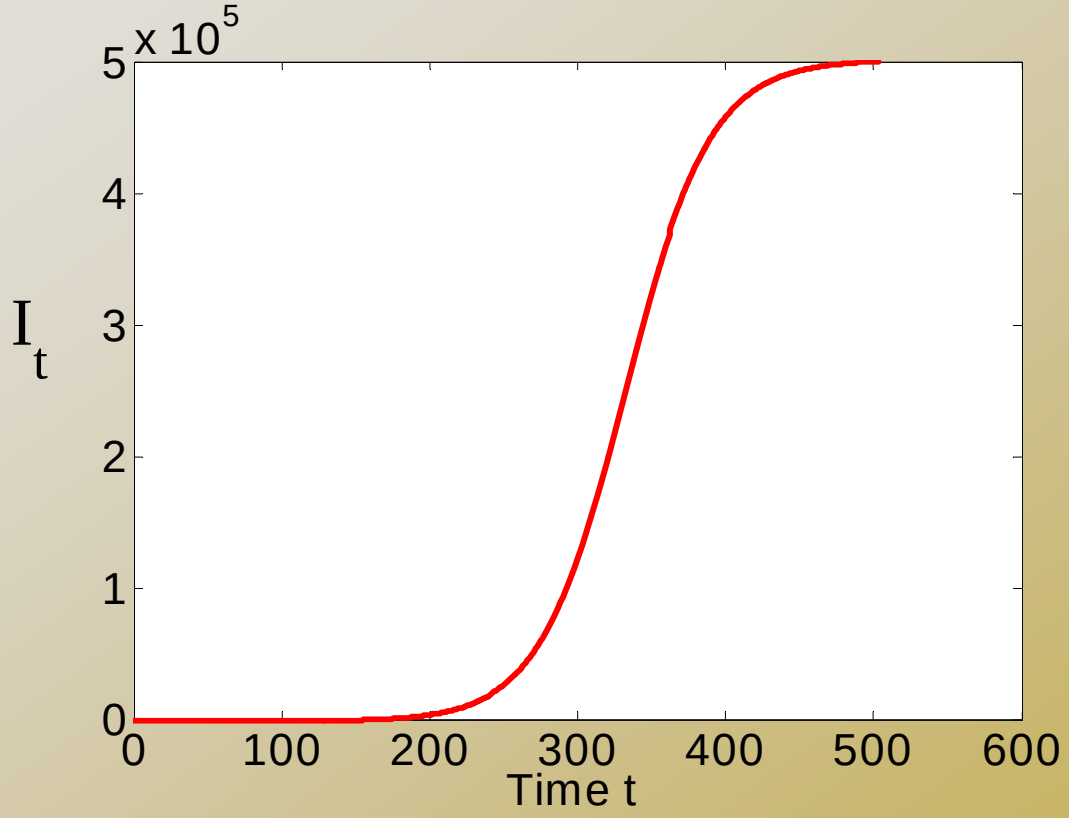
$$\frac{dI_t}{dt} = \frac{\eta}{\Omega} I_t (N - I_t)$$

$$\propto \eta \cdot I_t \cdot \frac{N - I_t}{\Omega}$$

Prob. of a scan hitting vulnerable

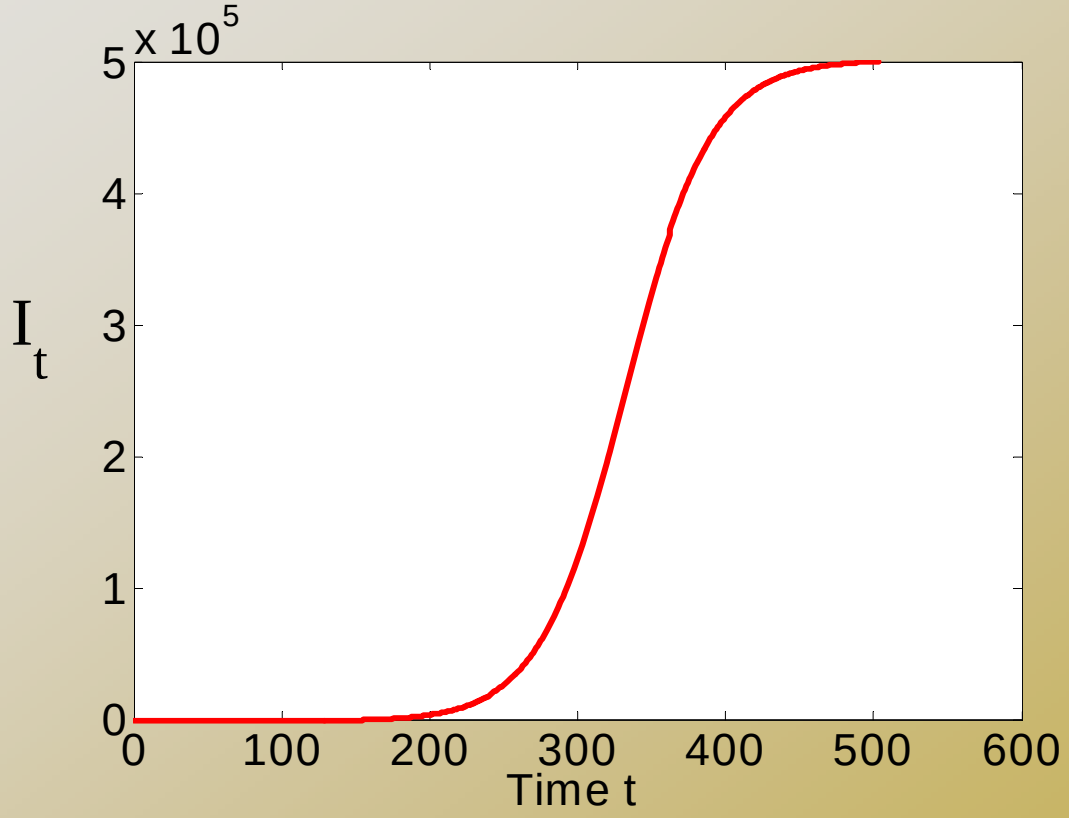
# of increased infected in a unit time

Simple worm propagation



$$\frac{dI_t}{dt} = \frac{\eta}{\Omega} I_t (N - I_t)$$

Simple worm propagation



$$\frac{dI_t}{dt} = \frac{\eta}{\Omega} I_t (N - I_t)$$

Witty worm modeling

- Witty's destructive behavior:
  1). Send 20,000 UDP scans to 20,000 IP addresses
  2). Write 65KB in a random point in hard disk

- Consider an infected computer:
  - Constant bandwidth → constant time T to send 20,000 scans
  - Random point writing → infected host crashes with prob. $p\ (p \ll 1)$
  - Crashing time approximate by

    Exponential distribution (λ) $\frac{1}{\lambda} = \frac{p}{T}$

Witty worm modeling

$$\frac{dI_t}{dt} = \frac{\eta}{\Omega} I_t (N - I_t)$$

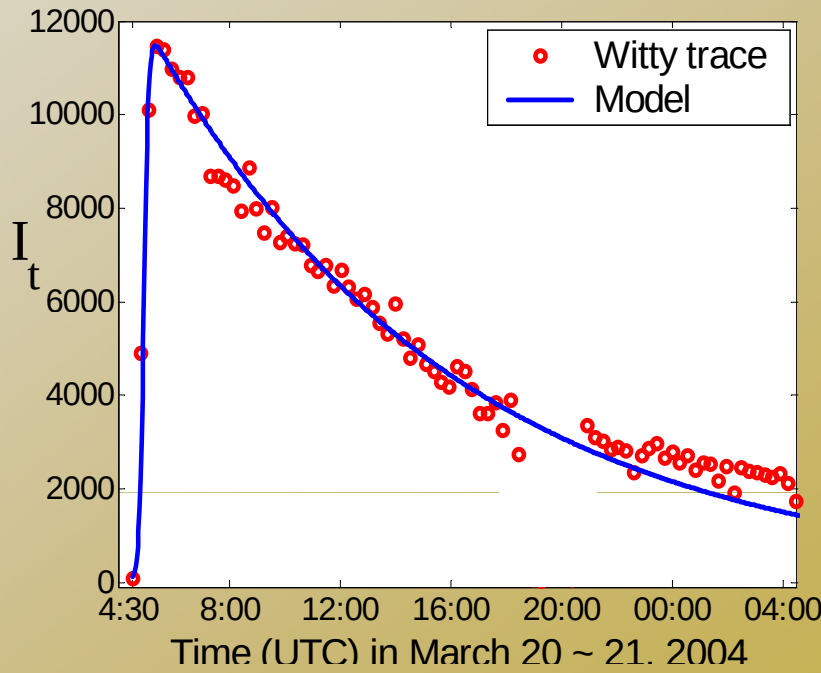
# of vulnerable at t

D_t : # of crashed infected computers at time t

$$\begin{cases} \frac{dI_t}{dt} = \frac{\eta}{\Omega} I_t (N - I_t - D_t) - \frac{dD_t}{dt} \\ \frac{dD_t}{dt} = \lambda I_t \end{cases}$$

Memoryless property

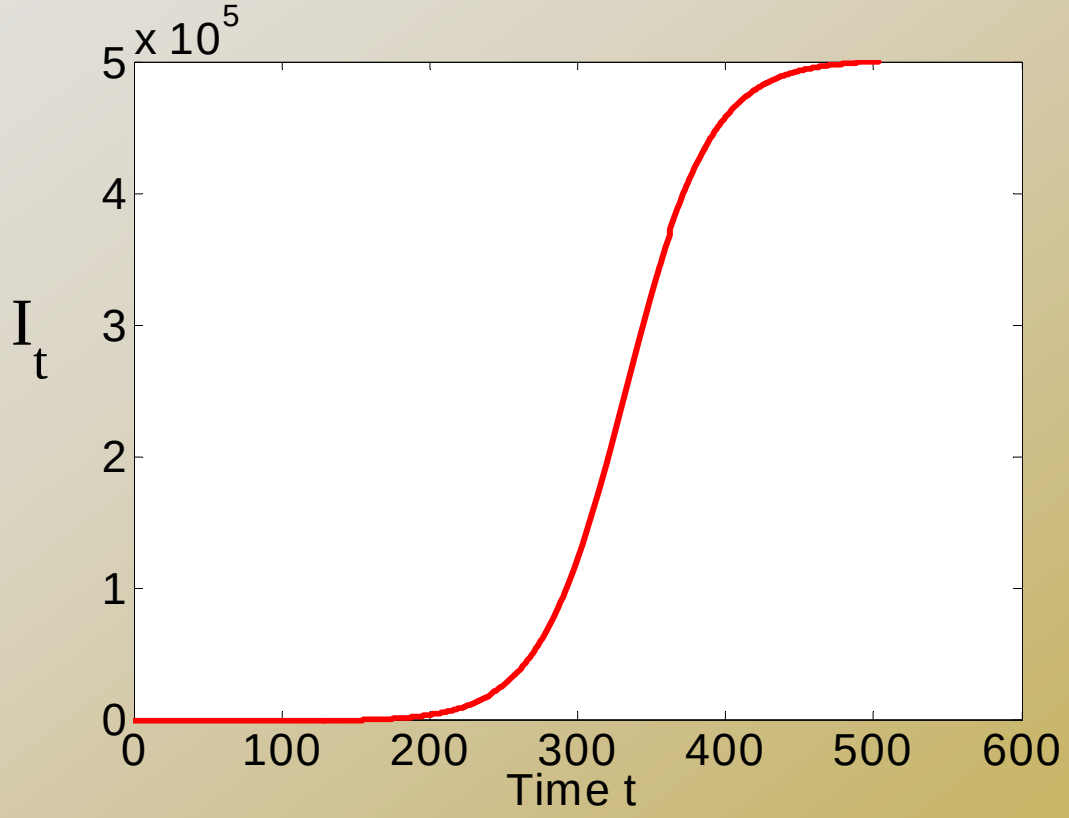
# of vulnerable at t



$\frac{1}{\lambda} = 11.1$ hours

*Witty trace provided by U. Michigan "Internet Motion Sensor"

Simple worm propagation



$$\frac{dI_t}{dt} = \frac{\eta}{\Omega} I_t (N - I_t)$$

Discrete-time Simulation

- Programming project 4

Discrete-Event Simulation

- Each infected node generates “events”.
  - An event is a scan hitting a target machine
  - Even List size == # of infected nodes
  - An event time?
    - The time for an infected scanning a next target
      - Geometric distribution (if we consider discrete time)
      - Exponential distribution

Discrete-Event Simulation

- Pseudo code:
  - [eventTime, k] = min(EventList) (suppose I nodes are infected)
  - Refill EventList[k] with next event time of the node
  - Check which node j this scan hits
    - If (Node[j].status == infected) do nothing
    - If (Node[j].status == vulnerable)
      - Node[j].status = infected
      - EventList add an entry, fill this entry with next event time
      - NodeIndex[I+1] = j /*remember the node index corresponding to EventList*/
      - I = I+1 /* one more get infected */