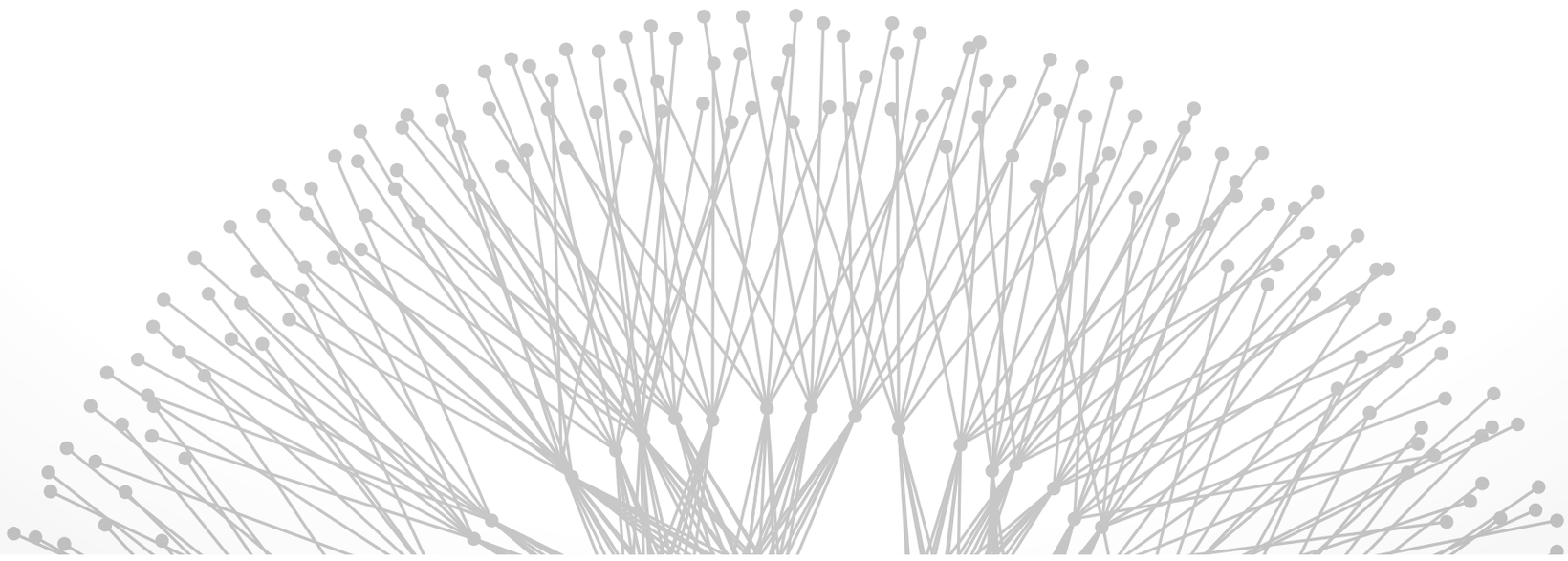
Denial of Service

Brighten Godfrey
CS 538 October 24 2013



but first,

Routing Security, continued

Not just malicious attackers

Many or most high-profile outages likely just configuration errors

Natural correspondence between attackers and bugs

- behavior unknown ahead of time
- defense is to limit and contain worst-case effects

What about a bug in the protocol?

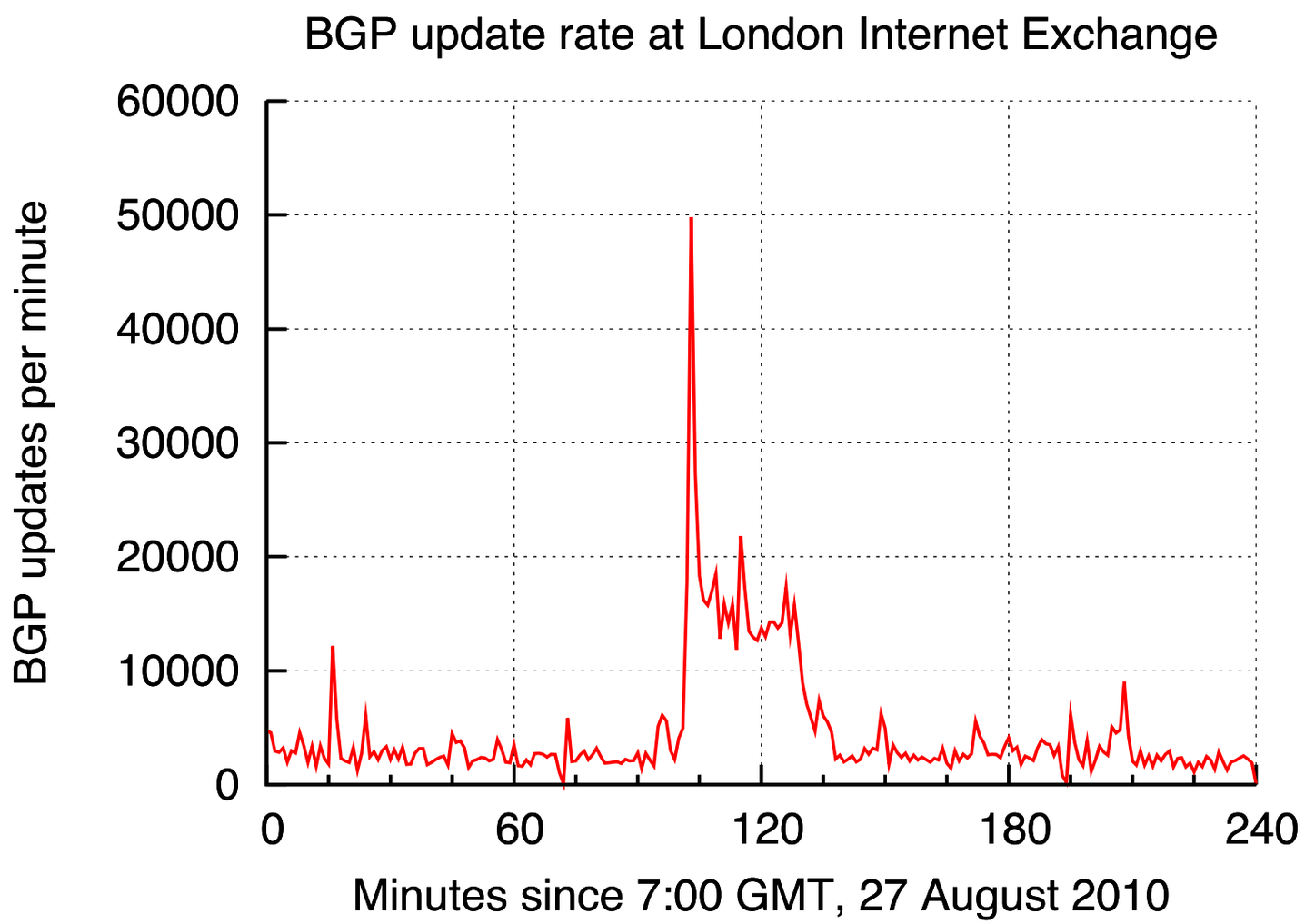
- worst-case scenario: zero-day exploit on large fraction of routers across the entire Internet
- many are running the same software!

A (bad) day in the life of the Internet

About 1% of Internet destinations disrupted for about 30 minutes

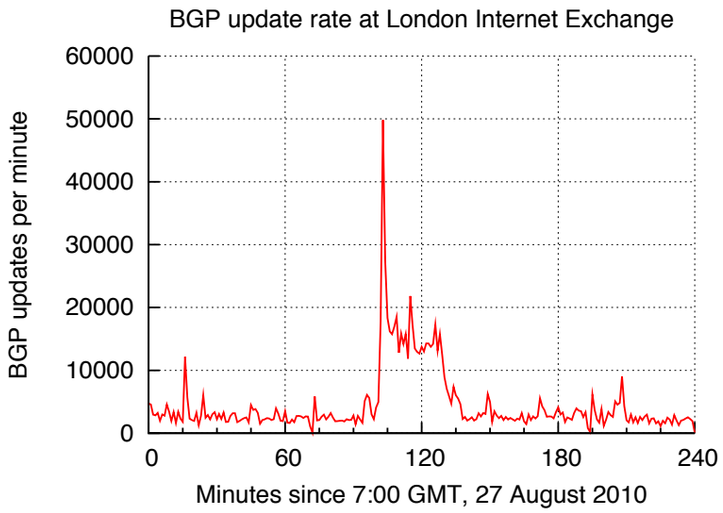
How did this happen?

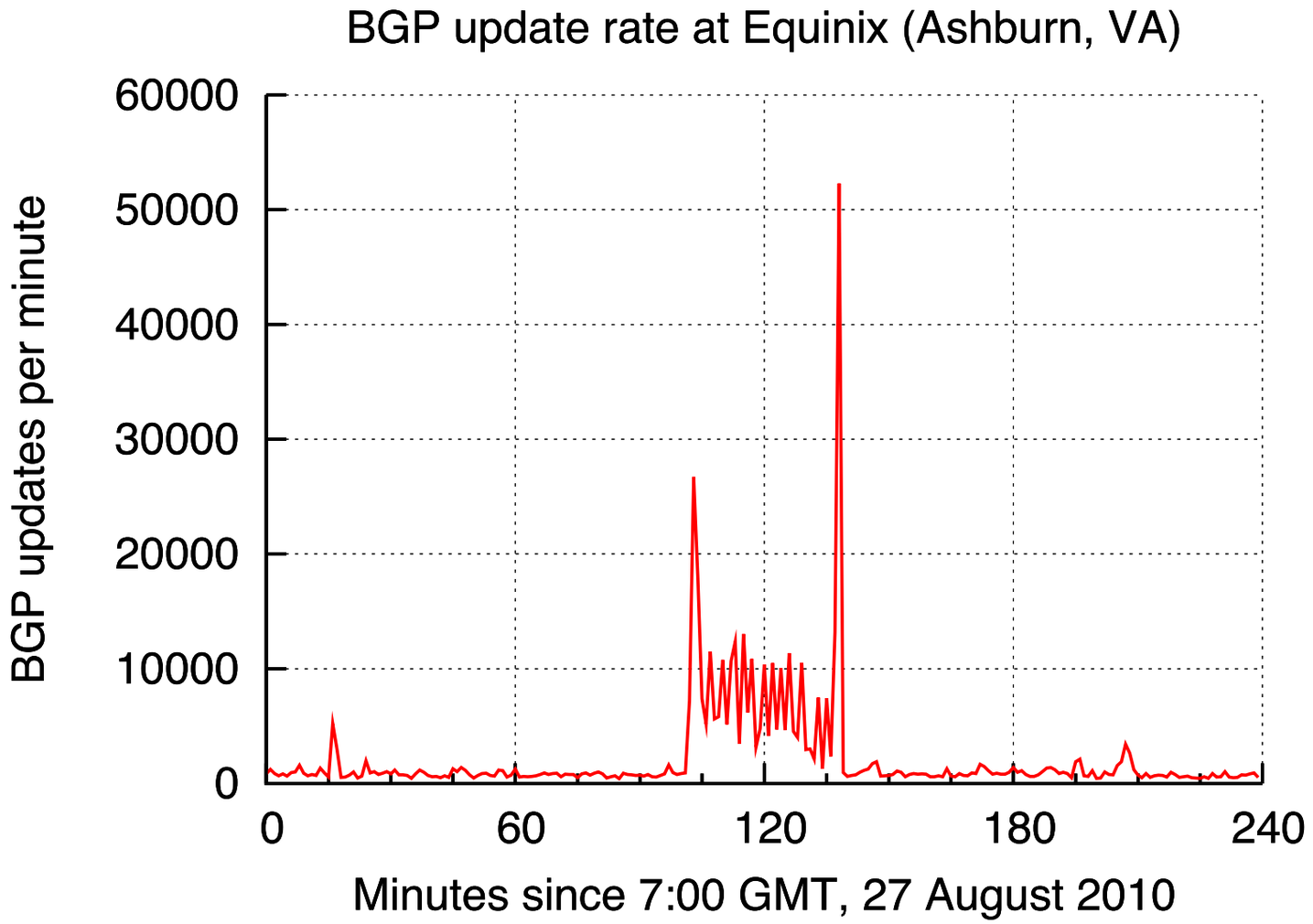
Internet had a bad Friday



[Plots by Brighten based on raw update feeds from Route Views]

Internet had a bad Friday

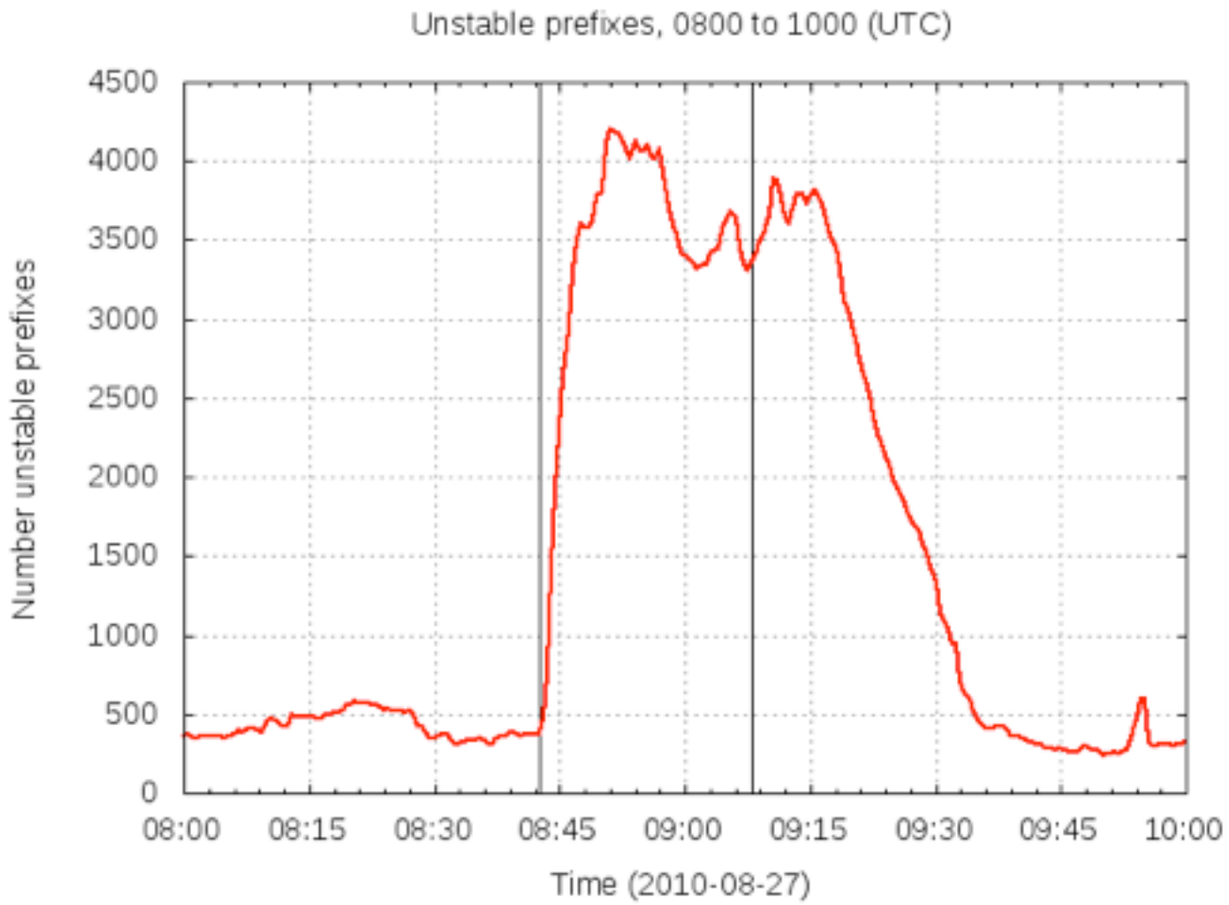


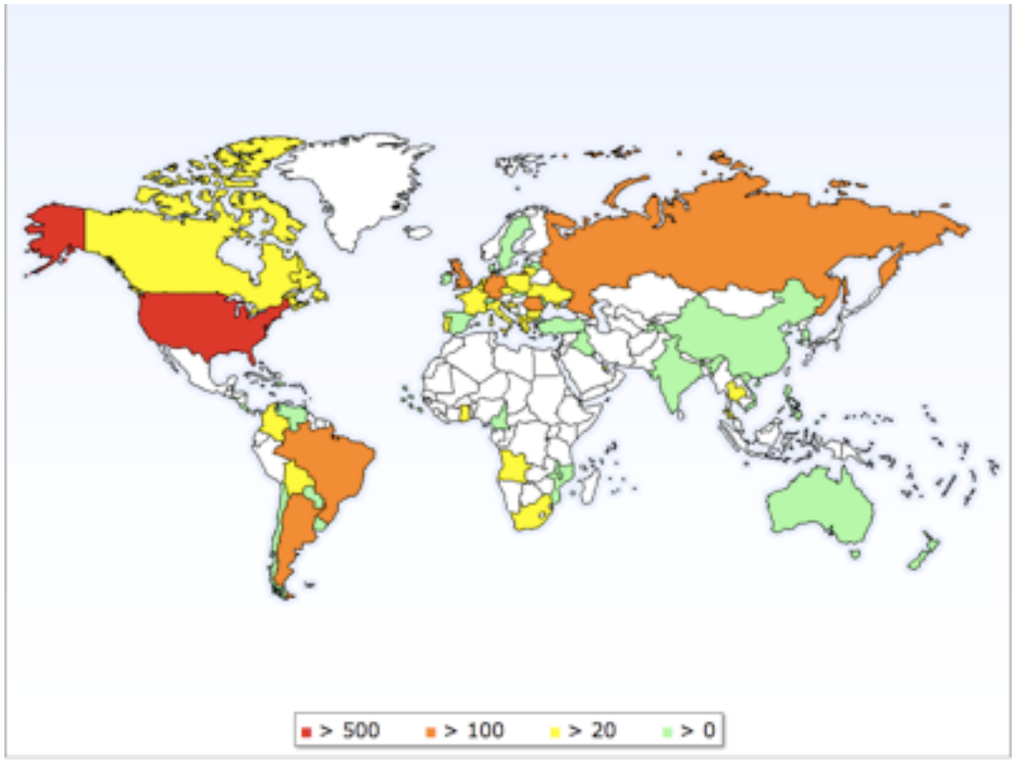


[Plots by Brighten based on raw update feeds from Route Views]

~1% of prefixes affected

[Earl Zmijewski, Renesys]





Brewing a storm

1. An unusual announcement
2. Propagation from router to router
3. Buggy software mangles announcement
4. while(true)
    1. Buggy router propagates announcement to neighbor
    2. BGP session dropped upon receipt of mangled message
    3. BGP session reestablished

Lessons

Many unsavory BGP announcements can be contained, but this one wasn't

- Spread geographically because it was an entirely valid announcement
- Spread to many prefixes because BGP spec lets one bad announcement from a router affect all traffic to that router

Widespread correlated failures from similar software

Bugs and attacks can have similar effects and solutions

- Lucky in this case: bug triggered by researchers, not attackers!

Onward to Denial of Service

DoS in the real world

Source: Arbor Networks

Disclaimers:

- Survey of 130 network operators (mix of Tier 1, 2, 3; enterprise networks, etc.), not direct measurement
- Arbor sells network security solutions :-)

http://dilbert.com/strips/comic/1999-04-27/

DDoS is frequent and can be big

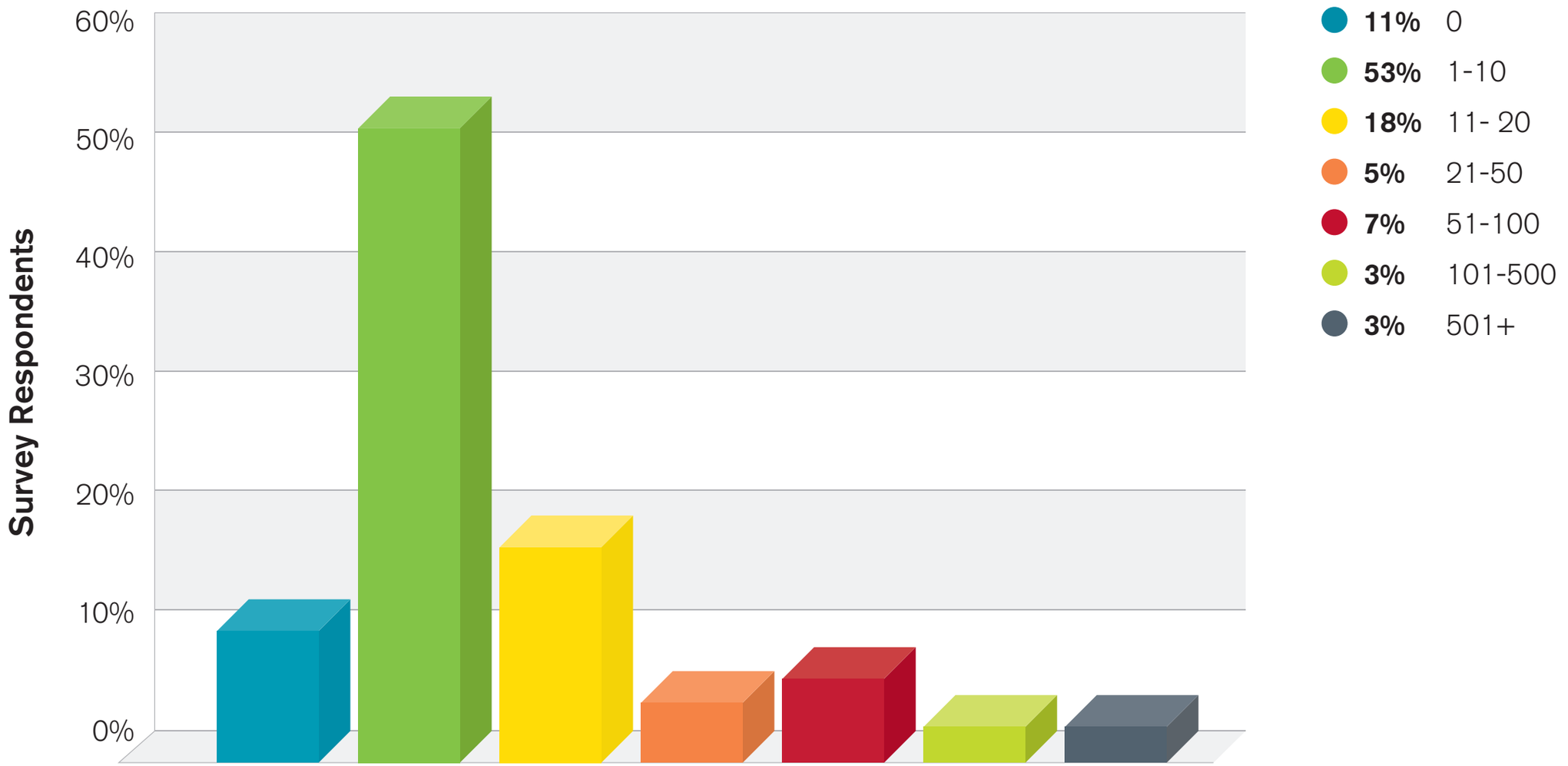


Figure 27 *Source: Arbor Networks, Inc.*

DDoS is frequent and can be big

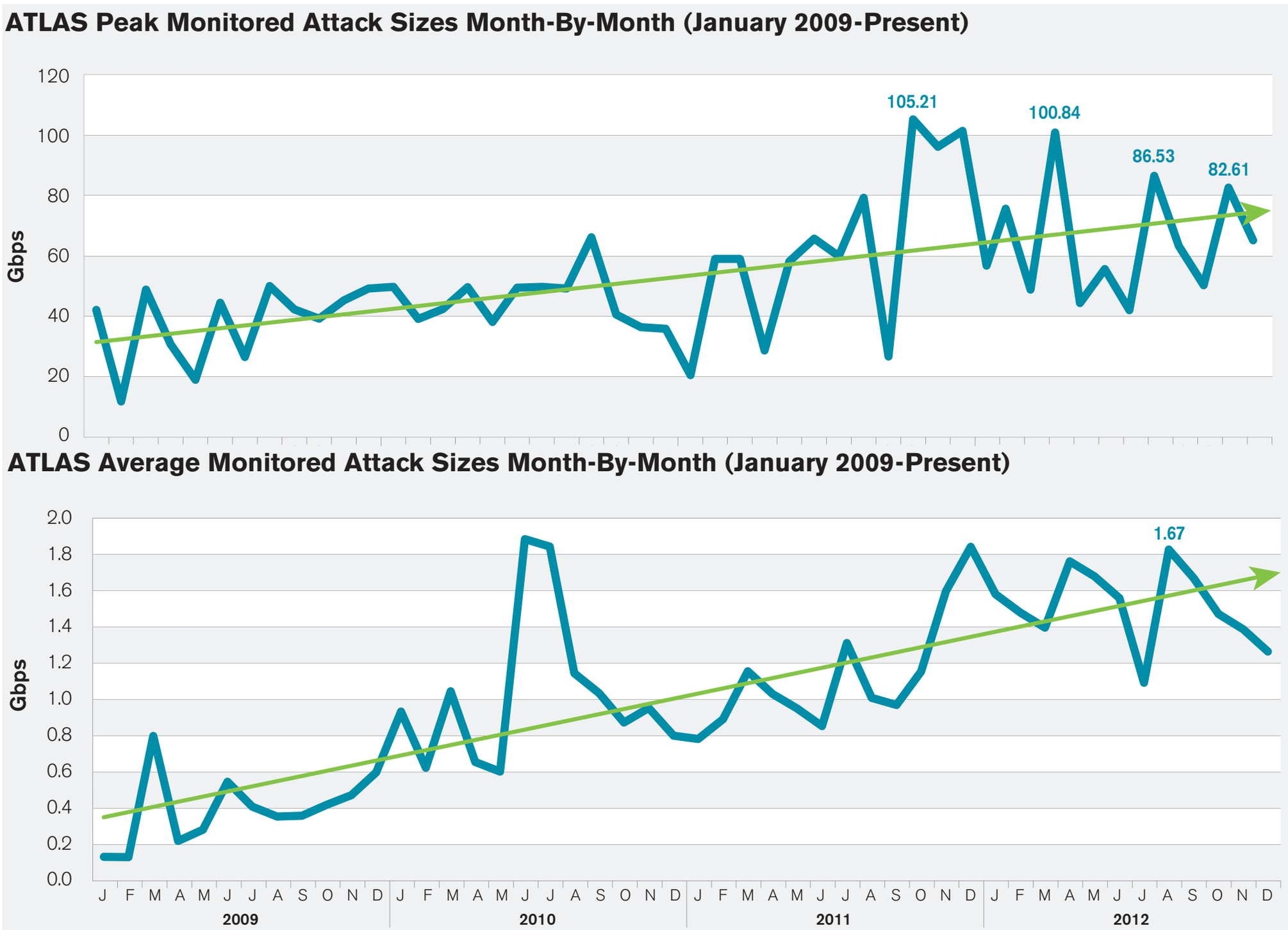


Figure 18 *Source: Arbor Networks, Inc.*

[Measurements from Arbor's ATLAS tool in 250 networks]

Many types of attacks

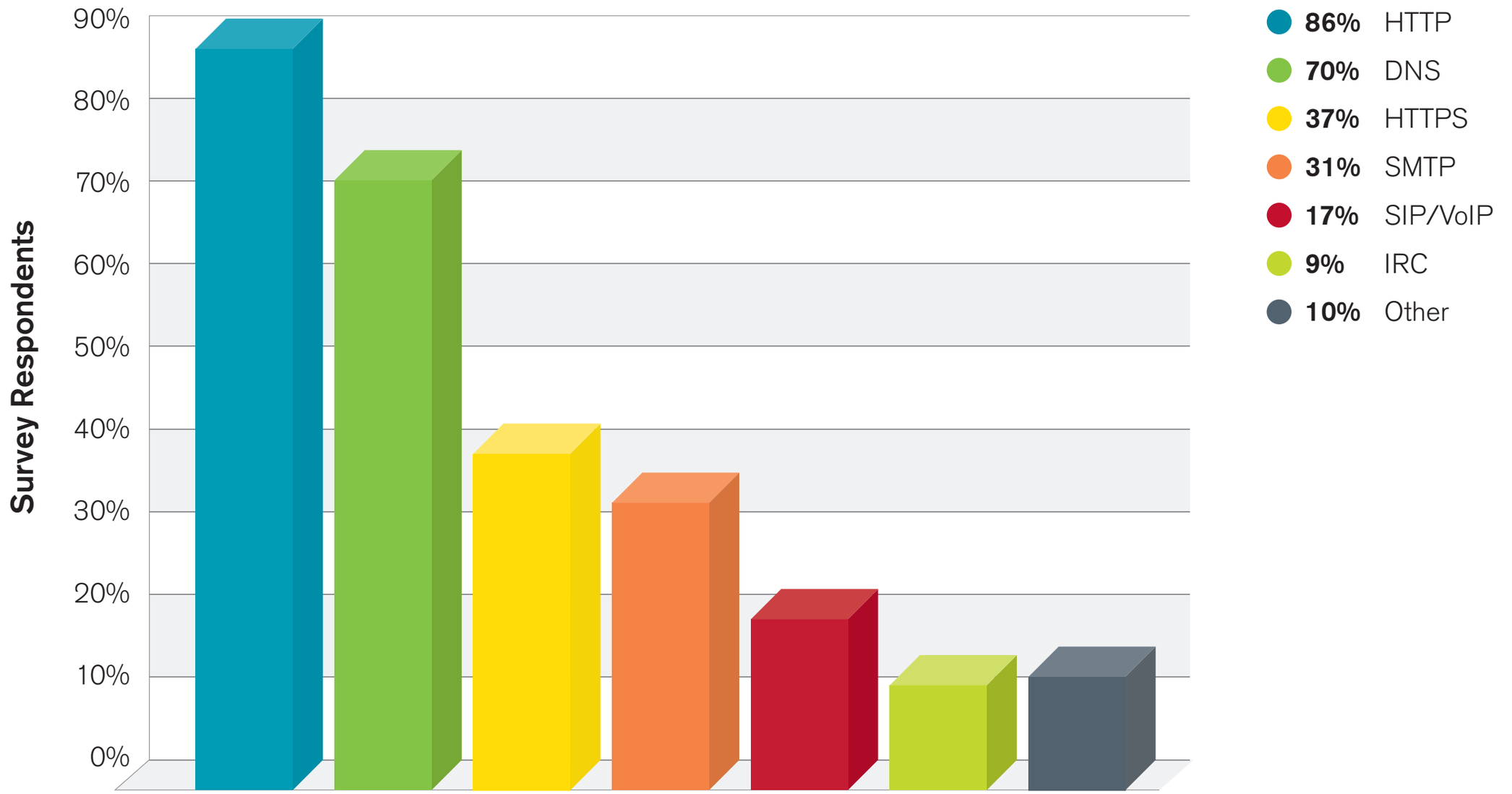
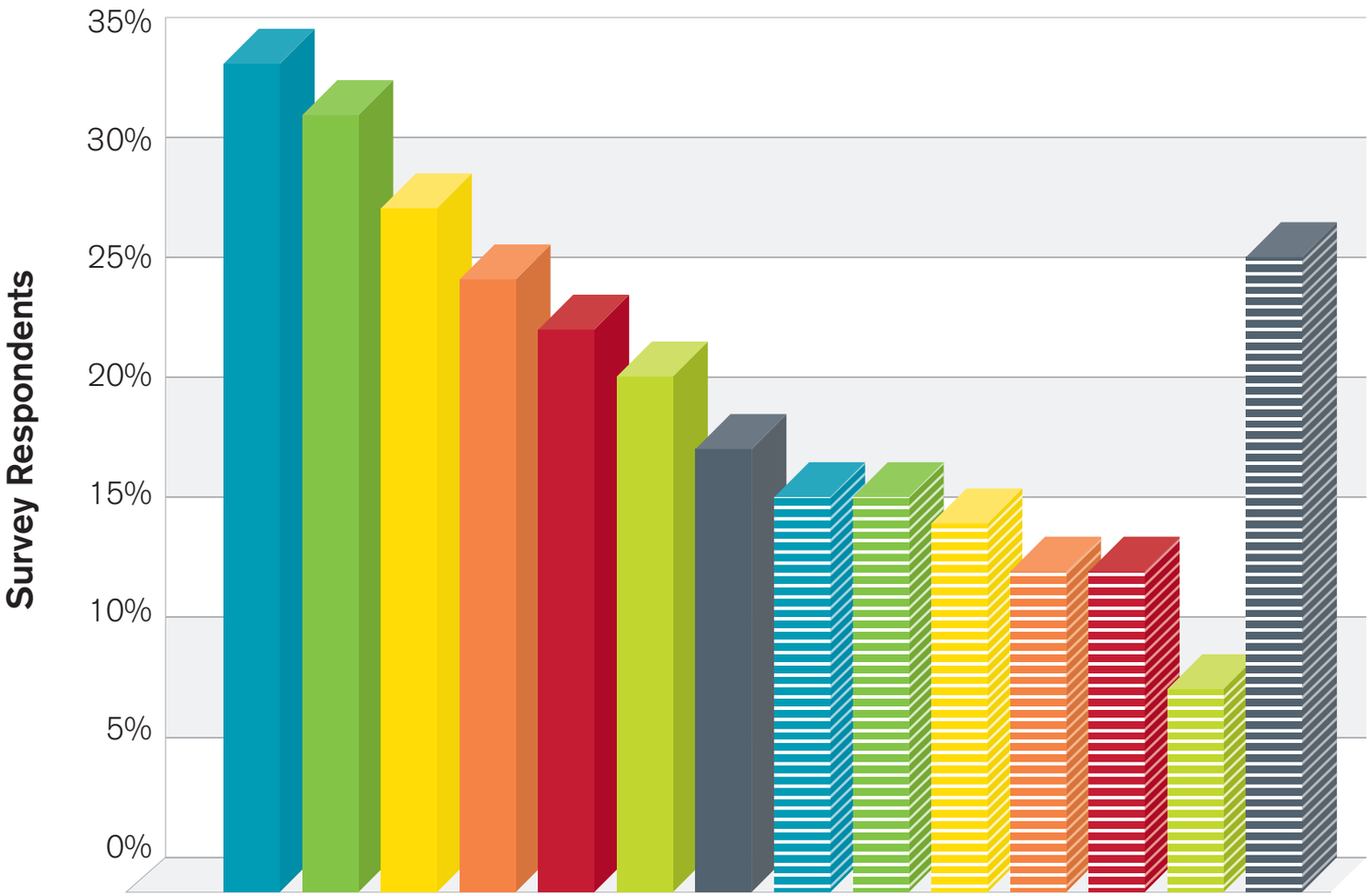


Figure 24 *Source: Arbor Networks, Inc.*

Motivation

Most Common Motivations Behind DDoS Attacks



- **33%** Political/Ideological Disputes
- **31%** Online Gaming-Related
- **27%** Nihilism/Vandalism
- **24%** Criminals Demonstrating DDoS Attack Capabilities to Potential Customers
- **22%** Social Networking-Related
- **20%** Interpersonal/Inter-Group Rivalries
- **17%** Misconfiguration/Accidental
- **15%** Competitive Rivalry Between Business Organizations
- **15%** Diversion to Cover Compromise/Data Exfiltration
- **14%** Criminal Extortion Attempts
- **12%** Flash Crowds
- **12%** Financial Market Manipulation
- **7%** Intra-Criminal Disputes
- **25%** Unknown

Figure 16 *Source: Arbor Networks, Inc.*

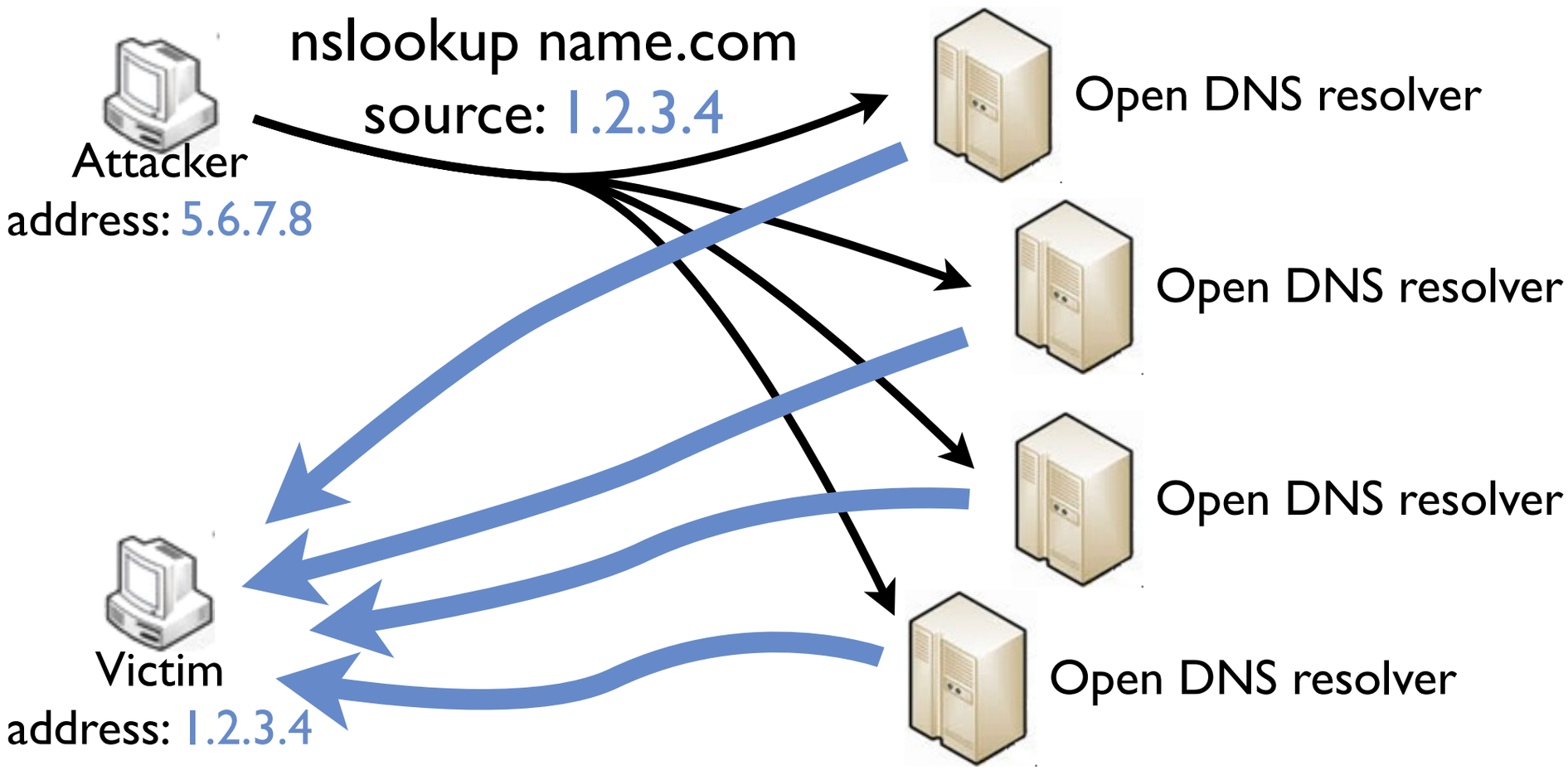
Comments on largest attacks

- "TCP/80 SYN flood toward Chinese online gaming (not gambling) site who was a DDoS mitigation customer of ours. Motivations unknown. Frequent on-and-off waves of attack traffic over several days, the largest of which topped out at 28.3 Mpps."

- "UDP port 22 small byte packets at high rate for less than 10 minutes, overran firewalls supposedly able to handle much higher pps rates."

- "UDP reflection/amplification attack, primarily a mix of port 53 and 520 with some SYN and ICMP backscatter. Suspected attack motivation was retaliatory attack to something our users posted on a web forum (destination of the attack was a web proxy)."

DNS Reflection and Amplification



DNS Reflection and Amplification

Reflection

- via source address spoofing + lack of handshake in DNS
- hides source
- enables amplification by converting attacker's request traffic into response traffic

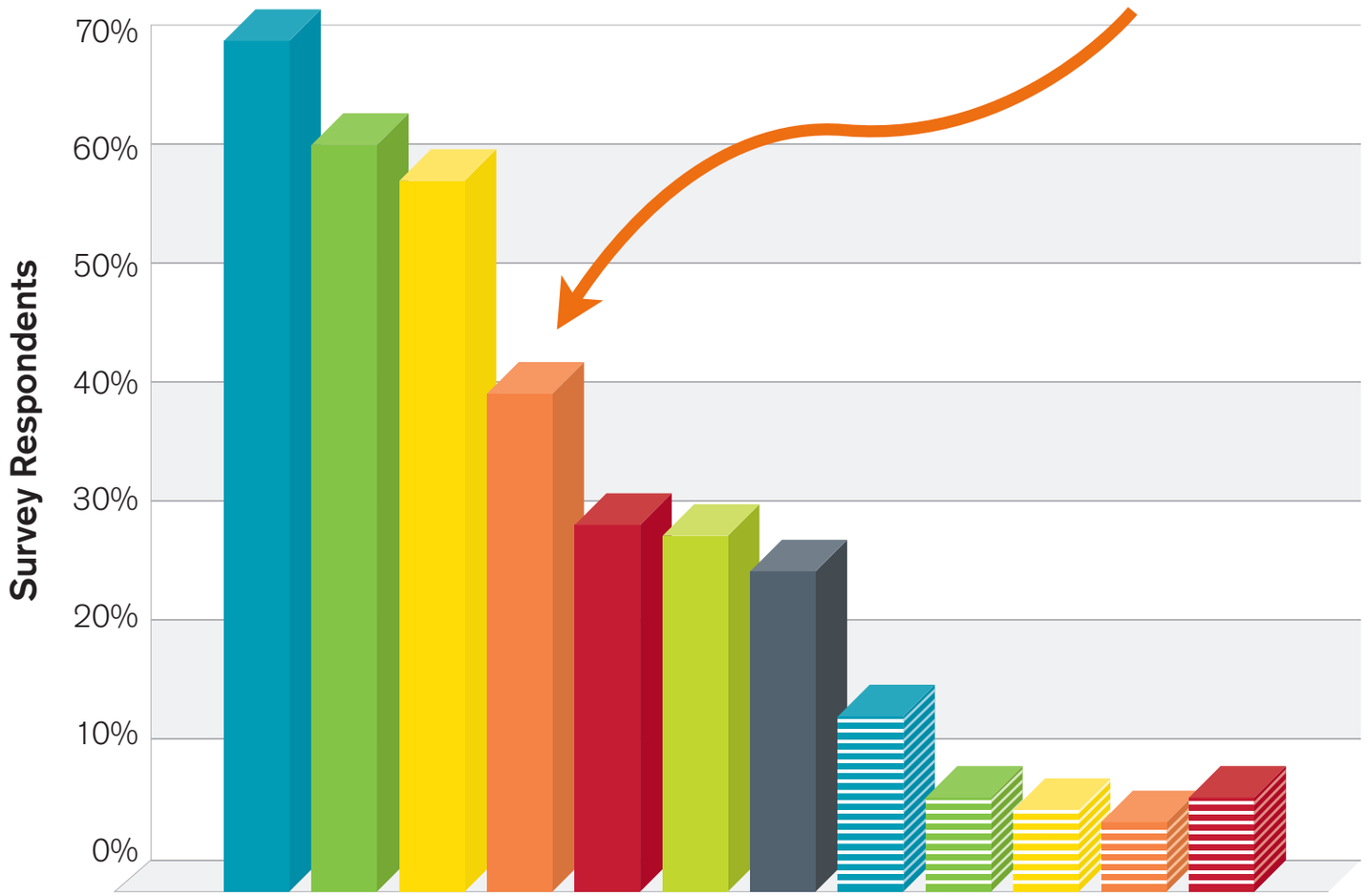
Amplification

- response is larger than request
- magnifies damage per unit of attacker work

DDoS defense

"destination-based remotely triggered blackholing"

Attack Mitigation Techniques

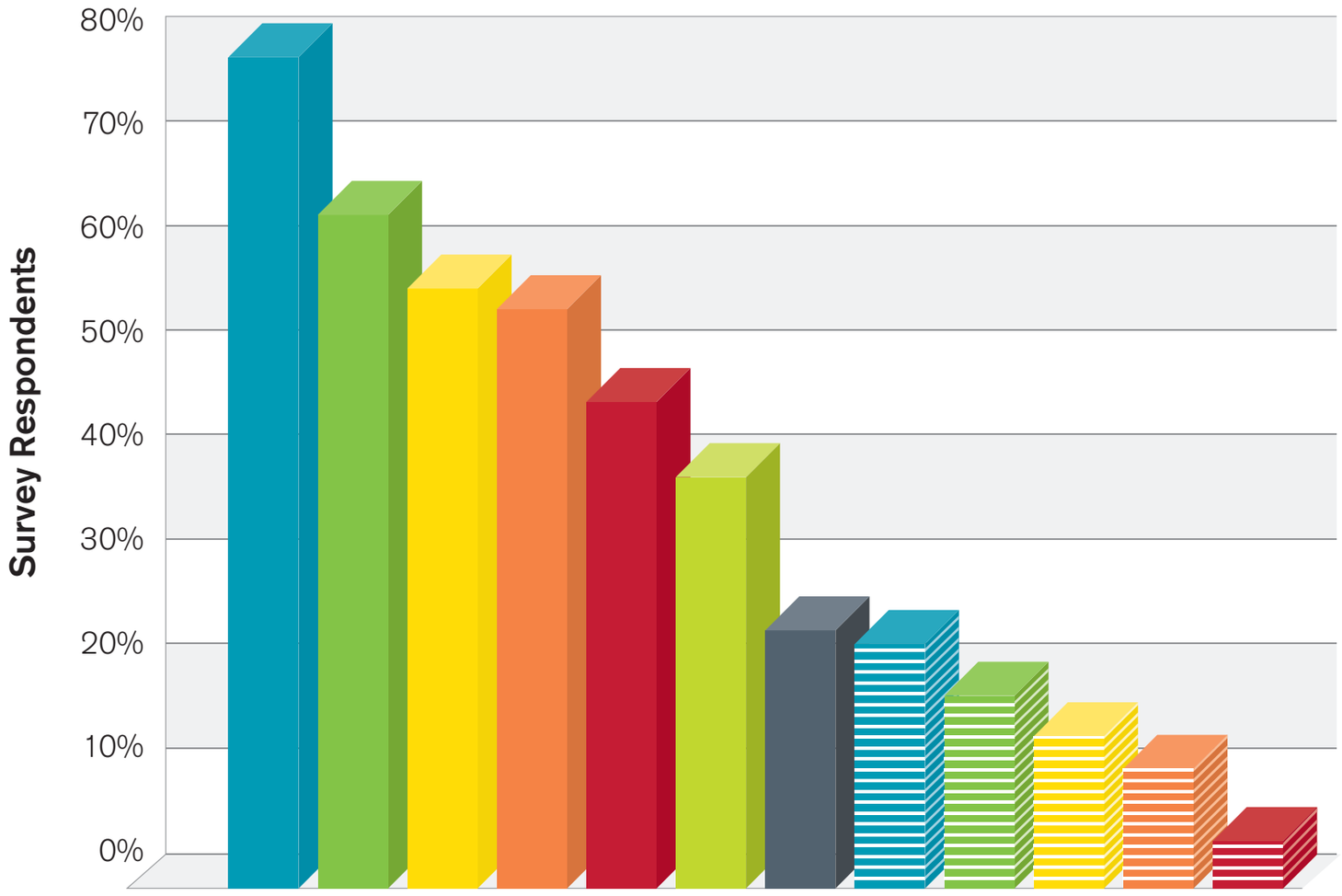


- **69%** Access Control Lists (ACLs)
- **60%** Intelligent DDoS Mitigation Systems (IDMS) Such As Peakflow SP Threat Management System (TMS)
- **57%** Firewall
- **39%** Destination-Based Remote Triggered Blackhole (D/RTBH)
- **28%** Source-Based Remote Triggered Blackhole (S/RTBH)
- **27%** IPS
- **24%** Load Balancer
- **11%** FlowSpec
- **5%** Content Delivery Network (CDN)
- **4%** DPI Systems
- **3%** None
- **5%** Other

Figure 32 *Source: Arbor Networks, Inc.*

DoS in context

Most Significant Operational Threats Experienced



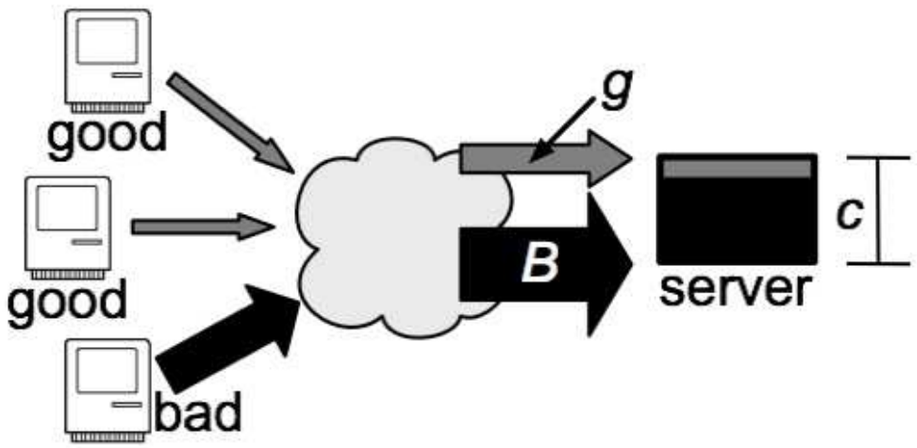
- **76%** DDoS Attacks Toward Customers
- **61%** Infrastructure Outage (Partial or Complete) Due to Failures or Misconfiguration
- **54%** DDoS Attacks on Services (DNS, Email)
- **52%** DDoS Attacks Toward Infrastructure
- **43%** Infrastructure Outages (Partial or Complete) Due to DDoS Attack
- **36%** Botted/Compromised Hosts on Service Provider Network
- **21%** Under-Capacity for Bandwidth
- **20%** Botted/Compromised Hosts on Corporate or Command and Control Network
- **15%** Advanced Persistent Threat on Corporate or Command and Control Network
- **11%** Malicious Insider
- **8%** Industrial Espionage or Data Exfiltration
- **2%** Other

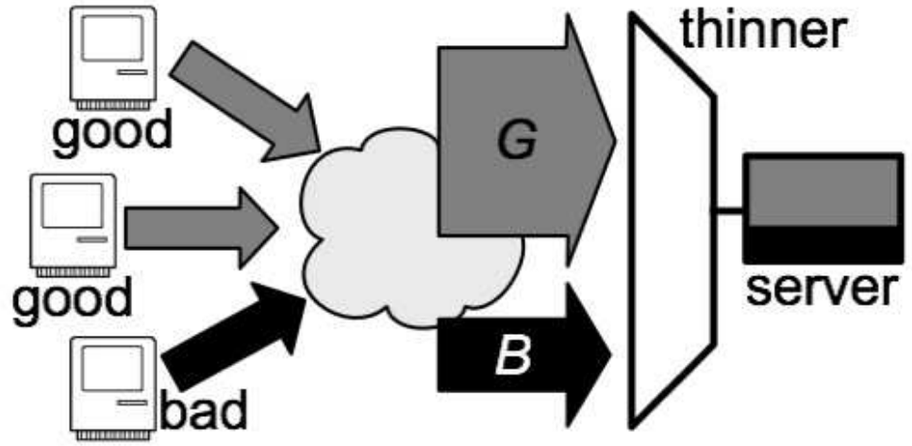
Figure 10 *Source: Arbor Networks, Inc.*

DDoS Defense by Offense

Walfish, Vutukuru, Balakrishnan, Karger, Shenker,
SIGCOMM 2006

Speak-up key idea





[Walfish et al.]

Mechanism

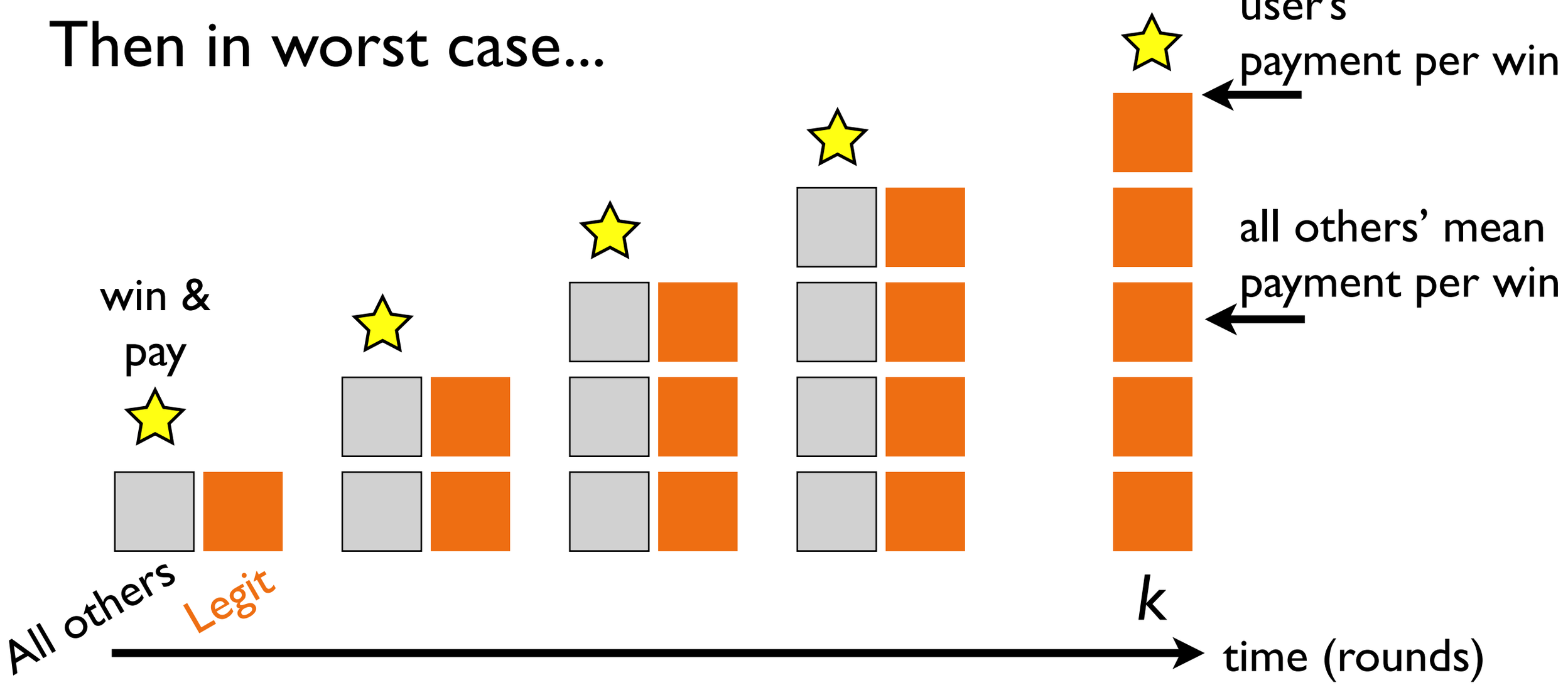
- Thinner guards access to server
- Runs "auction" for each service slot
- Whoever has sent most since last service gets service

Bounding attacker damage

Assume

- Legitimate user sends one unit traffic per round
- Obtains one unit service after *k* rounds

Then in worst case...



Two ways to view the paper

If attackers are selfish, let good clients be selfish too

- At least they compete fairly
- Vastly improved situation

Charge clients a currency

- Reduces amplification due to HTTP request being much less work than response
- Here, currency = bandwidth
- This happens today under DoS attack, whether you like it or not
- Just need to inform legitimate clients about the situation

Clear drawback: Spends bandwidth

Extra charging

- Clients might be charged more [Yen Shine Low]
- Customers may thus switch to services that don't use Speak Up [Suna Kim]

Worse performance

- Could hurt other client apps' performance [Danny Xu]
- Could congest services co-located with server [Shayan Saeed, Alok Taigi]

Questioning Assumptions

Assumed: Good clients typically use small % of their bandwidth capacity

When is this false?

Questioning Assumptions

Assumed: Clients can all send about the same amount

What about users with low or costly bandwidth?

- Unfair to them [Anthony Lang, Nirupam Roy]
- What would you do to fix it?

Interesting points from paper

What if multiple bots pretend to be one? [Zhenhuan]

- They get 2x the service
- But that's just a name change (2x1 vs. 1x2)
- "Ironically, taxing clients is easier than identifying them"

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?