Security Review of Protocols

CSYS 4483-01/CSYS 6683-01
Network Defense

Tirthankar Ghosh, Ph. D.

Vulnerabilities with IP

IP spoofing: A source can send packets with fake IP address.

- Authentication based on source address will not work.
- Fake return address is included.

IP Address Spoofing

- When spoofing is used with connectionless protocols (like UDP or ICMP), the activity is not easy to detect.
- Fraggle attack: sending spoofed UDP packets to port 7 (echo). The attacker sets both source and destination ports to 7 on two hosts that the attacker is targeting.

IP Address Spoofing (cont’d)

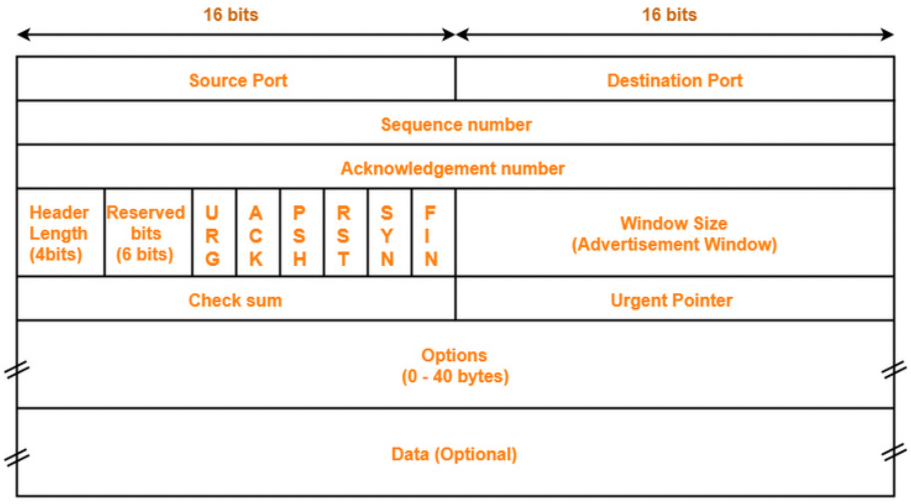
- Spoofed packets can also be used to cause amplification effect if they are sent to a broadcast address.
- TCP packets are never sent to a broadcast address.
- Smurf attack: An attacker spoofs an ICMP Echo Request packet with the source address indicating the intended victim, and the destination address as the subnet broadcast address.
- Essentially, all border routers are configured to reject traffic directed to the subnet broadcast address.

IP Packet Fragmentation

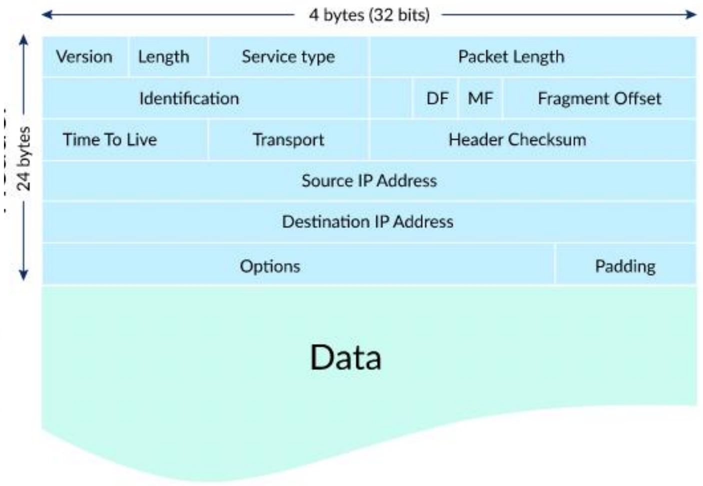
- All hosts must accept packets with a minimum length of 68 bytes (an internet header may be up to 60 bytes, and the minimum fragment is 8 bytes) (RFC 791).
- Problems with fragmentation:
  - If duplicate fragments are received with differing contents, which fragment to save?
  - For overlapping contents in fragments, which one will take precedence?
  - An attacker creates a packet with Fragment Offset of 65,528, and 1480 bytes of data, thus making the total packet length of 67,008 (maximum packet length can be 65,535). Possible that other data in the OS can be overwritten, causing the system to crash.

Vulnerabilities with IP (cont'd..)

- IP fragmentation attack – Read RFC 1858.
  - Tiny fragment attack
  - Overlapping fragment



TCP Header



ARP Abuses

- ARP Flooding
- MAC Spoofing
- ARP Spoofing

ARP Flooding

- In a switched network, a switch maintains a cache of ARP responses to route traffic to a host.
- When the cache is full, a switch either:
  - Reverts back to the hub mode
  - Flushes its buffer
- In both cases, traffic destined to a specific port will “leak”, which is of potential interest to hackers.
- Hackers can create a flood of spoofed ARP reply packets overflowing a switch’s ARP cache, and forcing it to the hub mode.

MAC Spoofing

- Practically every Ethernet adapter can be reprogrammed to have any desired hardware address.
- Hackers can reprogram the Ethernet adapter on a system to spoof that of another system on the network.

ARP Spoofing

- ARP response packets can be spoofed to divert and disrupt traffic.
- Hackers can combine ARP spoofing with Denial of Service (DoS) attack on specific target host preventing it from responding.
- Can be used for Person-in-the-Middle attack (most times referred to as Man-in-the-Middle or MITM)

Vulnerabilities with TCP and UDP

- Exploiting half-open TCP connection.

- TCP Sequence number attack:
  - Guessing initial sequence number to fool the target host.

- UDP spoofing: It is easier to spoof UDP packets because of no handshaking.
  - Each system using UDP has to have its own authentication mechanism.

TCP SYN Flood Attack

- Exploiting half-open connection state.
- Remedial measures:
  - Limiting connection rate
  - Purging stale connections
  - Using SYN cookies
    - Initial sequence number is cryptographically generated from IP address and port number.
    - No need to keep pending connections in queue.
    - Biggest drawback is that cryptographic operation demands increased CPU utilization.
    - Video tutorial

TCP Control Packets with Data

- RFC 793 does not prevent transport of data in a SYN, FIN or RST packet.
- Normally, TCP/IP stacks will not send data in these packets.

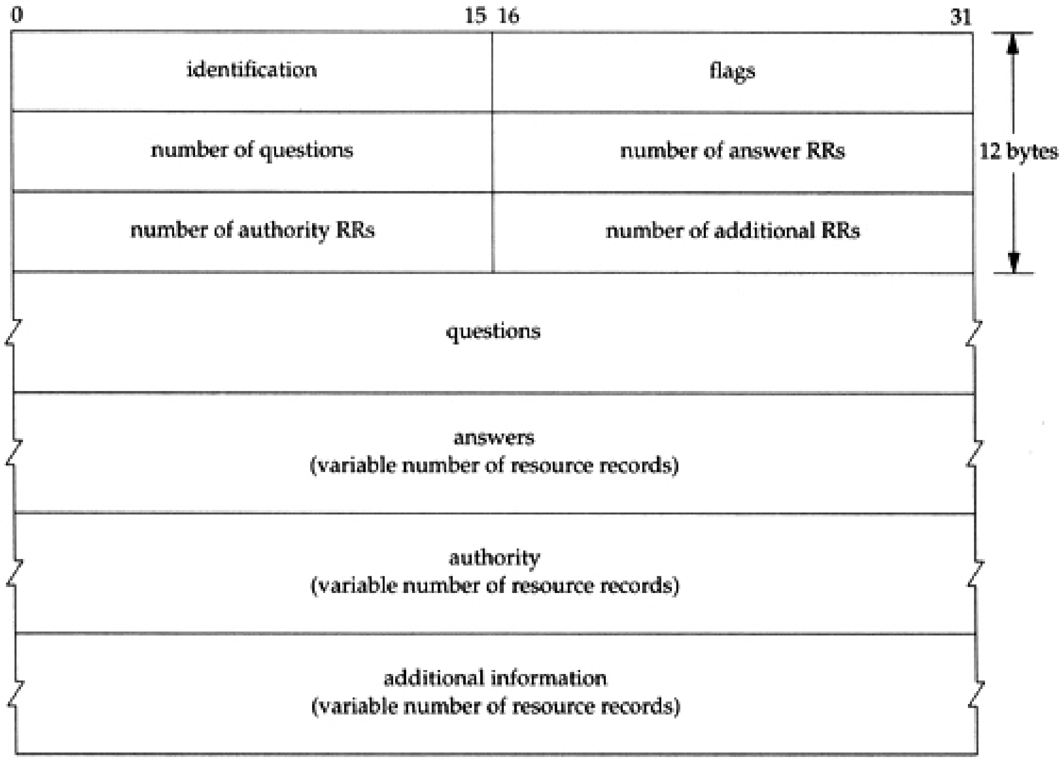
Vulnerabilities with ICMP

- Used to inform hosts of a better route to the destination, to report trouble with a route, or to terminate a connection because of network problem.

- Hackers can use ICMP to tear down connections, or creating new paths to destinations.

DNS

- DNS uses two logically separate trees, the first maps host names to IP addresses, the second maps IP addresses to names.
- DNS Query and Response



0 15 16 31

identification | flags

number of questions | number of answer RRs

number of authority RRs | number of additional RRs

12 bytes

questions

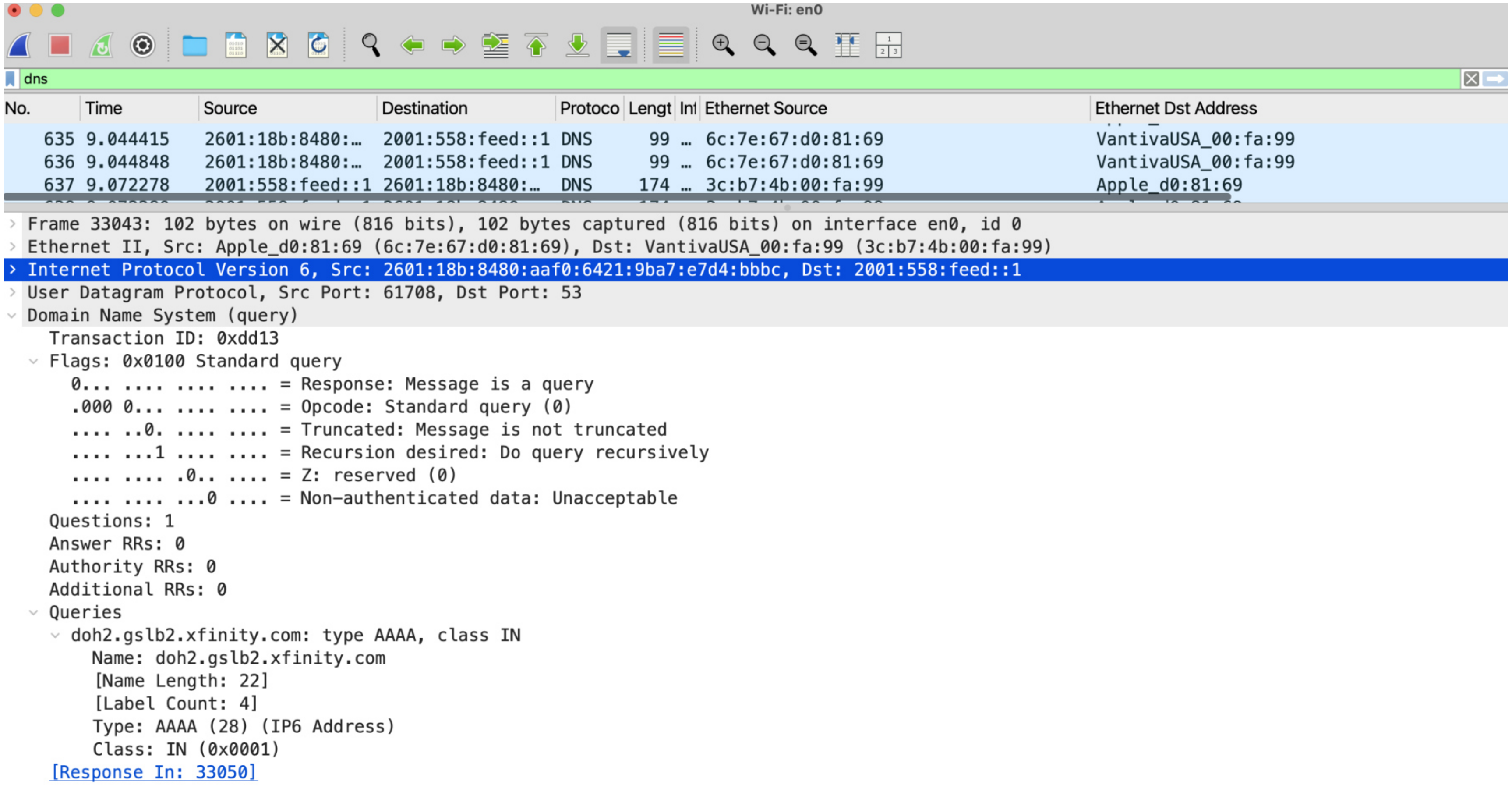
answers
(variable number of resource records)

authority
(variable number of resource records)

additional information
(variable number of resource records)

Ref.: https://flylib.com/books/en/3.223.1.151/1/

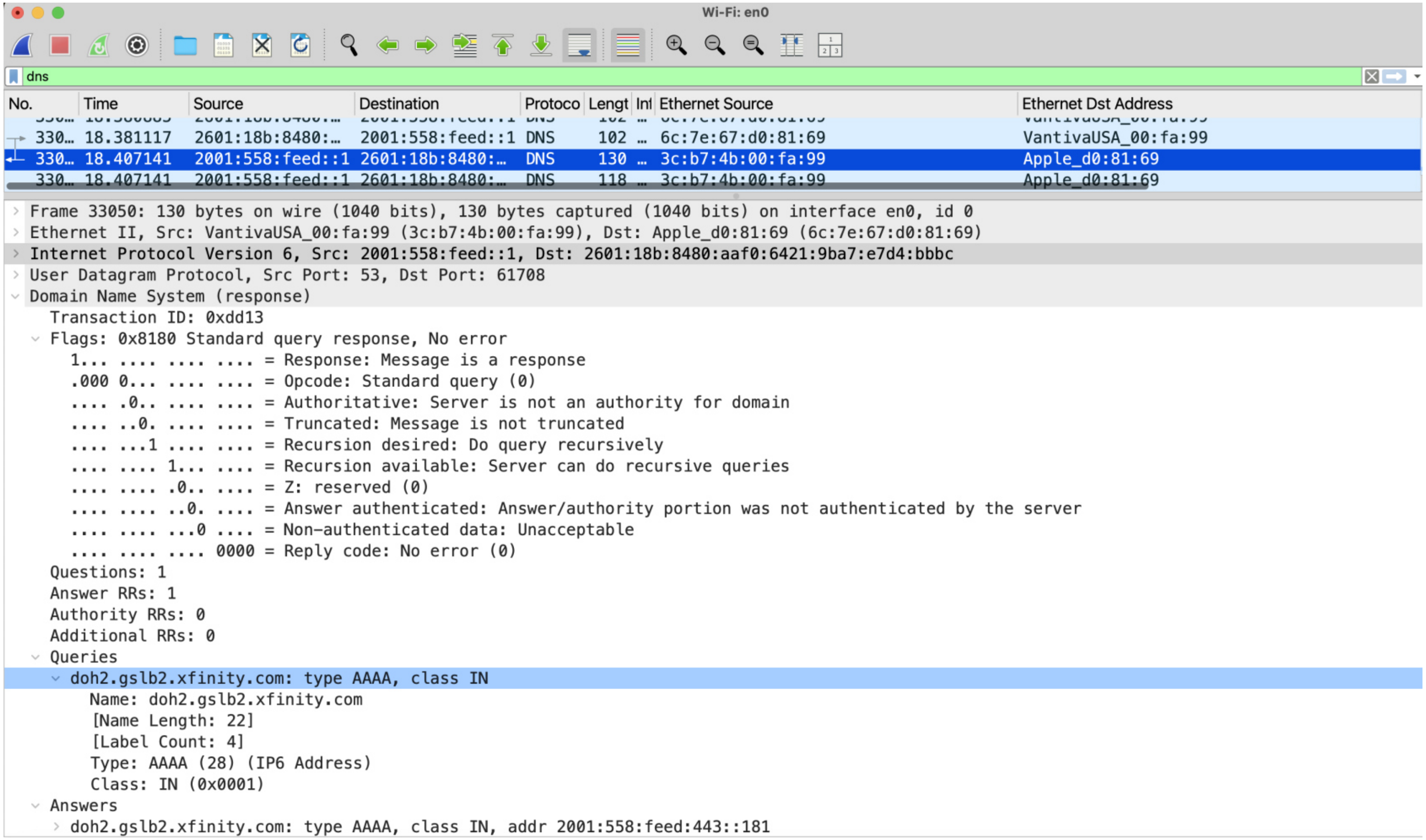
DNS Query



```
No.      Time        Source             Destination        Protoco Lengt Int Ethernet Source      Ethernet Dst Address
     635 9.044415    2601:18b:8480:…    2001:558:feed::1   DNS        99 …   6c:7e:67:d0:81:69    VantivaUSA_00:fa:99
     636 9.044848    2601:18b:8480:…    2001:558:feed::1   DNS        99 …   6c:7e:67:d0:81:69    VantivaUSA_00:fa:99
     637 9.072278    2001:558:feed::1   2601:18b:8480:…    DNS       174 …   3c:b7:4b:00:fa:99    Apple_d0:81:69
```

```
> Frame 33043: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface en0, id 0
> Ethernet II, Src: Apple_d0:81:69 (6c:7e:67:d0:81:69), Dst: VantivaUSA_00:fa:99 (3c:b7:4b:00:fa:99)
> Internet Protocol Version 6, Src: 2601:18b:8480:aaf0:6421:9ba7:e7d4:bbbc, Dst: 2001:558:feed::1
> User Datagram Protocol, Src Port: 61708, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xdd13
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v doh2.gslb2.xfinity.com: type AAAA, class IN
        Name: doh2.gslb2.xfinity.com
        [Name Length: 22]
        [Label Count: 4]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
    [Response In: 33050]
```

DNS Response



```
dns
```

```
No.    Time       Source            Destination       Protoco Lengt Inf Ethernet Source        Ethernet Dst Address
330…  18.381117  2601:18b:8480:…   2001:558:feed::1  DNS     102   …   6c:7e:67:d0:81:69      VantivaUSA_00:fa:99
330…  18.407141  2001:558:feed::1  2601:18b:8480:…   DNS     130   …   3c:b7:4b:00:fa:99      Apple_d0:81:69
330…  18.407141  2001:558:feed::1  2601:18b:8480:…   DNS     118   …   3c:b7:4b:00:fa:99      Apple_d0:81:69
```

```
> Frame 33050: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface en0, id 0
> Ethernet II, Src: VantivaUSA_00:fa:99 (3c:b7:4b:00:fa:99), Dst: Apple_d0:81:69 (6c:7e:67:d0:81:69)
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:18b:8480:aaf0:6421:9ba7:e7d4:bbbc
> User Datagram Protocol, Src Port: 53, Dst Port: 61708
v Domain Name System (response)
    Transaction ID: 0xdd13
  v Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v doh2.gslb2.xfinity.com: type AAAA, class IN
        Name: doh2.gslb2.xfinity.com
        [Name Length: 22]
        [Label Count: 4]
        Type: AAAA (28) (IP6 Address)
        Class: IN (0x0001)
  v Answers
    > doh2.gslb2.xfinity.com: type AAAA, class IN, addr 2001:558:feed:443::181
```

Vulnerabilities with DNS

- DNS Cache poisoning attack
  - Bailiwick checking
- Mitigation
  - DNSSEC – how DNSSEC works