MAGMA Working Group
Internet-Draft
Expires: January 7, 2005

G. Daley
G. Kurup
Monash University CTIE
July 9, 2004

# Trust Models and Security in Multicast Listener Discovery
## draft-daley-magma-smld-prob-00.txt



Abstract

The Multicast Listener Discovery (MLD) is used by IPv6 routers to discover the presence of multicast listeners (i.e. nodes that wish to receive multicast packets) on their directly attached links, and to discover which multicast addresses are of interest to those neighbouring nodes. The existing protocol specification (MLDv2) discusses the effects of on-link forgery of MLD packets but provides no protection from on-link attacks.

By taking advantage of or abusing Multicast Listener Discovery, bogus

devices may cause incorrect state and disruption to multicast or unicast packet delivery. This memo considers the trust models for the MLD protocols, and their interaction as well as their interaction with link-layer and multicast proxy devices. It provides a security and threat analysis for each model.

Table of Contents

## 1. Introduction

Multicast Signalling is required to support subscription and management of multicast listeners in IPv6 networks. Abuse of the existing trust used in multicast signalling may have effects significant not only on the local link, but for multiple hops in the Internet.

Multicast data streams are touted as a mechanism for providing scalable deployments of multi-consumer oriented applications on the Internet. In IPv6, multicast hosts and routers communicate their multicast capabilities and group membership using Multicast Listener Discovery (MLDv2 or MLD) [5].

Although Multicast Listener Discovery only operates within a single IP link, interaction between hosts and routers and change in states due to MLD reports may cause routing changes in multicast routers beyond the current link, when associated with non-link-local groups. Additional considerations for Multicast Listener Discovery in different access network environments are provided in [6], [7] and [8].

Since multicast is touted as a mechanism to handle large bandwidth data streams, malicious modifications of data streams on other subnets is a significant cause for concern. Additionally, the limited feedback mechanisms provided for multicast data streams (many of which use UDP) mean that service theft and network denial-of-service are easier than in bidirectional streams oriented communication.

Multicast Listener Discovery protects from off-link attacks through prevention of forwarding and use of link-local source addresses[5]. This means that all attacks caused by MLD originate from hosts either on a target link, or in the case of routing changes, a device which is in the recipient for a particular group or source.

While identifying the source of an attacker is certainly possible, this does not mitigate the potential of attacks, nor the consequences in the case of abuse. Of particular interest in this analysis are several characteristics of MLD which lend it to attacks.

Mandatory Query response: While MLD doesn't have any particular message authentication, any device which is acting as a router may force mandatory signalling responses from other hosts on-link.

Queries Elect the Querier Router: Sending of MLD queries can be used to elect or de-select a Querying multicast router. This may be used to modify parameters on a network and conceivably support

denial-of-service.

MLDv1 can bid down MLDv2: Backward compatibility mechanisms for interworking between the current MLD (MLDv2) and Multicast Listener Discovery Version 1 (MLDv1) allow hosts to change the MLD compatibility state on a router by sending reports [5]. This may be used to force changes in the source model used for off-link multicast routing.

Reports cause off-link changes: The reports which are sent for joining arbitrary multicast groups cause changes to off link routing state when new groups are joined, or when routing halts after a group or source is excluded.

Reporting can cause Querying: Host transmitted report messages can be used to instigate queries from a router when the last group member leaves a group.

Unprivileged multicast API: Access to arbitrary multicast groups is typically available through the host API. This allows generic tasks on a host computer to join or abuse multicast groups.

This document discusses the effect of these features in a variety of network environments, and discusses attack scenarios which arise in these environments. Particularly, it covers the trust models in the following areas:

- Trust between hosts and routers for multicast group management.
- Trust between access network components, especially where multicast snooping is required.
- Trust in proxied multicast networks.

This document compares the signalling in MLD and related protocols with other signalling protocols, with similar trust models. As part of this comparison, discussion of security methods applied to those protocols and their applicability to MLD is provided.

Finally, while IPv4 is the prevalent networking technology today, this document provides analysis of the trust models for multicast group management signaling in IPv6 only (MLDv1 and MLDv2). If sufficient interest and timing resources are available, assessment of trust in IPv4 multicast group management may be attempted in a later version of the draft [3].

### 1.1 Previous Work

Previous attempts to secure Multicast groups have focussed on access and abuse of multicast group data[18] while not protecting signalling, or have relied upon group signalling keys, which have trust scalability and deployment issues.

Security considerations for IGMPv3 in IPv4 (Section 9 [3] ) proposes a security mechanism for multicast group management based on IPSec AH [11][10].

It provides signalling and message integrity based on shared keys where any possessor of the shared key can undertake transmission of 'authenticated' messages.

Similarly, it proposed the application of to-be-developed key exchange procedures to ensure that Query and Leave messages could be authenticated. To date no such key exchange mechanisms are deployed for IPv4.

In either case (key exchange or shared key) host multicast group management reporting is unsecured, since at the time, IPSec AH security associations weren't capable of binding to arbitrary multicast destinations.

Such mechanisms are clearly not extensible to an arbitrary group of users, and require manual configuration. Such manual configuration is out of the spirit of IPv6 autoconfiguration, and may not be possible to fix in MLD.

A comparable protocol to Multicast Group Management is IPv6 Neighbour Discovery, which resolves last hop link-layer address mappings and routing between hosts and routers [12]. It is noteworthy that at a similar period, IPv6 Neighbour Discovery proposed similar systems for authentication of message exchanges. Since both multicast group management and Neighbour Discovery are involved in the automatic configuration there are serious chicken-and-egg problems for IPv6 systems to use IPSec based key exchanges [16][17].

### 1.2 Structure of this Document

This document provides trust models and threat descriptions for MLD hosts, routers, proxies and snooping switches.

Multicast group management trust model analysis has been broken down into three sections within this document. We analyse the base protocol as specified by the Multicast Listener Discovery version 2 RFC-3810 [5]. We then extend the considerations to include

link-layer snooping effects [8][6]
and MLD Proxying [7].

Traditional signalling directly between hosts and routers is tackled within Section 2. This subsumes the election of routers for Querying operation and refers mainly to the MLDv2 and MLDv1 base specifications.

Link-layer multicast snooping effects are discussed in Section 3, especially in the additional requirements and implicit trust developed with link-layer switching hardware. This corresponds primarily to the definitions provided in the multicast snooping specification [8].

Trust for multicast group management signal proxying is handled in Section 4. This describes the differences between the trust models available in the direct signalling from Section 2 due to the placement of multicast group management proxies.

A summary of the classes of threats is offered in section Section 5.

After reviewing trust and threats within the group management protocols, the existing message formats for MLDv2, and Multicast Router Discovery are described in Section 6. Particular attention is paid to the specification of message lengths and how additional space within messages is treated.

## 2. Trust Models in Multicast Group Management Signalling

Direct Multicast Listener Discovery signaling between hosts and routers consists of Queries, sent by routers, and Reports which are sent by hosts[5].

Actions may be taken by routers or hosts upon receiving either of these messages. These actions exhibit implicit trust relationships, which may be the subject of abuse.

### 2.1 Routers' Trust of Hosts

MLDv2 signalling is used by routers to determine if a set of multicast data is of interest to hosts on a link.

The router receives reports from when hosts add to, subtract from or modify the listening state of their set of sources or groups. Also hosts report multicast Group and (Source,Group) status periodically, in response to router queries.

When a router receives a single report message, changes to multicast

routing tables of off-link routers may occur (for non link-local groups). This may cause attack amplification effects to occur when a device causes routing change at multiple levels of the multicast routing topology.

Additionally, reports which requests for multicast groups or sources may have an effect on the perceived quality of service for other devices, since multicast data streams do not undertake end-to-end rate limiting. Addition of multicast data streams effectively reduce the available bandwidth on all links where the data are received.

If the multicast routing infrastructure is not aware of topological bandwidth constraints, hosts may cause denial-of-service by spuriously (or accidentally) requesting many large data streams.

Additionally, for some types of messages (MLDv2 State Change Reports, MLDv1 Done Reports) Query messages are required to be sent from the Querier router upon their reception. A node which produces such Report messages may be able to cause multiple transmissions by the Querier router (up to the Querier's robustness value) from a single report message. With these messages though, a bogus device is unable to end transmission to legitimate group members. This is because the group members will reply to the queries generated upon State Change Report reception (increasing the signalling load).

Bogus or replayed reports for the current state of a multicast data stream may be used to maintain the transmission of a particular multicast data stream for a longer period than is necessary. This may either be used to drain network resources or to flood routing state changes from the router when multiple groups are dropped simultaneously from the interest list upon expiry of Multicast Address Listening Intervals.

The existence of the MLDv1 compatibility mode may cause a router to lose source specific information on particular groups, though it continues to send V2 Queries. In this case it may be possible to cause the router to use Any-Source-Multicast (ISM) routing instead of Single-Source-Multicast in the short term. This is described in the security considerations section (10) of the MLDv2 specification [5]. This is especially critical when existing listeners EXCLUDE specific sources and the abused bid down causes the data which originates from this source to be delivered.

No authentication or authorization of multicast hosts and their multicast group management signalling is client requests is defined in IPv6. Most of the attacks defined may be performed without impersonating other nodes or defying the MLD specifications. Since joining groups and modifying source filters are defined as part of

the user-level APIs for MLDv2, it is plausible to believe that applications may cause these effects without requiring privileged access to operating systems [5].

## 2.2 Hosts' Trust of Routers

In multicast group management, the reception of a Query message requires response from a multicast listener. This response is typically a current state report of the groups or sources and groups which the client is interested in listening to.

This response is required, otherwise the host may lose multicast delivery for any or all of the multicast streams which are queried.

Where host suppression is not in use [5], a router specifying a very small Maximum Response Code (Timer) in its Query may cause multicast report bombing at fine granularity with a single message. In some cases, this may have severe consequences in terms of packet loss or delay on other data sources or signalling.

Hosts have no idea which is a valid Query, since no authentication or authorization of routers is undertaken. Even choosing to respond to queries from the router with the lowest source address may not help, since it is trivial for non-routers to create such addresses.

## 2.3 Routers' trust of Routers

In multicast group management, only one router per link is responsible for eliciting reports from multicast clients. This Querier Router is elected through an address identifier. Modifications of a router's address may make it a favoured router in querier election.

Election occurs when a router with an address lower than any seen in a recent Query sends a Query message on the link. Upon reception of a Query from a router with a lower address, all routers should stop Querying.

This system assumes that the router which transmits with the lower address is a legitimate router, and that the other routers will cease transmission upon receiving such a Query.

While there is no direct service disruption in the case that a non-authorized router continues Querying, this device may now vary the Query interval and timeout parameters. This may have an impact on packet delivery by increasing the signalling load on the link.

By increasing the Querier's Robustness Value, the leave latency for

multicast packet delivery is increased on the link. This may lead to congestion, as new multicast delivery streams overlap with those for devices no longer on a link.

Legitimate routers, once downgraded to Non-Querier by the presence of a fake Querier, can remove Groups to be forwarded if it has not received a report from listeners within its Multicast Address Listening Interval. Since a router is required to accept and process queries directed to any of its listener addresses (Section 5.1.15 of MLDv2) it is possible that routers will stop sending queries without hosts ever receiving the Query message. This is because the Querier election strategy ensures that a Querier Router stops sending Queries as soon as it receives any Query from a preferred router. In this fashion a router may continue to receive general queries advertised only to itself, and no responding reports will be received from listener hosts.

In the case that the unauthorized router sends queries only once and then stops, the other routers will stop Querying for the duration of the Other Querier Present Timeout [5]. As this is based on the Querier's Robustness Value and Query Interval advertised in the false Query, Querier re-election may be halted for a long time [5]:

```
 = max[Robustness Variable] * max[Query Interval] +
                 (max[Maximum Response Delay]/2000 )
 = ( 7 * 31744 + (6290432/2000)) = 225353 seconds.
```

If a router exists which doesn't stop Querying when a router with a lower address exists, then even more packets will be transmitted on the link. Hosts will receive both sets of queries and will have to respond to both. Therefore, the presence of any misbehaving device (using any address) is similarly harmful to the case where a false router is elected.

## 2.4 Hosts' trust of Hosts

Hosts do not trust other hosts' reports except in MLDv1, where they are used for host suppression[4].

## 2.5 Threats Specific to MLDv1

Report messages which respond to queries are delayed over a random interval specified by the Querier router. Hosts may avoid transmitting a response packet if they are configured to use MLDv1, if it has already seen a response [4]. This is called host suppression, and is discussed further in Section 2.4.

Hosts may suppress their own reporting in the case that they receive

an MLDv1 report for the same group. As mentioned in section Section 3.4, the use of host-suppression may have negative consequences on snooping networks.

Therefore, it may be possible to engineer situations where hosts are denied service by being tricked into host suppression on snooping networks.

## 3. Trust Models for Link Layer devices (Snoopers)

Multicast listener snooping mechanisms [8] and Multicast Router Discovery [6] can be used to control local delivery of multicast traffic within the last IP hop. Interference with multicast snooping operation can be used to modify multicast packet flow within a link.

In this case, not only off-link multicast reception from the router is involved, but link-local packet delivery such as is used in IPv6 Neighbour Discovery[12].

Switches must be informed using multicast group management reports so that multicast packets are distributed to interested listeners in the link-layer domain.

### 3.1 Switches' Trust of Routers

Multicast Routers need to know of the presence of every group and source within the IP hop. Therefore, snooping switches need to include routers' switch ports as receivers of all groups. There is trust implied in switches' monitoring of routers, which may be abused.

Switches' monitoring of router presence ensures that non-local routing occurs for multicast streams originating on-link, and allows reception of multicast group management messages for local listeners.

Switches therefore need to identify routers to include them in all multicast transmission groups for off-link traffic.

Monitoring Query messages is ineffective, since only one router will Query. Multicast Router Discovery provides a mechanism where all routers with multicast capabilities should advertise their presence when solicited by switches [6]. Periodic updates from multicast routers serve to update state, sending to the link-local all-snoopers group.

This is similar to unicast IPv6 Router Discovery and potentially could be done using Neighbour Discovery Options [12].

Currently no mechanism exists to determine if a responding device is a router, and therefore whether all multicast traffic should be sent to the switch port. Additionally, bogus Multicast Router Terminate messages received on the same port as a router may be used to halt reception of all multicast data by the router[6].

For IPv6 Router Discovery, Securing Neighbour Discovery[15] procedures have been proposed, to provide authorization for delegated trust of routing operation. This mechanism has been proposed as a model for authenticating Multicast Router Discovery, even where the message formats differ from Neighbour Discovery.

Without a similar mechanism, a host may pretend to be a router by sending bogus Multicast Router Advertisements and swamp a LAN segment with all off-link multicast traffic until a snooping timeout occurs.

### 3.2 Switches' Trust of Hosts

Snoopers are required to modify forwarding state to include those switch ports and LAN segments which have interested listeners. Reception of reports or done messages are used to change group delivery state within the multicast domain.

Changes to snoopers' port state may be assumed by switches to only be possible from the port attached to the host. In some environments, though, it may be possible to steal service from legitimate owners by moving listener state from one port to another within a link, using impersonation or report replay.

Another issue is when inappropriate traffic is sent over a particular switch port. For example, it may not be appropriate for the all-routers' or all-snoopers' group messages to be sent across a wireless link.

Access control of certain classes of groups therefore should be considered.

### 3.3 Switches' Trust of Switches

Routers receiving multicast router solicitations should respond so that snoopers send all multicast packets to them.

Since not all LAN segments are snooping segments, responses to Multicast Router Discovery Solicitations may be transmitted across multiple LAN segments (though sent to all-snoopers group).

Therefore, in order to avoid excess transmission to unnecessary LAN segments, it would be useful to ensure that the solicitor has some

authority to send multicast router solicitations.

In some snooping environments, the snooping switches act as MLD signalling proxies, in which case the trust models which apply are defined in Section 4.

### 3.4 Hosts' Trust of Switches

When host-suppression is in use, it is well known that multicast snooping may have difficulties in maintaining multicast snoop state.

Actually this was one of the scenarios which led to removal of this feature from modern multicast group management protocols [5]. Nevertheless, some multicast snooping devices seek to prevent this issue occurring by never forwarding multicast group management reports to ports where a router isn't attached.

Also, these switches may forge group membership queries in order to generate multicast snoop state. In this case, the hosts will receive queries from devices which aren't a part of the network layer routing infrastructure, and may not be 'authorized' to send queries. Such switches share many attributes in common with MLD proxies (Section 4).

## 4. Trust Models for Proxied Multicast Group Management

Some networks will not have explicit multicast routing protocol exchange between devices on the multicast forwarding path. These networks trust a proxy to perform necessary Multicast Listener Discovery Signalling to cause packet delivery onto the local link.

In this case, it is necessary to send messages received from requesting multicast clients toward multicast routing infrastructure through proxied intermediate routing hops.

A proxying device undertakes MLD signalling on the interface closer to the multicast infrastructure, requesting the aggregates of the groups and sources that hosts on other of its interfaces request.

Thus on one interface, the proxy acts as a host (toward a router) and on another, the proxy acts as a router (to multicast clients).

### 4.1 Proxies' trust of Routers

Proxies talk to multicast routers on their upstream interface in a manner which mimics current host-to-router interactions for multicast group management.

The proxy multicast group management specification requires that the elected Querier device act as the forwarding proxy device. Therefore any device elected as the Querier router is assumed to be able to provide forwarding support [7].

When interacting with a Querier router, the proxy makes no further assumptions about the authorization of the router except those made in Section 2.1.

### 4.2 Routers' trust of Proxies

The proxy sends multicast group management reports to the router on behalf of devices which aren't on an interface connected to the router.

In this case, since the proxy isn't the eventual destination of the multicast stream, decisions as to access control cannot be undertaken when summarized information is passed to routers[7].

In the case that the proxy is able to supply credentials for each of the requesting hosts on the other interface, transparency may be restored, at the cost of protocol change.

Additionally, on the proxies' downstream interfaces, it may be that there is a proxy which attempts to undertake Querying function in the presence of a real multicast router.

[7] encourages setting the address of the proxy to a very low value in order to guarantee Querier election. Clearly, when a multicast router which is connected to the Internet exists, it should be elected instead.

At this time, there is no mechanism which allows the router or proxy to determine precedence other than administrative choice of router/ proxy address.

### 4.3 Hosts' trust of Proxies

On links where services are proxied further up a network, hosts undertake signalling with the proxy instead of to a router. Interactions and authorization are based on the host-to-router model in Section 2.1, although the proxy may not be part of the authorized network-layer routing infrastructure.

Authorization for routers to proxy may be assigned by an upstream router or proxy, except that this may be difficult if the devices do not have some pre-existing trust.

As such, a host should always prefer a router with authorization over one without, which may just be proxying. Currently, though, there is no way to determine whether a Querier is actually a proxy or not.

The proxy acts as a router in the case that it is the Querier, and hosts rely upon the fact that their responses to queries mean that listener tables for their network are set up appropriately. In the case that the Querier fails to generate appropriate listener reports on upstream interfaces, though, packet flow may fail.

### 4.4 Proxies' trust of Hosts

Proxies which are Queriers have the same trust of end-hosts which exists for the router-to-host model in Section 2.1. In this case though, the host may in itself be a proxy and the notes from section 4.2 also apply.

### 4.5 Proxy's trust of Topology

Multicast proxies rely upon the idea that there are no loops in the forwarding topology for multicast.

Since no routing protocols are used between proxies to detect loops, it is possible for an attacker to set up forwarding loops which will cause damage to packet transmission on multiple links[7].

## 5. Summary of Threats to Multicast Group Management

The threats in MLD can be summarized by the role assumed by an attacker. Below are summaries of attacks ascribed to particular attacker roles, which are pertinent regardless of the access network topology.

### 5.1 Bogus Querier

Any device may become a bogus querier, whether a router or not.

The effects of being a bogus querier are that Querier election may be preempted, or that multicast group management signalling may be elevated.

### 5.2 Bogus Group Member

An attacker may be able to join many groups, potentially subscribing many fake members to a particular group.

In MLDv2, all group members are tracked by multicast routers and snooping switches, and bogus membership may cause such state to be

exhausted.

The subscription and unsubscription of bogus group members (even to bogus groups or sources) may cause signalling off-link to other multicast routers.

Where multicast routing of packets occurs based on bogus membership or source filtering, bandwidth resources may be consumed.

### 5.3 Bogus Switch

Whether or not multicast snooping is taking place, the presence of Multicast Router Solicitations may make routers send Multicast Router Advertisements. These forced advertisements may be used by bogus switches to consume network bandwidth.

### 5.4 SSM to ASM bid-down

Where an attacker can send an MLDv1 report for a group which is being SSM routed, the router will switch to any-source-multicast, possibly causing significantly higher bandwidth utilization [5].

## 6. Existing protocol formats and messages

Message definitions for MLDv2 [5] and Multicast Router Discovery [6] are described.

### 6.1 MLDv2 Report Messages

The MLDv2 report message currently consists of an ICMPv6 header, with the protocol (ICMPv6) and length of the datagram described in previous network layer headers, followed by a sequence of multicast address records.

The number of multicast address records is described in a field of the fixed MLDv2 Report header, although the address records themselves are of variable length.

Each Multicast address record contains two length indicators: one of which indicates the number of 16 octet source addresses, and an Auxiliary data length specification. Using these values, the message receiver is able to locate the end of the multicast address record.

MLDv2 [5] specifies that data beyond the end of the last multicast address record is ignored, except for the purpose of checksum calculation (Section 5.2.11 of [5]).

### 6.2 MLD Query Messages

MLD Query Messages share the same, initial message format, having the same ICMPv6 code[4][5]. Therefore they have common format up until the end of the MLDv1 Query.

MLDv2 [5] specifies that the algorithm used to distinguish if a Query is v1 or v2 is to inspect the length of the Query and if it is greater than 22 octets, the message is an MLDv2 Query.

MLDv1 messages therefore may not have additional information placed at the end of them.

The additional room requirement in the MLD Query is to add fixed fields describing Query semantics and timing, as well as a specified number of multicast stream source addresses.

[5] specifies that data beyond the end of the base Query fields are ignored, except for the purpose of checksum calculation (Section 5.1.12 of [5]).

### 6.3 Multicast Router Solicitation Messages

Multicast Router Solicitation messages are used by switches to request Advertisement from multicast routers. There are no configuration related parameters in this 4 octet message, and no explicit delays required by responding routers. Responding routers are asked to rate limit response advertisements, though [6].

Recent discussion at IETF 59 on this message format seemed to agree that data after the end of a message should be ignored (although not for ICMPv6 checksums). In this case, the additional length would be implied by the length of the IP datagram minus the fixed message portion and IP headers.

### 6.4 Multicast Router Advertisement Messages

Multicast Router Advertisement Messages are defined with a common format in both IPv4 and IPv6. Within IPv6, the message belongs to the set of ICMPv6 messages (as do MLD messages), and have the same general checksum requirements.

The message itself is 8 octets long as defined in section 3.2 of [6], containing fixed fields for a checksum and the router's multicast advertisement interval. It also has fields for Query intervals and robustness variables derived from the router's multicast group management configuration.

No fields correlating between solicitation and advertisement are made, nor is there any indication of the freshness of the message (no sequence numbers or timestamps). Replay of previously received messages is therefore trivial if a malicious node is on the path.

Recent discussion at IETF 59 on this message format seemed to agree that data after the end of a message should be ignored (although not for ICMPv6 Checksums). In this case, the additional length would be implied by the length of the IP datagram minus the fixed message portion and IP headers.

### 6.5 Multicast Router Termination Messages

While Multicast Router Discovery currently defines a Terminate message, for Multicast Listener Discovery, Terminate messages are only used as explicit done messages in MLDv1 [4] and not MLDv2 [5].

No configuration related parameters exist for this 4 octet message.

Recent discussion at IETF 59 on this message format seemed to agree that data after the end of a message should be ignored (although not for ICMPv6 Checksums). In this case, the additional length would be implied by the length of the IP datagram minus the fixed message portion and IP headers.

### 6.6 Summary of Messages and formats

The IPv6 versions of all messages discussed provide some extra space at the end of the message except for MLDv1 queries.

If the room at the end of the message was used for security information such as a signature, freshness information and explicit identification of the signer, this may be used to provide some authenticity and traceability to the messaging.

Existing implementations would be able to read the messages, but not interpret the security information.

Due to the inability to add information to the MLDv1 Query, it may be impossible to provide any security for MLDv1 devices. Since this protocol is superceded by MLDv2, devices wishing to support security have a potential alternative though.

## 7. Comparisons to other Signalling Protocols

The development of other signalling protocols within the IETF may give some pointers as to pitfalls in the allocation of trust within multicast group management signalling, as well as indications of how

such mechanisms themselves' achieve more reliable security.

The following sections describe other signalling protocols and highlight relevant similarities to Multicast Group Management protocols such as MLD.

## 7.1 Routing Protocols

Original unicast routing protocol specifications for IPv4 such as the Routing Information Protocol allowed hosts to participate in routing decisions. In fact, some workstation implementations shipped with the RIP routing daemon switched on by default.

One of the basic issues with a system which allows hosts to make routing changes, is that it is both open to abuse and subject to changes in host status for routing changes.

Subsequent definitions of routing protocols and their discovery mechanisms have separated these functions. See the next two subsections for descriptions of such discovery mechanisms.

In the case that routers wish to ensure that routing infrastructure changes are not at the whim of attackers, it is either necessary to share a configuration which allows mutual authentication between routers, or segregates routing protocol decisions from access networks.

While Multicast Group Management segregates the roles of listening host from multicast router, hosts may still cause direct routing change through the addition or subtraction of groups on a link.

This may be used to cause rapid change within the routing topology, without traceability, in a manner which may be used to defeat existing routing protocol hysteresis mechanisms.

A secure multicast group management mechanism would be either be able to determine when an attack on the routing infrastructure is in operation, or prevent its effects on off-link devices.

## 7.2 Dynamic Host Configuration Protocols

Dynamic Host configuration protocol allows devices to receive link-specific configuration information, and routing configuration. Typically, this allows the host to receive and transmit unicast packets from an assigned IP address.

The router in this state, keeps track of information about the configuring host and its addresses. Numerous simultaneous attempts

at configuration may be used to exhaust resources (such as address pools).

Additionally, Dynamic Host Configuration protocol relays may not actually provide address allocation services themselves, and rely upon a central server elsewhere in the network[13][14]. This leads to the potential that local signalling (or co-ordinated local signalling) can be used to cause changes rapidly enough to impair the central server's operation.

This may be analogous to effects achievable in an unsecured multicast group management environment.

### 7.3 Neighbour Discovery

IPv6 Neighbour Discovery provides mechanisms by which nodes show their reachability and constructs unicast network layer to link-layer bindings, for the purposes of local packet delivery within a link.

Additionally, Router Discovery provides automatic configuration of default unicast routing, based on periodic advertisement to multicast link-local destinations[12].

Securing Neighbour Discovery is a protocol which provides authentication of Neighbour Discovery bindings for particular subclasses of unicast addresses, based on Cryptographically Generated Addresses[15].

All of the changes caused by Neighbour Discovery are local to the configuration state of hosts within the link, since the off-link IPv6 unicast routing topology is unchanged by Neighbour Discovery.

While this is the case, there is still some validity to the mechanisms employed by SEND to provide some authentication for routing discovery, where devices advertise not only their presence but their authorization to route.

It is notable that no proposal to handle secure proxying of neighbour discovery messages [9][15]. A similar mechanism would likely be needed for both SEND and multicast group management on proxies.

## 8. Comparisons to other Multicast Security Mechanisms

There has been a slew of work within the IRTF and IETF on multicast. Within the security domain, the work of GSAKMP and MSEC groups has been principally on managing access to the data content within a multicast data stream, rather than the routing updates to prevent actual flow reception[18].

In an environment where the presence of multicast flows and signalling cause resource exhaustion, the readability of the content stream doesn't particularly matter. In this case, it may be valuable to ensure that devices aren't allowed to request traffic without being traceable or accountable to the routing infrastructure.

## 9. Discussion of Possible Security Mechanisms

At this stage the level of interest in work on group management signalling security is minimal.

The existence of specifications to secure local delivery of IPv6 unicast packets though, indicates that at least it may be worth determining if similar security is desirable or applicable for multicast group membership management.

## 10. IANA Considerations

There are no IANA actions specified in this document.

## 11. Security Considerations

This document describes threat and trust models for multicast group management, primarily from the point of view of IPv6 Networks.

There may be inaccuracies in the described trust arrangements particularly in the case of IPv4. The Authors welcome any feedback which would clarify, correct or update such information.

## 12. Acknowledgments

## 13. References

### 13.1 Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[3] Cain, B., Deering, S., Kouvelas, I., Fenner, B. and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[4] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener

Discovery (MLD) for IPv6", RFC 2710, October 1999.

[5] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[6] Haberman, B. and J. Martin, "Multicast Router Discovery", draft-ietf-magma-mrdisc-00 (work in progress), February 2004.

[7] Fenner, B., He, H., Haberman, B. and H. Sandick, "IGMP/MLD-based Multicast Forwarding ('IGMP/MLD Proxying')", draft-ietf-magma-igmp-proxy-06 (work in progress), April 2004.

[8] Christensen, M., Kimball, K. and F. Solensky, "Considerations for IGMP and MLD Snooping Switches", draft-ietf-magma-snoop-11 (work in progress), May 2004.

### 13.2 Informative References

[9] Thaler, D. and M. Talwar, "Bridge-like Neighbor Discovery Proxies (ND Proxy)", draft-thaler-ipv6-ndproxy-02 (work in progress), February 2004.

[10] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[11] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[12] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[13] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[14] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[15] Arkko, J., Kempf, J., Sommerfeld, B., Zill, B. and P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ndopt-05 (work in progress), April 2004.

[16] Nikander, P., Kempf, J. and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[17] Loughney, J., "IPv6 Node Requirements", draft-ietf-ipv6-node-requirements-09 (work in progress), May 2004.

[18] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

## Authors' Addresses

Greg Daley
Centre for Telecommunications and Information Engineering
Department of Electrical adn Computer Systems Engineering
Monash University
Clayton, Victoria 3800
Australia

Phone: +61 3 9905 4655
EMail: greg.daley@eng.monash.edu.au

Gopi Kurup
Centre for Telecommunications and Information Engineering
Department of Electrical adn Computer Systems Engineering
Monash University
Clayton, Victoria 3800
Australia

Phone: +61 3 9905 XXXX
EMail: gopakumar.kurup@eng.monash.edu.au

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.