Denial of Service

Brighten Godfrey
CS 538 October 18 2012

DoS in the real world

Source: Arbor Networks

Disclaimers:

- Survey of 111 network operators, not direct measurement
- Arbor sells network security solutions :-)

Figure 17 Source: Arbor Networks, Inc.

DDoS is frequent and can be big

Average Number of DDoS Attacks per Month

Legend:
- 0
- 1-10
- 11-20
- 21-50
- 51-100
- 101-500
- 500+
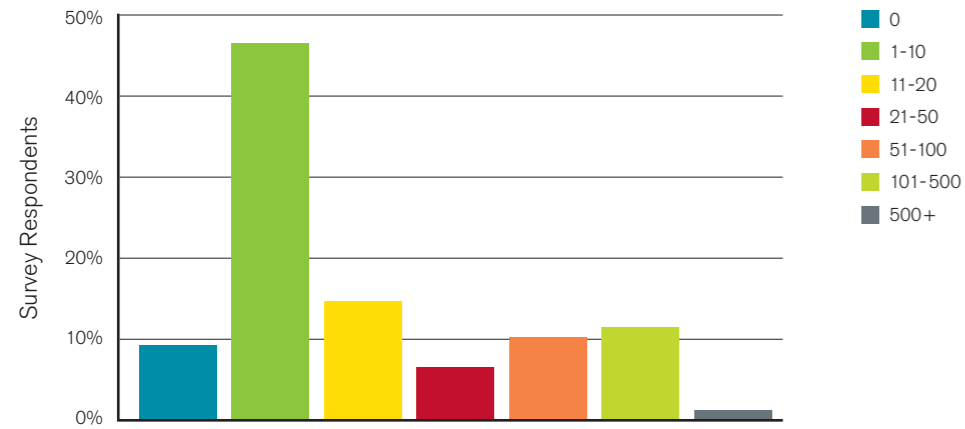
Figure 17 Source: Arbor Networks, Inc.

Largest Bandwidth Attacks Reported

Legend:
- Commercial NetFlow analyzers
- In-house developed scripts/tools
- Open Source NetFlow analyzers
- Open Source SNMP-based tools
- Deep Packet Inspection
- Commercial SNMP-based tools
- Other

Years: 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011
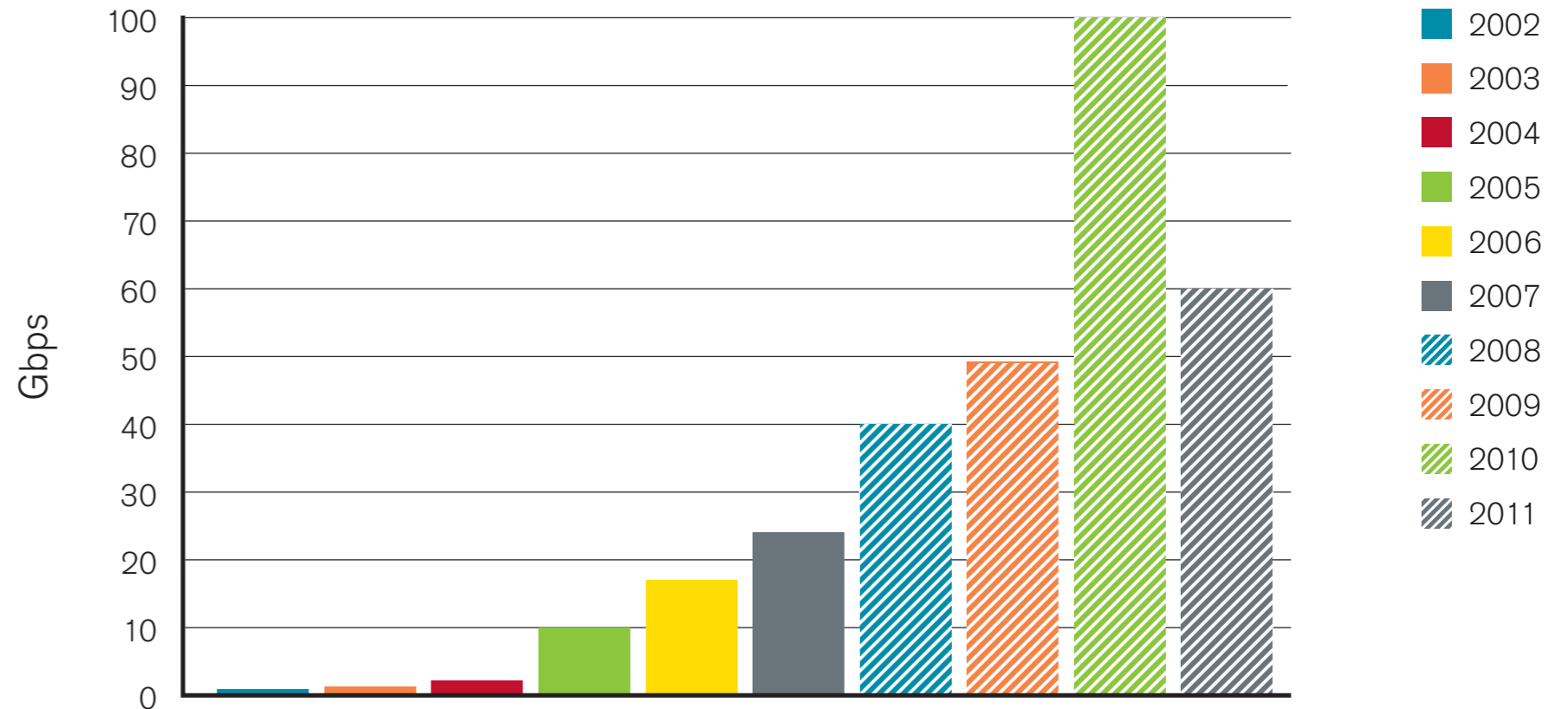
Figure 15 Source: Arbor Networks, Inc.

Many types of attacks

Largest Observed Attack Vectors

- Flood-Based (e.g., UDP, ICMP)
- Protocol-Based (e.g., RST, SYN, Frag)
- Application-Based (e.g., URL, GET, DNS, SQL)
- Other

45%
6%
26%
23%
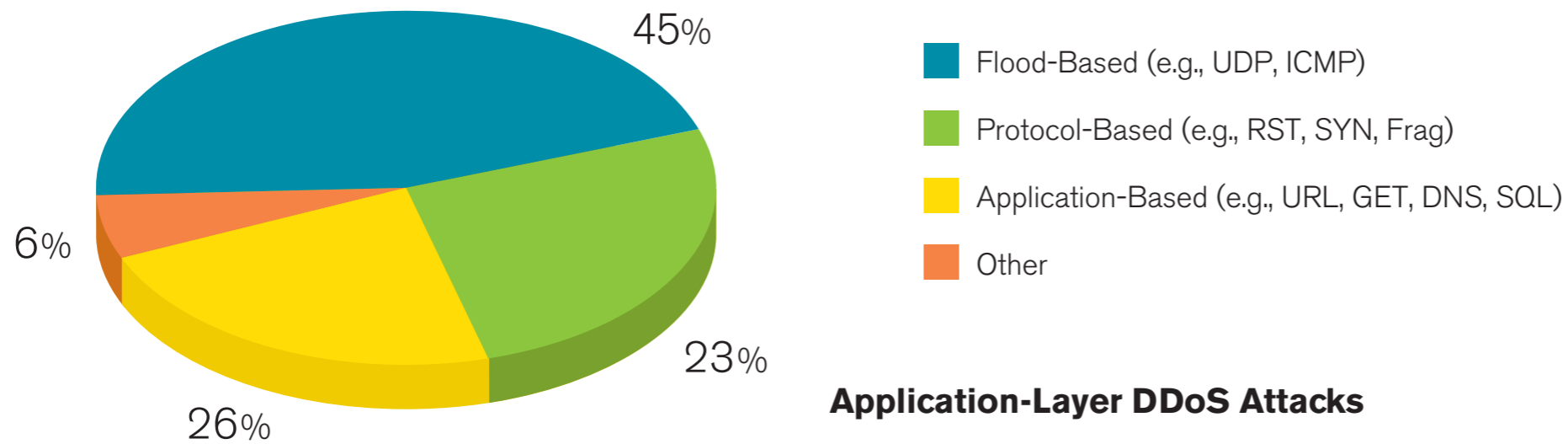
Figure 6: *Largest Observed Attack Vectors*
Source: Arbor Networks, Inc.

[2009 data]

Application-Layer DDoS Attacks

- HTTP
- DNS
- SMTP
- HTTP/S
- SIP/VoIP
- IRC
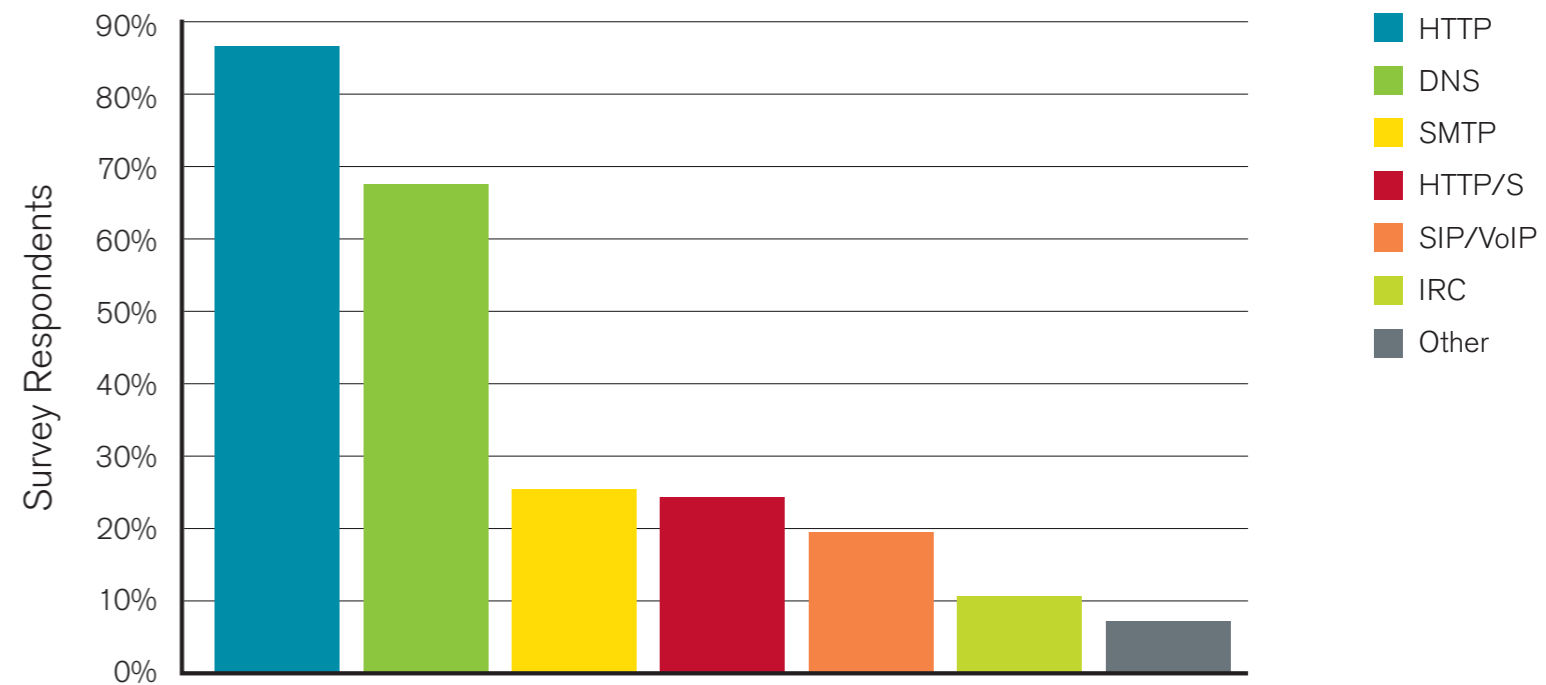- Other

Survey Respondents

Figure 7 *Source: Arbor Networks, Inc.*

Attack Motivations Considered Common or Very Common
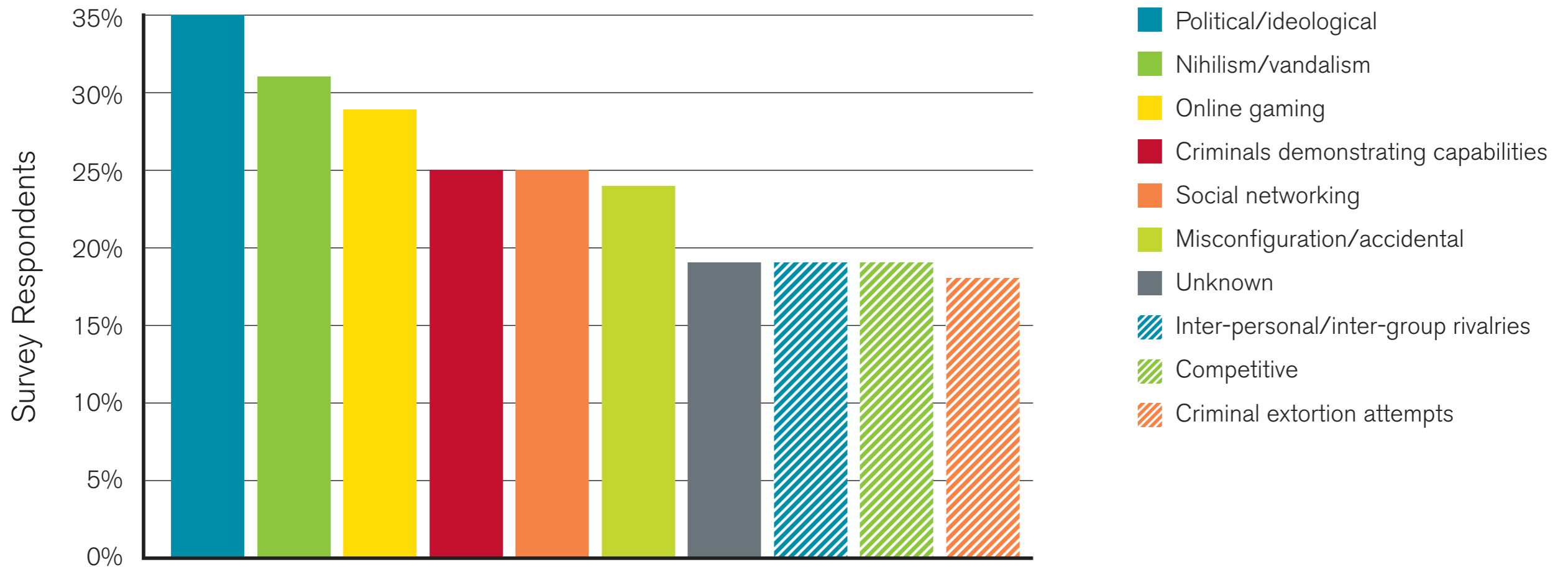
Figure 20 *Source: Arbor Networks, Inc.*
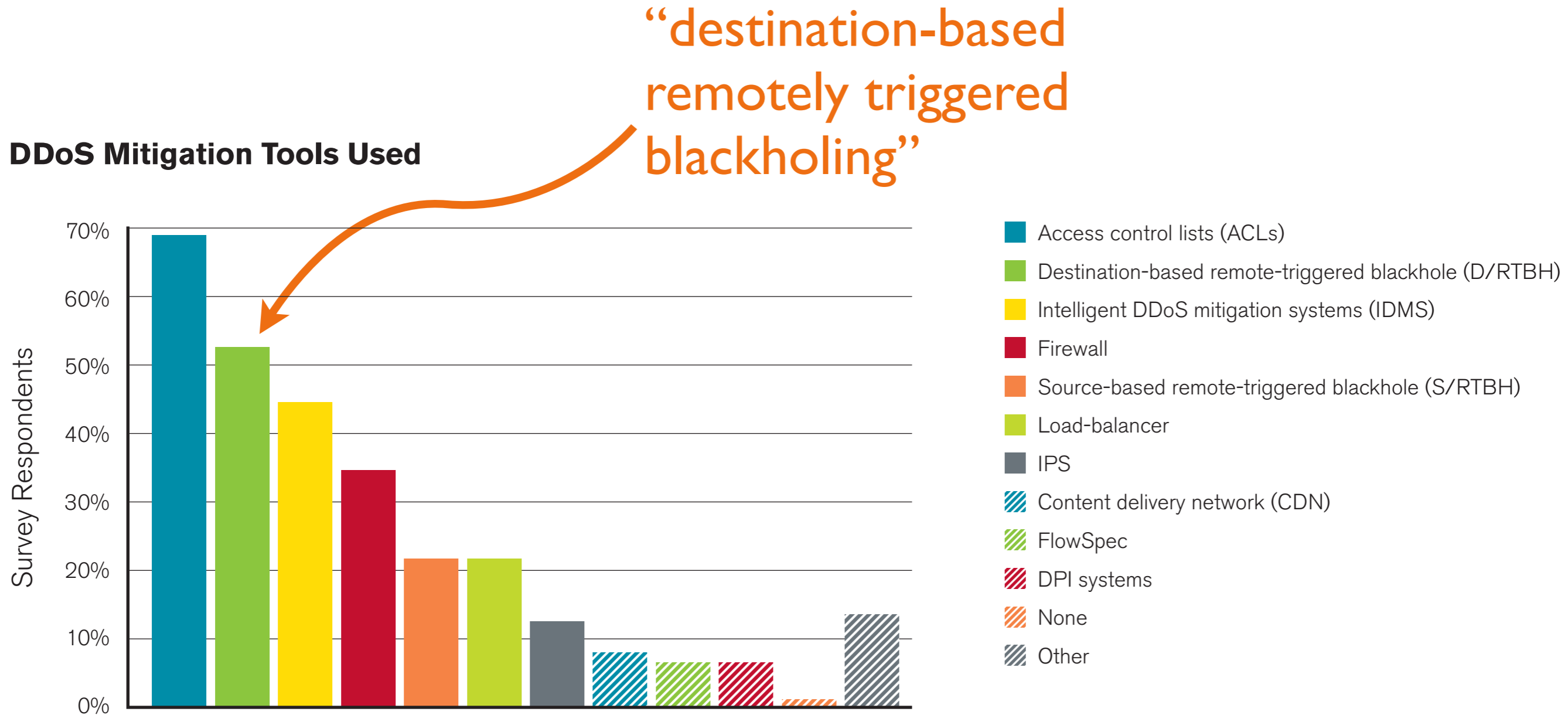
DDoS defense

"destination-based remotely triggered blackholing"

DDoS Mitigation Tools Used

Legend:
- Access control lists (ACLs)
- Destination-based remote-triggered blackhole (D/RTBH)
- Intelligent DDoS mitigation systems (IDMS)
- Firewall
- Source-based remote-triggered blackhole (S/RTBH)
- Load-balancer
- IPS
- Content delivery network (CDN)
- FlowSpec
- DPI systems
- None
- Other

Figure 27 *Source: Arbor Networks, Inc.*

Most Significant Operational Threats
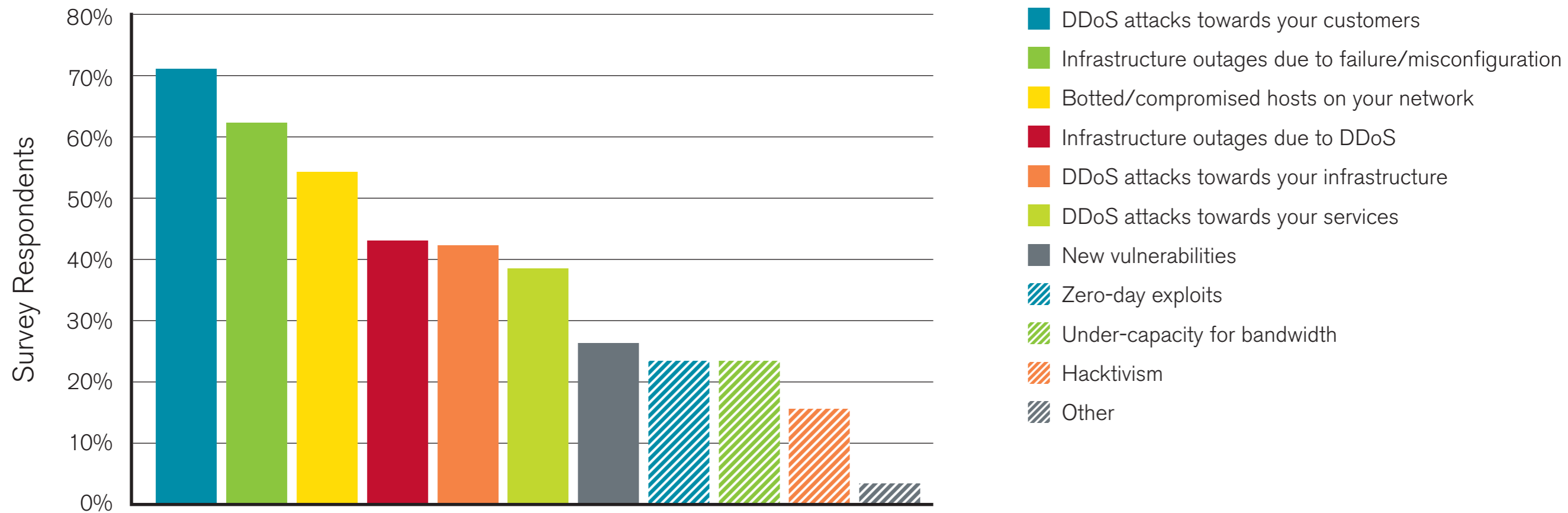

Figure 6 *Source: Arbor Networks, Inc.*

Announcements

Week after next: midterm project presentations

- Be ready by Tuesday of that week
- 5 minute presentation, 5 minute questions
  - What problem are you solving?
  - Why has past work not addressed the problem?
  - What is your approach for solving it?
  - What are your preliminary results & progress?