Preventing UDP Flooding Amplification Attacks with Weak Authentication

Edoardo Biagioni
University of Hawaii at Manoa
Department of Information and Computer Sciences
esb@hawaii.edu

Denial of Service attacks on the Internet

- **Internet-connected servers have finite ability to process incoming traffic**
- **an attacker can prevent a server from processing useful incoming traffic by sending it lots of useless traffic**
- **this is a Denial of Service (DoS) attack**
  - also known as a **Flooding** attack

DoS with spoofed source IP

- **if the DoS traffic comes from a single source IP, the server administrator can block all traffic from that IP**
- **but the attacker can send data with spoofed source IP addresses**
  - the administrator cannot block all these addresses
  - many ISPs don’t check source IP addresses

Flooding Amplification attacks

- **Some Internet services respond to one packet with many packets**
- **e.g. the old telephone tree: you call 10 people, each of which calls 10 people, etc.**
  - AllNet works in this way
- **if such an amplifier receives a packet from a spoofed IP address, it replies to that address**
  - with more data than it received
- **the attacker sends the target's IP address as the source IP!!**
  - the amplifier replies by sending data to the target

Flooding Amplification attack details

- **The attacker selects a set of amplifying servers**
  - server could be DNS, NTP, or other
  - only UDP, because TCP 3-way handshake does not complete for spoofed IP source addresses
- **Packets sent to these servers elicit a reply to the target**
  - the DoS comes from these “innocent” third-party servers
- **works even without amplification**
  - but attacker needs more bandwidth than target
- **works better with amplification!**

Outline

1. **Denial of Service attacks √**
2. **Flooding Amplification attacks √**

   Successful Flooding Amplification attacks in 2013 and 2014
3. **Prevention**
4. **Weak Authentication**
   - Stateless Weak Authentication
   - AllNet
5. **Evaluation**

2013/2014 UDP Flooding Amplification attacks

- **2013 attack targeted spamhaus**
  - DNS servers used as amplifiers
- **2013/4 attack targeted cloudflare**
  - NTP servers used as amplifiers
- **the targets had now direct way of identifying the attackers**

Preventing Flooding Amplification

Two necessary ingredients for a successful attack:

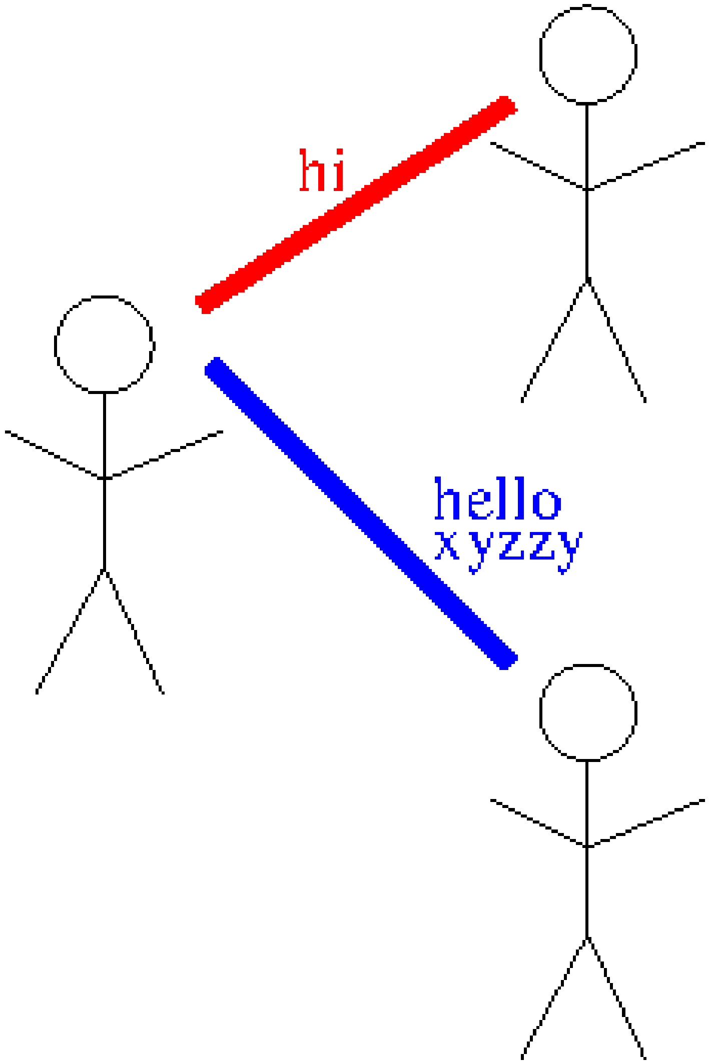
- spoofed source IP address
- traffic amplification

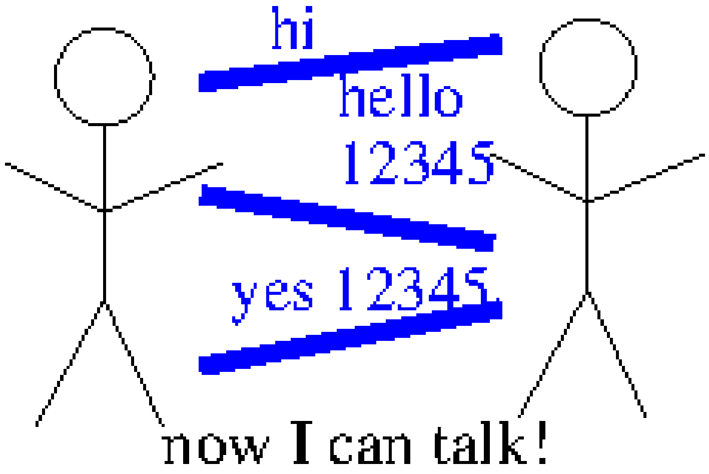
1. **Convince ISPs to filter out spoofed source addresses**
   - too much work for ISPs, many do not filter
2. **Make servers not amplify traffic**
   - must be done for each type of UDP server

Weak Authentication

- **Authentication: evidence of who you are**
- **Weak Authentication: evidence that you can receive traffic at a specific IP address**
  - e.g. in the TCP 3-way handshake, the answer to the second packet provides the server with evidence that the client received the second packet

Weak Authentication Examples





Cookies for Weak Authentication

- **If Alice sends a bit string *s* to IP *x***
- **and in return, receives *s* from *x***
- **then Alice has evidence that IP *x* is participating in the protocol**
- **refinement: *s* is a combination (hash) of an unpredictable value with *x* itself**
  - then Alice can verify any returned *x* without having to store the pair *(s, x)* – stateless authentication!
- **TCP cookies combine IP and seq number**

AllNet

- **designed to work well on the Internet**
  - UDP and TCP
- **when there is no Internet, designed to work on ad-hoc networks**
- **sending to anyone who might need the message**
  - many redundant message transmissions
- **amplification!!**

Weak Authentication for AllNet

- **a UDP packet from an unknown IP elicits a small response with secret *s***
  - *s* is a cookie based on the IP address (IPv4 or IPv6)
  - the address is hashed with a local secret
- **if a response carries *s*, the IP is added to the list of destinations for UDP traffic**
- **in practice, AllNet on UDP regularly sends keepalive/heartbeat messages, and these can carry *s***
- ***s* (i.e. the local secret) can change over time**

Evaluation

- **When strict authentication is turned on for AllNet:**
  - failing to respond to an authenticating keepalive keeps us from receiving any traffic
  - sending many packets to an AllNet, without responding, only receives an authenticating response once every 10s
- **When responding correctly, traffic is carried as usual**
- **Weak authentication adds one round-trip time to the exchange**

Integration

- first, distribute code that responds to the weak authentication
- later, can deploy code that only amplifies after weak authentication
- because AllNet forwards packets widely, some of the forwarders can be strict, and others not, and we still have connectivity while accomodating older code
- once all have upgraded, can be strict

Summary

- Weak Authentication only guarantees that the sender can see what we sent to them
- Weak Authentication efficiently discards packets from spoofed IPs

→ Weak Authentication prevents Denial of Service Amplification attacks with spoofed source IPs

Denial of Service attacks and TCP

- **TCP is particularly vulnerable to DOS:**
  - TCP SYN packets make the server allocate memory
  - if a packet in a connection is dropped, TCP intentionally slows down to avoid causing congestion
    - if many packets are dropped, TCP slows down to one packet/RTT
- **On the other hand, spoofed source Ips cannot succeed with the TCP 3-way handshake**