Network Security

Mark Allman
mark.allman@case.edu

EECS 325/425

*“The warden threw a party in the county jail,
The prison band was there and they began to wail"*

Network Security

Network Security

- Network opens a whole raft of security issues

Network Security

- Network opens a whole raft of security issues

- Highlights the disconnect between …
  - …the world in which the core technology was developed
  - …the world that has emerged

Network Security

- Network opens a whole raft of security issues
- Highlights the disconnect between …
  - …the world in which the core technology was developed
  - …the world that has emerged
- Security issues are part of the Internet's "success disaster"

“Drive By” Issues

“Drive By” Issues

- E.g., auth DNS servers lying + prefetching is an instance “drive by” issues
- I.e., if we can coax a client to access some host in some way that can be used as an attack vector

“Drive By” Issues

- E.g., auth DNS servers lying + prefetching is an instance “drive by” issues
- I.e., if we can coax a client to access some host in some way that can be used as an attack vector
- E.g., “drive by malware” distributed via mere web page visits

In The Eye of the Beholder…

In The Eye of the Beholder…

- Sometimes one activity is viewed as both …
  - … an attack
  - … a legitimate business practice

In The Eye of the Beholder…

- Sometimes one activity is viewed as both …
  - … an attack
  - … a legitimate business practice

- E.g., an RDNS re-writing error messages

In The Eye of the Beholder…

- Sometimes one activity is viewed as both …
  - … an attack
  - … a legitimate business practice

- E.g., an RDNS re-writing error messages

- This is an example of a "tussle" in networks

Surveillance

- Watching network traffic can provide a fine-grain view into “private” activity

- Even “meta data”—such as DNS lookups—can provide a clear window into users’ activities

Surveillance

Surveillance

- How much is OK? How much is too much?

Surveillance

- How much is OK? How much is too much?

- By law, ISPs allowed to look at your traffic to engineer their network

Surveillance

- How much is OK? How much is too much?

- By law, ISPs allowed to look at your traffic to engineer their network
- By your agreement, Google can delve into your activity for their profit

Surveillance

- How much is OK? How much is too much?

- By law, ISPs allowed to look at your traffic to engineer their network
- By your agreement, Google can delve into your activity for their profit

- Drawing general lines is difficult …
- …yet, the lines we choose impacts how we develop and deploy technology

Surveillance

Surveillance

- What to do?

Surveillance

- What to do?
- IPsec
  - encrypt most of the IP layer and everything above

Surveillance

- What to do?
- IPsec
  - encrypt most of the IP layer and everything above
- TLS
  - encrypt application payload, but nothing below

Surveillance

- What to do?
- IPsec
  - encrypt most of the IP layer and everything above
- TLS
  - encrypt application payload, but nothing below
- VPN, anonymization networks (e.g., Tor)
  - tunnel traffic through untrusted networks to some trusted place

Interposing

Interposing

- DNS shows us that the Internet's core protocols that send information in clear text are susceptible to fraudulent forgery of all kinds
  - e.g., providing bogus answers to questions we don't like
  - e.g., entities that mimic the roots

Interposing

- DNS shows us that the Internet's core protocols that send information in clear text are susceptible to fraudulent forgery of all kinds
  - e.g., providing bogus answers to questions we don't like
  - e.g., entities that mimic the roots
- What to do?

Interposing

- DNS shows us that the Internet’s core protocols that send information in clear text are susceptible to fraudulent forgery of all kinds
  - e.g., providing bogus answers to questions we don’t like
  - e.g., entities that mimic the roots
- What to do?
  - sign and/or encrypt

Cache Poisoning

Cache Poisoning

- Inserting a fraudulent entry into a cache
- Doesn’t directly attack a particular transaction
- But, aims to plant a trap of sorts for all subsequent transactions

Cache Poisoning

- Inserting a fraudulent entry into a cache
- Doesn’t directly attack a particular transaction
- But, aims to plant a trap of sorts for all subsequent transactions
- What to do?

Cache Poisoning

- Inserting a fraudulent entry into a cache
- Doesn’t directly attack a particular transaction
- But, aims to plant a trap of sorts for all subsequent transactions

- What to do?
  - sign and/or encrypt

Spoofing

Spoofing

- In TCP/IP, the devices themselves identify themselves in packets by setting the source address

Spoofing

- In TCP/IP, the devices themselves identify themselves in packets by setting the source address

- Therefore, nothing prevents a device from setting the source IP fraudulently
  - in general, this doesn’t work as the host will not see the return traffic
  - in attacks, this may not matter or *may be the point!*

Preventing Spoofing

Preventing Spoofing

- What to do?

Preventing Spoofing

- What to do?

- Ingress / egress filtering
- Solution requires wide-scale buy-in

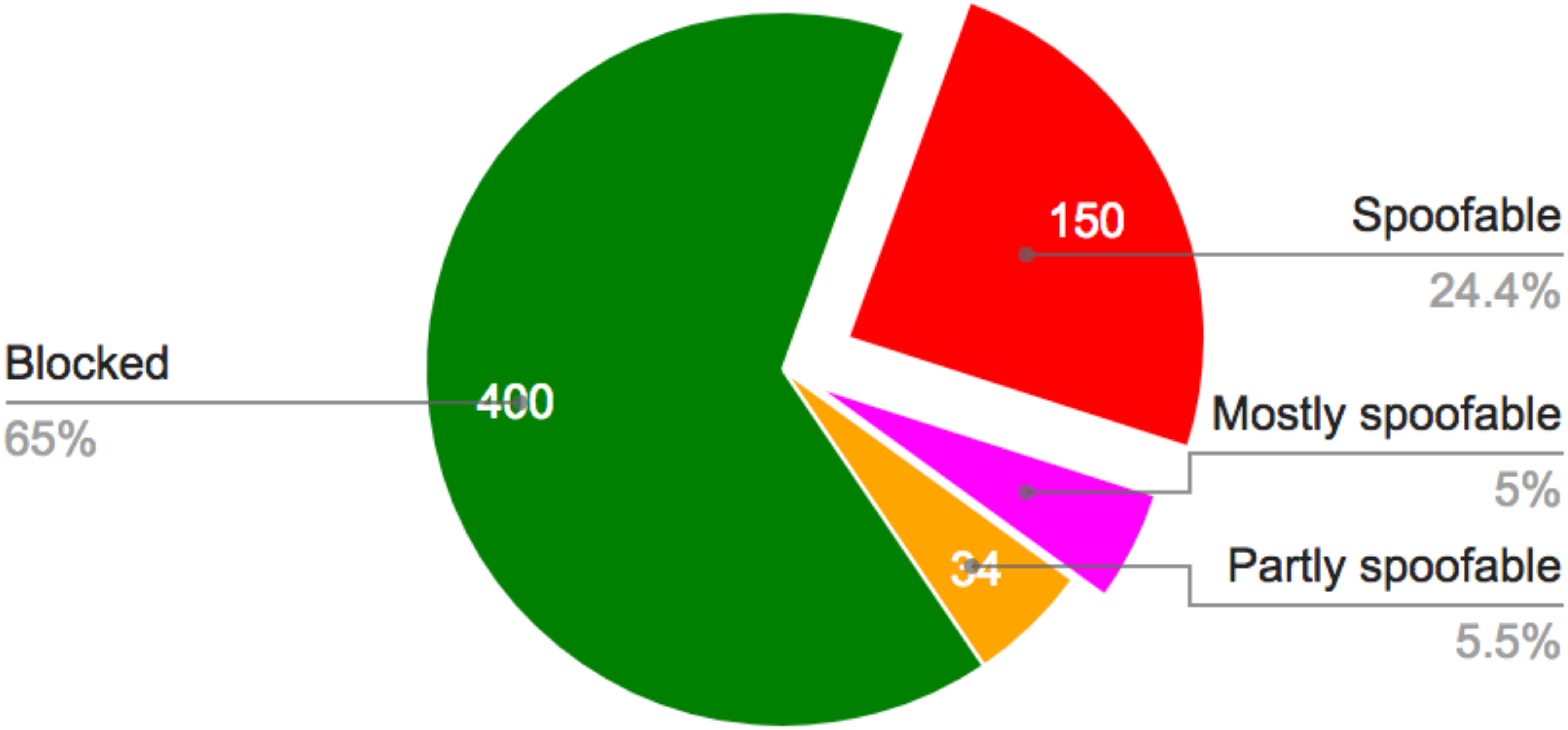
Preventing Spoofing

- What to do?

- Ingress / egress filtering
- Solution requires wide-scale buy-in

- Incentives are less-than-ideal
  - "I get nothing if I deploy"
  - "I get something if everyone else deploys"

Is Spoofing Possible?



CAIDA’s Spoofer Project

Reflection

Reflection

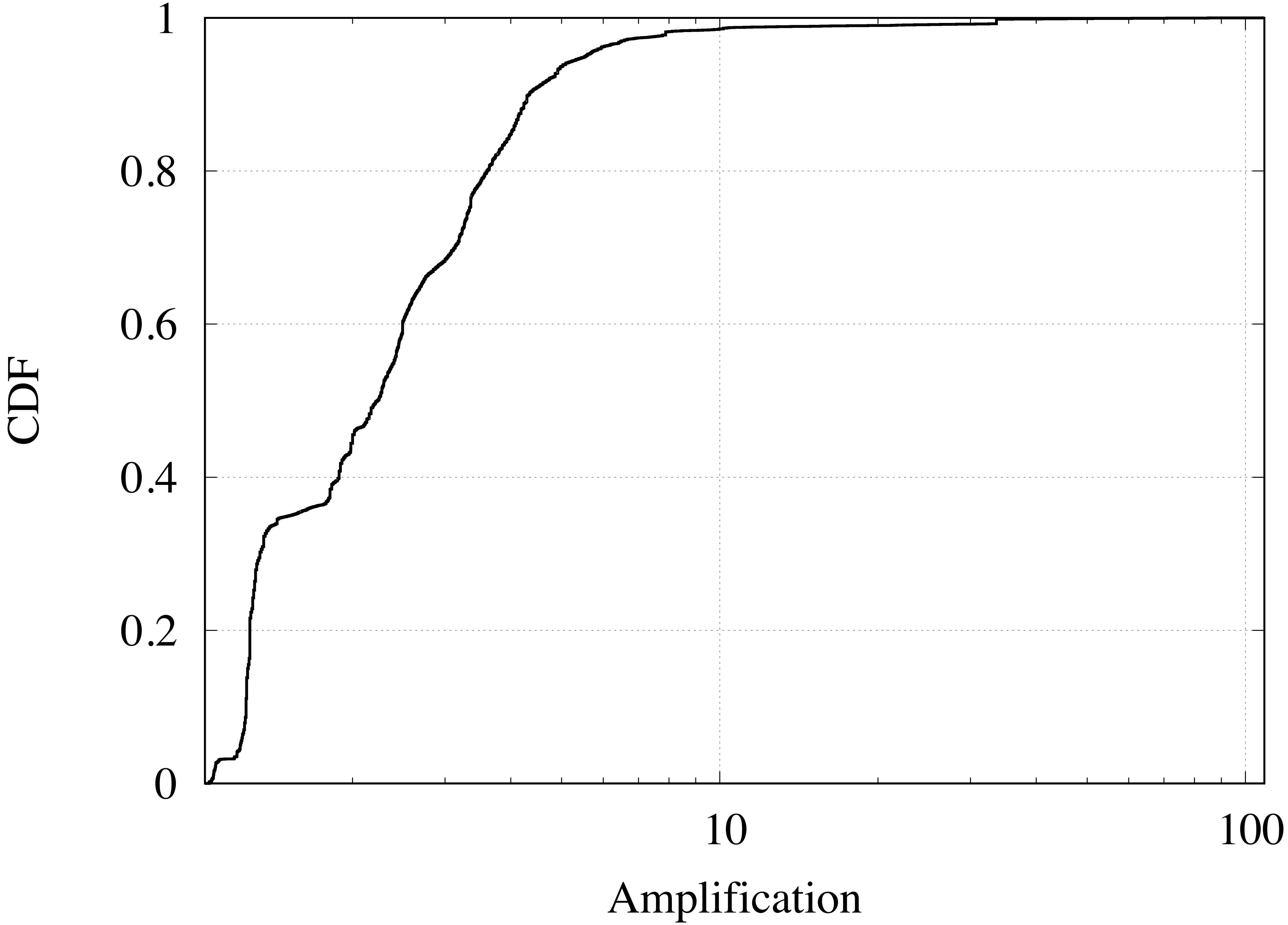
- Coaxing a third-party to transmit traffic to a victim
  - to hide identity
  - to circumvent policy

Amplification

Amplification

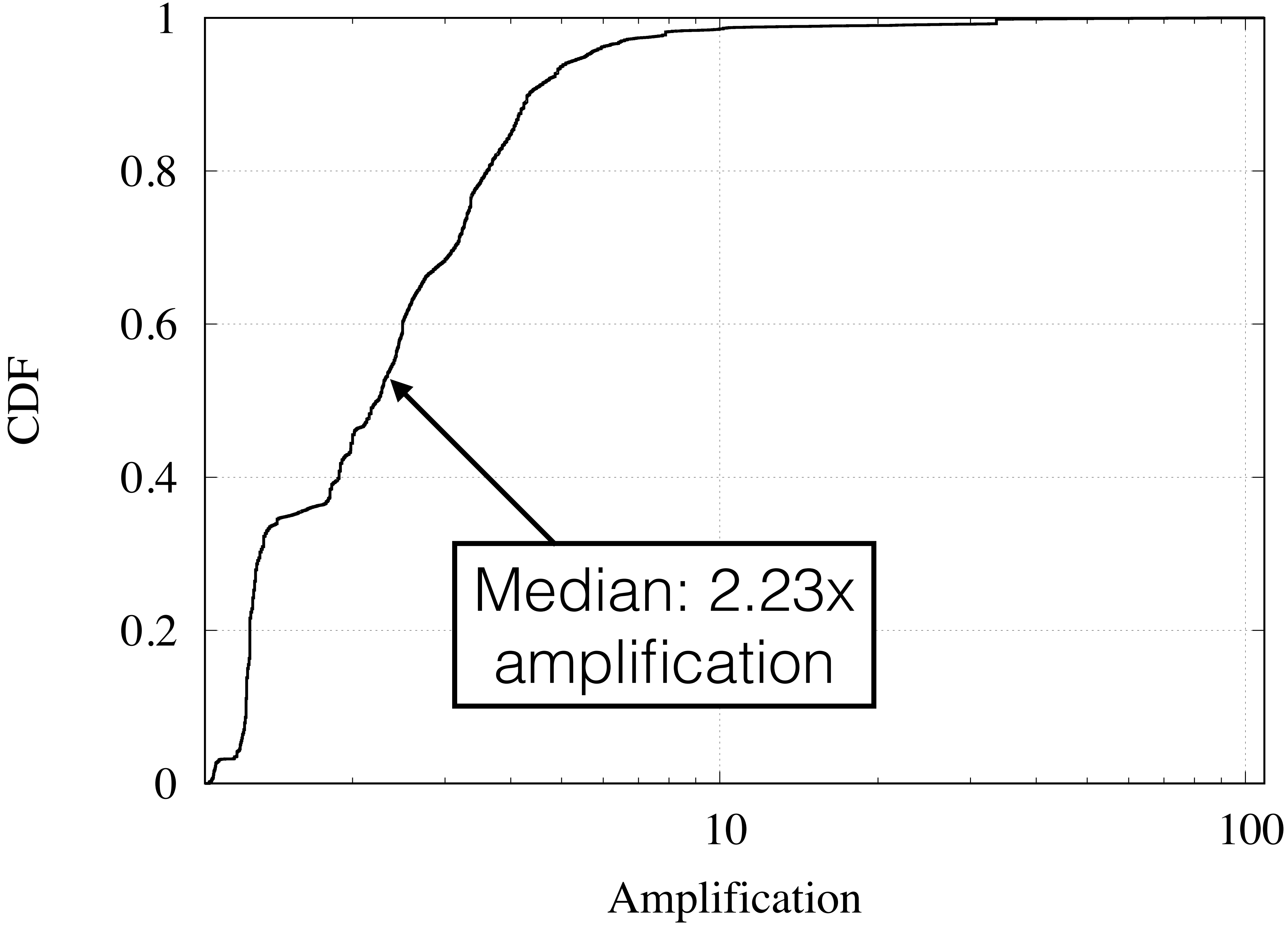
- Reflection is often coupled with amplification
- I.e., with a small request we can coax a reflector to send a larger response to a victim

DNS Amplification



Data from ICSI, Sep 2016

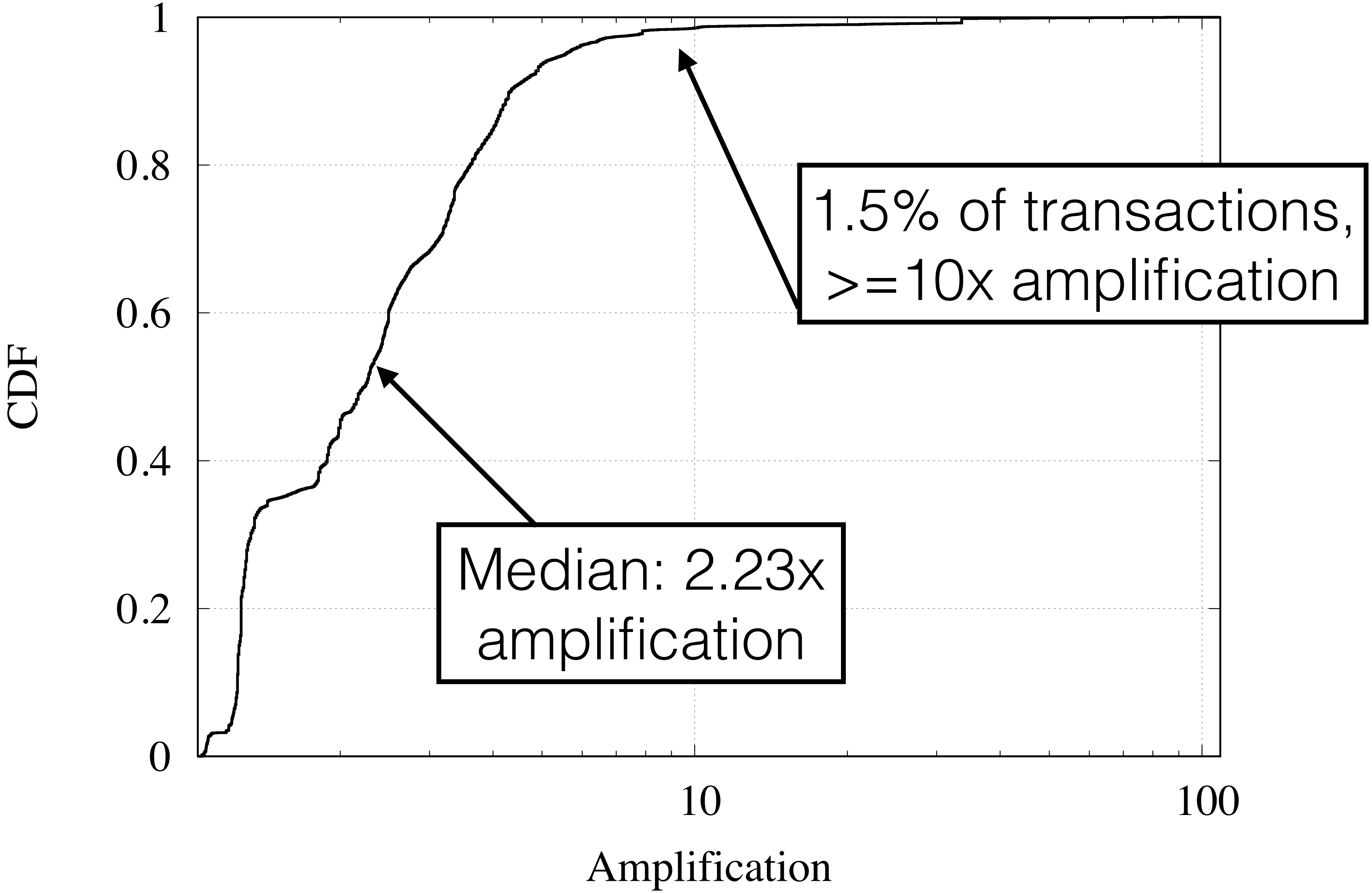
DNS Amplification



Median: 2.23x amplification

Data from ICSI, Sep 2016

DNS Amplification



1.5% of transactions, >=10x amplification

Median: 2.23x amplification

Data from ICSI, Sep 2016

Denial-of-Service

Denial-of-Service

- Use a resource so someone else can’t

DDoS

DDoS

- Distributed Denial-of-Service

DDoS

- Distributed Denial-of-Service

- Leverage a large number of hosts around the network to use resources
  - can more effectively use more resources, so the more hosts an attacker controls the larger the attack can be

DDoS

- Distributed Denial-of-Service
- Leverage a large number of hosts around the network to use resources
  - can more effectively use more resources, so the more hosts an attacker controls the larger the attack can be
  - “botnets”

DDoS

- What to do?
  - (ugh)

DDoS

- Often about using capacity so legitimate transactions get squeezed out
    - i.e., just no room left

DDoS

DDoS

- But, we don't need a firehose to cause problems

DDoS

- But, we don’t need a firehose to cause problems

- E.g., consider a TCP connections

DDoS

- But, we don't need a firehose to cause problems

- E.g., consider a TCP connections
  - originator starts a TCP connection by sending a SYN

DDoS

- But, we don’t need a firehose to cause problems

- E.g., consider a TCP connections
  - originator starts a TCP connection by sending a SYN
  - recipient instantiates state upon receipt
    - track window size, sequence numbers, packet buffer, etc.
  - i.e., recipient *allocates recourses*

DDoS

DDoS

- What if an attacker sent tons of SYNs, but then stopped transmitting?
  - i.e., no legit connection
  - can be combined with spoofing

DDoS

- What if an attacker sent tons of SYNs, but then stopped transmitting?
  - i.e., no legit connection
  - can be combined with spoofing
- The attacker would consume host resources that could not be used for legit traffic

DDoS

- What if an attacker sent tons of SYNs, but then stopped transmitting?
  - i.e., no legit connection
  - can be combined with spoofing

- The attacker would consume host resources that could not be used for legit traffic

- Called a “SYN flood”

DDoS

DDoS

- What to do about a SYN flood?

DDoS

- What to do about a SYN flood?

- Timeouts
    - “SYN caches”

- “SYN cookies”

DDoS

DDoS

- SYN cookies

DDoS

- SYN cookies
  - do not instantiate state upon SYN arrival

DDoS

- SYN cookies
  - do not instantiate state upon SYN arrival
  - carefully craft the recipient's initial seqno returned in the SYN+ACK
    - e.g., as the hash of the ISN in the SYN and a secret

DDoS

- SYN cookies
  - do not instantiate state upon SYN arrival
  - carefully craft the recipient's initial seqno returned in the SYN+ACK
    - e.g., as the hash of the ISN in the SYN and a secret
  - when the ACK of the SYN+ACK arrives, it can be validated as being legit …
    - … and now we instantiate state

DDoS

DDoS

- SYN cookie disadvantage:

DDoS

- SYN cookie disadvantage:
  - can't encode everything in the ISN
  - e.g., the window scale factor is given in the SYN and then never again
  - e.g., often can't deal with TCP options

Security Mitigations

Security Mitigations

- Good hygiene
  - keep software up-to-date
- Anti-virus scanners

Security Mitigations

- Good hygiene
  - keep software up-to-date
- Anti-virus scanners
- Firewalls / access control lists
  - limit who can access a particular service
  - host-based & network-based

Security Mitigations

Security Mitigations

- Intrusion Detection Systems (IDS)
  - monitor network for suspicious traffic
  - flag for analyst

Security Mitigations

- Intrusion Detection Systems (IDS)
  - monitor network for suspicious traffic
  - flag for analyst
- Intrusion Prevention System
  - hybrid of firewalls and IDS
  - i.e., monitor traffic and automatically initiate blocking of suspicious traffic

Security

- Just the tip of the iceberg …
- These are some of the most thorny problems we face
  - …and oftentimes because they boil down to *policy issues*