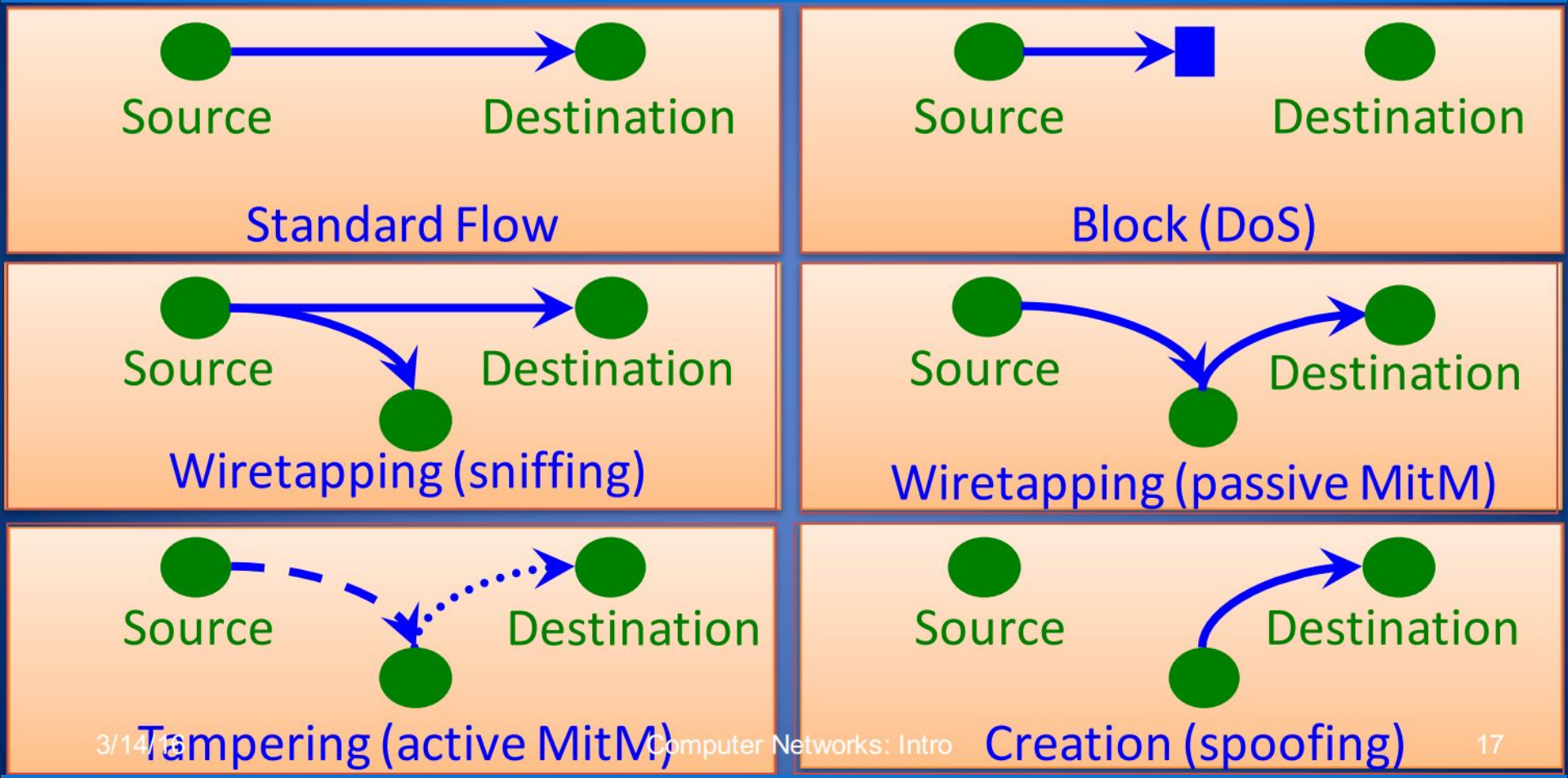
Denial of Service

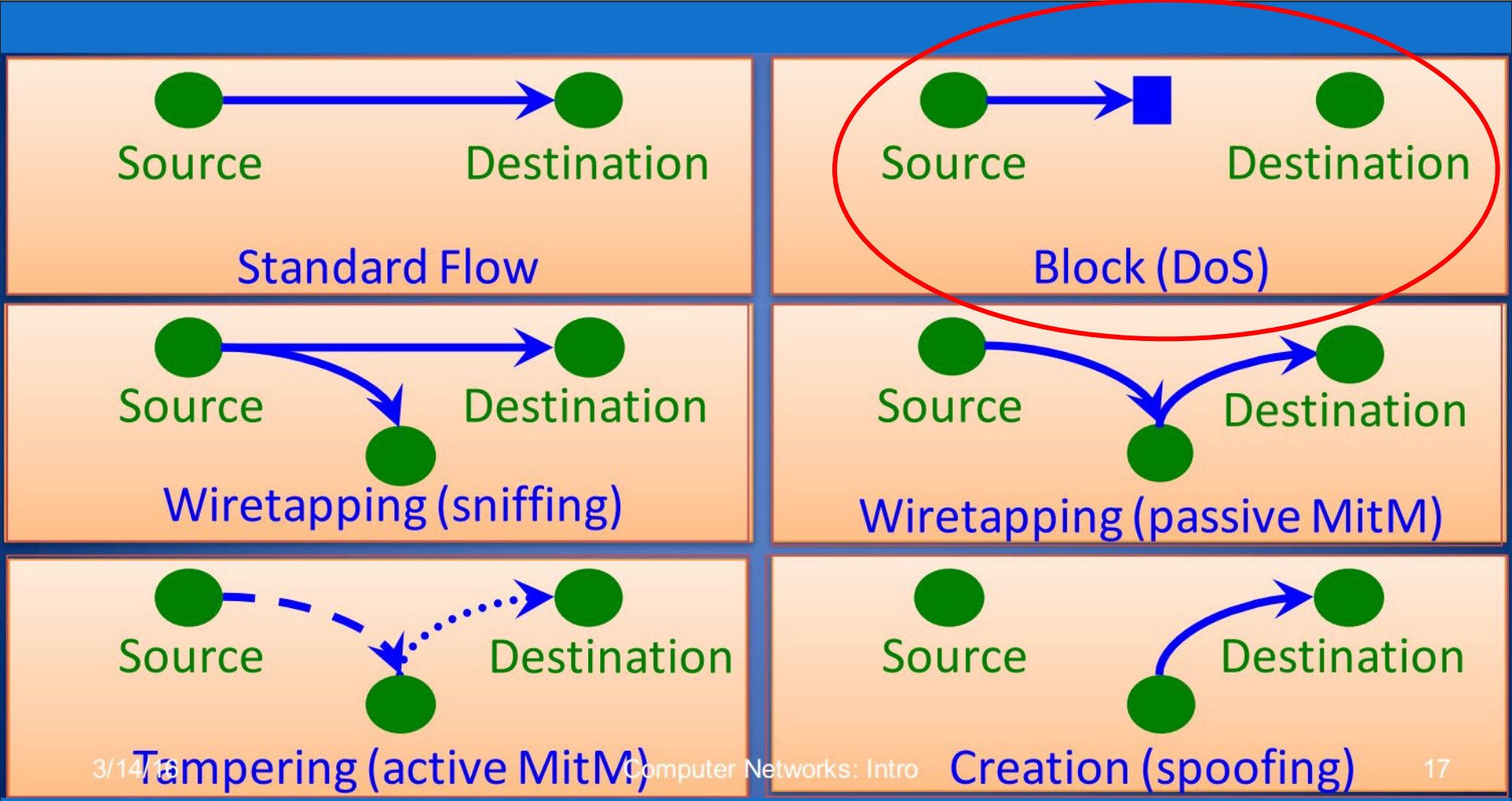
Recall: Goals of communications sec.

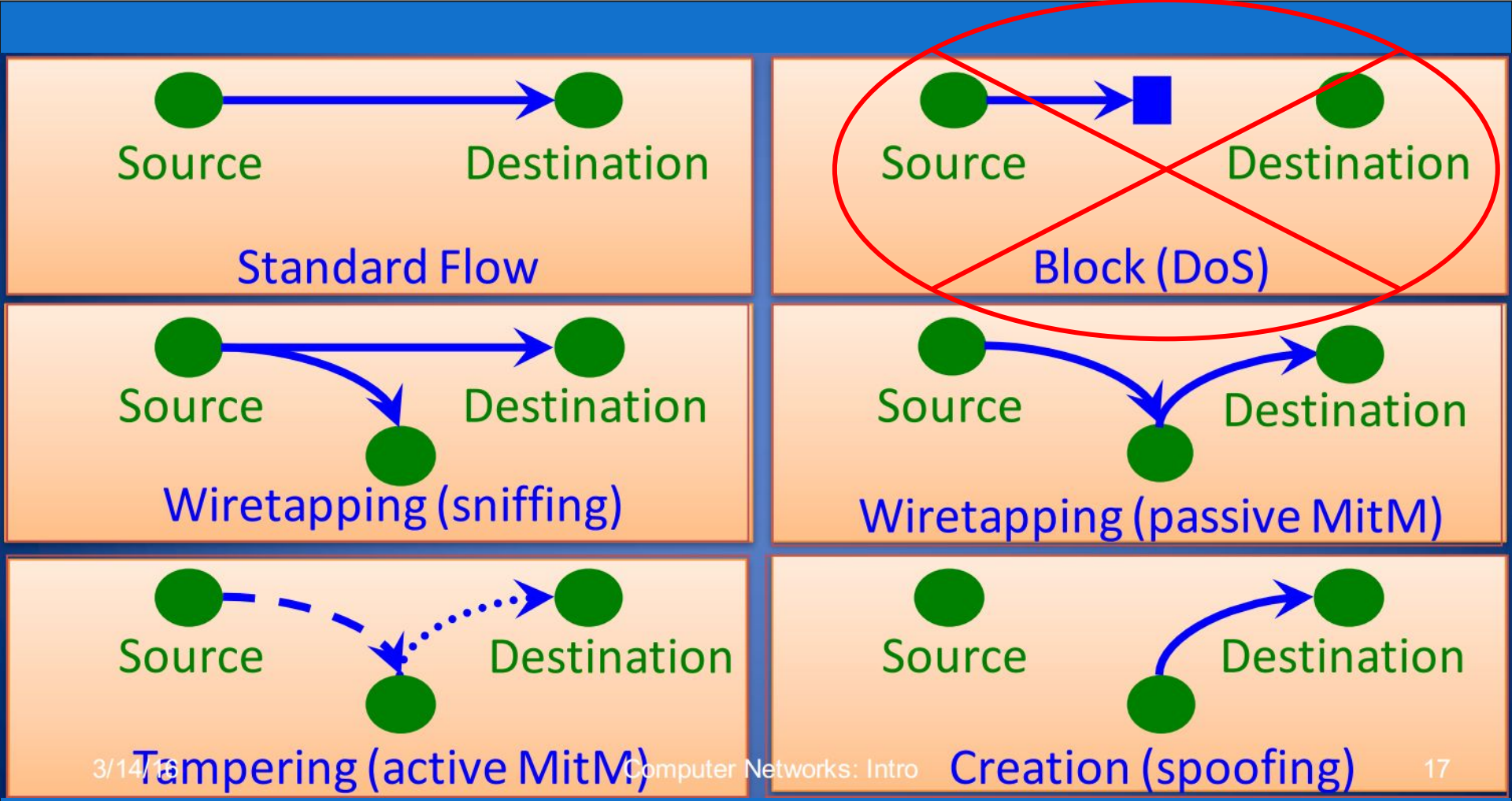
- Confidentiality
- Integrity
- Availability

Recall: Goals of communications sec.

- Confidentiality
- Integrity
- Availability

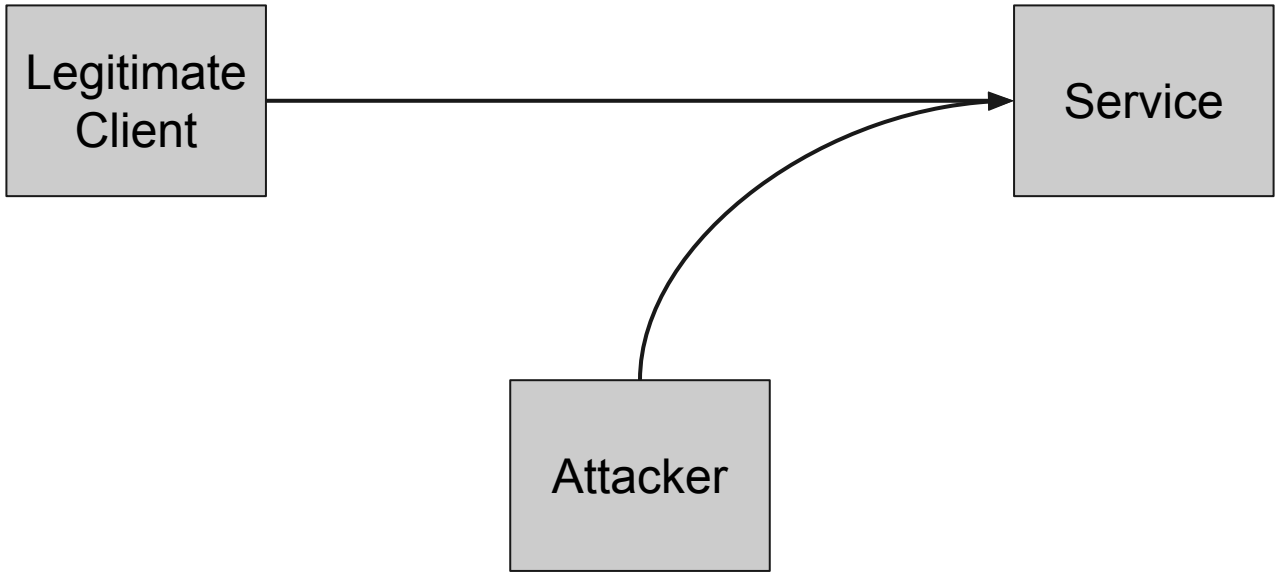

Source
Destination
Standard Flow
Source
Destination
Block (DoS)
Source
Destination
Wiretapping (sniffing)
Source
Destination
Wiretapping (passive MitM)
Source
Destination
Tampering (active MitM)
Source
Destination
Creation (spoofing)


Source
Destination
Standard Flow
Source
Destination
Block (DoS)
Source
Destination
Wiretapping (sniffing)
Source
Destination
Wiretapping (passive MitM)
Source
Destination
Tampering (active MitM)
Source
Destination
Creation (spoofing)


Source
Destination
Standard Flow
Source
Destination
Block (DoS)
Source
Destination
Wiretapping (sniffing)
Source
Destination
Wiretapping (passive MitM)
Source
Destination
Tampering (active MitM)
Source
Destination
Creation (spoofing)

Overview of Non-MitM DoS Attack

- Players
  - Service
  - Clients of the service
  - Attacker
- Goal: consume service's resources so they aren't available for legitimate clients


Legitimate Client
Service
Attacker

Classic Denial of Service

- Idea: find requests that are expensive for the service to perform
- Example: PHP's hash tables
  - Non-cryptographically secure hash function
  - "Chaining" to handle hash collisions
  - Attackers can engineer "multicollisions"
    - Turn hash table into one linked list
    - O(n) insertion and lookup
    - $O(n^2)$ for n elements

Classic Denial of Service: PHP

- Estimates from the bug report
  - POST requests can have key/value pairs
  - PHP stores these in `$_POST` (a hash table)
  - Maximum POST request size: 8MB
  - Estimated time to construct table on an Intel Core i7:

Classic Denial of Service: PHP

- Estimates from the bug report
  - POST requests can have key/value pairs
  - PHP stores these in `$_POST` (a hash table)
  - Maximum POST request size: 8MB
  - Estimated time to construct table on an Intel Core i7:

4 hours of CPU time

Classic Denial of Service

- Other examples of DoS attacks:
  - Billion laughs
  - Zip bomb
  - Ping of death
  - Pentium `F00F` bug

Distributed Denial of Service (DDoS)

- DoS like that is *very* powerful, but…
- Uncommon to find in the wild
- What to do?

Distributed Denial of Service (DDoS)

- What to do?
  - You've found the most expensive request
  - What's left?
  - Send as many of them as you can

Distributed Denial of Service (DDoS)

- **Distributed** Denial of Service
  - Distribute your attack across many machines
- In practice, usually PCs infected with malware
  - Each PC is called a “zombie” or “bot”
  - The entire collection of bots is a “botnet”

Distributed Denial of Service (DDoS)

- PC security is bad, so lots of machines can get infected
- Botnets can get **big**
  - Conficker (late 2000s): 3-4 million bots
  - Mariposa (late 2000s): 1 million bots
  - ZeroAccess (early 2010s): 2 million bots
- With millions of bots, you can do **lots** of computation and send **lots** of network traffic

Amplification Attacks

- You've found an expensive request
- You've acquired lots of computers
- Can you still do better?

Amplification Attacks

- You've found an expensive request
- You've acquired lots of computers
- Can you still do better?
- Yes: amplification attacks

Amplification Attacks

- Idea: trick third-party service into attacking for you
- Usually the goal is to send lots of network traffic
  - The resource is network bandwidth itself
  - “Layer 3” attacks - consume bandwidth of IP packets
- Best explained by example...

Spamhaus Attack

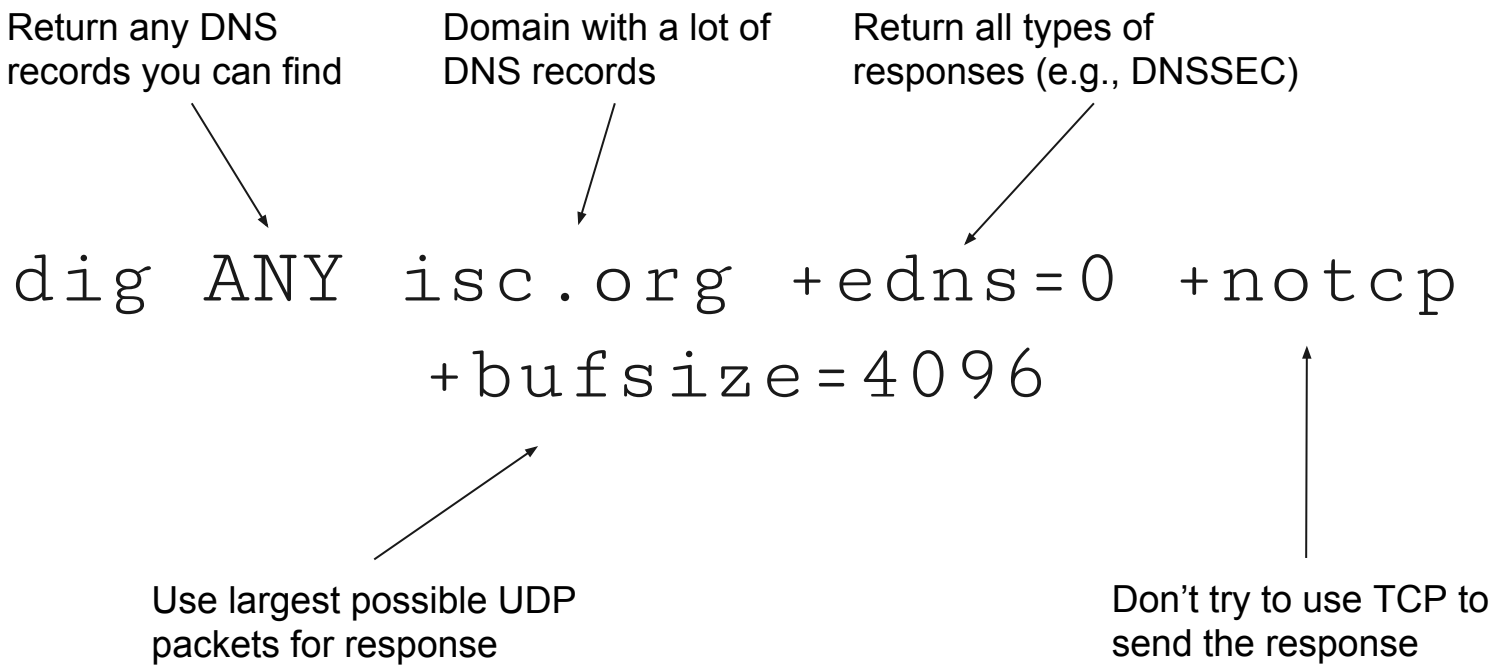
- March 2013
- 5-7 servers
- 3 networks
- ~300 Gbps traffic to Spamhaus
  - Most don’t get above 100 Gbps
  - Largest DDoS attack ever at the time
- How?

Spamhaus Attack

- Two ingredients:
  - Open DNS resolvers - accept queries from any IP
  - Networks that allow source IP spoofing
- Spoof victim's IP as the source IP
- Send DNS requests to these resolvers:

```
dig ANY isc.org +edns=0 +notcp
    +bufsize=4096
```

Spamhaus Attack



Spamhaus Attack

```
dig ANY isc.org +edns=0 +notcp
+bufsize=4096
```

64-byte query…

Spamhaus Attack

```
dig ANY isc.org +edns=0 +notcp
+bufsize=4096
```

64-byte query…

3,363-byte response…

Spamhaus Attack

```
dig ANY isc.org +edns=0 +notcp
+bufsize=4096
```

64-byte query…

3,363-byte response…

~50x amplification factor

Spamhaus Attack

- “DNS Amplification”
- 300 Gbps
- 30,956 open DNS resolvers
- 50x amplification factor
- 6 Gbps of input traffic
- 5-7 compromised servers
- 1 Gbps traffic from each server