Distributed Denial of Service Attacks

Steve Crocker
Chair, SSAC

June 25, 2007

San Juan, Puerto Rico

Agenda

- Types of Attacks
- DDoS attacks
- Amplified DDoS attacks - 2006
- Estonia - May 2007
- What do Do

Types of Attacks

- Penetration
- Eavesdropping
- Man-in-the-Middle
- Flooding

Penetration

- Attacker gets inside your machine
- Can take over machine and do whatever he wants
- Achieves entry via software flaw(s), stolen passwords or insider access

Eavesdropping

- Attacker gains access to same network
- Listens to traffic going in and out of your machine

Man-in-the-Middle (‘MITM”)

- Attacker listens to output and controls output
- Can substitute messages in both directions

Flooding Attack

- Attacker sends an overwhelming number of messages at your machine; great congestion
- The congestion may occur in the path before your machine
- Messages from legitimate users are crowded out
- Usually called a Denial of Service (DoS) attack, because that’s the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack

Effects of Attacks

- Modification of internal data, change of programs
  - Includes defacement of web sites
- Destruction of data
- Unauthorized Disclosure
- Denial of Service (DoS)

Attacks and Effects

	Mod	Des	Disc	DoS
Penetration	X	X	X	X
MITM		X	X	
Eavesdropping			X	
Flooding				X

Denial of Service Attacks

- A Denial of Service (DoS) attack is an orchestrated traffic jam
- Purpose is to shut down a site, not penetrate it.
- Purpose may be vandalism, extortion or social action (including terrorism)
  - Sports betting sites often extorted
- Large numbers of attacks -- few visible
  - Estonia
  - Root servers, TLD operations

Distributed DoS (DDoS)

- Most common DoS attacks use thousands of computers
  - Sometimes hundreds of thousands
- Individual computers ("zombies") are penetrated and marshaled into common force ("bot armies")
- Tools easily available
- Bot armies available for rent

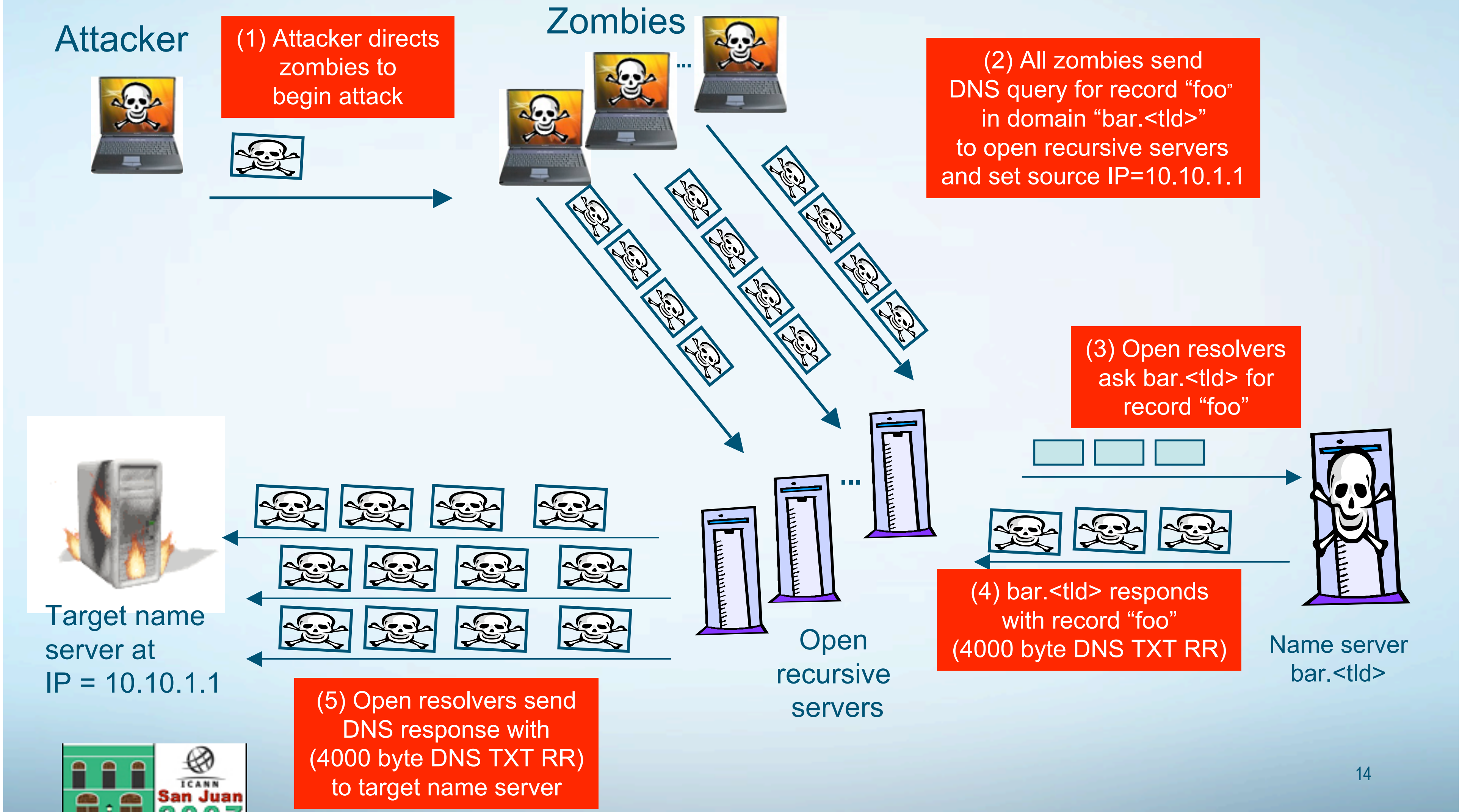
Amplified DDoS Attacks

- New wrinkle observed last year
- Bots send DNS queries with false return addresses
- Responses are aimed at target
- Responses are much larger than queries

January - February, 2006

- Authoritative TLD DNS servers attacked
- Variant of a well-known DDoS attack
- Attacks generated from 2 - 8 Gbps
- Failures occurred at multiple points
- Resulted in disruption of DNS services
- Included many TLDs without any apparent motive in most cases

Anatomy of the Amplification Attack



(1) Attacker directs zombies to begin attack

(2) All zombies send DNS query for record “foo” in domain “bar.<tld>” to open recursive servers and set source IP=10.10.1.1

(3) Open resolvers ask bar.<tld> for record “foo”

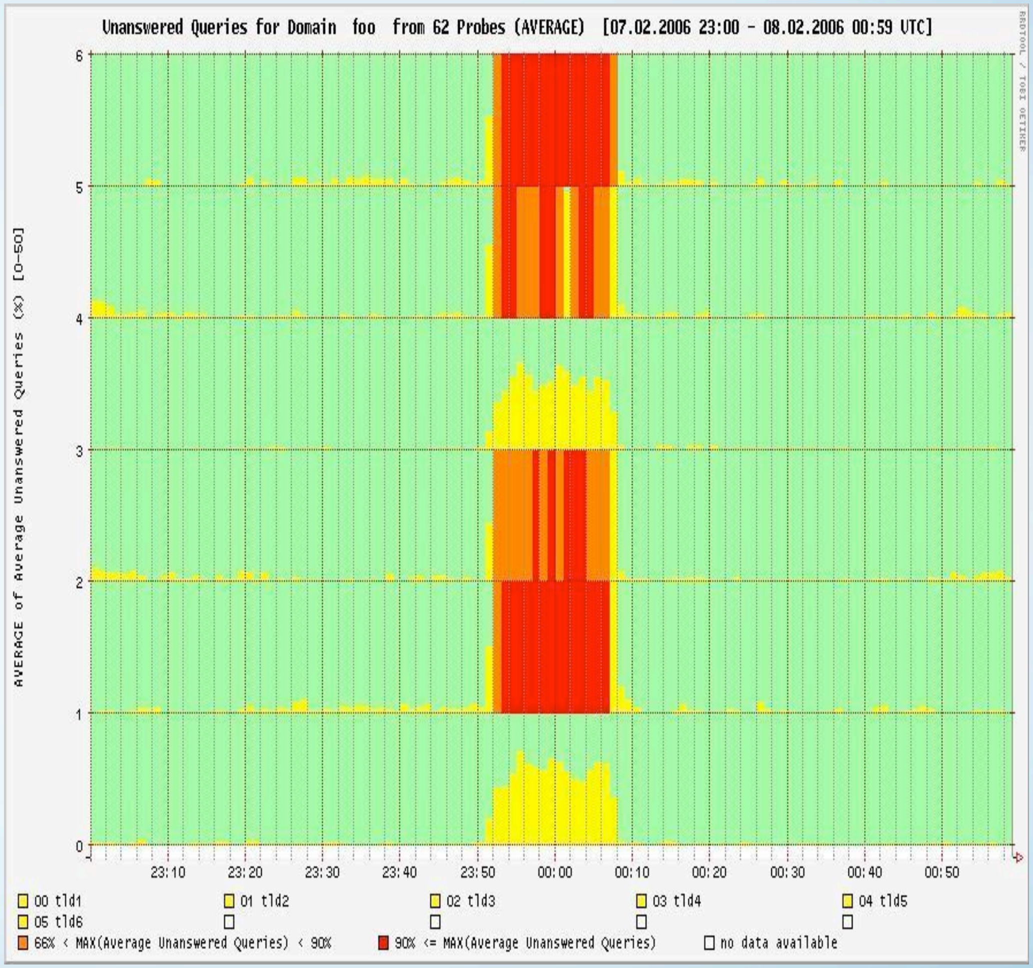
(4) bar.<tld> responds with record “foo” (4000 byte DNS TXT RR)

(5) Open resolvers send DNS response with (4000 byte DNS TXT RR) to target name server

One Attack

Graph of responses to monitoring probes by the authoritative nameservers for a TLD before, during, and after an attack in February 2006.

Vertical Axis shows the six TLD Server IP addresses. Red shows complete failure to answer, yellow indicates slow answers. For reference, Servers 1 and 4 show lesser impact than Servers 2, 3, 5, and 6. The horizontal axis shows actual time. This attack lasted 14 minutes.



Graphs courtesy of RIPE NCC.

Attack Metrics (1)

- 51,000 open recursive servers were involved
- 55 byte query resulted in a 4,200 byte response, for a 1:76 amplification
- 8 gbps attack requires a total of 108 mbps of queries.
- Each recursive server saw 2,100 bytes of queries, or 38 qps, and responded with 160 kbps in answers
- Assuming compromised hosts have minimum 512kb DSL modem, only 200 compromised hosts were required

Attack Metrics (2)

- Source networks would see no effect
- Recursive servers saw minimal traffic or query increase
- Victim network providers had catastrophic experience
- Victim DNS provider was sent the equivalent of 150 million qps
- At best, 1 in 100 real queries were answered

Estonia Attack

- Estonia
- Protests & Cyber Attacks
- Response

Estonia

- 1.4 million people
- Substantial ethnic Russian minority
- Extensive Internet use
  - – Banking, voting, petrol purchase, etc.
  - – 60% use Internet daily
  - – “Real life” and Internet intermingled
- Only a few connections to other countries

Protests & Cyber Attacks

- Relocation of Russian statue triggered protests
  - Outside Estonia as well as inside
- Defacement and DDoS
- Attacks were dominated by bot armies
- Almost all traffic came from outside

Response

- Excellent coordination inside Estonia
  - CERT, ISPs
- Technical people and government institutions communicated, cooperated
- Help from outside
- External traffic to government stopped

References

- mp3 talk from Hillar Aarelaid http://www.ripe.net/ripe/meetings/ripe-54/presentations/friday.html. mp3: http://www.ripe.net/ripe/meetings/ripe-54/podcasts/plenary-10.mp3
- (talk is at 38 minutes)

Comments & Possible Policy Options

- DDoS attacks are a serious problem
  - Good hygiene protects against penetration
  - No good protection against DDoS
- Coordinated community action required
- CERTs, etc. good for response
- Need better design and operation

Two Specific Actions

- Require address validation
  - All packets coming into a network must have a valid return address
  - Won’t solve the full problem but will reduce a large range of attacks
- Label and prioritize traffic coming from protected sources
  - Reward non-zombie sites

References

SAC004 Securing The Edge (17 October 2002)

SAC008 DNS Distributed Denial of Service (DDoS) Attacks (31 March 2006)

http://www.icann.org/committees/security/ssac-documents.htm