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.

types of routing protocol

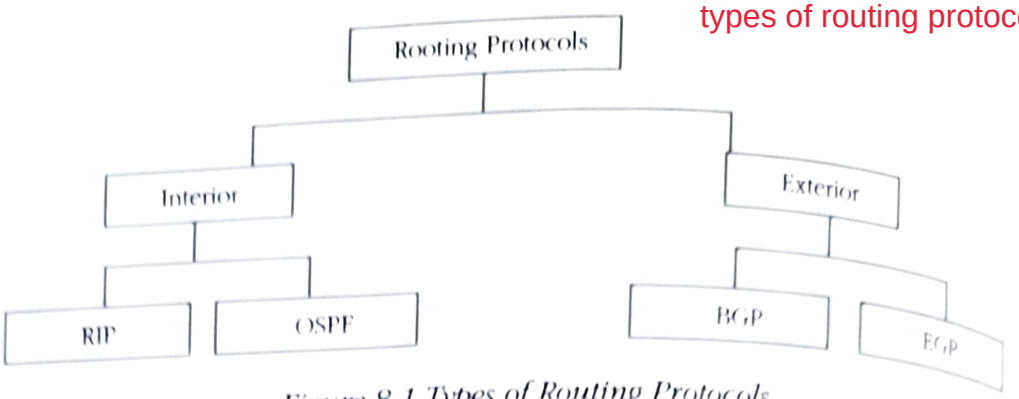

Figure 8.1 Types of Routing Protocols

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

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 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 protocols such as Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Internetwork Packet Exchange (IPX) RIP, IPX Service Advertisement Protocol (SAP), and Routing Table Maintenance Protocol (RTMP), broadcast their complete routing table periodically, regardless of whether the routing table has changed. This periodic advertisement varies from every 10 seconds for RTMP to every 90 seconds for IGRP. When the network is stable, distance vector protocols behave well but waste bandwidth because of the periodic sending of routing table updates, even when no change has occurred. When a failure occurs in the network, distance vector protocols do not add excessive load to the network, but they take a long time to re-converge to an alternate path or to flush a bad path from the network.

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 (NLSP), 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.

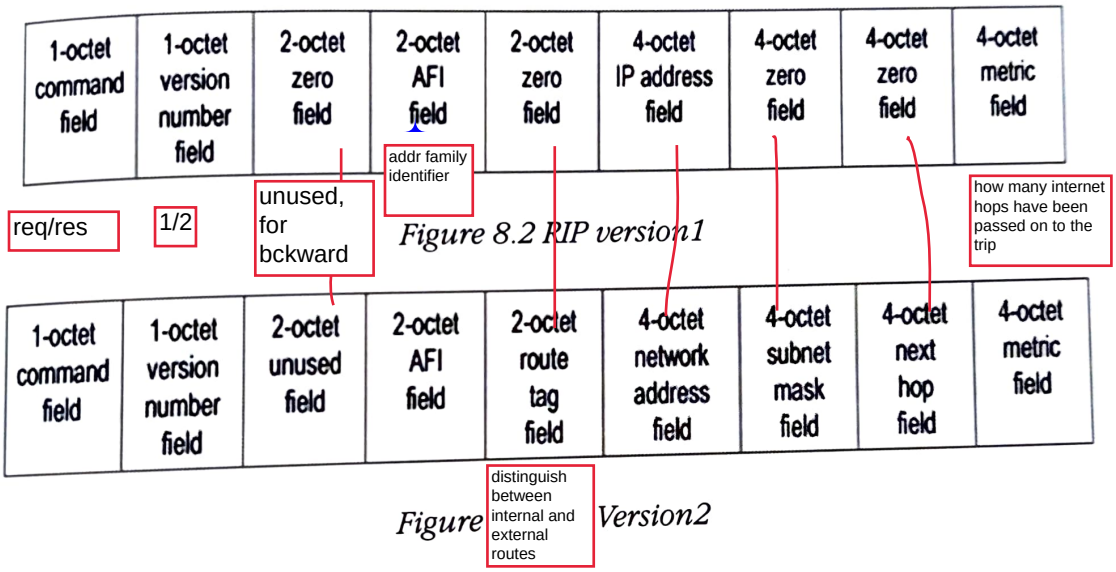

Figure 8.2 RIP version1

Figure 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

rip1 was designed for having better version as mnay fields are reserved (0), except the metric field as it needs to be a value between 0 to 16 acc to RIP1, and for compability RIP2 agrees and 16 is to be interperted as infity 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 routetimes 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) — new entry with same metric

Replace existing entry with the new advertised one

Else if (advertised hop-count after increment is smaller) — entry with smaller distance

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

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 Attcks

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 remotely 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.

- It allows unsolicited route advertisements. In other words, spoofed advertisements (responses) are accepted and processed even though no requested for it.
- RIP datagrams are not authenticated.

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 implementated are
  - Route monitoring and looking glasses
  - Real-time monitoring of route path changes
  - Traffic accounting

8.3 Open Shortest Path First (OSPF) intra-domain

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 reply 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

1. hackers can map the ntwork topology

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 AllOSPFRouters. 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.

unicast point to point request from outside ospf domain

- 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 traditionalOS, 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 to detect and prevent. There are three fields: metrics, sequence number and age which are particularly vulnerable and therefore these fields are the targets of usual attacks. However, with Keyed-MD5 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 MD5 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.

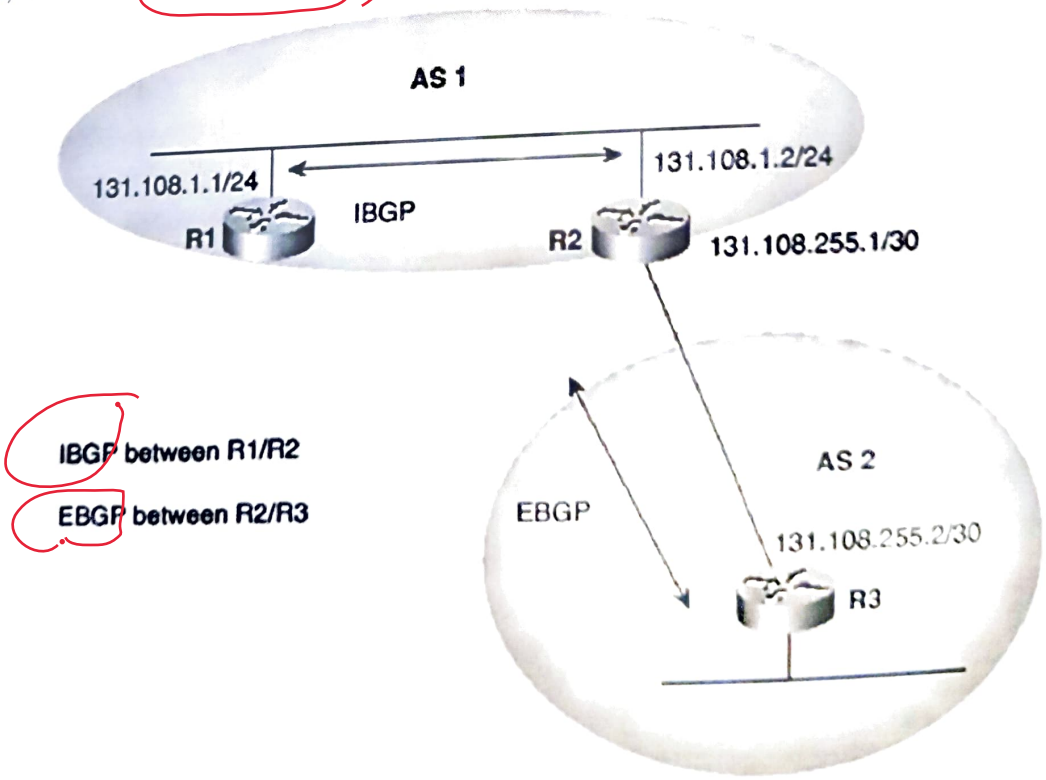

Figure 8.4 BGP Architecture

Figure 8.4 shows that the autonomous systems (AS1) is connected to AS2 through router R2 in AS1 to router R5 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.
- **Keepalives** - These messages are sent periodically to ensure 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.

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, forc1ing 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 ASs 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 ASs denoted in the path string. An ASs can modify the path it receives from other Ases by inserting or deleting ASs 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, 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 TCP transactions or crash altogether. These attacks are harmful enough to the individual routers, but become even more consequential when the distributed 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 digest of the TCP header and BGP data is included in each packet passing between the BGP speakers. The authenticity of the packet data is ensured because the digest could have only be 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 (DSUA) 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 removing 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 the heuristics it represent, and can only remove announcements which are overtly bad.

- **Secure BGP (S-BGP):** SBGP 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.

- IPsec 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 is 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 reach ability 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 Gcould 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

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.