Security issues in network control protocols

FERREIRO JORGE, ANDINA DIEGO
Departamento de Sistemas, Señales y Radiocomunicaciones
Universidad Politécnica de Madrid
Ciudad Univeristaria, s/n - Madrid
SPAIN

Abstract: - This paper focuses on the network infrastructure security measures currently proposed and at a certain point deployed in live networks. Security mechanisms proposed for network control protocols –mainly layer three routing protocols– are studied and their current limitations are highlighted. Quality of service, multicast related protocols and the active network paradigm are also taken into consideration.

Key-Words: - Security, routing, RIP, OSPF, ISIS, multicast, QoS, active networks.

1 Introduction

Now that the very first days of the Internet and the TCP/IP technologies are over and that all the associated technologies are maturing, many important issues are still arising. As many new mechanisms whose main purpose is to improve network services, in terms of functionality, availability or any other, new potential security threats come into scene, even some that were previously only considered in end systems.

Routing protocols have some security mechanisms specified that provide certain guarantees. There are currently two main types of routing protocols. Distance-vector protocols, with properties that make them suitable for some networks –details are out of the scope of this paper– have some mechanisms that provide some security. Routing Information Protocol version 2 –RIPv2– (RFC2453 [1]) may have for example implemented clear text authentication or MD5 based security (RFC2082 [2]). Link-state protocols such as Open Shortest Path First version 2 –OSPFv2– (RFC2328 [3]) and integrated IS-IS (RFC1195 [4]) have similar options (RFC2328 itself and draft-ietf-isis-hmac-03.txt [5]). OSPF has also a more complex mechanism described in RFC2154 [6] using digital signatures. Border Gateway Protocol version 4 –BGPv4, RFC1771 [7]–, as a slightly particular type of distance-vector, often referred as path-vector, although not using a custom mechanism, uses the TCP MD5 signature option (RFC2385 [8]) to achieve some security. Due to the nature and purpose of this protocol, some modifications have been proposed to achieve higher levels of security, such as SBGP [9] making use of certificates and thus of PKI. At the time of this writing, an IETF workgroup (rpsec) is about to be formed to document thread models and security requirements for routing systems,

More recent developments in networks have lead to multiprotocol label switching (MPLS) networks, that make use of Label Distribution Protocol –LDP– (RFC3036 [10] and RFC3037 [11]) to distribute label information. RFC3037 references RFC2385 to secure the communication using the TCP MD5 signature option the same way as BGP does. No new mechanisms are specified.

Quality of service is other of the network mechanisms that has created much expectation in the last few years. The Resource ReSerVation Protocol –RSVP– (RFC2205 [12]), currently used mainly for both resource allocation signaling and MPLS traffic engineering information distribution, is other protocol that due to its end-to-end nature needs security mechanisms to identify users. Some other cryptographic mechanisms for RSVP are described in RFC2747 [13]. Other QoS mechanisms, such as weighted fair queuing [14], also have some limitations inherent to their own nature that need to be considered.

All the issues that may appear in the unicast routing protocol should be considered in multicast routing protocols. Protocol Independent Multicast routing protocol –PIM– Sparse Mode –SM– (RFC2362 [15]) and Core Based Trees version 2 –CBTv2– (RFC2189 [16], RFC2201 [17]) can have its messages authenticated as described in several drafts. The paradigm of active networks on the other hand, creates new challenges in the study of security. The Abone –experimental active network– is providing a test field to learn the security implications that active networking [18] implies. Many of the threats that

were only considered in end systems must be taken into account in active nodes.

2 Routing protocol security

Routing protocols have been since the very beginning of the TCP/IP networks the control protocols of excellence. These protocols can be roughly classified as distance-vector or link-state protocols. Distance-vector protocols typically share their routing tables with their neighbors and process this information in order to build their own routing table. Link-state protocols on the other hand share topology information so that every router in the network can calculate which the best way to reach a certain destination is.

2.1 RIP

RIP (Routing Information Protocol) was first described in RFC1058 [19] and revised to RIPv2 in RFC1388 [20] and then in RFC1723 [21] and RFC2453. RIP-enabled devices share their routing tables sending unacknowledged messages over UDP port 520. RIP (RIPv1 from now on), has a packet

command	version	must be zero
address-family identifier		must be zero
IP address		
must be zero		
must be zero		
metric		

RIPv1 packet format

format as described in the figure.

The processing of RIP requests (command code 0x1) specified in the RFC states that requests made to any RIP interface (event "silent" ones) must be responded, without any restriction. This leads to a situation in which more devices or users than expected would be gaining certain information about the network. This situation also makes to device serving routes use CPU resources for purposes other than originally intended. This might potentially result in denial-of-service attacks (although this are rarely considered in routers and will not be considered anymore in the rest of the paper). If we consider that the RFC does not limit the TTL values of the messages involved, potentially any host in the whole network is a potential attacker. These problems can be avoided with the use of filters that deny any traffic directed to infrastructure IP addresses (but perhaps a few controlled packets, such as ICMP requests and responses or some high UDP ports used by applications such as traceroute).

In the case of RIP responses (command code 0x2), the RFC states: "processing is the same no matter how responses were generated". Validation checks include UDP port verification and ensuring that the packet comes from a host in a directly connected network. There is no authentication or any other security mechanism. Any device in the whole network could potentially spoof the source IP address of RIP responses and corrupt the RIP database and thus the whole routing table. This can also be solved with the appropriate use of filters in the network. On the other hand any directly connected host can send any harmful information without control.

RIPv2 fills some of the empty fields creating extensions to support subnet masks, next hops and route tags. Although this adds functionality, the possibility of using next hops other than the source address of the IP packet as used in RIPv1 is potentially dangerous and should be taken into consideration when securing devices.

RFC1058 defines from the very beginning a simple clear text authentication scheme (coded with type 2). This only prevents against some misconfigurations, but cannot be considered a full security mechanism.

MD5 authentication, defined in RFC2082, is the strongest mechanism proposed up to date for RIPv2. RIPv2 packet is created the same way, but no checksum is calculated, authentication type is set to 3 and the authentication password is reused to store a packet offset to locate

2.2 OSPF

OSPF is described in RFC2328, making obsolete RFC2178 [22] and RFC1583 [23]. OSPF-enabled devices share topological information sending messages directly on top of IP, protocol number 89. Routes gather topological information from all the routers in the area (distributed in LSA, Link State Advertisements) and run the Dijkstra algorithm to find the shortest path to every destination.

Router domains can be divided in areas to limit the flooding of topological information and scale further, with the restriction that every area must be either physically connected to the backbone area or logically connected (using the so called "virtual links") to it.

Version	Type	Packet length
Router ID		
Area ID		
Checksum		AuType
Authentication		
Authentication		

OSPF packet header

RFC2328 states that all protocol exchanges are authenticated. But, it is also true that one method of authentication is "none". OSPF packet header contains an authentication type field, with possible values:

AuType	Description
0	Null authentication
1	Simple password
2	Cryptographic auth.
All others	Reserved

Simple password authentication, the 64-bit field is configured in a per-network basis. This is useful just for simple misconfiguration scenarios. As the password is transmitted in clear text, anyone with physical access to the medium can easily get the password and generate messages itself.

With cryptographic authentication, a shared key is used to generate and verify message digest appended to the end of the packet. Also a non-decreasing sequence number, named cryptographic sequence number, provides anti-replay protection (once it has been incremented, not in the short term).

must be zero	Key ID	Auth data length
Cryptographic sequence number		

OSPF auth. field with the cryptographic option

Keys used in this option have four timers associated with it that limit their availability: KeyStartAccept, KeyStartGenerate, KeyStopGenerate and KeyStopAccept.

The OSPF packet and the secret key, plus some padding are used to generate the message digest. The RFC describes the use with MD5, although this mechanism could be easily adapted to any other algorithm. This mechanism is useful to protect protocol packets exchanged between neighbors.

Other alternative for securing OSPF is proposed in RFC2154 (and [24]). This proposal adds digital signatures to OSPF LSA data. The originator signs link state information and the signature is kept as the message travel throughout the area. Routers signing their LSA are therefore authenticated sources of information.

LS Age	Options	LS Type
Link Stat ID		
Advertising Router		
LS Sequence Number		
LS Checksum	Length	
LSA Data ...		
Signature ...		
Rtr Key Id	TE ID	Sign Length

Signed LSA

In addition of signing existing LSA, a new LSA is defined: the "Router Public Key LSA", coded as type 16, which contains certificate information to be flooded.

The certificate mechanism assumes that there is a trusted entity (TE) known by all the routes responsible or signing them.

LS Age	Options	LS Type
Link Stat ID		
Advertising Router		
LS Sequence Number		
LS Checksum	Length	
Certificate ...		
Signature ...		
Cert Length	Sign Length	

Router Public Key LSA (PKLSA)

This mechanism also helps to provide authorization. Among other information, certificates included in the PKLSA have the field #Net Ranges, which include the range of IP addresses the router is authorized to advertise in its LSA.

The trusted entity would be responsible of signing the certificates routers send in the PKLSA and thus checking all the information contained in them.

This mechanism, although provides authorization, does not prevent routers sending false information about the networks it is authorized to advertise. For example, autonomous system border routers could

propagate false information about other domain routers or area border routers could propagate false information about other areas (although some checking could be performed if there is more than one ABR for a certain area).

Router ID			
TE Id	TE Key ID	Rtr Key ID	Sig Alg
Create Time			
Key Field Length		Router Hole	#Net ranges
IP Address			
Address Mask			
IP Address / Address Mask for each Net Range...			
Router Public Key			
Certification			

OSPF certificate format

Although this proposal is much stronger than any other, draft-etienne-rfc2154-flaws-00 [28] still shows that there may be some flaws to be solved.

2.3 Integrated ISIS

Integrated ISIS is protocol primarily defined for ISO networks and for its use with CLNP in ISO10589. It has been later extended to serve as an IP routing protocol in RFC1195 [4]. Similar to OSPF in its nature, every router generates a LSP (Link State PDU) containing topological information, which is flooded later to other routers. These can therefore compute the best path to a destination using a SPF (Shortest Path First) algorithm.

In general, information is contained in variable length attributes (TLV, type-length-value). TLV type 10 is reserved for authentication in ISO10589, where the value is reserved, 1 means clear text authentication and 255 is reserved for private authentication methods. Another TLV is reserved in RFC1195. TLV number 133 has a similar meaning (but value 255 is not defined and the password length restrictions imposed by ISO10589 is removed).

From the security point of view, there is an important fact in ISIS. It does not run on top of IP. When used in a pure IP network this means that ISIS PDU are not routable at all, reducing the probability of remote attacks.

There is also an HMAC-MD5 authentication scheme with a similar approach as MD5 based authentication options discussed previously for RIP and OSPF defined in an IETF draft [5]. This document allocates type 54 (0x36) for HMAC-MD5 authentication. The length of the authentication value would be 16 and the length field in the TLV 17. The message digest is computed with the password and the ISIS PDU (with the authentication value field – the one being computed– set to zero). Different keys can be used for level-1 sequence number and link state PDU (Area Authentication String), for level-2 sequence number and links state PDU (Domain Authentication String) and for ISIS Hello PDU (Link Level Authentication String).

2.4 BGP

Border Gateway Protocol (BGP) version 4 is defined in RFC1771 [7] and is intended primarily to handle interdomain routing information. BGP, as an EGP (Exterior Gateway Protocol), poses different challenges than the previous IGP (Interior Gateway Protocol). It runs over TCP, port 179, and has been complemented by other numerous RFC.

BGP passes updates routing information between autonomous systems (AS) throughout the Internet. BGP speakers typically know the chain of AS a packet may cross to reach a certain destination (AS_PATH), together with some attributes that assist in routing based on policies.

RFC only makes it necessary to check the peer IP address in any message. This means that any attacker could spoof the peer IP address and send bogus messages that could disrupt routing tables. In addition it is also vulnerable to any TCP attack.

RFC2385 [8] considers adding the MD5 signature option to TCP. Every segment sent on a TCP connection would contain the MD5 digest produced by applying the MD5 algorithm to the TCP header, data (details are out of the scope of this paper) and a shared key. This mechanism makes it possible to authenticate the source of the message.

There is a detailed security analysis in draft-murphy-bgp-vuln-00 [25]. Issues such as AS authentication, address space “ownership” verification and router authorization among others are raised. Vulnerabilities are considered for each BGP message.

Some proposals have been made to avoid these vulnerabilities. draft-ward-bgp-ipsec-00 [26] and draft-clynn-s-bgp-protocol-00a [27], for example, consider the use of IPSec and certificates to secure BGPv4. [29] defines X.509v3 extensions to include IP addresses and AS information in certificates. These extensions make it possible to check if the router source of the information is authorized for its publication or not.

3 MPLS

New paradigms are now being deployed. One example is MultiProtocol Label Switching. It is defined in a set of RFC (RFC3031 [30], RFC3032 [31] …) and there are many new services deployed using its unique characteristics.

The way MPLS works is encapsulating other protocols in a MPLS header. This header contains labels, which are read in devices to know where to route them. The protocol responsible for this label distribution is known as LDP (Label Distribution Protocol).

3.1 LDP

LDP is specified in RFC3036 [32] and its applicability is stated in RFC3037 [33]. It runs on top of TCP, port 646 (and thus inherits its vulnerabilities).

RFC3036 considers the possibility of using the TCP MD5 option previously commented for BGP. This could provide some authentication mechanism to this protocol.

4 QoS Security

Quality of Service is other of the challenges many networks are facing now. Either in the Integrated Services model (RFC1633 [34]), making use of RSVP for resource reservation, or the Differentiated Services (RFC2475 [35]), most of the new networks are considering implementing some flavor.

4.1 RSVP

The Resource Reservation Protocol is defined in RFC2205. Its primary purpose is to signal resource requirements (typically bandwidth) from end-system to end-system, although it is also used for MPLS Traffic Engineering applications as well (RFC3209 [36]).

The way RSVP works is traveling the path data is to be sent through in two ways. In the first go, a Path message would be requesting reservation of the desired resources hop by hop to the destination and after a Resv message would travel back to the origin to notify all the hops that the reservation process was successful (if it were).

Due to its nature, RSVP is susceptible of being used for DoS attacks. Potentially unauthorized users or forged messages could request reservation of resources until they are locked up. To avoid this problem, cryptographic authentication mechanisms have been proposed in RFC2747. As other mechanisms discussed in this paper, it is based on HMAC-MD5 and monotonically increasing sequence numbers. As with previous proposals, no key distribution infrastructure is specified, so manual distribution is needed.

When addressing security in an RSVP environment, there is an issue with IPSec streams. As these flows cannot be differentiated by higher-level headers (which are encrypted) port numbers cannot be used to separate sessions. RFC2207 [37] proposes the use of the security parameter index (IPSec SPI) for this purpose.

Detailed study and considerations regarding RSVP security can be found in [38] and [39]

4.2 Queuing

Although not control protocols, internal queuing strategies in network devices should also be considered as potential security holes in network infrastructures. For example, in [40], it is stated that:

> *"Allocation per source-destination pair allows a malicious source to consume an unlimited amount of bandwidth by sending many packets all to different destinations."*

Further investigation is still needed to further understand the security implications of queuing mechanisms and possible countermeasures.

5 Multicast routing security

Although it cannot be said that the Internet is multicast enabled today, it is true that multicast is becoming more important. Multicast routing protocols, while considered by many as still being developed, are in place in many networks (mostly enterprise networks).

Multicast routing protocols work in conjunction with IGMP, which provides mainly group registration information to routing devices. IGMP security is not addressed in this paper.

5.1 PIM

Nowadays probably the most deployed multicast routing protocol is Protocol Independent Multicast (PIM), and in the Sparse Mode flavor (SM). It is defined in RFC2362 and completed in many other RFC.

The RFC does not state anything more than saying that IPSec can be used.

5.2 CBT

The other multicast routing protocol defined by the IETF is the so-called Core Based Trees (CBT). It is specified in RFC2189 and RFC2201.

CBT does not take into account any security. It lets security rely on upper layers in the OSI protocol and lets it be driven by the end hosts/applications. The RFC states that *little published work exists on the topic of multicast security*.

Further investigation is also needed in this area.

6 Active networks

Active networks rely on the idea of having programmable routing devices. Packets passing through them would program them from the classic action of forward to whatever is considered appropriate.

Although active networks are in the very first stages of development, it should be noticeable that security is even more challenging than we are used to with other network paradigms.

Initiatives such as Abone will probably contribute to clarify these issues.

7 Conclusion

Although apparently security discussions do not consider network control protocols, closer inspection shows that there are indeed some mechanisms that provide a certain level of security.

IP unicast routing protocols have at least the possibility of authenticating other parties, and in the case of OSPF there is even a much more complex mechanism that provides more guarantees. Most of them are based on MD5 digest and just provide authentication and integrity of the messages. Some degree of authorization is achieved with the use of PKI in some proposals for OSPF and BGP. LDP and RSVP share similar approaches to authenticate other peers using MD5, but there is no authorization scheme.

On the other hand, it has been found that further investigation is still needed to really know the security implications that newer queuing mechanisms carry and how to secure multicast routing protocols. Many of the threats considered up to date involve using more resources than expected and resulting in DoS. Authorization mechanisms need to be developed to avoid this possibility.

Further investigation is also needed in active networks security. Its nature will probably push security to be considered a must from the very beginning.

For almost any case it is still necessary to define a threat model and make a formal analysis of all the security implications. Up to date there has been only proposals that address certain security weaknesses instead of covering the whole scenario.

References:

[1] G.Malkin. RIP Version 2. Internet Standard. RFC2453. November 1998.

[2] F. Baker, R. Atkinson. RIP-2 MD5 Authentication. Internet Proposed Standard. RFC2082. January 1997.

[3] J. Moy. OSPF Version 2. Internet Standard. RFC2328. April 1998.

[4] R.W. Callon. Use of OSI IS-IS for routing in TCP/IP and dual environments. Internet Proposed Standard. RFC1195. December 1990.

[5] T. Li, RJ Atkinson. IS-IS Cryptographic Authentication. Internet Draft. Network Working Group. draft-ietf-isis-hmac-03.txt. July 2001.

[6] S. Murphy, M. Badger, B. Wellington. OSPF with Digital Signatures. Experimental. RFC2154. June 1997.

[7] Y. Rekhter, T. Li. A Border Gateway Protocol 4 (BGP-4). Internet Draft Standard. RFC1771. March 1995.

[8] A. Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. Internet Proposed Standard. RFC2385. August 1998.

[9] C. Lynn, J. Mikkelson, K. Seo. Secure BGP (S-BGP). Work in progress. draft-clynn-s-bgp-protocol-0?.txt. December 2001.

[10] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas. LDP Specification. Internet Proposed Standard. RFC3036. January 2001.

[11] B. Thomas, E. Gray. LDP Applicability. Informational. RFC3037. January 2001.

[12] R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin. Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification.Internet Proposed Standard. RFC2205. September 1997.

[13] F. Baker, B. Lindell, M. Talwar. RSVP Cryptographic Authentication. Internet Proposed Standard. RFC2747. January 2000.

[14] A. Demers, S. Keshav, and S. Shenker. Analysis and Simulation of a Fair-queueing Algorithm, *Proc. ACM SigComm 89*, pp 1-12.

[15] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei. Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol

Specification. Experimental. RFC2362. June 1998.
[16] A. Ballardie. Core Based Trees (CBT version 2) Multicast Routing – Protocol Specification -- .Experimental. RFC2189. September 1997.
[17] A. Ballardie. Core Based Trees (CBT) Multicast Routing Architecture. Experimental. RFC2201. September 1997.
[18] T. Faber, B. Braden, B. Lindell, S. Berson, K. Bhaskar. Active Network Security for the Abone. November 2001.
[19] C.L. Hedrick. Routing Information Protocol. Historic. RFC1058. June 1988.
[20] G. Malkin. RIP Version 2 Carrying Additional Information. Internet Proposed Standard. RFC1388. January 1993.
[21] G. Malkin. RIP Version 2 - Carrying Additional Information. Internet Standard. RFC1723. November 1994.
[22] J. Moy. OSPF Version 2. Internet Draft Standard. RFC2178. July 1997.
[23] J. Moy. OSPF Version 2. Internet Draft Standard. RFC1583. March 1994.
[24] S.L. Murphy and M.R. Badger. Digital Signature Protection of the OSPF Routing Protocol. *In Internet Society Symposium on Network and Distributed Systems Security,* 1996.
[25] S. Murphy. BGP Security Analysis. Internet Draft. draft-murphy-bgp-vuln-00.txt February 2002.
[26] D.Ward. Securing BGPv4 using IPSec. Internet Draft. draft-ward-bgp-ipsec-00.txt. January 2002.
[27] C. Lynn and K.Seo. “Secure BGP /S-BGP)”. draft-clynn-s-bgp-protocol-00a.txt. December 2001
[28] J. Etienne. OSPF with digital signature against an insider. Internet Draft. draft-etienne-rfc2154-flaws-00.txt. May 2001.
[29] C. Lynn, S. Kent, K. Seo. X.509 Extensions for IP Addresses and AS Identifiers. Internet Draft. draft-ietf-pkix-x509-IPaddr-AS-extn-00.txt February 2002.
[30] E.Rosen, A. Viswanathan, R. Callon. Multiprotocol Label Switching Architecture. Internet Standard. RFC3031. January 2001.
[31] E. Rosen et al. MPLS Label Stack Encoding. Internet Standard. RFC3032. January 2001.
[32] L. Andersson et al. LDP Specification. Internet Standard. RFC3036. January 2001.RFC3036
[33] B. Thomas et al. LDP Applicability. Internet Standard. RFC3037. January 2001.
[34] R. Braden et al. Integrated Services in the Internet Architecture: an Overview. Informational Draft. RFC1633. June 1994.
[35] S. Blake et al. An Architecture for Differentiated Services. Informational Draft. RFC2475. December 1998.
[36] D. Awduche et al. RSVP-TE: Extensions to RSVP for LSP Tunnels. Internet Standard. RFC3209. December 2001.
[37] L. Berger, T. O'Malley. RSVP Extensions for IPSEC Data Flows. Internet Standard. RFC2207. September 1997.
[38] Talwar, V; Nhrstedt, K. Securing RSVP for multimedia applications Department of Computer Science. University of Illinois. *ACM MM 2000 Electronic Proceedings*. 2000
[39] T Wu, S. Wu, F. Gong. Securing QoS: Threats to RSVP Messages and Their Countermeasures. *Proceedings IWQoS, pages 62-64, 1999*. 1999
[40] A. Demers, S. Keshavt, S. Shenker. Analysis and Simulation of a Fair Queueing Algorithm. *Proc. ACM SigComm 89, pp 1-12*. 1989