MIDCOM Working Group
Internet Draft
Document: draft-ietf-midcom-requirements-00.txt
Category: draft

R P Swale
BTexaCT
P A Mart
Marconi Communications
P Sijben
Lucent Technologies
Feb 2001

Requirements for the MIDCOM architecture and control language

Status of this Memo

Abstract

This document presents the requirements for the MIDCOM Architecture and the associated control language.

Table of Contents

1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

2. Definitions

Flow a sequence of IP packets communicated from one host and port to another host and port.

3. Requirements for the MIDCOM architecture

The MIDCOM architecture 8 elements are identified within the MIDCOM environment:

application client: An application client is a function resident on a host that represents the user of an application. It MAY require packet processing services to reach an application server where middleboxes are deployed in the network path.

application server: An application server is a function resident on a host that provides application functionality. It MAY require packet processing services to reach an application client where middleboxes are deployed in the network path.

MIDCOM Client: A MIDCOM Client is an entity that uses the MIDCOM protocol to request operations on a MIDCOM Packet Processor to enable specified end to end flows between application clients and/or servers.

MIDCOM Server: A MIDCOM Server terminates requests for the use of MIDCOM Packet Processing resources from a MIDCOM Client.

MIDCOM Agent (MA): A MIDCOM Agent is a server or stateful proxy that controls a MIDCOM Packet Processor to enable specified end to end flows between application clients and/or servers. A MIDCOM Agent SHALL be a trusted client for the MIDCOM protocol. A MIDCOM Agent MAY be either a MIDCOM Controller or a MIDCOM Application Gateway, depending upon its role.

MIDCOM Controller (MC): A MIDCOM Controller establishes trust and authorise requests for packet processing services. A MIDCOM Controller comprises a MIDCOM Client, a MIDCOM Server and an Authorisation function.

MIDCOM Application Gateway (MAG): A MIDCOM Application Gateway is a trusted MIDCOM Client that requests packet processing services from a MIDCOM Packet Processor in accordance with the needs of the application it supports.

MIDCOM Packet Processor (MPP): A MIDCOM Packet Processor is the kind of middlebox in the scope of MIDCOM. It forwards packets and manipulates the headers of IP packets as directed by a MIDCOM client.

Figure 1 shows how the various elements of the MIDCOM achitecture relate.

```
                            +---------------------------------------------+
 Policy description | +-----------+        +------------------+ |
 Language           \|  |           |        |                  | |
--------------------X |  Policy   \        /  authentication  | |
                    /|  |           |\     /|  server           | |
                     | +-----------+ \   / +------------------+ |
                     +---------------\++/------------------------+
                                      ||
                                      ||
 +-------------+ +------------------++---------------+ +----------
+
 |+----------+ | |MIDCOM Controller ||                | |middlebox
|
 ||          | | |+-------+  +-------++----+ +------+ | |+-------+
|
 ||client    +-+-++server +--+authorisation+-+client+-+-++server |
|
 ||          | | ||       |  |function     | |      | | ||       |
|
 |+----------+ | |+-------+  +-+---------+--+ +------+ | |+-------+
|
 |             | |            |         |             | |
|
 |+-----------+| |            |         |             | |
|
 ||credentials|| |+-----------+--+  +--+----------+  | |+--------+
|
 ||           ++-++client         |  |  credentials|--+-++client  |
|
 |+-----------+| ||authentication |  |             |  | ||authen- |
|
 |             | |+---------------+  +-------------+  | ||tication|
|
 |             | |                                    | |+--------+
|
 |+-----------+| +------------------------------------+ |
|
 ||           ||                                        |+---------
+|
 |application++----------------------------------------++Packet
||
 +-----------+|
||Processor||
 +-------------+                                        |+---------
+|
                                                        +-----------
+
```

Figure 1. Relationships between MIDCOM functions.

The remainder of this section declares requirements on each of the elements in the architecture.

3.1 MIDCOM Client

A MIDCOM Client SHALL have either a Trusted or an Un-trusted relationship with a MIDCOM Agent.

3.2 MIDCOM Server

A MIDCOM Server SHALL establish an appropriate level of trust with any MIDCOM Clients with which it communicates. This MAY include communication with un-trusted MIDCOM Clients if desired.

Where no trust relationship is maintained between a MIDCOM Client and Server, each request received by the MIDCOM Server SHALL be authorised, including any necessary authentication, before the MIDCOM Server takes any action on the request.

3.3 MIDCOM Controller (MC)

A MIDCOM Controller SHALL establish trust and authorise requests for packet processing services. A MIDCOM Controller comprises a MIDCOM Client, a MIDCOM Server and an Authorisation function.

Based upon the established identity of the requesting MIDCOM Client, the Authorisation function SHALL authorise the request based upon either local policies or policies from the MIDCOM Policy Server.

Where no trust relationship is maintained between a MIDCOM Client and MIDCOM Controller, each request received by the MIDCOM Controller SHALL be authorised, including any necessary authentication, before the MIDCOM Controller takes any action on the request.

3.4 MIDCOM Packet Processor (MPP)

A MIDCOM Packet Processor is a kind of middlebox within the scope of MIDCOM. It forwards packets and manipulates the headers of IP packets as directed by a MIDCOM client.

The MPP SHALL NOT alter packet information unless they appear in the packet header information

Other than the communication of control information between the controlled MIDCOM Packet Processor device and the MIDCOM Controller no packets will be allowed to flow across the MIDCOM Packet

Processor without prior instructions from the controller. i.e. the default operation is that "no packets will be allowed".

On receipt of a request to allow a flow with a particular flow specification the MIDCOM Packet Processor shall indicate whether or not available resources allow the flow to be carried.

The MPP MAY report the observed behaviour of a nominated flow.

The MPP SHALL report or otherwise make information available to the associated MIDCOM Client when a granted flow contravenes the parameters agreed. The MPP SHALL not permit the flow of any packets contravening a prior agreement.

The MIDCOM Packet Processor MAY provide QoS transport facilities for the packet flows. For example setting of DS-bytes, MPLS mappings

The MIDCOM Packet Processor acts as a MIDCOM Server and SHALL only accept requests from MIDCOM Clients with which it has a trust relationship.

The MIDCOM Packet Processor shall support multiple simultaneous MIDCOM clients. Each controller may be acting on behalf of one or more applications. No relationship between controllers MAY be assumed by the MIDCOM Packet Processor.

The MIDCOM Packet Processor shall support the forwarding of signalling received to one, or more, appropriate destination address/port combinations to the appropriate controllers, e.g. a MIDCOM Application Gateway.

3.5 MIDCOM Policy Server (MPS)

The MIDCOM architecture SHALL include a policy function. Its purpose SHALL be to determine the flows that MAY be supported across one or more MIDCOM Packet Processors.

3.6 Distribution of MIDCOM elements

It SHALL be possible for the functional components within the MIDCOM framework to be distributed.

4. General Requirements for the MIDCOM Control Language

4.1 MIDCOM Control Protocol Requirements

The MIDCOM Control Language SHALL be used between MIDCOM Clients and MIDCOM Servers.

The MIDCOM Control Language SHALL describe the desired behaviour of the MIDCOM Packet Processor for the purposes of a requested flow(s).

The syntax and semantics of the MIDCOM Control Language SHALL be independent of the application(s)requesting packet processing services.

The syntax and semantics of the MIDCOM Control Language SHALL be extensible.

The protocol SHALL support time-constrained operation. This may include, amongst other things, the use of short messages and minimal messages per operation.

The protocol SHALL NOT assume 0 (zero) delay in communication paths.

The protocol SHALL be capable of being used over low speed links.

The protocol SHALL provide per message acknowledgements, in order to achieve reliable communication.

The protocol SHALL support unsolicited messages, for event reporting and alarms.

The protocol SHALL permit the synchronisation of state machines between peer entities by adding state information to messages in normal operations or by the use of explicit query messages.

An operation SHALL be needed to permit a flow, with a given flow specification and address translation, across the MIDCOM Packet Processor. It shall be possible to indicate whether packets should be carried or discarded when a given flow specification is exceeded.

An operation SHALL be needed to stop a flow across the MIDCOM Packet Processor.

The protocol SHALL include the association of a "Packet modifier" to describe the required re- writing of header fields of accepted packets. The "Packet modifier" MUST be able to change the following protocol header fields

IPv4: IP addresses, TOS field

IPv6: IP addresses, traffic class field, flow label

UDP: port numbers

TCP: port numbers

Note that if modifiers are used then packet checksums MUST be recalculated.

The protocol SHALL allow for the capability to carry attributes from other protocols the MPP MAY support for the use by the MPP.

The protocol SHALL include failure reasons that allow the client behaviour to be modified as a result of the information contained in the reason. Failure reasons SHOULD be chosen such that they do not make an attack on security easier.

The protocol SHALL contain version inter-working capabilities. If a peer does not understand an option it must be clear whether the action required is to proceed without the unknown attribute being taken into account or the request is to be rejected. Where attributes MAY be ignored if not understood, a means MAY be provided to inform the client about what has been ignored. This MAY be provided as a version and capability exchange mechanism.

4.2 MIDCOM Authentication Protocol Requirements

4.2.1 MIDCOM Client Authentication Protocol Requirements

The MIDCOM Client Authentication Protocol SHALL be used between MIDCOM Controllers and MIDCOM Clients.

The MIDCOM Client Authentication Protocol SHALL describe the desired behaviour of the MIDCOM Packet Processor for the purposes of a requested flow(s).

The syntax and semantics of the MIDCOM Client Authentication Protocol SHALL be independent of the application(s)requesting packet processing services.

The syntax and semantics of the MIDCOM Client Authentication Protocol SHALL be extensible.

4.2.2 MIDCOM Authentication Server Protocol Requirements

The MIDCOM Authentication Server Protocol SHALL be used between MIDCOM Controllers and MIDCOM Authentication Servers.

The MIDCOM Authentication Server Protocol SHALL describe the desired behaviour of the MIDCOM Packet Processor for the purposes of a requested flow(s).

The syntax and semantics of the MIDCOM Authentication Server Protocol SHALL be independent of the application(s)requesting packet processing services.

The syntax and semantics of the MIDCOM Authentication Server Protocol SHALL be extensible.

4.3 MIDCOM Policy Protocol Requirements

The MIDCOM Policy Protocol SHALL be used between MIDCOM Agents and MIDCOM Policy Servers.

The MIDCOM Policy Protocol SHALL describe the desired behaviour of the MIDCOM Agent for the purposes authorising requested flow(s).

The syntax and semantics of the MIDCOM Policy Protocol SHALL be independent of the application(s)requesting packet processing services.

The syntax and semantics of the MIDCOM Policy Protocol SHALL be extensible.

5. Performance Requirements for the MIDCOM Architecture

To be done.....

6. MIDCOM Control Language Actions and Attributes

The following sub-sections present requirements that guide the choice of MIDCOM Protocol(s).

To be done.....

6.1 MIDCOM Control Action and Attribute Requirements

To be done.....

6.2 MIDCOM Authentication Action and Attribute Requirements

To be done.....

6.2.1 MIDCOM Client Authentication Action and Attribute Requirements

To be done.....

6.2.2 MIDCOM Authentication Server Action and Attribute Requirements

To be done.....

6.3 MIDCOM Policy Action and Attribute Requirements

To avoid accumulation of stale rules, in case of controller failures, rules MUST have an associated timer, which may be set using the MIDCOM Policy Protocol. If a timer value is not set a default value shall be used. The default value MUST be the same for all systems that are capable of direct interaction.

The timer associated with a rule SHALL be reset on request from the requesting client that established the rule.

The policies communicated SHALL permit rules to be specified in terms of:

For IPv4:	source and destination IP address or group of them determined by a netmask, protocol number, TOS field
IPv6:	source and destination IP address or group of them determined by a netmask, next header fields (Note that multiple fields may need to be traversed until a match is found.), traffic class field
UDP:	source and destination port numbers or group of them
TCP:	source and destination port numbers or group of them, "SYN packets" permission
ICMP:	type and code
IGMP:	type

The protocol SHALL permit the expression of direction to be associated with a rule. The direction SHALL be specified in terms that apply to the client's view of the packet processor. This directionality SHALL be expressed as "in", "out" or "Loopback" (meaning both "in" and "out" of the same side of the same controlled packet processor).

The protocol SHALL provide an ability to indicate desired rule-processing precedence to enable controlled devices to resolve conflicts between multiple applicable matching rules in a predictable manner.

Default precedence SHALL be assigned by the MIDCOM Policy Server when no precedence is specified for a rule. Multiple rules MAY share a single precedence.

The protocol SHALL permit specification of an "Action" for a rule. "Action" takes the values 'pass packets', 'drop packets with or without ICMP notification'.

The protocol SHALL include the association of a "Packet modifier" with a rule to describe the required re- writing of header fields of accepted packets. The "Packet modifier" MUST be able to change the following protocol header fields

IPv4: IP addresses, TOS field

IPv6: IP addresses, traffic class field

UDP: port numbers

TCP: port numbers

Note that if modifiers are used packet checksums MUST be recalculated.

7. Security Considerations

The MIDCOM architecture MUST enable a trust relationship to be established between a client and a MIDCOM Controller or middlebox for the purposes of permitting flows between the client and other hosts that flow via a MIDCOM Packet Processor.

In the trusted case, the trust is derived from some aspect of the session in which the trusted party is involved, for example the security association. In the untrusted case, trust is derived from the presentation and authentication of credentials that are offered for each request.

Peers using this protocol must be authenticated in order for message exchange to proceed.

Trust relationships within the MIDCOM architecture SHALL be explicitly established. Automatic discovery mechanisms shall not be permitted other than between mutually authenticated peers. This in order to prevent hacking into the MIDCOM Packet Processor by impersonating a controller.

The MIDCOM protocols SHALL permit strong encryption to be used to protect the privacy on requests and responses.

The MIDCOM protocols must allow for strong encryption to be used to protect the trustworthiness of the requests and responses. This in order to prevent hacking into the MIDCOM Packet Processor by intercepting communication.

8. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

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

9. Acknowledgements

Jiri Kuthan
Jonathan Rosenberg
Andrew Molitor
Pyda Srisuresh

10. Author's Addresses

Philip Mart
Marconi Communications Ltd.
Edge Lane
Liverpool
United Kingdom
Email: philip.mart@marconi.com

Paul Sijben
Lucent Technologies
EMEA BV
Huizen
Netherlands
Email: sijben@lucent.com

Richard Swale
BTexaCT
Adastral Park
Ipswich
United Kingdom
Email: richard.swale@bt.com