

The XenoService — A Distributed Defeat for Distributed Denial of Service

Jianxin Yan, Stephen Early, Ross Anderson

Computer Laboratory, Cambridge University

Distributed Denial of Service

- **Exploits a number of subverted machines (attack bots)**
- **Launches a large coordinated packet flood, which is**
 - more than a target can cope with
 - very difficult to stop
- **Exploits much the same vulnerabilities as previous DoSs**
 - UDP flood, SYN flood, ICMP directed broadcast ('smurf'), etc.

3 methods proposed to combat DDoS attacks:

- **Secure hosts:** nowhere to install attack bots
- **Egress filtering:** prevent IP spoofing
- **Fixes for specific vulnerabilities**
 - SYN flood ← SYN cookie
 - Smurf attack ← reduce smurf “amplifiers”
 - Etc.

Our Comments:

- **None of these will provide a complete solution**
- **DDoS is a system problem, not a matter of any specific technology**

Incentive issues

- **“How can I prevent this type of attack happening to ME?”**
 - There is little users can do to protect themselves directly, as DDoS attacks exploit vulnerabilities in others’ systems!
- **Scenario #1: virus**
 - Pay \$100 to prevent yourself from attacks of virus
- **Scenario #2: DDoS**
 - Economic incentives change
 - Rational choice:
 - Not pay this money to stop Amazon being attacked
 - Keep the money and hope not to be one of the small minority that become a target

Incentive issues

- **DDoS: an example of Tragedy of the Commons**

Tragedy of the Commons (1833)

- Every peasant has an interest in protecting a shared resource (*grazing*), but has a stronger motive to cheat (*by putting an extra sheep on the common land*)

Tragedy of the Commons (2000)

- Everyone has an interest in protecting a shared resource (*Internet security*), but has a stronger motive to cheat (*by connecting insecure computers*) in order to save costs/effort

- **Solution:**

- Traditional Chinese solution: Imperial Civil Service
- **Internet: need economic incentives**

Liability issues

- **View of an economist (Hal Varian) :**
 - Force the owners of systems from which attacks originate to pay for the damage they cause.
 - Liability should fall on whoever is in the best position to manage it.
 - The majority of users have no idea how to defend their computers, so costs should fall on the network operator.
- **Normal users have no liability at all?**
 - No. → attack bots everywhere!
 - Yes. → sanction on users imposed by ISP. ✓
- **Longer term: sue vendors over vulnerabilities in their software/hardware?**

How can you deal with the problem NOW?

- **Have huge bandwidth** (e.g., www.microsoft.com)
 - but expensive
- **Have widely replicated web service** (e.g., Akamai)
 - still expensive if enough bandwidth
- **Dynamic DNS:** One site \Leftrightarrow one DNS name \Leftrightarrow multi IP addrs
 - distribute the load to different machines
 - dilute DDoS attack traffic
 - attackers can get IP addrs just like genuine customers
- **Above all limited by static allocation of resources**
 - must provide in advance for maximum DDoS traffic everywhere
- **Also, costs fall on the owner of the attacked site, not on the owners of networks from which attacks come**

The XenoService: pull Economics & Technology together

- **XenoService**

- a distributed network of web hosts (*Xenoservers*)
- responds to a DDoS (or a surge in genuine demand, e.g., slashdot) on any hosted site by replicating it rapidly and widely
- the attacked site can quickly acquire more network connectivity than Microsoft → absorb a packet flood and continue trading;
- effective economic incentives for the principals to behave properly

→ **A distributed means of defeating DDoS**

Xenoservert[†]:

- Developed at SRG, Computer Lab of Cambridge University
- Developed to distribute applications so as to
 - circumvent long communication latencies
 - avoid transferring data over congested or expensive network links
- QoS guaranteed resource management
 - applications receive QoS guarantees for requested resources
 - prevent DoS attacks due to excessive resource usage by applications
- Accounted execution of untrusted code
- Enables replication of dynamic as well as static content

[†]From the Greek ξενος, a travelling stranger invited into one's house for rest and sustenance.

The XenoService: *a distributed means of defeating DDoS*

- **Business Model**

- ISPs worldwide install Xenoservers; offering a resilient web hosting service at a premium price
- QoS of each website is monitored
- When QoS deteriorates, website is immediately replicated to other Xenoservers
- Incentive for ISPs: maintain sufficient Xenoservers to meet whatever service levels set in contracts
- An ISP can rent additional capacity from other ISPs if needed
- Insure against the costs of absorbing severe DDoS attacks

The XenoService: Some Applications

- **XenoService can be:**
 - Operated as a public commercial service
 - Used in closed environment
- **Government environment**
 - Obvious targets of DDoS, e.g. Dept. of Justice
 - Natural capacity to replicate a service under attack to huge numbers of other servers (Commerce, Energy, Health, Immigration, ...)

Conclusion

- **Liability enforcement helps prevent DDoS, but it is absent or insufficient**
- **Dynamic web site replication supported with**
 - appropriate technology
 - sensible business model enforcing liability issue



A large part of the solution for DDoS