

# Ground Systems and Cyberwar

*Stuart Staniford,  
President  
Silicon Defense*



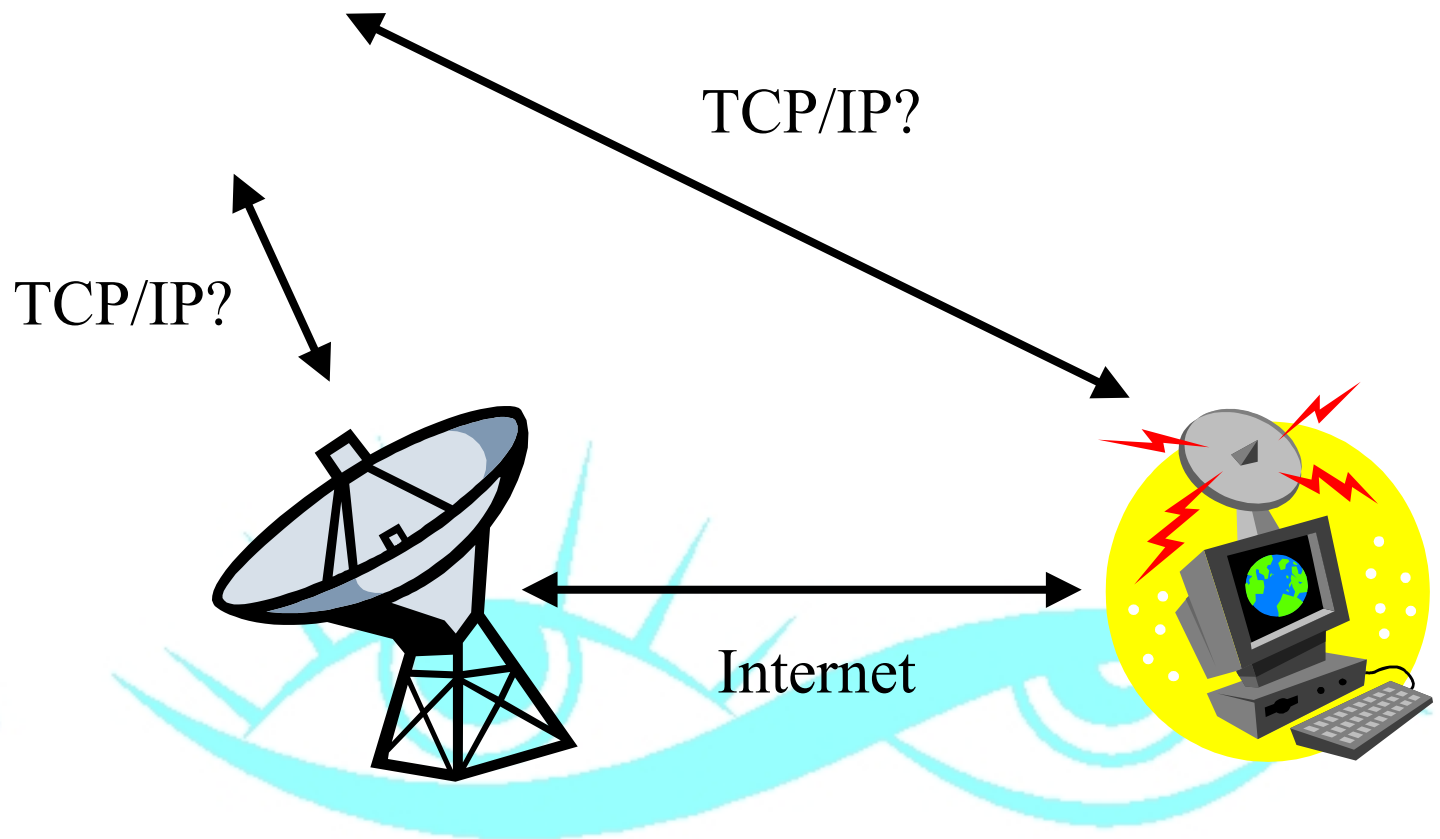
3/13/02



# *Who I am/am not*

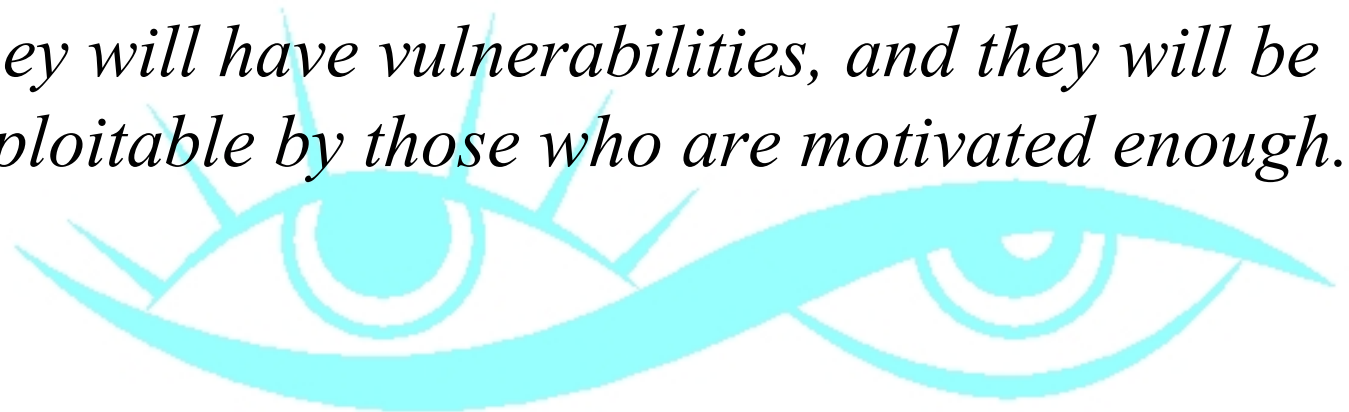
- *I am not*
  - *A ground-systems expert*
  - *Knowledgeable about space or satellites*
- *Knowledge limited to reading last year's talks.*
- *I am*
  - *An Internet security expert*
  - *Background in computer intrusion detection*
  - *Heavily involved in cyberwar research*

# *Notional Architecture*



# *The Bad News*

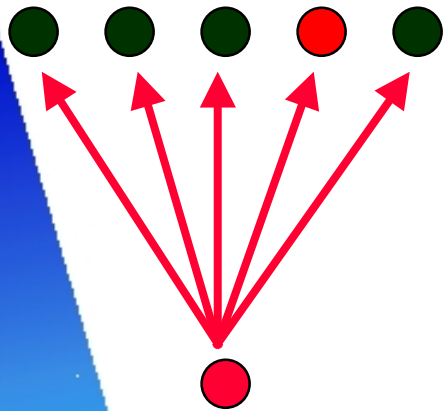
- *Internet Security is in very bad shape*
- *We don't know how to build secure COTS*
- *We don't know how to secure large networks*
- *Therefore these satellite architectures will not be 100% secure.*
- *They will have vulnerabilities, and they will be exploitable by those who are motivated enough.*



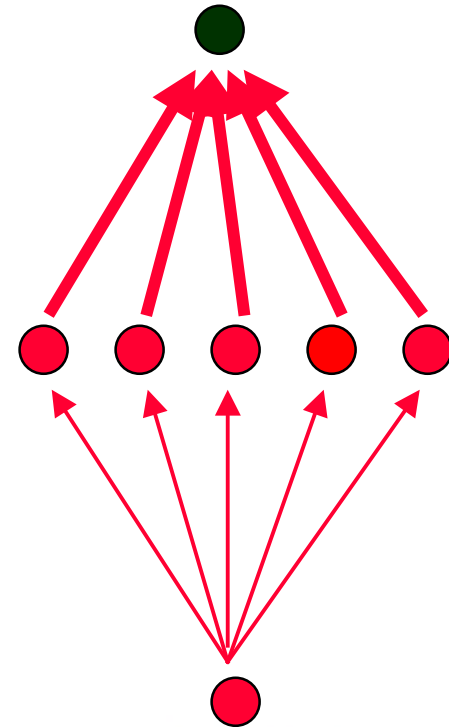
# *Software Vulnerabilities*

- Software always has flaws
- Some are security relevant
- Four phase lifecycle of a vulnerability
- Currently X vulnerabilities in common Internet software
- Many more unknown
- High class adversary can find and exploit new ones

# DDOS attacks

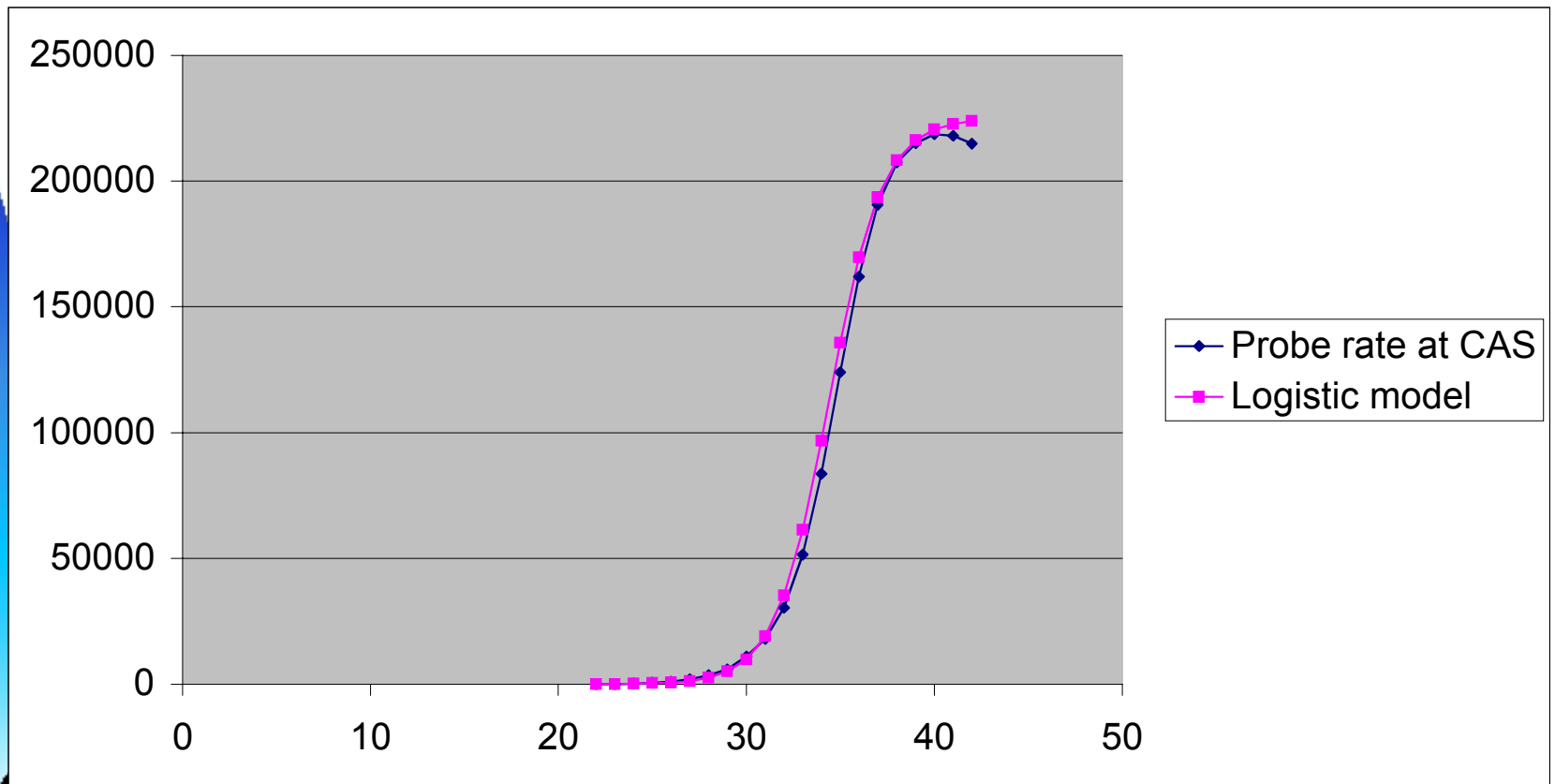


Scan, automated compromise, '000s of hosts randomly



Network of '000s of zombies bombard single target with junk data.

# Worms



$K = 1.8, > 360,000$  hosts infected



# Network Infrastructure Attacks

- There's potential major problems with
  - DNS
  - Routing
  - PKIs



# *Cyberwar*

- Large cyber-attack forces
- Trained, disciplined
- Intelligence preparation
- Concentration of force
- Surprise
- Manouver



# *Solutions?*

- Good housekeeping
  - Firewalls, patches, user education, encryption, turn off unnecessary services, IDS monitoring,...
- Obscurity
- Redundancy
- Expect rough waters ahead at some point