iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 2 **Issue:** IX **Month of publication:** September 2014

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

# Security Problems and Their Defenses in TCP/IP Protocol Suite

Shubham Kumar[1], Vishal Sharma[2], Shubham Chabbra[3], Toshar Namsot[4]
[1,2,3,4]*CSE Department*
*DCE Gurgaon*

***Abstract:*** ***The Transmission Control Protocol/Internet Protocol (TCP/IP) is combination of different protocols at various layers.TCP/IP is the basic communication language or protocol of the Internet and private networks either an intranet or an extranet. The TCP/IP suite has many design weaknesses so far as security and privacy are concerned. Some of these are protocol design weaknesses, whereas rest is defects in the software that implements the protocols. In this paper, I focused mainly on protocol level issues, rather than implementation flaws. In this paper, we discuss about the security issues related to the some of the protocols in the TCP/IP suite.***

***Keywords: IP (Internet Protocol), RIP (Routing Information Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol).***

## I. INTRODUCTION

This paper is an overview of security attacks in the core protocols (IP, UDP and TCP) and other protocols like EGP,BGP, RIP, ICMP and DNS. However, we do not address the exploits in various application protocols. Some of these are protocol design weaknesses per se, whereas the rest are defects in the software that implements the protocols. IP, UDP, TCP and infrastructure protocols were designed at a time when security concerns were almost non -existing and trust was assumed. While this paper summarizes design Weaknesses in the TCP/IP suite from a security point of view, it is important to remember that many implementations have "fixed" these weaknesses, but are not described in RFCs. We assume that the reader is fluent in TCP and IP details. Protocol weaknesses can be divided into those due to i) the design of the protocol itself, and ii)the configuration, deployment and daily operation of the DNS servers. As can be expected, there is a strong interplay between the two. All major OS have made improvements in their implementations of the protocol stack that mitigate or disable many of the attacks described below. Of course, the attack tools also improve. A number of enhancements for TCP/IP have been made that are not yet in common use. Several of them (e.g., DNSSEC and IPV6) involve heavy use of encryption and require more computing power. As computing power in end -user hosts increases, we expect to see these universally deployed.

## II. TCP SYN ATTACKS (OR SYN FLOODING)

UDP is a connectionless protocol belongs to the transport layer. It is a thin protocol on top of IP providing high speed but low functionality.UDP does not guarantee the delivery of datagrams. Messages can be delivered out of order, delayed or even lost. Datagrams may get duplicated without being detected. The UDP protocol is used mostly by application services where squeezing the best performance out of existing IP network is necessary, such as trivial file transfer protocol (TFTP), NFS and DNS. Unfortunately, UDP cannot provide security and privacy of the data flow.

A UDP flood attack sends a large number of UDP packets to random ports. Such ports may be open or closed. If open, an application listening at that port may be open or closed. If closed, the network layer, replies with an ICMP Destination Unreachable Packet. Thus, the victim host will be forced into sending many ICMP packets and wasting computing cycles. If the flooding is large enough, the host will eventually be unreachable by other clients. The attacker will also IP-spoof the UDP packets, both to hide and to ensure that the ICMP return packets do not reach him.

Surprisingly, using legitimate applications or OS services an attacker can generate a storm of packets. On many systems, the standard services known as chargen that listens typically at port 19 and echo that listens typically at port 7 are enabled. Chargen sends an unending stream of characters intended to

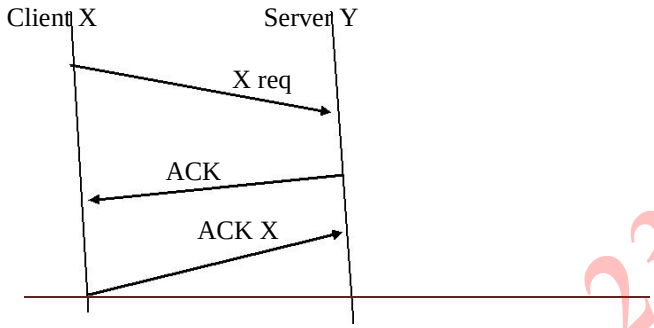
IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

ISSN: 2321-9653

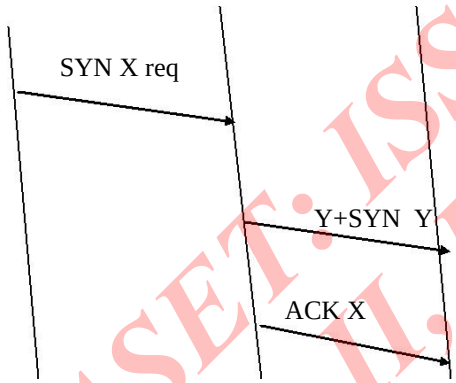


be used as test data for terminals. The echo service just echoes what it receives. It is intended to be used for testing reachability, identifying routing problems, and so on. An attacker sends a UDP packet to the port 19 with the source address spoofed to a broadcast address and the source port spoofed to 7.The chargen stream is sent to the broadcast address and hence reaching many machines on port 7.Each of these machine will echo back to the victims port 19.This ping-pong action generates a storm of packets. An attack called fraggle uses packets of UDP echo service in the same fashion as the ICMP echo packets.

Normal TCP handshake




TCP SYN Flood Attack




*A. Defenses*

Both end-host and network-based solutions to the SYN flooding attack have merits. Both types of defense are frequently employed, and they generally do not interfere when used in combination. Because SYN flooding targets end hosts rather than attempting to exhaust the network capacity, it seems logical that all end hosts should implement defenses, and that network-based techniques are an optional second line of defenses that a site can employ.

## III. UDP EXPLOITS

UDP is a connectionless protocol belongs to the transport layer. It is a thin protocol on top of IP providing high speed but low functionality.UDP does not guarantee the delivery of datagrams. Messages can be delivered out of order, delayed or even lost. Datagrams may get duplicated without being detected. The UDP protocol is used mostly by application services where squeezing the best performance out of existing IP network is necessary, such as trivial file transfer protocol (TFTP), NFS and DNS. Unfortunately, UDP cannot provide security and privacy of the data flow.

A UDP flood attack sends a large number of UDP packets to random ports. Such ports may be open or closed. If open, an application listening at that port may be open or closed. If closed, the network layer, replies with an ICMP Destination Unreachable Packet. Thus, the victim host will be forced into sending many ICMP packets and wasting computing cycles. If the flooding is large enough, the host will eventually be unreachable by other clients. The attacker will also IP-spoof the UDP packets, both to hide and to ensure that the ICMP return packets do not reach him Surprisingly, using legitimate applications or OS services an attacker can generate a storm of packets. On many systems, the standard services known as chargen that listens typically at port 19 and echo that listens typically at port 7 are enabled. Chargen sends an unending stream of characters intended to be used as test data for terminals. The echo service just echoes what it receives. It is intended to be used for testing reachability, identifying routing problems, and so on. An attacker sends a UDP packet to the port 19 with the source address spoofed to a broadcast address and the source port spoofed to 7.The chargen stream is sent to the broadcast address and hence reaching many Integrated machines on port 7.Each of these machine will echo back to the victims port 19.This ping-pong action generates a storm of packets.

An attack called fraggle uses packets of UDP echo service in the same fashion as the ICMP echo packets.

*A. Defenses*

To defend, most host disable many UDP services such as the chargen and echo mentioned above. Because UDP is better suited for streaming applications, there are suggestions to run UDP over SSL or even create a protocol immediately above UDP. Routing protocol is used. Some of these attacks succeed only if the remote host does source address -based authentication; others can be used for more powerful attacks. A number of these attacks described below can also be used to accomplish denial of service by confusing the routing tables on a host or gateway.

## IV. ROUTING INFORMATION PROTOCOL (RIP) ATTACKS

IJRASET: ISSN: 2321-9653 Volume II, Issue IX, September 2014

The Routing Information Protocol (RIP) is used to propagate routing information on local networks, especially broadcast media. Typically, the information received is unchecked. This allows an intruder to send bogus routing information to a target host, and to each of the gateway along the way, to impersonate a particular host. The most likely attack of this sort would be to claim a route to a particular unused host, rather than to a network; this would cause all packets destined for that host to be sent to the intruder's machine.(Diverting packets for an entire network might to be too noticeable; impersonating an idle work-station is comparatively risk-free).Once this is done, protocols that rely on address -based authentication are effectively compromised.

This attack an yield more subtle, and more serious, benefits to the attacker as well. Assume that the attacker claims a route to an active host or workstation instead. All packets for that host will be routed to the intruder's machine for inspection and p ossible alteration. They are then resent, using IP source address routing, to the intended destination. An outsider may thus capture passwords and other sensitive data. This mode of attack is unique in that it affects outbound calls as well; thus, a user calling out from the targeted host can be tricked into divulging a password. Most of the earlier attacks discussed are used to forge a source address; this one is focused on the destination address. This and are the earliest mentions of routing attacks in the literature. The attacks described here-abusing the routing protocols for eavesdropping and/or packet modification -remain a very serious threat. Indeed, a National Research Council study identified routing attacks as one of the two major threats to the internet. While there are proposals to solve this problem, nothing has been implemented; all of the proposed solutions have their drawbacks. Defense against routing attacks must still be considered a research problem.

Routing attacks have happened frequently by accident. In the most famous case, known as the "AS 7007" incident, an ISP started advertising that it had the best routes to most of the internet. Even after they powered down their router, it took more than four hours for the global routing tables to stabilize.

*A. Detection of IP Spoofing*

We can monitor packets using network-monitoring software. A packet on an external interface that has both its source and destination IP addresses in the local domain is an indication of IP spoofing. Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

*B. Prevention of IP Spoofing*

All routers must employ proper IP filtering rules. They should only route packets from source that could legitimately come from the interface the packet arrives on. Most routers now have options to turn off the ability to spoof IP source address by checking the source address of a packet against the routing table to ensure the return path of the packet is through the interface it was received on

## V. DOMAIN NAME SYSTEM

The Domain Name System(DNS) provides for a distributed database mapping host names to IP addresses. An intruder who interferes with the proper operation of the DNS can mount a variety of attacks, including denial of service and password collection. There are a number of vulnerabilities. The original DNS specifications did not include security based on the fact that the information that it contains, namely host names and IP addresses, is used as a means of communicating data. As more and more IP based applications developed, the trend for using IP addresses and host names as a basis for allowing or disallowing access (i.e., system based authentication) grew. Unix saw the advent of Berkeley "r" commands (e.g., rlogin,rsh etc.) and their dependencies on host names for authentication. Then many other protocols evolved with similar dependencies, such as NFS, HTTP etc. The existence of DNS server on behalf of the client. If the server passes the query onto another DNS server that has the incorrect information, whether placed there intentionally or unintentionally, then cache poisoning can occur. Malicious cache poisoning is commonly referred to as DNS spoofing.

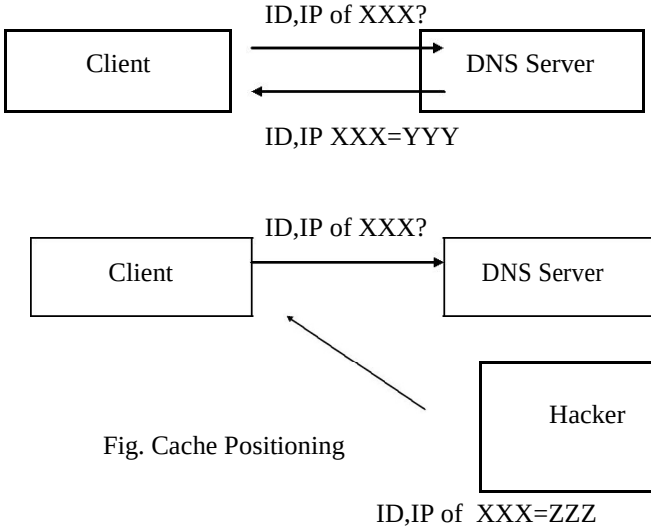



Fig. Cache Positioning

IJRASET: ISSN: 2321-9653 Volume IX, Issue IX, September 2014

widespread use of such protocols as the r-commands put demand on the accuracy of information contained in the DNS. False information within the DNS can lead to unexpected and potentially dangerous exposu res. The majority of weaknesses within in the DNS fall into the following categories: Cache Poisoning, client flooding, dynamic update vulnerability, information leakage and comprise of the DNS server's authoritative database

*A. Security Threats of the DNS*

*DNS zone transfers* Questioning the legitimacy of a zone transfer request is left out of the protocol. It is also possible to include a zone transfer gratuitously as part of response to a legitimate query. *DNS Cache Poisoning* Cache poisoning happens whenever a DNS server does not have the answer to a query within its cache, the DNS server can pass the query onto another DNSSEC.

*DNS Forgery* The DNS answers that a host receives may have come from an attacker who sniffs a query between the victim resolver and the legitimate name servers and responds to it with misleading data faster than the legitimate name server does. The attacked host may in fact be a DNS server.DNS forgery is also called spoofing.

*Domain Hijacking* A domain is hijacked when an attacker is able to redirect queries to servers that are under the control of the attacker. This can happen because of cache poisoning, forgery or a domain server has been compromised.DNS hijacking is also known as redirection.

*B.Defenses* In 1994, the IETF formed a working group to provide security extensions to the DNS protocol in response to the security issues surrounding to the DNS i.e

DNSSEC. Adequate protection against information leakage is already provided through such things as split DNS configuration.

## VII.CONCLUSION

The TCP/IP suite has many design weaknesses so far as security and privacy are concerned, all perhaps because in the era (1970s) when the development took place network attacks were unknown. The flaws present in many implementations exacerbate the problem. A number of these are due to the infamous buffer overflow which is preventable by better programming practices. However, considerable blame belongs to the many ambiguous RFCs. In this paper, we highlighted the protocol attacks and their defenses.

## REFERENCES

[1]. S.M.Bellovin. A look back at "Security problems in the T CP/IP Protocol suite".

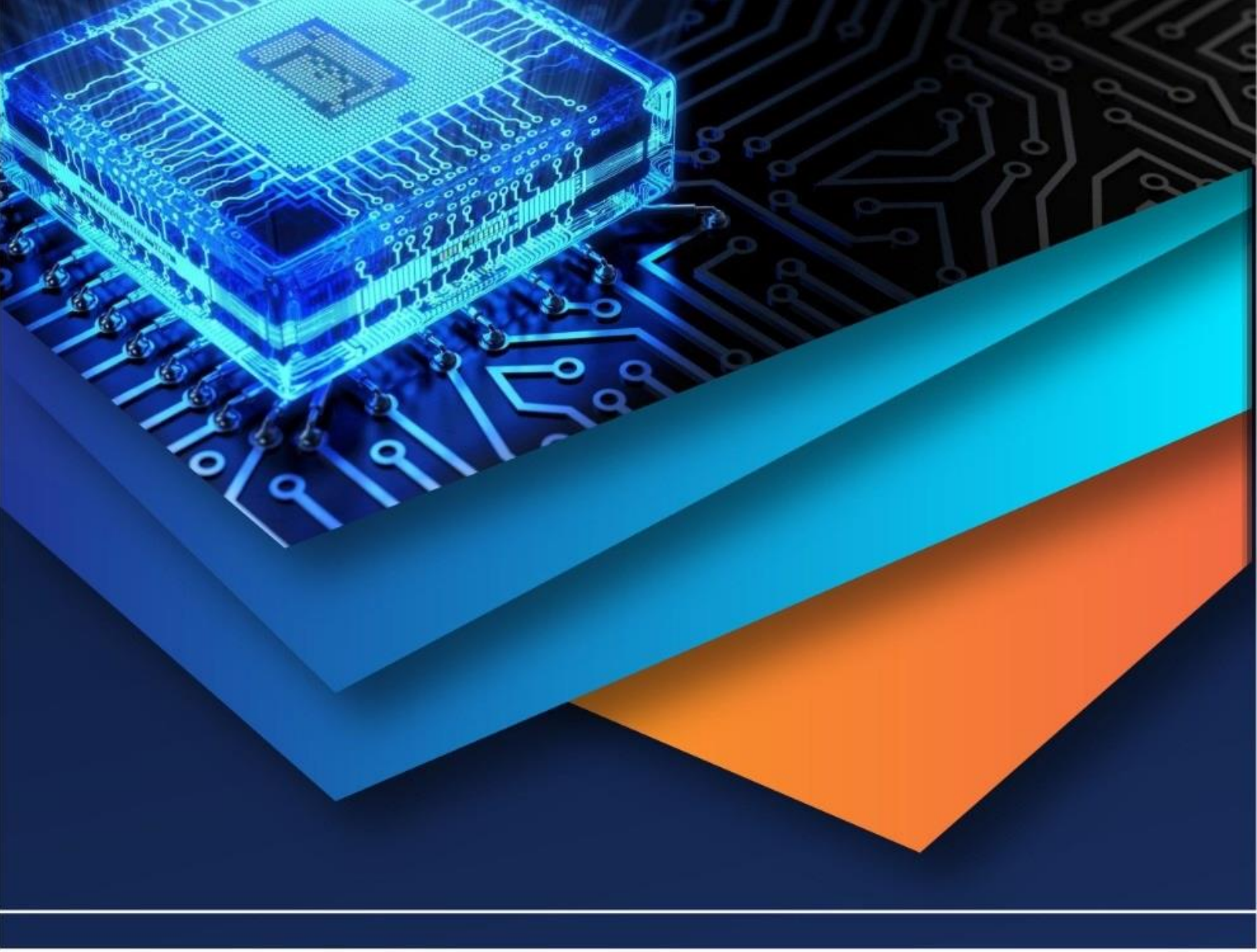
[2]. S.M.Bellovin, security problems in the T CP/IP protocol suite,ComputerCommunicationsReview.http://www.research. att.com/~smb/papers/ipext.pdf

[3]. Larson, M.and Liu, C.," Using BIND: Don't get spoofed again", SunWorld, November1997 http://www.sunworld.com/ bind.html swol-11-1997/swol-11-

[4]. Stevens, Glenn."T he Domain Name Service". June 2 1,1995.http://eeunix.ee.usm.maine.edu/guides/dns/dns.html

[5]. I.Arce, Attack trends: More bang for the bug: AN account of 2003's attack trends, IEEE Security & Privacy [6]. R.Barden, editor. Requirements for Internet hosts-

IJRASET : ISSN: 2321-9653 Volume II, Issue IX, September 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)