Secure Grid Computing: an Empirical View

IFIP WG 10.4 Workshop on Grid Computing and Dependability

Carl Landwehr (clandweh@nsf.gov**)**
Cyber Trust Coordinator
National Science Foundation

… with thanks to Matti Hiltunin, Bill Cheswick & Brian LaMacchia

July 2, 2005

Grid Computing Application area:

Matti's talk definitions:

Grid computing: collaborative use of computers, networks, databases, scientific instruments, and data; potentially owned and managed by multiple organizations. –

- Scale: thousands of machines common
- Geographic: worldwide distribution common; transfer large volumes of data across the world
- Administrative: span multiple domains
- Trust: execute tasks on untrusted computers

- Most successful grid application in practice?
- Perhaps it's controllers and zombies conducting DDOS attacks and sending spam!
- Multiple domains, encrypted signals, coordinated computation, shifting sets of processors, …

NETWORKWORLD

Shakedown on the ‘Net

By Ellen Messmer, NetworkWorld.com, 05/16/05

… extortionist launches a distributed-denial-of service (DDoS) attack, flooding the access to your Web site with unwanted traffic or knocking it offline.

…Does the business pay up?

… it appears that all too often victimized businesses are giving in to the shakedown.

… it’s hard to bring these ‘Net shakedown artists to justice.

…The cost for a few months of anti-DDoS service can add up to a payment to an extortionist, so some see it as an equal burden monetarily.

That’s a sad state for the industry to be in.

http://www.networkworld.com/weblogs/security/008861.html

The Marketplace: Botnet Rental Rates

- From IFIP WG 10.4 47th mtg, Brian La Macchia
- Data fall 2004
- 6 cents per bot-week on offer:
  - Price: $350 weekly, $1,000 monthly
  - Type of service:
    - exclusive (one slot only)
    - Always online (5,000-6,000)
    - Update every (10 minutes)
- Other examples:
  - 3.6 cents per bot-week
  - 2.5 cents per bot-week

How the Market for Zombies Can Lead to Secure Grid Computing

- Today, unmonitored, unpatched home PCs are a big source of zombies used in DDoS attacks
- How to improve patch rate on these PCs?
- Possible service: vendor provides free remote patching and updating service for PCs

Late 1990's: Venture Capital Approach

- Startup company offers the service
- Make it "free":
  - Customer just downloads a bit of software
  - Software occasionally shows the user an ad to pay for itself
  - Periodically visits server with latest patches, etc., and downloads them
- Company lives on the advertising revenue
- User endures slight annoyance or perhaps pays a small annual subscription fee to avoid ads
- Company goes public and investors get rich!

2005:
Internet Cyber Security Ecology

- Blackmailer locates potential victim business
- Blackmailer seeks source of zombies
- Home user connects new PC to the Internet
  - Maybe it has a flaw, a weak password, misconfiguration
  - Maybe user browses to web site that installs flawed spyware
- Hacker scanning for victims exploits flaw to compromise machine and turn it into a zombie

Cyber Security Ecology (concluded)

- Hacker strategy: make money by selling access to the machine for spamming, DDoS attacks, etc.
- Hacker tactics:
  - 1. **Close other holes on the machine** so that other competing hackers can't seize his asset
  - 2. **Use just enough of the machine to make money** without bothering home user (or user will discover his exploits and kick him out)
- Sell to the blackmailer
- Victim business pays blackmailer,
- Blackmailer pays zombie-provider ("herder")
- Home user's computer stays patched, produces revenue by computing functions for others

Symbiosis!

- Hacker sells cycles on machine that user didn't need anyway
- In return, hacker protects user from everyone else, like a barracuda shepherding a school of scissortails

The future we want?

- **Maybe not, but it may be the future we get!**

- **We need to get out of this box!**