CprE 530

Lecture 15

Topics

- TCP vulnerabilities
- UDP
- UDP vulnerabilities
- DNS

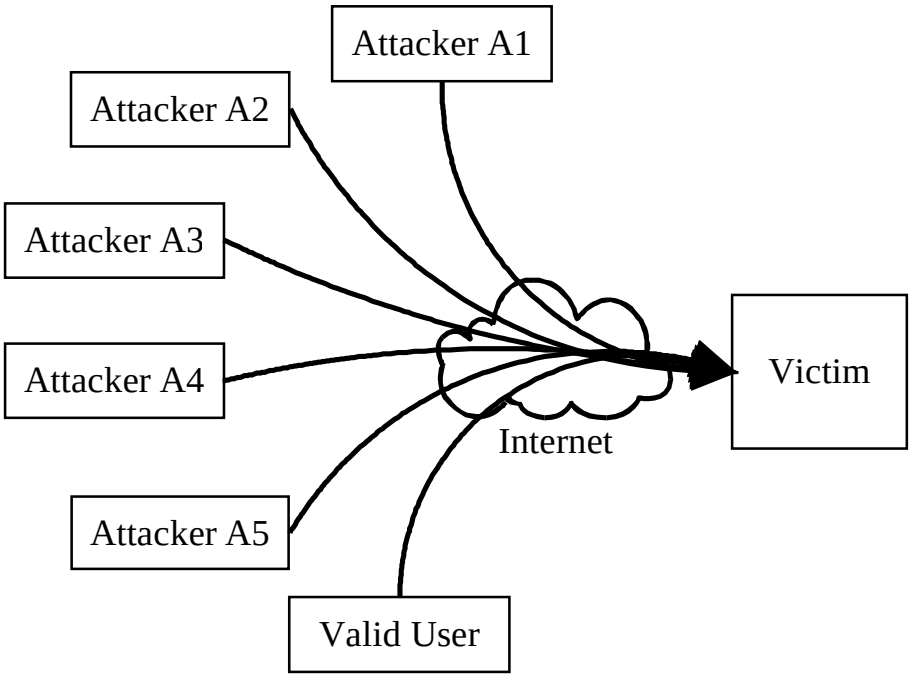
Header Based

- There have been several attacks using invalid flag combinations.
- Most have been fixed, however this is now used to help determine the type of operating system
  - Probing attacks
    - Invalid header responses
    - Initial values
      - sequence numbers
      - Window size

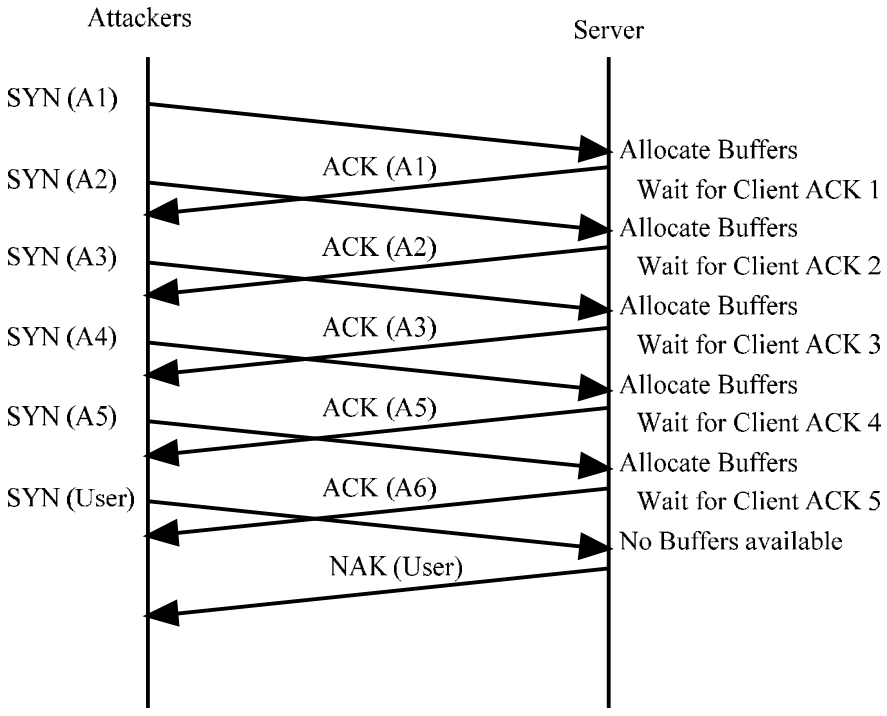
Protocol Based

- Syn flood
- Reset Packets
- Session Hijacking

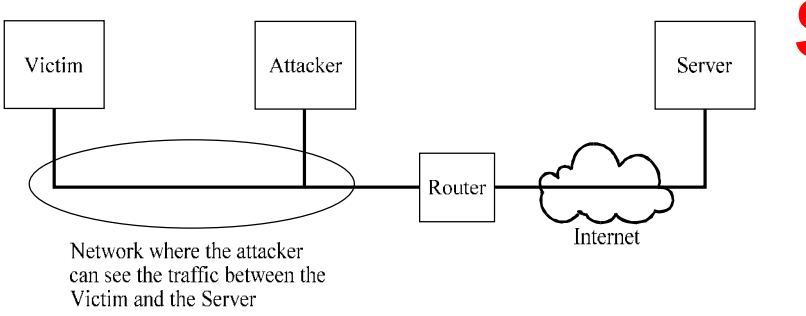
SYN Flood



SYN Flood



Reset Shutdown



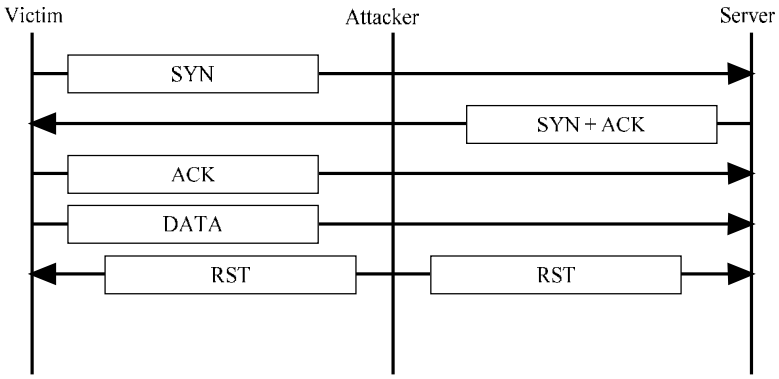
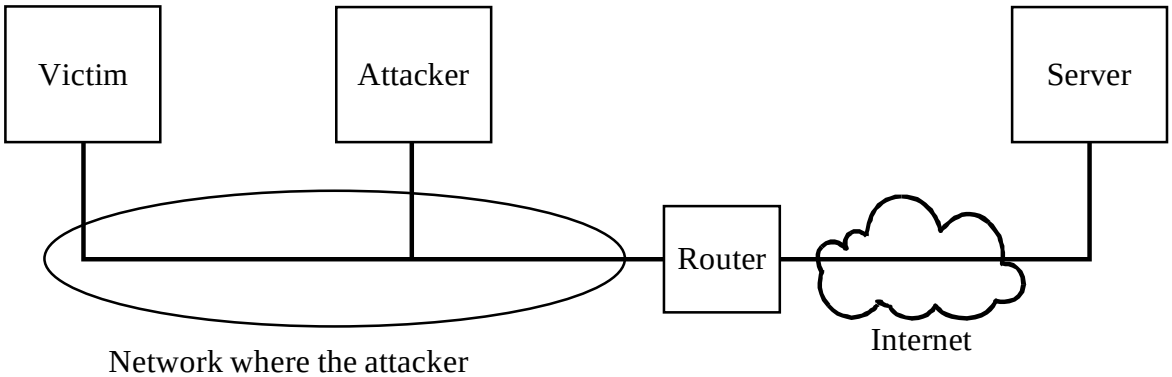
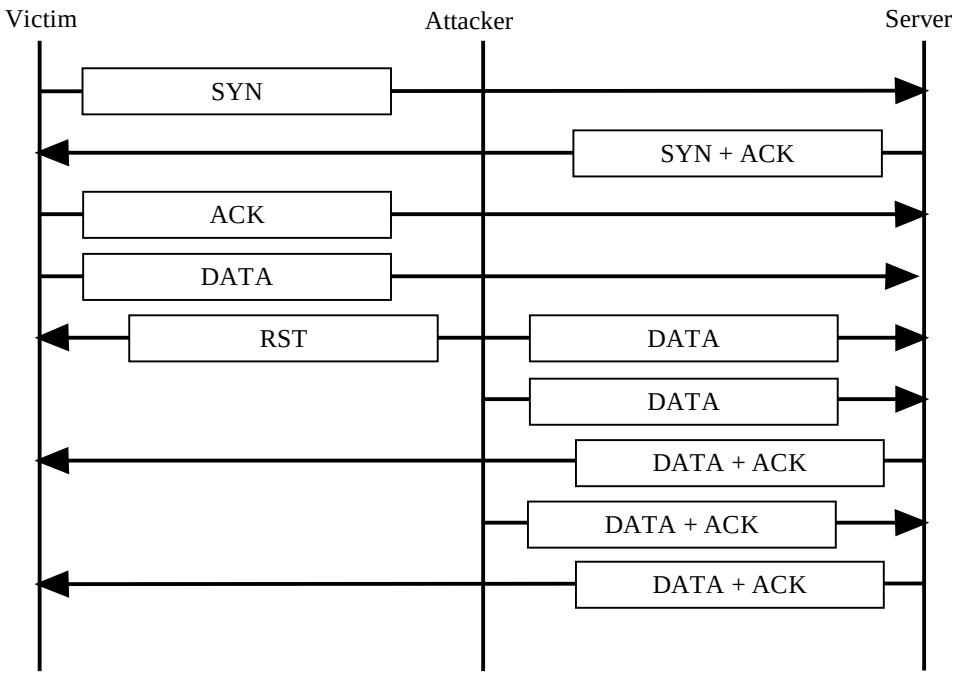


Figure 7.8 RST Connection Shutdown

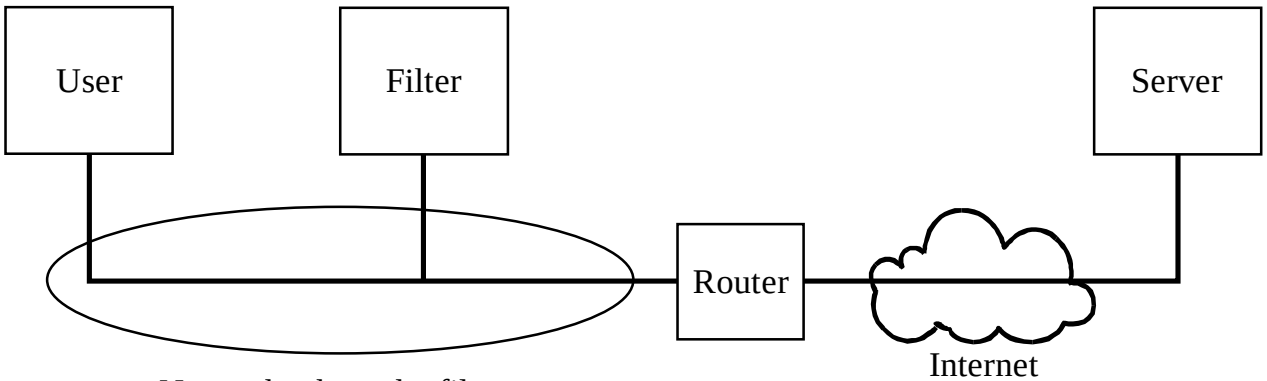
Session Hijacking



Session Hijacking

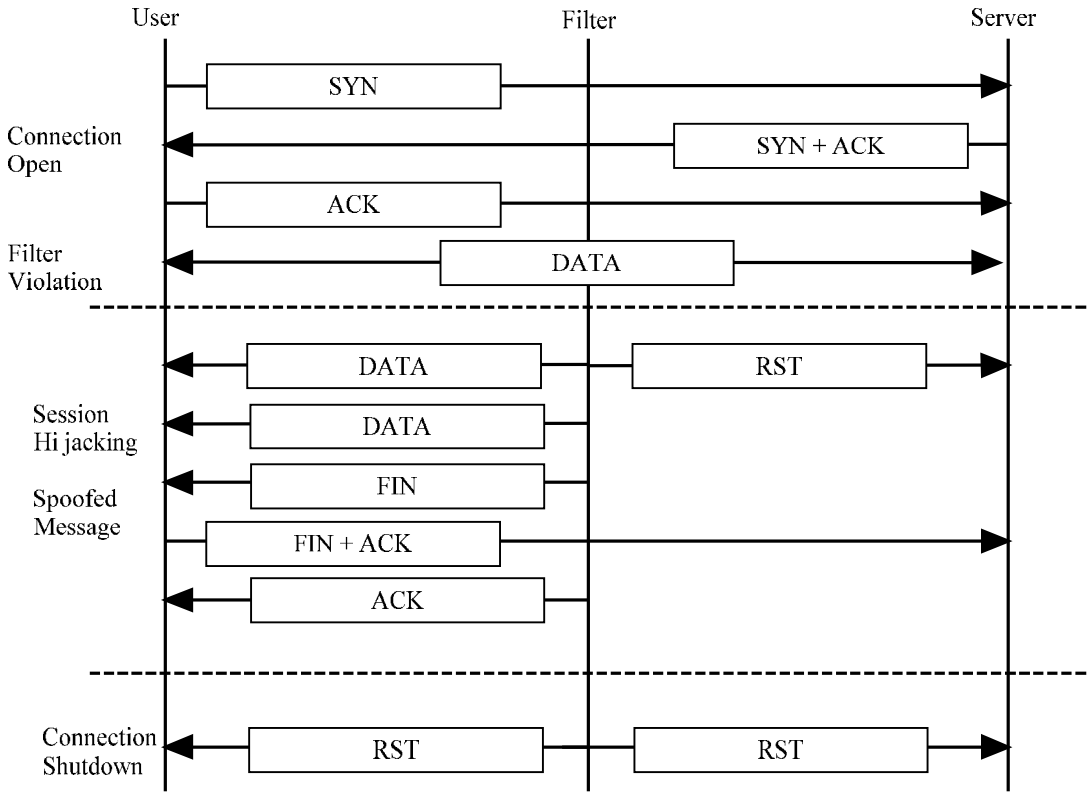


Passive Network Filter



Network where the filter
can see the traffic between the
user and the server

Passive Network Filter



Mitigation

- Encryption can fix Session hijacking
- Reset is harder
- Syn flood is hard

Authentication Based

- No authentication in TCP
- Ports might be considered an authentication of the application

Traffic Based

- Flooding (using all of the TCP resources)
- QOS
- Sniffing

User Datagram Protocol

- Designed to allow connectionless protocols
- Typical applications will send one packet and wait for a single response.

Source Port	Destination Port
UDP Total Length	Checksum

UDP Attacks

- Header & Protocol: None since there is no protocol and very simple header
- Authentication: same as TCP
- Traffic: typically not a problem. Sniffing is a potential problem, but most UDP protocols don't try to hide data. Flooding is hard with UDP.
- Mitigation: Most organizations block all UDP except port 53 (DNS)

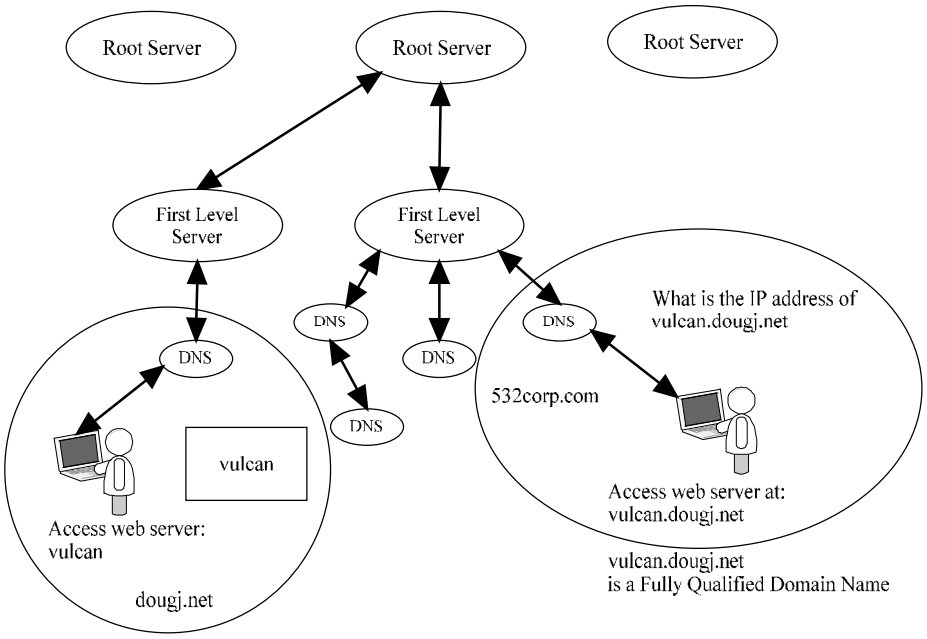
Domain Name Service

- Designed to give organizations a way of controlling their name space
- Distributed control over computer name to IP address mapping
- DNS normally uses UDP and port 53
  - If the answer is bigger than 512 bytes, can use TCP

Domain Names

- Tree Structure - max 128 levels, root = level 0
- Domain name: www.iastate.edu
  - Each name between the dots is called a **label**
  - Label <= 63 characters
- Fully qualified domain name: www.iastate.edu.
  - Adds "." at the end
- Partially qualified domain name
  - Supported by the client
  - The leftmost part of a domain name
  - E.g., www. Gets filled in to www.iastate.edu by the client

DNS Name Space



vulcan	.	dougj	.	net
Label	.	Label	.	Label

Server Types

- Server Types
  - Root Server
  - Primary Server
  - Secondary Server
- Can only push data from Primary to Secondary (not Secondary to Primary)

DNS Queries

- DNS Queries
  - Name to Address
  - Address to Name
- Resolver: Client code that queries DNS using two lookup methods:
  - Recursive
  - Iterative

Reverse Query

- IP to Name
- 129.186.5.100 – what is its name
- Query is made to:
  - 100.5.186.129.in-addr.arpa.
- This way it can be parsed just like a name
  - 129 then 186 then 5 then 100

Reverse Lookups

- IP to Name conversion
- Not all IP addresses will resolve to a name

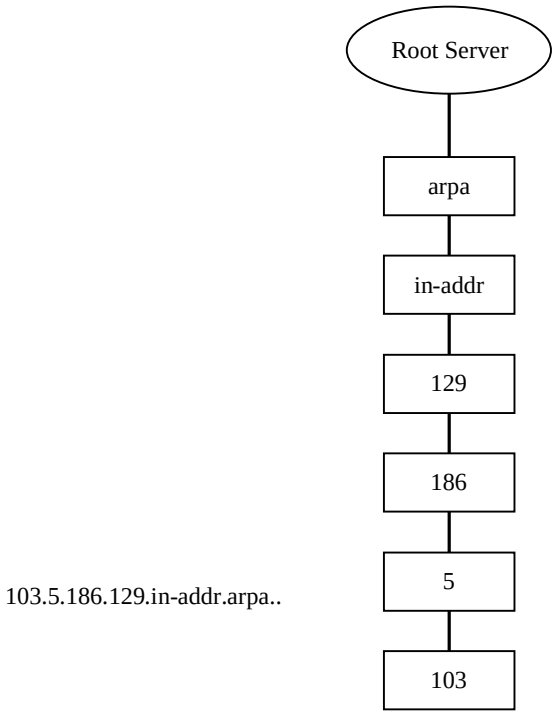


Figure 7.13 DNS Reverse Name Hierarchy

DNS System

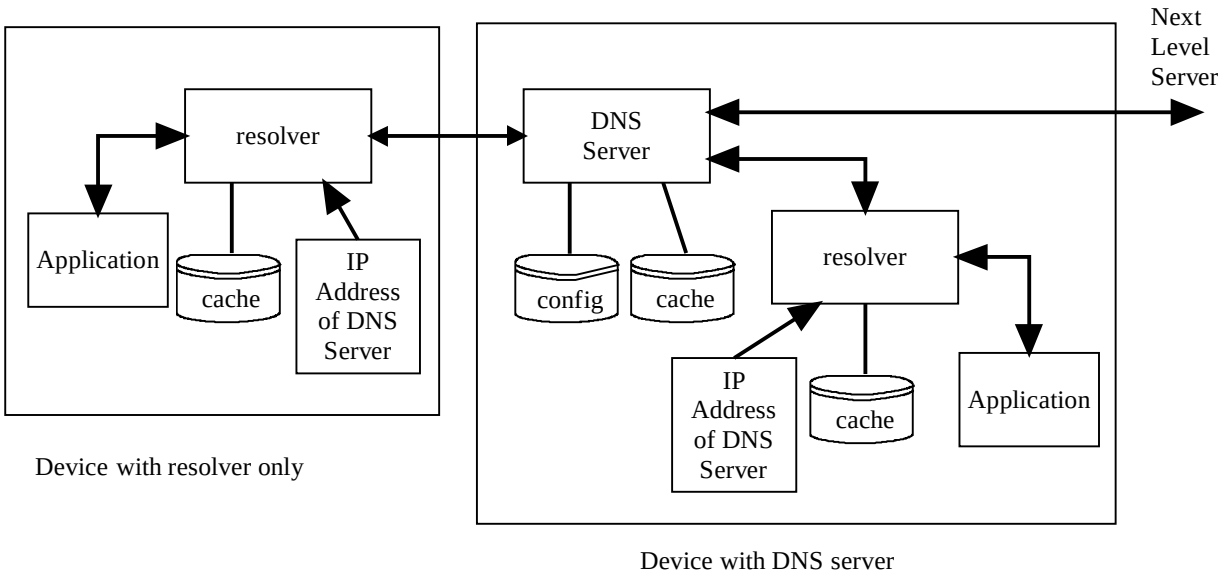


Figure 7.14 DNS System

Recursive Query Method

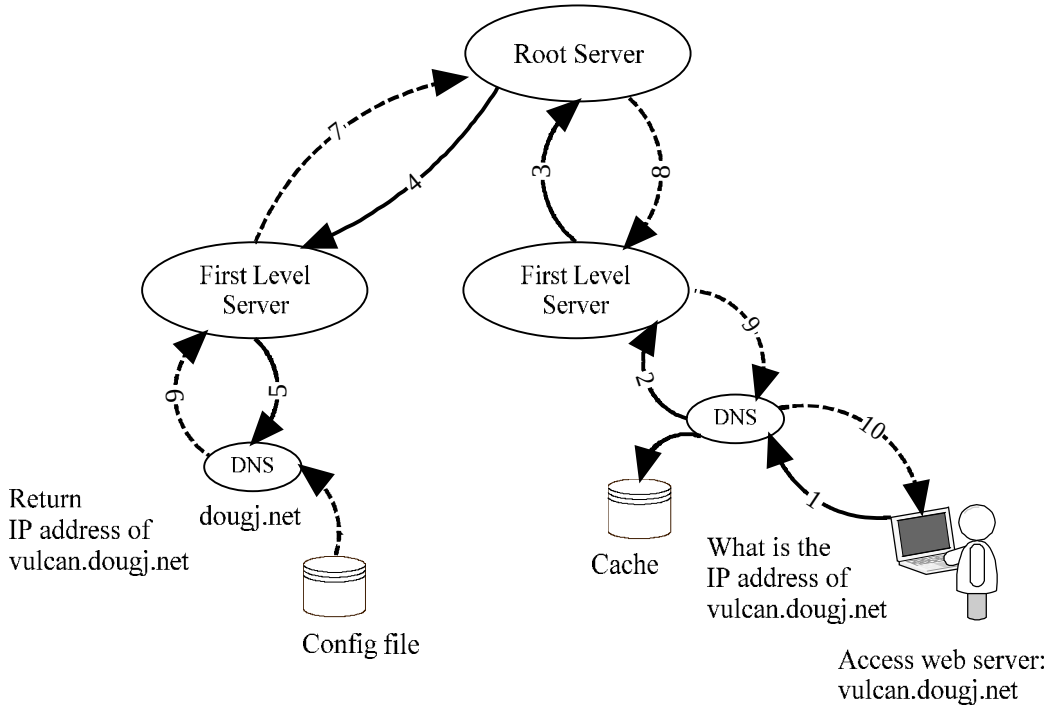


Figure 7.15 DNS Recursive Mode

Iterative Query Method

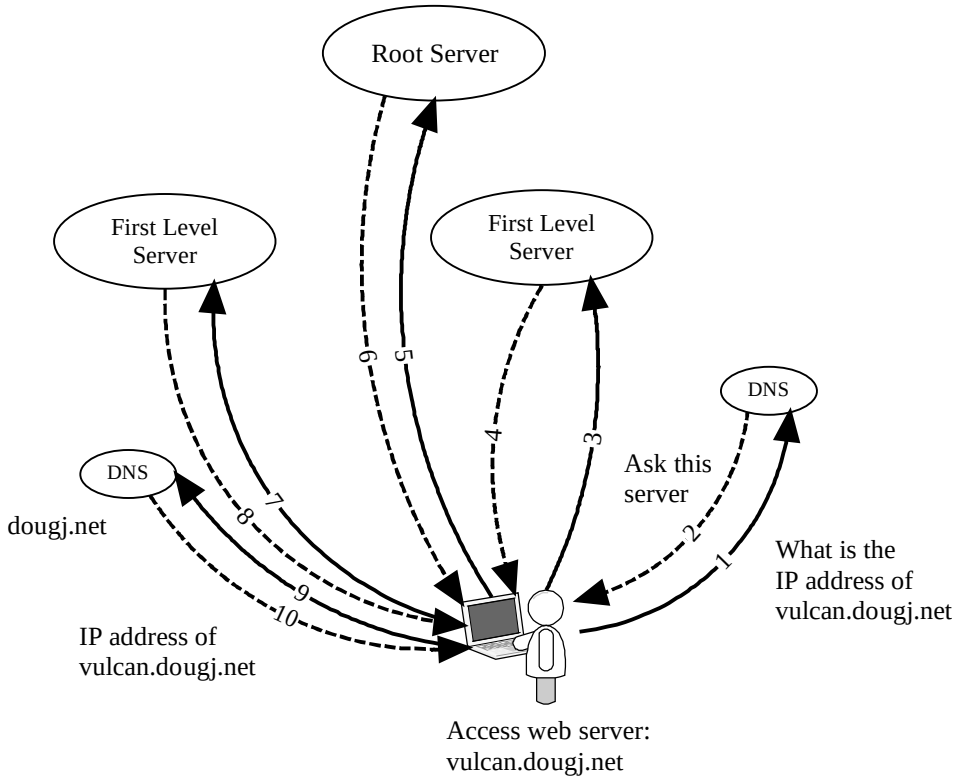


Figure 7.16 DNS Iterative Mode

Responses

- If the answer comes back from any DNS server that has the answer cached it is called unauthoritative
- To handle the stale cache issue there is a time to live for each response.

DNS Uses Two Messages

- Query := two fields
  - header | question
- Response := five fields
  - header | question | answer | authoritative | additional

DNS Packet Format

ID	Flags	
Number of Questions	Number of Answers	Fixed Header
Number of Authoritative Answers	Number of Additional Records	
Question		Question Section
Query Type	Query Class	

Query Packet

QR	Opcode	AA	TC	RD	RA	0	0	0	rCode

Flags

DNS Packet Format

ID	Flags	
Number of Questions	Number of Answers	Fixed Header
Number of Authoritative Answers	Number of Additional Records	
Question		Question Section
Query Type	Query Class	
Answer(s)		
Authoritative Answer(s)		
Additional Records		

Response Packet

QR	Opcode	AA	TC	RD	RA	0	0	0	rCode

Flags

DNS Message Header

- Header = 12 bytes
  - Id = 2 bytes
  - Flags = 2 bytes (see next slide)
  - # of questions = 2 bytes
  - # of answers = 2 bytes (0 in query)
  - # of authoritative answers = 2 bytes (0 in query)
  - # of additional answers = 2 bytes (0 in query)

Flags Field

- 1 bit – Q/R 0=query, 1= response
- 4 bits – opcode
  - 0 = standard
  - 1 = inverse
  - 2 = server status request
- 1 bit AA – 1 = Authoritative answer
- 1 bit TC – 1 = answer > 512 bytes
- 1 bit RA – 1 = recursion available
- 3 bits of zero
- 4 bits – response code (see next slide)

Response codes

- 0 No Error
- 1 format error
- 2 problem at name server
- 3 domain reference problem
- 4 query type not supported
- 5 administratively prohibited

DNS Question section

- Variable length – Query name
- 16 bits – query type
- 16 bits – query class

DNS Query Name

- 6vulcan2ee7iastate3edu0
- Numbers are the count fields, they are in binary
- The count fields are only 6 bits to tell the difference between a count value and a offset pointer used for compression

DNS Types

- 1- A – Address
- 2 – NS – Name server
- 5 – CNAME – Alias
- 6 – SOA – Start of Authority
- 11 – WKS – Well known services
- 12 – PTR – IP to name conversion
- 13 – HINFO – Host info
- 15 – MX – Mail exchange
- 28 – AAAA – IPV6 address
- 252 – AXFR – Request a zones transfer
- 255 – ANY – Request all records

DNS Resource Record

- Domain name – Variable length (pointer to the name in the query section
- Domain type (16 bits) same as query
- Domain class (16 bits) same as query
- Time to Live (32 bits) number of seconds, 0 = don't cache
- Resource data length (16 bits)
- Resource data (variable length)

Resource data

- Number (4 bytes – V4)
- Domain name (variable length)
- Offset pointer (upper two bits of first byte = 11
- Char string – 1 byte length followed by characters

Compression

- 11 [address of the beginning byte]
- 12 is the first byte of the question section

Header & Protocol attacks

- Header
  - Not many attacks, bad headers are rejected.
  - Can be used to leak data through a firewall
- Protocol
  - Simple protocol
  - Can use the DNS port number to communicate through a firewall

Authentication

- Bad DNS Entries
  - Break in DNS server
  - Rouge DNS server
  - DNS cache poisoning
  - Bogus DNS replies
- Scope of Damage

DNS attack damage scope

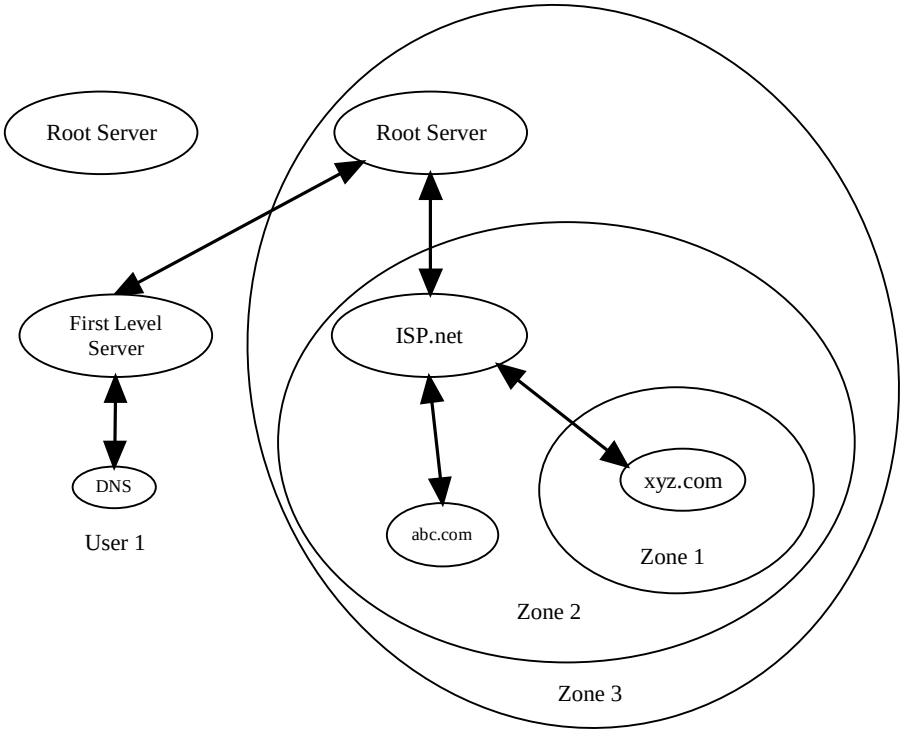


Figure 7.18 DNS Attack Damage Scope

Traffic

- DNS server flooding can cause delayed to dropped responses. DNS client will try 4 times so they often will get an answer
- Sniffing is not a problem

DNS

- DNSSEC is a new protocol and server that offers authenticated DNS with certificates.
  - Not widely adopted
- DNS is a major weak point in the Internet. Taking down the DNS system can take down the entire Internet.

Transport Layer Security

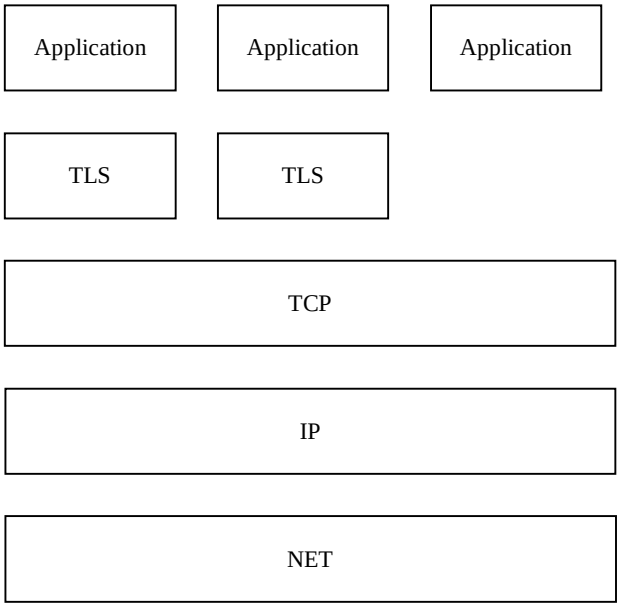


Figure 7.19 TLS Stack

TLS Protocol

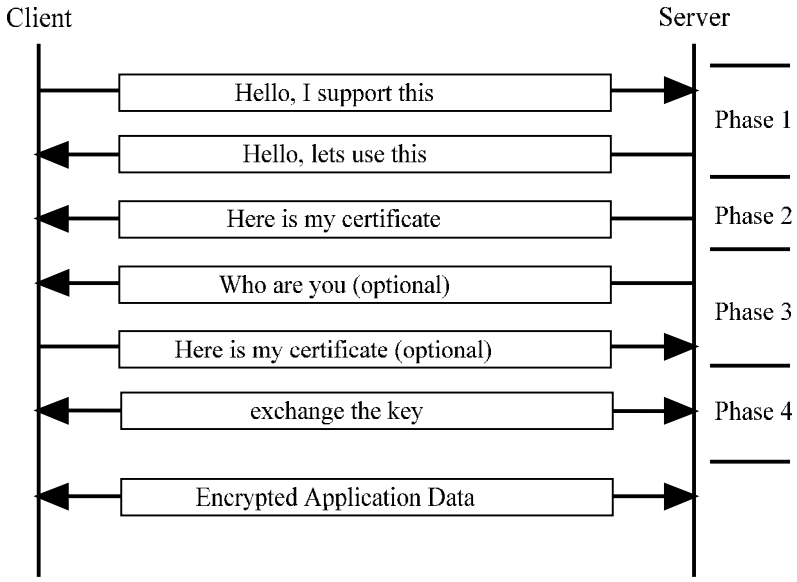


Figure 7.20 TLS Protocol