

Chapter 8

TCP/IP Routing Protocols

The goal of routing security is to provide efficient, secure and robust way for routing. Traditional interior and exterior routing protocols do not provide adequate security mechanisms for current needs of Internet communication. This chapter focuses on the inherent vulnerabilities of traditional routing protocols and how these insecure protocols can be exploited to assist in launching other attacks within a network. This chapter introduces some common security problems in RIP, OSPF and BGP and solutions for routing security.

8.1 Types of Routing Protocols

Internet is built over TCP/IP stack of which routing is the network layer and central part. Routing is the act of moving information across a network (with at least one node in between). Routing involves two basic activities: determining optimal routing paths and protocol use metrics for evaluation of paths. Routing algorithms initialize and maintain routing tables which contain route information. The purpose of routing protocols is to learn available routes that exist on the enterprise network, build routing tables and make routing decisions. There are a number of protocols available for use here. The options available in TCP/IP protocol suite are RIP, IGRP, EIGRP, OSPF, BGP. The routing protocols are broadly categorized into two types: inter domain (Exterior) protocols and intra-domain protocols (Interior). A network under the administrative control of a single organization is called an autonomous system (AS). The process of routing within an AS is called intradomain routing and routing between ASes is called interdomain routing. Within an AS, routers communicate with each other through the process of intradomain routing. BGP is the defacto standard for interdomain communication whereas RIP, IGP, OSPF are the protocols used for intra domain routing as shown in Figure 8.1.

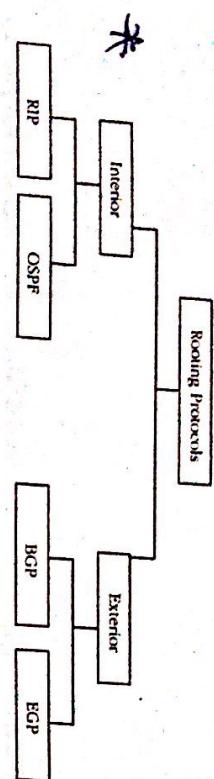


Figure 8.1 Types of Routing Protocols

The routing protocol must be coupled with a medium access control (MAC) protocol. The routing protocol specifies to whom a node should transmit the packet and the MAC protocol specifies when it should transmit the packet. With the growing awareness of network security, it is believed that more sophisticated attacks could be developed and aimed at the heart of Internet: routers.

Static Routing: The simplest form of routing is static routes. The routing information is preprogrammed by the network administrator. When changes to the network occur, the route information must be manually changed throughout the network.

There are a number of advantages to using static routes. Static routing is very resource efficient, as it routing uses no additional network bandwidth, doesn't use any router CPU cycles trying to calculate routes, and requires far less memory. It is also the most secure form of routing protocol.

However, there are a number of disadvantages to static routing that eliminate it as a viable alternative on the <Client> network. First and foremost, in the rapidly changing topology of a wireless network, it is impractical for a network administrator to manually program the routing changes as they occur. Secondly, in the case of a network failure, static routing is usually not capable of choosing alternate paths.

Dynamic Routing: In dynamic routing, the routing tables are updated periodically. Distance Vector Routing protocols are dynamic.

Distance Vector Routing: Distance vector routing provides a tremendous advantage over static routing. Routers are able to discover the state of the network, and to propagate changes as they occur. The most common, and most ubiquitous of distance vector routing protocols is the Routing Information Protocol, or RIP.

RIP is a link-state routing protocol that periodically transmits the entire routing table to all immediate neighbors, they can add significant traffic. This is particularly problematic on a wireless network with limited bandwidth.

- Distance vector protocols are slow to converge, or adapt to network topology changes. After a change to the network, and before all the routers have converged, there is the probability of routing errors and lost data.
- Distance vector routing protocols base their routing decisions on distance, or the number of "hops" from one network to another. It does not take into consideration the speed or bandwidth of a network path. Therefore, routers may route traffic through paths that are suboptimum.

Link-State Protocols: Link-state routing protocols, such as Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and NetWare Link Services Protocol (NLP), were designed to address the limitations of distance vector routing protocols (slow convergence and unnecessary bandwidth usage). Link-state protocols are more complex than distance vector protocols, and running them adds to the router's overhead. The additional overhead (in the form of memory utilization and bandwidth consumption when link-state protocols first start up) constrains the number of neighbors that a router can support and the number of neighbors that can be in an area. When the network is stable, link-state protocols minimize bandwidth usage by sending updates only when a change occurs. A hello mechanism ascertains reachability of neighbors. When a failure occurs in the network, link-state protocols flood Link-State Advertisements (LSAs) throughout an area. LSAs cause every router within the failed area to recalculate routes. The fact that LSAs need to be flooded throughout the area in failure mode and the fact that all routers recalculate routing tables constrain the number of neighbors that can be in an area.

Link state routing protocols, like distance vector protocols, are dynamic. They propagate route information across networks. However, they have a number of advantages over distance vector protocols.

Advantages: One of the major advantages of link-state routing is that they calculate the best route for data based on cost rather than distance. The algorithms used to determine cost vary from protocol to protocol, but it is generally based on a link's bandwidth. Thus, the router that the data packet takes to get to its destination is optimized.

Advantages of Distance Vector Routing: Distance vector routing provides a tremendous advantage over static routing. Routers are able to discover the state of the network, and to propagate changes as they occur. The most common, and most ubiquitous of distance vector routing protocols is the Routing Information Protocol, or RIP.

Disadvantages of Distance Vector Routing: There are also some disadvantages to distance vector routing that preclude its use on the <Client> network:

- As distance vector routing protocols periodically transmit the entire routing table to all immediate neighbors, they can add significant traffic. This is particularly problematic on a wireless network with limited bandwidth.
- Distance vector protocols are slow to converge, or adapt to network topology changes. After a change to the network, and before all the routers have converged, there is the probability of routing errors and lost data.
- Distance vector routing protocols base their routing decisions on distance, or the number of "hops" from one network to another. It does not take into consideration the speed or bandwidth of a network path. Therefore, routers may route traffic through paths that are suboptimum.

Link-State Protocols: Link-state routing protocols, such as Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and NetWare Link Services Protocol (NLP), were designed to address the limitations of distance vector routing protocols (slow convergence and unnecessary bandwidth usage). Link-state protocols are more complex than distance vector protocols, and running them adds to the router's overhead. The additional overhead (in the form of memory utilization and bandwidth consumption when link-state protocols first start up) constrains the number of neighbors that a router can support and the number of neighbors that can be in an area. When the network is stable, link-state protocols minimize bandwidth usage by sending updates only when a change occurs. A hello mechanism ascertains reachability of neighbors. When a failure occurs in the network, link-state protocols flood Link-State Advertisements (LSAs) throughout an area. LSAs cause every router within the failed area to recalculate routes. The fact that LSAs need to be flooded throughout the area in failure mode and the fact that all routers recalculate routing tables constrain the number of neighbors that can be in an area.

Link state routing protocols, like distance vector protocols, are dynamic. They propagate route information across networks. However, they have a number of advantages over distance vector protocols.

Advantages: One of the major advantages of link-state routing is that they calculate the best route for data based on cost rather than distance. The algorithms used to determine cost vary from protocol to protocol, but it is generally based on a link's bandwidth. Thus, the router that the data packet takes to get to its destination is optimized.

Disadvantages: Additionally, link state protocols do not transmit their entire topology database across the network on a periodic basis. Once the network has converged, protocol traffic is limited to changes in specific links (link state advertisement packets) and keep-alive or "hello" packets.

Finally, convergence times for link state protocols are generally much shorter than for distance vector protocols. A network based on link-state routing will recognize and adapt to failures and changes much more quickly.

They are generally much more complex than either static routes or distance-vector routing. This translates into higher implementation costs, higher CPU utilization, and greater memory requirements.

Advanced Distance Vector Protocol

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector protocol that has some of the properties of link-state protocols. Enhanced IGRP addresses the limitations of conventional distance vector routing protocols (slow convergence and high bandwidth consumption in a steady state network). When the network is stable, Enhanced IGRP sends updates only when a change in the network occurs. Like link-state protocols, Enhanced IGRP uses a hello mechanism to determine the reachability of neighbors. When a failure occurs in the network, the search for feasible successors can be aggressive in terms of the traffic it generates (updates, queries and replies) to achieve convergence.

Path Vector Protocols

There is really only one Path Vector routing protocol and it is Border Gateway Protocol version 4 (BGP-4). This is the primary routing protocol used on the Internet to share routing updates between Autonomous Systems (AS). An Autonomous System is a network under a single administrative and technical control. AS's are typically defined by the boundaries of a single company or organizational entity. BGP-4 is typically used between Internet Service Providers (ISPs) and between companies and the multiple ISPs they use for upstream Internet connectivity. BGP-4 routers operate in either External BGP (EBGP) or Internal BGP (IBGP) configurations depending on whether the connectivity is between ASs or within ASs respectively. Since <Client> currently default routes toward their Internet points of presence there is little reason for <Client> to use this protocol. Regardless, BGP-4 would not be used within the corporate network and only in the future it would be used in a limited capacity at the Internet edges of the <Client> intranet.

8.2 Routing Information Protocol(RIP)

RIP (RFC1723) is a protocol used by routers to exchange routing information. RIP is a dynamic distance vector routing protocol and was developed for smaller IP based networks. RIP uses UDP port 520 for route updates. RIP calculates the best route based on hop count. Like all distance vector routing protocols, RIP takes some time to converge and it requires less CPU power and RAM.

RIP Packet Format

There are two versions of RIP: Version 1 (RIP-1) is a widely deployed protocol with a number of known limitations. Version 2 (RIP-2) is an enhanced version designed to alleviate the limitations of RIP while being highly compatible with it. It is based on non-authenticated messages. RIP packet consist of nine fields as shown in figure 8.2.

1-octet command field	1-octet version number field	2-octet unused field	2-octet AFI field	2-octet zero field	4-octet IP address field	4-octet zero field	4-octet zero field	4-octet metric field
field	field	field	field	field	field	field	field	field

Figure 8.2 RIP Version1

Figure 8.3 RIP Version2

The different fields in RIP message are

1. Command (request or response)
2. Version number (RIP 1 or 2)
3. Zero (unused; provide backward compatibility)
4. Address-family identifier (AFI) (Specifies the address family used)
5. IP Address (specifies the IP address for the entry)
6. Metric (indicates how many internet work hops (routers) have been passed on a trip).
7. Route tag (provides a method for distinguishing between internal routes (learned by RIP) and external routes learned from other protocols).
8. Subnet mask contains the subnet mask (for the entry zero no subnet mask).

9. Next hop (Indicates the IP address the next hop to which packets for the entry should be forwarded)
10. Hop count metric is the number of hops to the destination. The hop count for a directly connected interface is 1, and each intermediate router increments it by 1 to a maximum of 15, with 16 indicating that no route exists to the destination.
- Both active and passive RIP participants listen to all broadcast messages and update their routing table according to the vector-distance algorithm.

RIP-2 is a draft standard protocol with status as elective. RIP-2 extends RIP-1. It is less powerful than other recent Interior Gateway Protocols such as OSPF. The intention of RIP-2 is to provide a straightforward replacement for RIP-1 which can be used on small to medium-sized networks, can be employed in the presence of variable subnetting. RIP-2 takes advantage of the fact that half of the bytes in a RIP-1 message are reserved (must be zero) and that the original RIP-1 specification was well designed with enhancements in mind, particularly in the use of the version field. One notable area where this is not the case is in the interpretation of the metric field. RIP-1 specifies it as being a value between 0 and 16 stored in a four-byte field. For compatibility, RIP-2 preserves this definition, meaning that it agrees with RIP-1 that 16 is to be interpreted as infinity, and wastes most of this field.

RIP-2 also supports the use of multicasting rather than simple broadcasting. This can reduce the load on hosts which are not listening for RIP-2 messages. This option is configurable for each interface to ensure optimum use of RIP-2 facilities when a router connects mixed RIP-1/RIP-2 subnets to RIP-2-only subnets. Similarly, the use of authentication in mixed environments can be configured to suit local requirements.

8.2.1 RIP Operation

RIP is an implementation of the Distance-Vector protocol. RIP uses the Bellman-Ford algorithm to calculate its routes and network topology. Each router sends a list of distance-vectors each of its neighbours periodically. The metric must be a positive integer. This metric measures the cost to get to the destination. In RIP, this cost describes number of hops.

Table 8.1 Sample RIP Table

Destination	Hop Count	Next Hop	Info
143.5.8.0	8	143.5.0.0	
197.3.2.1	5	172.3.4.5	

When RIP is started, it sends a message to each of its neighbors on well-known UDP port 520 asking for a copy of the neighbor's routing table. This message is a query command set to 1 with an address family of 0 and a metric of 16. The neighboring routers return a copy of their routing tables.

- When RIP is in active mode, it sends all or part of its routing table to all of its neighbor routers by broadcasting and/or by sending it on any point-to-point links to its neighbors. This is done every 30 seconds. The routing table is sent as a reply with command is 2, even though it is unsolicited.
- When RIP discovers a metric has changed, it broadcasts the change to other routers.
 - When RIP receives a reply, the message is validated and the local routing table is updated if necessary.

To improve performance and reliability, RIP specifies that once a router (or host) learns a route from another router, it must keep that route until it learns about a better one (with a strictly lower cost). This prevents routes from oscillating between two or more equal cost paths.

When RIP receives a request, other than one for the entire table, it is returned as the response with the metric for each entry, set to the value from the local routing table. If no route exists in the local table, the metric is set to 16.

RIP routes learned from other routers time out unless they are re-advertised within 180 seconds (6 broadcast cycles). When a router times out, its metric is set to infinity, the invalidation of the route is broadcast to the router's neighbors, and 60 seconds later, the route is deleted from the local routing table.

RIP Update Algorithm

Receive: a response RIP message

1. Increment the hop count for each advertised destination*
2. Repeat for each advertised destination*

If (destination is not in own routing table)

Add the destination to table

Else If (next-hop field is the same)

Replace existing entry with the new advertised one

Else if (advertised hop-count after increment is smaller)

Replace existing entry with the new advertised one.

RIP Timers: The time between each update by default is 30 seconds modified by a small random time to avoid synchronization problems. Time-out occurs if no updates are received. After the last successful update, router wait for this much time before marking the route for deletion. Default timeout is 180s. When a route has been marked for deletion, its metric is set to 16, and after this amount of time it is removed from

Taking down a RIP enabled network.

memory. Default time for this process is 120s. RIP sends its updates over UDP protocol. RIP listens to updates on port 520.

8.2.2 RIP Vulnerabilities and Attacks

This section describes some of the weaknesses of RIP and attacks due to it.

RIP Vulnerabilities

- RIPv1 uses broadcast whereas RIPv2 uses multicast. In contrast to RIPv1, RIPv2 supports subnet masks and a simple authentication mechanism. Routing tables can be modified leniently by an attacker. As a result, the target system may be unable to communicate with regular endpoints. Complex 'man-in-the-middle' attacks could also be crafted.
- The maximum cost allowed in RIP is 16 which mean that the network is unreachable. Thus RIP is inadequate for large networks that is, those in which legitimate hop counts approach 16.
- RIP does not support variable length subnet masks. There is no facility in a RIP message to specify a subnet mask associated with the IP address.
- RIP has no facilities to ensure that routing table updates come from authorized routers. It is an unsecure protocol.
- RIP only uses fixed metrics to compare alternative routes. It is not appropriate for situations where routes need to be chosen based on real-time parameters such as measured delay, reliability, or load.
- The protocol depends upon counting to infinity to resolve certain unusual situations. The resolution of a loop would require either much time or much bandwidth. As the size of the routing domain grows, the instability of the vector-distance algorithm in the face of changing topology becomes apparent. RIP specifies mechanisms to minimize the problems with counting to infinity which allows RIP to be used for larger routing domains, but eventually RIP will be unable to cope. There is no fixed upper limit, but the practical maximum depends upon the frequency of changes to the topology, the details of the network topology itself, and what is deemed as an acceptable maximum time for the routing topology to stabilize.
- The longest number of hops supported by RIP is 15. Routes with a metric value larger than 15 are discarded. Furthermore, routes typically expire after 180 seconds. Therefore, active routers advertise their routes periodically, such as every 30 seconds, to prevent them from being automatically deleted from route tables.
- It is UDP-based (typically using port 520) and stateless. It does not use internal sequence numbers.

Attacks on RIP

- It is trivially easy to spoof RIP. There are no sequence numbers to predict, sessions to hijack, authentication passwords to sniff, trust relationships to spoof, or crypto keys to crack. By spoofing RIP, it is possible to manipulate route tables on routers and hosts.
- It is also easy to identify (active) RIP-enabled routers and download their route tables by sending them a request message. A single router may be requested via UDP unicast, or all routers on a network may be requested via a single UDP broadcast datagram.

- A router makes routing decision of an IP packet based on a data structure called routing table, which keeps the status of each path linked to that router. If RIP is used, a router will periodically generate LSU (Link State Updates) that describe the latest status of the links to the router and disseminate those updates to the other neighboring routers. Then, based on LSU received, routers update their own routing tables and cooperate in forwarding the IP packets from source to destination.

Potential threats to the routing infrastructures come mainly from the spoofing intrusions and some of them can lead to the results of denial of service. A faulty router can modify the packets passing through it or discard the packets at all. This may bring some networks or hosts unreachable. Furthermore, a malicious or compromised router can send bogus routing control packets like LSU, to other routers, which may in turn cause all the packets switch to itself and it can then eavesdrop the content within the packets. Another scenario is that a router sends bogus LSU's that makes other routers think that some reachable hosts are unreachable.

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 gateways 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. Once this is done, protocols that rely on address-based authentication are effectively compromised. This attack can 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 possible alteration.

They are then resent, using IP source address routing, to the intended destination. An outsider may thus capture passwords and other sensitive data.

8.2.3 RIP Defense Mechanisms

- RIP to be more skeptical about the routes it accepts. In most environments, there is no good reason to accept new routes to your own local networks. A router that makes this check can easily detect intrusion attempts. Unfortunately, some implementations rely on hearing their own broadcasts to retain their knowledge of directly-attached networks. The idea, presumably, is that they can use other networks to route around local outages. While fault-tolerance is in general a good idea, the actual utility of this technique is low in many environments compared with the risks.
- It would be useful to be able to authenticate RIP packets; in the absence of inexpensive public-key signature schemes, this is difficult for a broadcast protocol. Even if it were done, its utility is limited; a receiver can only authenticate the immediate sender, which in turn may have been deceived by gateways further upstream. Even if the local routers don't implement defense mechanisms, RIP attacks carry another risk: the bogus routing entries are visible over a wide area. Any router (as opposed to host) that receives such data will rebroadcast it; a suspicious administrator almost anywhere on the local collection of networks could notice the anomaly. Good log generation would help, but it is hard to distinguish a genuine intrusion from the routing instability that can accompany a gateway crash.
- Whenever possible, RIP should be used with MD5 authentication enabled. This approach transmits a one-way cryptographic hash with each RIP message. The hash is generated by appending an authentication key (up to 16 characters in length) to the message prior to hashing with the MD5 algorithm.
- Other defense techniques which can be implemented are
 - Route monitoring and looking glasses
 - Real-time monitoring of route path changes
 - Traffic accounting

8.3 Open Shortest Path First (OSPF)

OSPF is a link state Interior Gateway Protocol (IGP) developed for use in Internet Protocol (IP)-based internetworks. The well known Dijkstra's algorithm is used to calculate the shortest path tree. It uses cost as its routing metric. A link state database is constructed of the network topology which is identical on all routers in the area. As an IGP, OSPF distributes routing information between routers belonging to a single autonomous system (AS). An AS is a group of routers exchanging routing information

via a common routing protocol. The OSPF protocol is based on shortest-path-first, or link-state, technology.

8.3.1 OSPF Operation

- Open Shortest Path First is a true link state protocol developed as an open standard for routing IP across large multi-vendor networks. A link state protocol will send link state advertisements to all connected neighbors of the same area to communicate route information.
- Each OSPF enabled router, when started, will send hello packets to all directly connected OSPF routers.
 - The hello packets contain information, such as router timers, router ID and subnet mask.
 - If the routers agree on the information they become OSPF neighbors.
 - Once routers become neighbors they establish adjacencies by exchanging link state databases.
 - Routers on point-to-point and point-to-multipoint links automatically establish adjacencies.
 - Routers with OSPF interfaces configured as broadcast (Ethernet) and NBMA (Frame Relay) will use a designated router that establishes those adjacencies.
- OSPF defines three forms of authentication:

Null Authentication. LSAs are not authenticated and therefore can be easily spoofed. Only a simple checksum is generated to detect unintentional data corruption, but this can be easily defeated or spoofed.

Simple Password. A shared password (8 bytes long) is embedded in the clear in LSA messages. This method is trivial to defeat by sniffing the network and intercepting passwords or altering LSAs in transit.

Cryptographic Authentication. Similar to MD5 authentication in RIP v2, a shared authentication key is hashed with the LSA (link state advertisement) message to produce an cryptographically secure MD5 hash. This hash is then transmitted with the LSA and validated by all receiving OSPF processes using the same authentication key. The key itself is never transmitted over the network. Furthermore, a monotonically increasing sequence number protects against replay attacks, although there does exist a brief window of opportunity for replay attacks until the sequence actually increments.

8.3.2 OSPF Vulnerabilities and Attacks

This section describes various vulnerabilities and attacks on OSPF

Vulnerabilities in OSPF

- OSPF only provides authentication, not confidentiality. Therefore, hackers can sniff the network for LSA messages in order to map out the network topology. This is extremely useful information for reconnaissance.

- Even though OSPF is designed and deployed to be used as an intradomain routing protocol, in most scenarios and situations an OSPF router will still accept unicast IP packets directly addressed to itself. On physical point-to-point networks, the IP destination is always set to the address AllOSPFRoutes. On all other network types (including virtual links), the majority of OSPF packets are sent as unicasts, i.e., sent directly to the other end of the adjacency. This opens the door to attacks that may be originating from outside the OSPF domain. Timing the stream of different packets needed for a given attack poses a certain degree of difficulty if executed from a remote AS, but it may not be enough to stop a skilled and motivated attacker.

- A host-based router usually runs both traditional operating system (OS) and some routing software, which give it the capability to forward packets. The difference between these two environments from security perspective is critical: the former environment is usually exposed to more threats because of the following reasons:
 - Since a host-based router runs on traditional OS, all the vulnerabilities of that particular OS can be exploited as the entry door to gain privilege access, while the low-level architecture of commercial router is less well known, therefore less vulnerable

- A host tends to provide more network services to the outside since people are using it for multiple purposes, these network services could be the weak points of security. Implementation could be another problem.

- Configuration problems are probably one of the most obvious and common mistakes. A poorly configured router often opens the door for intruders exploiting its vulnerabilities.

Attacks on OSPF

- A host-based or commercial router can be compromised. Since the router is previously a legitimate one, it holds all the information from the past and could be exploited for further misuse.
- An intruding device, which is assumed to have certain tapping points physical access must have the capability to join into routing process, which requires some basic function such as HELLO protocol, database exchange protocol, and certain

state transition maintenance. Experience shows that without really participating into the routing domain, attacking result will hardly to be fruitful.

A host which does not join the routing domain is invisible from the routing context. This type of attacks are rare, but under certain conditions, it can happen and hard which are particularly vulnerable and therefore these fields are the targets of usual attacks. However, with Keyed-MDS protection, most of these vulnerabilities could be eliminated except the age field.

- Periodic Injection: A router will never release or update its LSAs faster than once every MinLSInterval (5 seconds). This allows for almost permanent changes in the routing domain, if an attacker is flooding the OSPF domain with malicious LSAs at a rate higher than one every MinLSInterval. The router owner of the LSA may never fight back and it will collaborate in the flooding of malicious routing information on its behalf. The flooding happens because the malicious LSA is considered newer than the copy already present in the legitimate owner's Link State. After the malicious LSA has been already flooded a simple test reveals that the LSA contained erroneous information.

8.3.3 OSPF Defense Mechanisms

Following are some of the defence mechanisms to protect the OSPF from attacks

- Use loopbacks or manually configured router ID's; don't let OSPF choose the IP on a physical interface. It makes troubleshooting much more straightforward.
- Recommendations for securing the router from compromise follow with standard practices: Such as strong authentication and access controls and controlling physical access to the router.
- The OSPF attack requires many things, and is only successful if the attacker can send forged OSPF LSAs to your routers. Removing an attacker's capability to send OSPF updates of any kind reduces the impact that attack has on your network.
- The simple packet filters that are placed on "user ports" allow implementers to quickly and easily reduce the attack surface of their networks and spend more time on strategic initiatives.
- Implementation of MDS authentication for OSPF packets.

8.4 Border Gateway Protocols (BGP)

The Border Gateway Protocol (BGP) is the de facto interdomain routing protocol of the Internet. BGP versions enables you to create an IP network free of routing loops among different autonomous systems. An AS is a set of routers under the same

administrative control. The process of routing within an AS's called intradomain routing, and routing between AS's is called interdomain routing. BGP is called a path-vector protocol because BGP carries a sequence of AS's numbers that indicate the path taken to a remote network. This information is stored so that routing loops can be avoided. BGP uses Transmission Control Protocol (TCP) as its Layer 4 protocol (TCP port number 179). This allows TCP to ensure that updates are sent reliably, leaving the routing protocol to concentrate on gathering information about remote networks and ensuring a loop-free topology.

8.4.1 BGP Operation

A router running the BGP protocol is known as a BGP speaker. BGP speakers communicate across TCP and become peers or neighbors. TCP is a reliable connection-oriented protocol and by employing it, BGP does not need to provide error correction at the transport layer. Each pair of BGP neighbours maintains a session, over which information is communicated. BGP peers are often directly connected at the IP layer; that is, there are no intermediate nodes between them. This is not necessary for operation, as peers can form a multi-hop session, where an intermediate router that does not run BGP passes protocol messages to the peer. This is a less commonly seen configuration. BGP peers within the same AS (internal peers) communicate via internal BGP (IBGP). External BGP (EBGP) is used between speakers in different ASes (external peers). The routers that communicate using EBGP, which are connected to routers in different ASes, are called border routers. The architecture is shown in figure 8.4.

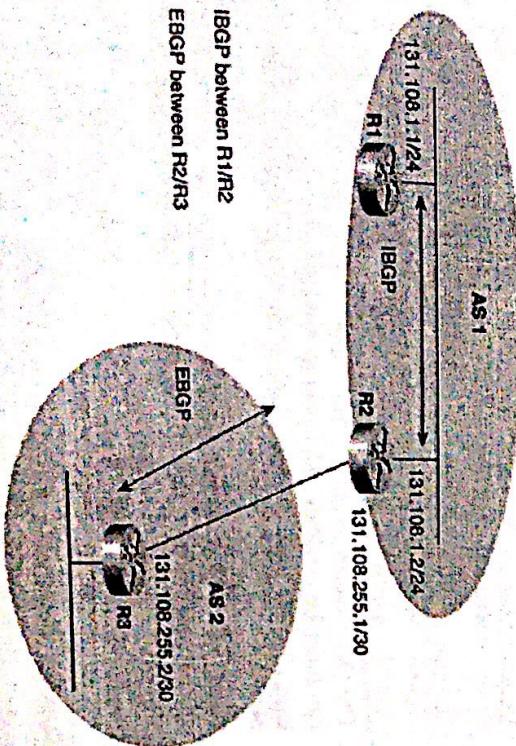


Figure 8.4 shows that the autonomous systems 1 (AS1) is connected to AS2 through router R2 in AS1 to router R3 in AS2.

BGP Messages

BGP version 4 uses the following four message types to ensure that peers are active and updates are sent:

- **Open messages** - These messages are used when establishing BGP peers. A BGP speaker sends an open message to a BGP neighbor to indicate that connections are still active or established.
- **Update messages** - Any change that occurs, such as a loss of network availability, results in an update message.
- **Notification** - These messages are used only to notify BGP peers of receiving errors.

The following statements characterize the primary correct operation features of BGP.

- Each UPDATE received by a BGP speaker from a peer was sent by the indicated peer contains routing information. The UPDATE was intended for receipt by the peer that received it.
- The peer that sent the UPDATE was authorized to act on behalf of its AS to advertise the routing information contained within the UPDATE to BGP peers in the recipient AS.
- The owner of an address space corresponding to a reachable prefix advertised in an UPDATE was authorized by its parent organization to own that address space.
- The first AS in the route was authorized, by the owners of the address space corresponding to the set of reachable prefixes, to advertise those prefixes.
- If the UPDATE indicates a withdrawn route, then the peer withdrawing the route was a legitimate advertiser for that route, prior to its withdrawal.
- The peer that sent the UPDATE correctly applied the BGP rules and its AS's routing policies in modifying, storing and distributing the UPDATE, in selecting the route, and in deriving forwarding information from it.
- The BGP speaker that received the UPDATE correctly applied the BGP rules and its AS's routing policies in determining whether to accept the UPDATE.

Figure 8.4 BGP Architecture

8.4.2 BGP Vulnerabilities and Attacks

Here we explain some inherent vulnerabilities underlying in BGP design and operation and describe attacks on BGP:

- **Attacks Against Confidentiality:** Two routers communicating over a channel may be assumed to have a contract of confidentiality; that is, they may expect that messages they send between each other will not be seen by any other parties. However, the channel over which they communicate may have been disrupted by a third party. A and B's messages between each other could be possibly observed by the attacker, C. C could be eavesdropping on the message stream between A and B, in an attempt to learn policy and routing information from the two parties.
- **Attacks against Message Integrity:** An additional risk occurs if C, the attacker, does not merely passively listen to updates, but becomes an active, unseen part of the communications channel. C can become a man in the middle between A and B and tamper with BGP messages. One method of tampering is message insertion, where C inserts forged BGP messages into the message stream. This can have the effect of introducing incorrect routing information. It can also force the connection between A and B to shut down, as erroneous BGP messages will abort the session. C can also affect the message stream through message deletion, where he selectively removes messages. BGP relies on keep-alive messages being periodically sent, and if they are not received, the connection will be closed. Another method of tampering is message modification, where C intercepts a message in flight and alters its contents before forwarding it. Finally, C can launch a replay attack, where he records messages between A and B and resends them to the original recipient. This approach can be used to confuse the routing protocols by re-asserting withdrawn routes or withdrawing valid ones. When sent in bulk, these messages can overwhelm the victim's routers, forcing them to crash and go offline.
- **Session Termination:** A consequence of modifying messages is the ability to terminate a BGP session. The following example demonstrates how an attacker takes advantage of the protocol's state machine model. Events received by BGP speakers cause their internal state to change, causing them to expect certain messages and react to them in a different manner. For example, if A and B are setting up a BGP session, A sends B an OPEN message and transitions into the OpenSent state. When B receives this message, he responds with an OPEN message. Upon reception of the message, A changes to the OpenConfirm state. When the session has been completely set up, both A and B are in the Established state, the state that BGP regularly operates in. If the attacker C inserts an OPEN message at this point, the session between A and B will be closed, because it violates the expected input. Another way to close the session is by forging a NOTIFICATION message, which indicates an error has occurred. When either A or B receives this message, they will terminate the BGP session. The BGP state machine introduces

several vulnerabilities. For example, the state machines require that the protocol be reset following any fault. As detailed in the following sections, such features can be exploited to decrease the stability or availability of the Internet.

Active or Passive wiretapping: Communication between BGP peers can be subjected to active or passive wiretapping. The BGP software, configuration information, or routing databases of a router may be modified or replaced via unauthorized access to a router, or to a server or management workstation from which router software is downloaded. These latter attacks transform routers into hostile insiders.

Fraudulent Origin Attacks: An autonomous system can advertise incorrect information through BGP UPDATE messages passed to routers in neighboring ASes. A malicious AS can advertise a prefix originated from another AS and claim that it is the originator, a process known as prefix hijacking. Neighboring ASes receiving this announcement will believe that the malicious AS is the prefix owner and route packets to it. The real originator of the AS will not receive the traffic that is supposed to be bound for it. If the malicious AS chooses to drop all the packets destined to the hijacked addresses, the effect is called a black hole. This attack makes the hijacked addresses unavailable. If the malicious AS chooses to forge all addresses in a block using hosts and devices within its control, the effect may be much more severe. Unless properly authenticated using some other security service, one can impersonate all of the services and resources of the hijacked address space. The malicious AS can then analyze the traffic it receives, possibly retrieving sensitive information such as passwords. Another method that a malicious AS can use to spread misinformation is to tamper with the path attributes of an UPDATE message. BGP is a path vector protocol, and routing to destinations is performed based by sending packets through the series of ASes denoted in the path string. An AS can modify the path it receives from other ASes by inserting or deleting ASes from the path vector, or changing the order of the ASes, in order to create routing delays or to allow the malicious AS to alter network traffic patterns. By altering attributes in an UPDATE message, such as the multiexit discriminator used to suggest a preferred route into an AS to an external AS or the community attribute used to group routes with common routing policies, traffic engineering and routing policy can be undermined. Another potent attack alters the paths to transit a malicious AS. In addition to correctly transiting the data, the malicious AS eavesdrops on application traffic of the originating AS. Such data, if not properly secured, could expose an enormous amount of information about the activities of the victim.

Denial of Service: Many of the attacks above can be considered denial of service attacks. Black holing a route, for example, causes denial of service for that prefix. Attacks and subverting the path can also lead to service delays or denials. For example, a sufficiently long route can cause the time-to-live (TTL) of a packet to be exceeded,

In the two peer case, denial of service has also been considered by a remote attacker using erroneous or false BGP messages to shut down a connection. Since BGP uses TCP as a transport protocol, it is subject to TCP attacks as well. For example, the TCP RST attack can cause a remote attacker to be able to reset a TCP connection between two BGP peers. Additionally, TCP is vulnerable to the SYN flood attack, where the three-way handshaking process is initiated, but never completed (the attacker never acknowledges the open handshake). The victim will run out of connection state memory and either be unable to perform any individual routers, but become even more consequential when the distributed TCP transactions or crash altogether. These attacks are harmful enough to the case is considered. If a router goes offline, then when it comes back online, its routing table will need to be recreated, and it re-announces all of the prefixes it is originating, a process known as a table reset. The neighboring routers dump their BGP tables to the peer that has just come online so that it has full data for making its routing decisions. Sifting through this information places a considerable computational burden on the router, and delays processing of normal traffic. If the router is continually knocked offline, the routes it advertises will disappear and reappear in peer routing tables. This is called route flapping and is detrimental to all routers, as extra computation and reconfiguration of routes becomes necessary if this happens often. In order to lower the burden, unstable routes are often penalized through a process called route dampening. Neighboring routers will ignore advertisements from the router for an increasing amount of time, depending on how often the route flapping occurs.

Protecting the TCP connection is an easy way to mitigate attacks on BGP sessions. A popular and inexpensive countermeasure against attacks on TCP is the use of message authentication codes (MACs). Recent enhancements to BGP suggest the use of a TCP extension that carries an MD5 digest based MAC. An MD5 keyed message authentication code (MAC) is included in each packet passing between the BGP speakers. The authenticity of the packet data is ensured because the digest could have only been generated by someone who knows the secret key. A number of variants consider hashing all or part of the TCP and BGP data message using one or more keys, which addresses many of the problems of spoofing and hijacking inherent to TCP. Suppression of these routes can be a highly effective denial of service attack.

8.4.3 BGP Defense Mechanisms

Improved physical and procedural security for network management facilities, and routers, and cryptographic security for BGP traffic between routers would help reduce some of these vulnerabilities. However, physical and procedural security is expensive and imperfect, and these countermeasures would not protect the Internet against accidental or malicious misconfiguration by operators, nor against attacks that mimic

such errors. Misconfiguration of this sort has been a source of Internet outages in the past and seems likely to persist. Some of the defense mechanisms are described below.

- **IPSec:** Many recent proposals have suggested the use of IPsec as a mechanism for securing the BGP session. IPsec is not specific to BGP, but is a suite of protocols that provide security at the network layer. These protocols define methods for encrypting and authenticating IP headers and payload, and provide key management services for the maintenance of long term sessions. The IPsec Internet Security Association and Key Management Protocol (ISAKMP) defines a framework for key management and negotiating security services while the Internet Key Exchange (IKE) protocol.
- **Generalized TTL Security Mechanism:** Originally called the "BGP TTL Security Hack", the Generalized TTL Security Mechanism (GTSM) provides a method for protecting peers from remote attacks. This approach builds on the premise that in the vast majority of BGP peering sessions, the two peers are adjacent to each other. The time-to-live, or TTL, attribute in an IP packet is set to a value that is decremented at every hop. For example, if a packet traverses four hops from source to destination, the TTL decrements by four. Routers using GTSM set the TTL of an IP packet to its maximum value of 255. When a BGP peer receives a packet, it checks the TTL and if this value is lower than 254 (decremented by one), the packet is flagged or discarded outright. This prevents remote attacks which come from more than one hop away, as those packets will have TTls lower than the threshold value of 254.
- **Defensive routing policies:** Defensive routing policies are used to filter bad and potentially malicious announcements, and to manipulate potentially dangerous attributes of received routes. BGP speakers commonly filter ingress and egress routes based on route policies. The policies filter prefixes that are documented special use addresses (DSUs) prefixes (e.g., loopback addresses), and bogons (advertisements of address blocks and AS numbers with no matching allocation data), also known as martians. The CIDR report keeps an updated list of bogons [CIDR 2004] which many organizations use to filter announcements. Filtering is also used to remove conflicting announcements. For example, announcements containing private Ases or from unexpected downstream ASes are automatically dropped by some BGP speakers. A policy of careful ingress and egress filtering greatly aids in maintaining security for both the local AS and its neighbors, and is widely held to be the most widely deployed and effective BGP security measure. Filtering is not a replacement for a strong security architecture. The filtering rules are fundamentally limited by the heuristics it represents, and can only remove announcements which are overtly bad.
- **Secure BGP (S-BGP):** S-BGP was the first comprehensive routing security solution targeted specifically to BGP. The S-BGP protocol and its associated architecture are currently under consideration for standardization by the Internet Engineering Task

- Force (IETF), the organization that provides Internet standards. Implementations of S-BGP exist, and its authors are actively experimenting with its use in operational networks. A primary element of S-BGP is its use of public key certificates to communicate authentication data. Public key certificates bind cryptographic information to an identity such as an organization. Anyone in possession of the public key certificate can validate information digitally signed with the private key associated with the public key. As the name would imply, the public key is widely distributed, and the private key is kept private [Rivest et al. 1978]. A Public key infrastructure (PKI) is a system for issuing, authenticating and distributing certificates. S-BGP implements security by validating the data passed between ASes using public key certificates.
- Esec is used to provide data and partial sequence integrity, and to enable BGP routers to authenticate each other for exchanges of BGP control traffic.
- Public Key Infrastructure (PKI) is used to support the authentication of AS's identity, and BGP router's identity.
- BGP transitive path attribute is employed to carry digital signatures covering the routing information in a BGP UPDATE message.

8.5 Exterior Gateway Protocol (EGP)

EGP was developed by Internet pioneers Bolt, Beranek and Newman (BBN) in the early 1980s. It was first formally described in an Internet standard in RFC 827. EGP is now considered obsolete, having been replaced by the BGP. However it is an important part of the history of TCP/IP routing, so it is worth examining briefly.

EGP is one of the first exterior gateway protocols, used to exchange route information between autonomous systems. Two routers first establish adjacency between each other by exchanging Hello and I-H-U (I Head You) messages. Once adjacency is determined, then the two routers are considered "neighbors" and can exchange route information. EGP is on top of IP. It is stateful and therefore includes a sequence number. However, it does not support authentication, so packets can be spoofed. EGP has been mostly replaced by BGP v4 for routing over the Internet.

8.5.1 EGP Operation

The Exterior Gateway Protocol (EGP) is intended for communications between the core gateways and so-called exterior gateways. An exterior gateway, after going through a neighbor acquisition protocol, is periodically polled by the core; it responds with information about the networks it serves. These networks must all be part of its autonomous system. Similarly, the gateway periodically requests routing information from the core gateway. Data is not normally sent except in response to a poll; furthermore, since each poll carries a sequence number that must be echoed by the

response, it is rather difficult for an intruder to inject a false route update. Exterior gateways are allowed to send exactly one spontaneous update between any two polls; this, too, must carry the sequence number of the last poll received. It is thus comparatively difficult to interfere in an on-going EGP conversation.

8.5.2 EGP Vulnerabilities and Attacks

- The fundamental problem with EGP is its inability to detect routing loops. Because there is an upper boundary on the distance EGP uses (255), you might be tempted to say that counting to infinity is at least a rudimentary loop-detection mechanism. It is, but the high limit combined with the typical Poll interval makes counting to infinity useless. Given a default Poll interval of 180 seconds, EGP peers could take almost 13 hours to count to infinity.
- One possible attack would be to impersonate a second exterior gateway for the same autonomous system. This may not succeed, as the core gateways could be equipped with a list of legitimate gateways to each autonomous system. Such checks are not currently done, however. Even if they were, they could be authenticated only by source IP address.
- A more powerful attack would be to claim reachability for some network where the real gateway is down. That is, if gateway G normally handles traffic for network N, and G is down, gateway G could advertise a route to that network. This would allow password capture by assorted mechanisms. The main defense against this attack is topological (and quite restrictive): exterior gateways must be on the same network as the core; thus, the intruder would need to subvert not just any host, but an existing gateway or host that is directly on the main net.
- A sequence number attack, similar to those used against TCP, might be attempted; the difficulty here is in predicting what numbers the core gateway is using. In TCP, one can establish arbitrary connections to probe for information; in EGP, only a few hosts may speak to the core. (More accurately, the core could only speak to a few particular hosts, though as noted such checks are not currently implemented). It may thus be hard to get the raw data needed for such an attack.

8.5.3 EGP Defense Mechanisms

- Improved physical and procedural security for network management facilities, and routers, and cryptographic security for EGP traffic between routers would help reduce some of these vulnerabilities. However, physical and procedural security is expensive and imperfect, and these countermeasures would not protect the Internet against accidental or malicious misconfiguration by operators, nor against attacks that mimic such errors.
- Routers also are susceptible to resource exhaustion attacks based on delivery of large quantities of management traffic, EGP or otherwise. This vulnerability

Review Questions

arises because these devices are designed with the not unreasonable model that management traffic is a very tiny percentage of all the traffic that arrives at a router. Router interfaces can deliver traffic to the management processor at very high rates, because they are designed to accommodate subscriber traffic flows. Solutions to this problem need to be generic, to accommodate all types of router management traffic.

8.6 Conclusion

Routing forms the backbone of communication network. This study of routing protocols will help in decision making for the routing security policy. In this chapter we explore various security flaws in routing protocols such as RIP, OSPF, BGP, EGP. The Attacks and countermeasures for these attacks are also discussed.

- Q 1. Explain routing. Define types of routing algorithms.
- Q 2. What is distance vector routing.
- Q 3. Explain working of RIP in detail.
- Q 4. Explain difference between RIP V1 and RIPV2.
- Q 5. Give message format of RIP.
- Q 6. Explain OSPF. Give features of OSPF.
- Q 7. Describe the different OSPF packet types.
- Q 8. Explain BGP. What are different types of BGP messages.
- Q 9. Explain BGP operation in detail.
- Q 10. Explain RIP vulnerabilities and attacks.
- Q 11. Explain defense mechanisms employed for routing attacks.
- Q 12. What is periodic injection in OSPF. How the problem is resolved?
- Q 13. Explain following
 - 1. BGP fraudulent origin attacks
 - 2. BGP Session termination attacks
- Q 14. Compare the routing protocols RIPv1, RIPv2, OSPF, BGP and EGP.
- Q 15. Explain the routing intrusion security measures.

Chapter 10

Network Intrusion Prevention Systems

Present e-business organizations and networks follow a layered security and protection approach to ensure security at different levels. Two significant requirements for building intrusion prevention systems are broad attack detection coverage and efficiency in operation, i.e. an intrusion prevention system must detect different type of attacks as early as possible and must operate efficiently in high speed networks. In this chapter, layered framework to build a network intrusion prevention system is explained which can detect a wide variety of attacks reliably and efficiently as compared to the traditional network intrusion detection technologies. This chapter presents intrusion detection and protection system software architecture and advantages of layered approach over traditional security technologies.

10.1 Introduction

Present networks are prone to a number of attacks, a large number of which are previously known. However, the number of previously unseen attacks is also on rise. The Internet architecture is designed in layered fashion for the ease of implementation and scalability. Given this traditional layered architecture of communication network, only a single system for defense is expected to detect attacks and prevent them. A variety of tools such as network surveillance, penetration testing, perimeter access control, firewalls, network, host and application intrusion detection systems, data encryption and others are used for the purpose. Signature based systems using pattern matching approaches can be used effectively and efficiently to detect previously known attacks in high speed networks. As a result, anomaly and hybrid systems are used to detect previously unseen attacks and have been proven to be more reliable in detecting novel attacks when compared with the signature based systems. A common practice to build anomaly and hybrid intrusion detection systems is to train a single system with labeled data to build a classifier which can then be used to detect attacks from a previously unseen test set. At times, when labeled data is not available, clustering based systems can be used to distinguish between legitimate and malicious packets. However, a significant disadvantage of such systems is that they result in a large number of false

alarms. The attack detection coverage of the system is further affected when a single system is trained to detect different type of attacks. To maximize attack detection, various systems employ both the signature based and the anomaly based systems together. This is because, a single anomaly detector is trained which is expected to accurately detect a variety of attacks and perform efficiently. Also the signature based systems suffer from signature update. The new signatures are required to be manually added to the system. Signature generation for the new attacks is also a challenge in this process. Thus, for a network intrusion detection system monitoring the incoming and outgoing network traffic and ensuring confidentiality, integrity and availability via a single system may not be possible due to several reasons including the complexity and the diverse type of attacks at the network level. Ensuring high speed of operation further limits the deployment, particularly, of anomaly and hybrid network intrusion detection systems.

Layered framework tries to achieve three main security objectives by checking confidentiality, availability and integrity. System implements attack occurrence check at each layer and predicts occurrence of attack by applying data mining algorithm on network traffic data. The availability objective can be achieved by not flooding the recipient with connections. As connection establishment is done at transport layer, availability attacks can be detected at Transport Layer. The major availability attack is denial-of-service. Connection flooding or SYN flooding may cause denial-of-service, as there are other possible reasons also. If some network control mechanism is applied at transport layer then denial of service can be controlled. Confidentiality is required to be checked during transmission at every router before forwarding the message. Spoofing or session hijacking attacks are affecting the confidentiality of the message as receiver is getting the data from unauthorized person. Usually these attacks take place when a legitimate user sends some information to the recipient. But attacker in between captures the packet and see all the information including source, destination, data part etc. At data link layer possibility of ARP attacks is more. To control these attacks use of network monitoring tool and static ARP cache table is required. Implementation of network monitoring, capture and analysis can be done at link layer. These precautionary measures will be implemented at individual layer. Also the information of attacks which are detected at any of the layer are received by data mining module and then passed on to the recommendation engine for action.

10.2 IPS Implementation Challenges

Before designing Intrusion Prevention System Model we need to analyze different issues in the implementation of IPS. We discuss some of the IPS challenges.

- Availability of Audit Data: The main goal of our system it should be application independent and can be used to detect intrusions in any protocol of TCP/IP. System must be trained before the system can be deployed online to detect

attacks. This requires training data which containing wide range of attacks along with normal data. To obtain such data may be difficult. However, training data can be made available using the available data sets or by directly collecting the real time data. The available standard dataset for intrusion detection such as KDD, DARPA can only be used for known attack detection and training phase. To make our system more strong router logs and security protocol sessions can be used in testing phase. The standard dataset can be used for training the intrusion detection system.

- Training data and Test data distribution: The standard large dataset which can be used for training and learning phase of intrusion detection system provides wide variety of attacks and normal instances. The difficulty is that the distribution of attack instances is not uniform in any available dataset. Some intrusion instances dominate the other intrusions. This will lead to incorrect machine learning output as the dominant features of dataset may affect the results. The training and test data required to be normalized and preprocessed before directly applying to the system. This process will be carried out at the initialization step of Intrusion Prevention System.

- Packet capture and processing Speed: As todays network are fast and speed on Internet have changed the paradigm of communication. The fast packet flows have raised a new challenge to the security systems of processing the packets with high speed without dropping them. Increasing the processing speed of Intrusion protection system is one of the major implementation challenges.

- Application deployment: We wish to propose a framework which is generic and can be deployed for a variety of applications and should be easily extended and deployed in the Service Oriented Architecture.

- Module Interfacing: IPS architecture handles protocol anomaly detection for basic protocols, routing protocols and security protocols. These modules apply the intrusion detections separately. Interfacing these modules to build an integrated system is one of main challenge. Correlation among the various protocols and their functionality exists. The challenge is to identify such correlations and integrate them.

10.3 Layered Approach for Intrusion Detection

Intrusion Prevention system consist of mainly four components packet capturing and preprocessing, Intrusion detection subsystem, Analysis Engine and recommendation system. These modules are organized in layered manner in such a way that the purpose of intrusion detection will be resolved at earliest. The layered approach for intrusion detection is shown in Figure 10.1

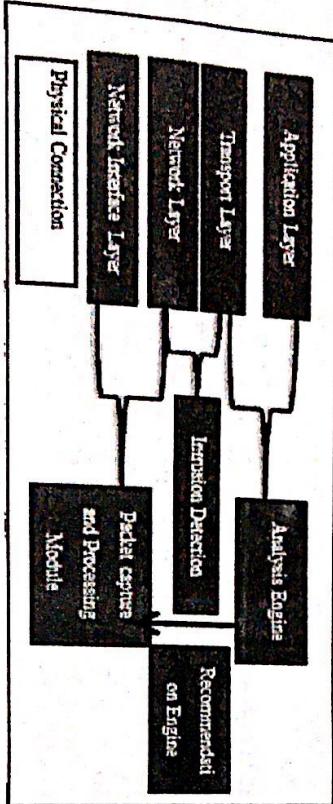
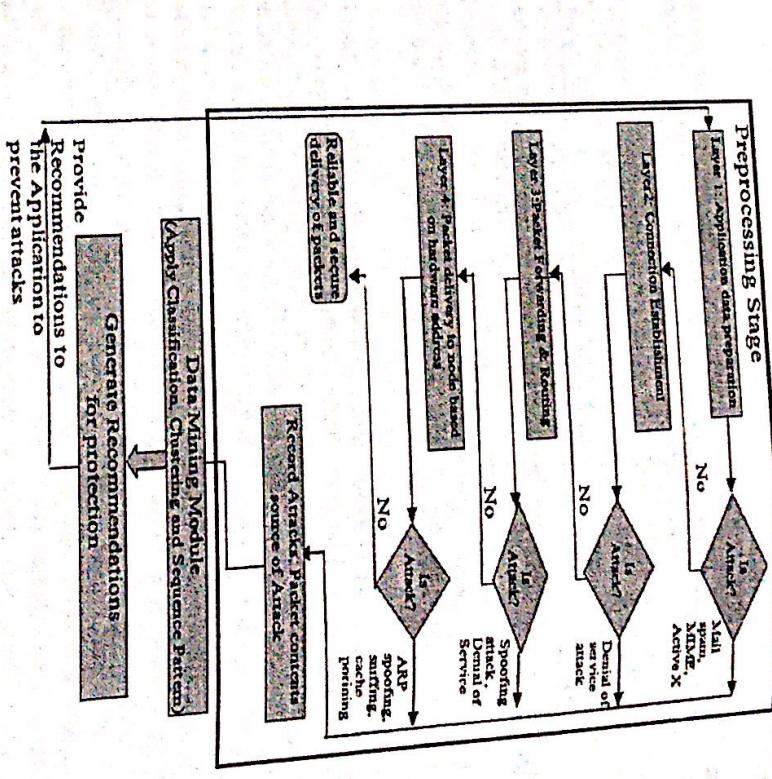


Figure 10.1 Layered Architecture of IPS

Our layered-based intrusion detection model gets its motivation from TCP/IP model, where number of protocols are assigned different task at different level. Every layer in layered intrusion detection system framework is trained separately and then deployed sequentially. We define four layers that correspond to the four attack groups mentioned in the dataset. They are interface layer, network layer, transport layer and application layer. Each layer is separately trained with a set of significant features. The layers act as filters that block any anomalous connection, thereby eliminating the need of further processing at subsequent layers which provides quick response to intrusion. The effect of such a sequence of layers is that the anomalous events are identified and blocked as soon as they are detected. Simple rule matching algorithm is applied for the purpose.

The system is loaded with intrusion signatures for well-known vulnerabilities of the protocols. If intrusion is found, system generates the alert for system administrator and traffic is blocked. Otherwise the packet is further processed for unknown attack detection. The analysis engine will generate the signatures for new attacks so that the system remains updated for all types of attacks.

Figure 10.2 Preprocessing Stage of IPS



As shown in Figure 10.2 we propose that intrusion protection system have three main modules namely preprocessing, data mining and recommendation. Preprocessing module gathers information, process it, cleanses it and stores it in structured format. Updating the data is also role of preprocessing module. Data mining module applies mining algorithm on data produced by preprocessing module. The mining results are used by recommendation module for decision making and for suggesting action to the application. Results are stored in the database for use by applications while preparing their data. The preprocessing modules have complex structure.

To provide evidence of our system development approach consider the following attack scenario. Each attacks scenario consists of following steps:

1. Reconnaissance: Information gathering in networks either in passive or active mode.
2. Identifying vulnerability and gathering information related to exploit.
3. Accessing the target identification information and compromising system.
4. Maintaining sessions to carry out more severe attacks.
5. Exploiting the various applications to cover the attack.

Reconnaissance is the first and most important step in an attack execution. It can be carried out in passive and active mode to collect information such as Source Addresses, Ports, Type of Network, and Type of protocols, Topology, Operating Systems and many more. Prior to perform exploit, attacker need information of vulnerabilities and flaws in the existing system. These flaws can open the door to attacker for exploits. Using reconnaissance and vulnerabilities attacker can gain access to the target machine and can compromise it. The various applications such as Email, Telnet, DNS are used so that Trojans can be inserted in the system.

From the above attacks scenario we can observe that the attacks are not directly executed but it is a step-by-step process. One attack requires involvement of multiple layers of TCP/IP model.

10.4 IPS Architecture

Present networks and enterprises follow a layered defense approach to ensure security at different levels by using a variety of tools such as network reconnaissance, access control, firewalls, network, host and application intrusion detection systems, encryption and others. However, with the rapid increase in the number and type of attacks, a single system is not effective enough of attaining high attack detection accuracy and high system throughput.

Due to the dynamic nature of network attacks deploying a combination of both network and host IPS provides the greatest level of protection for critical data and complex applications. Network IPS solutions are deployed inline at the network perimeter and are designed to protect our critical infrastructure by blocking internal and external attacks on the wire and are considered as the first line of defense while its integration with Host IPS are designed to protect critical systems and applications by blocking attacks at the host and are considered the last line of defense.

The layered framework for intrusion protection systems is presented which can be used as effective security measure in communication network. The system architecture and subsystems is given in Figure 10.3

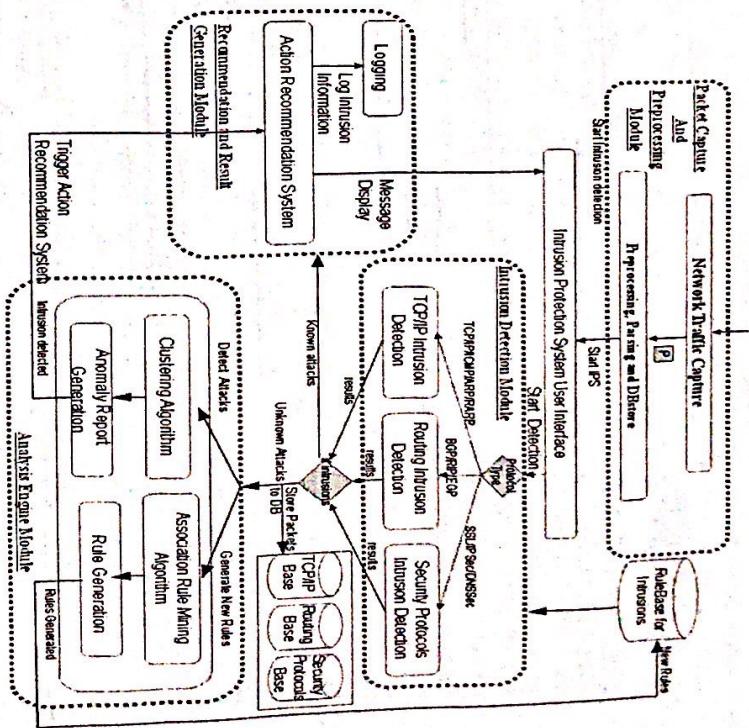


Figure 10.3 IPS Architecture

A network intrusion protection system using pattern matching and machine learning feature which will work at all layers of TCP/IP as well as for routing attack detection and prevention.

IPS system is divided into four major subsystems: data preprocessing system, rule matching system, analysis engine system and recommendation system. The four subsystems are tightly coupled to provide intrusion detection at any layer including TCP/IP suite protocols, routing protocols and security protocols. The machine learning system is independent of real time packet inspection and it will be initialized only after certain intervals. The analysis engine is also responsible for automatic signature generation of newly detected attacks which is implemented using association rule mining. Recommendation module is the interesting feature of our system as it provides the action against the detected intrusions. Each sub system is explained in detail in the following sections.

- Preprocessing Engine:** The system captures the packet through the network traffic sensor node. The packet is inspected to check whether it violates any constraint of the system. For example the source IP address is checked for the black listed IP address. If packet is valid and does not violate any rule, it is forwarded for preprocessing. Preprocessing is carried out for selecting the relevant features from the packet headers.
- Intrusion Detection Engine:** The next step is to apply signature matching algorithm to detect intrusions in the captured traffic. The attacks have some standard signatures which are verified with the contents of packets. This method applies the existing rules for detecting intrusions on the different protocols of TCP/IP suite. If signature matches, an alert is generated for intrusion. Else the packet is stored in the database for future analysis. IPS system consists of three subsystems based on the types of protocols. TCP/IP Intrusion Detection detects the well-known attacks on TCP and IP protocols. Routing Intrusion Detection detects the attacks on routing protocols such as RIP, BGP. Security Protocols Intrusion Detection provide protection against attacks on SSH, DNSsec.
- Analysis Engine:** Signature matching approach is smart enough in detecting known intrusions. But this approach is not suitable for unknown or zero day attacks. For the purpose we use anomaly detection techniques and frequent itemset generation methods. The analysis begins with application of frequent itemset mining to the collection of traffic database. The association rules will find out frequent itemsets from the pool of data with support and confidence values. This support and confidence values will help in decision making about the severity and sensitivity of intrusion. The rule database is frequently updated with new rules generated.
- Recommendation Engine:** The recommendation system decides the severity of intrusion based on parameters such as Euclidean distance, support or confidence value and performs action against the attacks. Another IPS response is to log network traffic which enables administrator to analyze network traffic and activity pattern of attacker.
- In IPS framework layered approach of TCP/IP architectural design and security objectives are chosen. As security is implemented individually at protocol level, the combining result of each protocol layer security will be more effective. If attack is not detected at one layer, it should be detected at next layer. Also each layer should be supported by feedback of previously detected attack and action. The layered security means to us that the system should be able to detect intrusions in any phase and at earliest. Another goal of system design is fast processing of packets and fast attack detection. The third important goal of our system is to detect known attacks as well as unknown attacks in the system. Another important feature of IPS system is automatic generation of signatures for the newly detected attacks and updating the system with new signatures. For the purpose a division of attacks, division of detection mechanisms