Some Thoughts on The Threat of Internet Worms

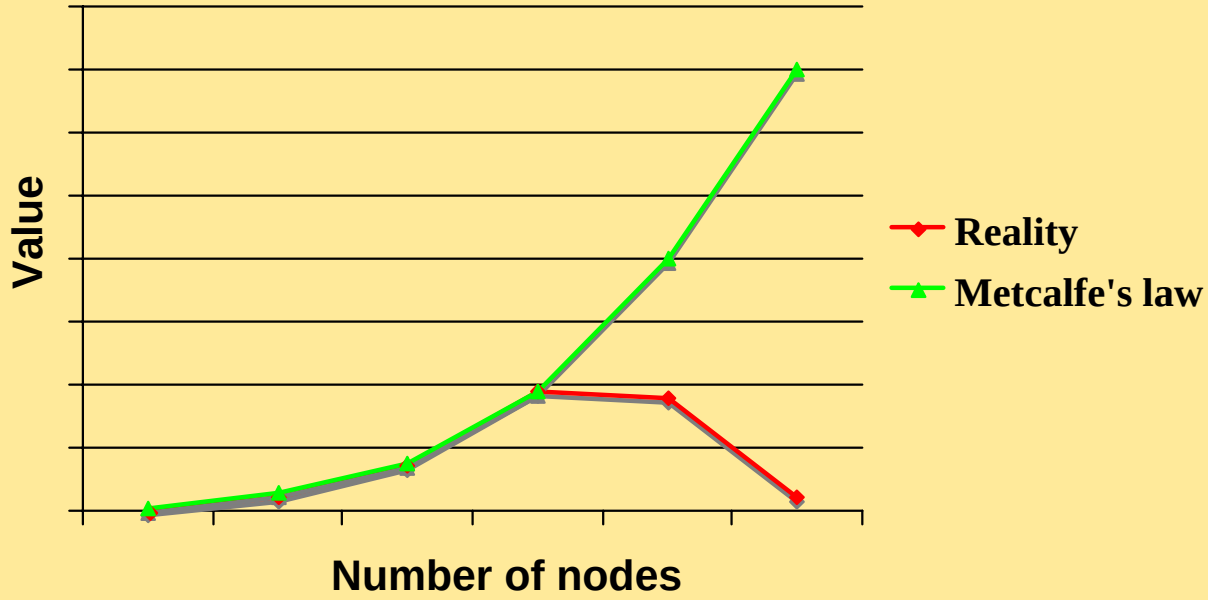
A security research perspective

Kostas G. Anagnostakis, Evangelos Markatos

ICS-FORTH, Greece

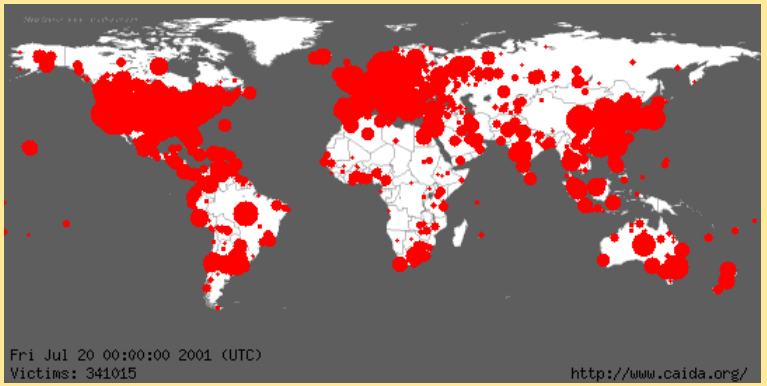
The big picture

- Metcalfe’s Law predicts that the value of a network increases in proportion to the square of the number of users
- Considering all the threats to Internet security, perhaps this law is invalidated?



The threat of Internet worms: a timeline

- Summer 2001: Code-Red worm
  - Infected 350,000 computers in 24 hours
  - Proof-of-concept
- January 2003: Sapphire/Slammer worm
  - Infected 75,000 computers in 30 minutes
  - Demonstrated the need for automated defense mechanisms
- March 2004: Witty Worm
  - Infected 20,000 computers in 60 minutes
  - A “niche” worm targeting a system deployed in <<0.1% of the Internet



Existing defense mechanisms

- First generation:
  - Faster software updates
  - Content-based detection/filtering of known worms
  - Network telescopes
  - Honeypots/honeynets
- In the pipeline:
  - Scan blocking
  - Content sifting

“Next-generation” worms: co-evolution!

- Attackers can easily circumvent defenses
  - **Day-zero** worms beat signature-based detection
  - **Polymorphic** worms beat content sifting
  - **Hitlist** worms beat scan-blocking
  - **Stealth** worms beat scan detection
- Worms can carry destructive payloads
  - Large-scale coordinated DDoS attacks
  - Data corruption
  - Flash system/device firmware

Observations on the current state of affairs

- So, why isn't the Internet "secure" yet?
  - Security is a moving target: networks get faster, attackers get smarter, new apps
  - Knee-jerk reaction: we're always one step behind
  - Insufficient cooperation
  - Lack of incentives
  - …Economics!

What do we need

- Automated defense mechanisms
- High-performance
- Flexibility
- Cooperation
- Incentives

SCAMPI, LOBSTER and NoAH

- SCAMPI (4/01-1/05):
  - R&D in scalable network monitoring
  - Developed a 10 Gbit/s monitoring adapter, and API
  - Faster content inspection for detecting attacks
- LOBSTER SSA (10/04-10/06):
  - Deploy a monitoring infrastructure across Europe
  - Quasi-public access to network data for operators, security analysts, researchers
  - Focus on cooperation
- NoAH SSA (1/05 -)
  - Deploy a network of affine honeypots
  - Focus on cooperation and application-level detection

Closing remarks

- No silver bullet. Need to work hard on:
  - Research (manpower-expertise-infrastructure)
  - Cooperation
  - Flexibility at all levels
  - Incentives