MIDCOM
Internet-Draft
Expires: February 9, 2005

M. Stiemerling
C. Cadar
NEC
S. Kiesel
UST/IKR
A. Mueller
August 11, 2004

SIMCO Protocol Implementation Interoperability Report
draft-stiemerling-midcom-simco-interop-00.txt

Status of this Memo

Copyright Notice

Abstract

This memo summarizes the results of the first interoperability event for the Simple Middlebox Control (SIMCO) protocol. SIMCO is an implementation of MIDCOM for controlling middleboxes, such as firewalls and NATs. The test scenarios are described and the results of each scenario for each implementation is given. Finally, enhancements to be made to the SIMCO protocol specification are

listed.

Table of Contents

1. Introduction

[3] defines a framework and an architecture for controlling middleboxes, such as firewalls and Network Address Translators (NATs). Requirements for a protocol for controlling middleboxes are defined by [4] and [2] specifies the semantics of such a protocol. The SIMCO protocol [1] complies with these specifications. It is a simple and efficient protocol exclusively designed for this purpose.

This memo describes test environment, scenarios and results of the first SIMCO interoperability testing event held on July 12th at University of Stuttgart. Participants were

- o University of Stuttgart, Institute of Communication Networks and Computer Engineering (UST/IKR)
- o NEC Network Laboratories Europe (NEC)

Section 2 of this memo describes the test environment and Section 3 specifies the scenarios for which interoperability was tested. At the event, feedback from implementers on the SIMCO protocol specification was received and it is summarized in Section 5.

2. Test Environment and Implementations

The used test network consisted out of a switched Fast Ethernet network dedicated to the SIMCO interoperability testing. Every computer was directly connected to the switch. Figure 1 shows the network configuration.

```
         +--------------+     +--------+     +--------------+
         |              |     |        |     |              |
         | SIMCO Client |-----| Switch |-----| SIMCO Server |
         |              |     |        |     |              |
         +--------------+     +--------+     +--------------+
                                   |
                                   |
                             +----------+
                             |          |
                             | Network  |
                             | Protocol |
                             | Analyzer |
                             |          |
                             +----------+
```

Figure 1: Interoperability Network Configuration

The implementations to be tested were based on draft-stiemerling-midcom-simco-05.txt.

UST/IKR's implementation is Linux based and implements SIMCO client and server. Firewalls as middleboxes are supported. PDR transaction, which is optional, is not implemented. NEC's implementation is FreeBSD based and implements SIMCO client and server. Firewalls and NATs as middleboxes are supported. PDR transaction, which is optional, is implemented.

Both implementations were connected via TCP during all tests, no TLS or IPsec was used. Wildcarding for address parameters was not tested in any test case.

3. Test Scenarios

This section describes all test scenarios and the corresponding results are described in Section 4.

3.1 Session Establishment without SIMCO Authentication

The SIMCO client is establishing a session by sending a SE request and is waiting for a SE positive reply. No SIMCO challenge response mechanism is used.

3.2 Session Termination

The SIMCO client is terminating an already established session by sending a ST request and is waiting for a ST positive reply. Afterwards the session must be terminated.

3.3 PRR with subsequent PEA and ARE

The SIMCO client is requesting a 'reserve' policy rule with PRR transaction and is waiting for a PRR positive reply. Afterwards the CLIENT sends a 'enable' policy rule after reservation with PEA request and is again waiting for a PEA positive reply. The policy rule's lifetime is not extended and the policy rule is not deleted by a client request, the clients is waiting for ARE notification send by the server, indicating the deletion of the policy rule.

3.4 PER with lifetime change, status request, and deletion

The SIMCO client is requesting a 'enable' policy rule by PER request and is waiting for the PER positive reply. Afterwards, the client is requesting a lifetime change PLC for a new lifetime of 200 seconds. A PL transaction follows this PLC, showing the prior installed policy rule. Finally, the client deletes the policy rule with a PLC and lifetime set to zero.

3.5 Policy list without policy rules loaded

The SIMCO client is requesting a policy rules list by PL request.

3.6 Disconnected operations

The SIMCO client requests two policy rules via PER request and after receiving the successful response it disconnects, meaning the termination of the SIMCO session, from the server by sending a ST request. After disconnecting, the client establishes again the session and requests a policy rule list by sending PL.

3.7 Requesting the policy rule’s status

The SIMCO client is requesting information about a prior installed policy rules by sending a PS request.

4. Test Results

This section gives the results of the interop event. The table shows three columns, the second shows the results for UST/IKR as server and NEC as client, the third one shows the results for UST/IKR as client and NEC as server.

Testcase	UST Server/NEC Client	UST Client/NEC Server
1	SUCCESS	SUCCESS
2	SUCCESS	SUCCESS
3	SUCCESS	SUCCESS
4	SUCCESS	SUCCESS
5	SUCCESS	SUCCESS
6	SUCCESS	SUCCESS
7	SUCCESS	SUCCESS

Figure 2: Test Result Table

5. Conclusions

This section summarizes the observations made by the implementors with respect to the SIMCO protocol sepcification:

1. Message type number:
   The differentiation between message types and sub-types needs to be clarified in the specification, since it is currently sometimes confusing.

2. Length of objects is unclear and sometimes wrong:
   The length of the header is measured as total length of the SIMCO packet, meaning that it is header plus payload. All other objects are measured as object data only, without counting the header. Further, some objects have wrong length values. SOLUTION: The length of header and objects should be noted in a unified way, either without header or with header included. The length values of each object must be checked.

3. Aggregated message type overview:
   It has been propose to give a table at the end of the document that summarizes all message types used.

4. Connection timeout for client:
   Currently, SIMCO specifies a server TCP connection timeout only. A TCP connection timeout for clients is not specified. SOLUTION: A TCP connection timeout value needs to be introduced and a value defined. Note that the server timeout feature was not tested and will be tested at the next interoperability event.

5. Definition of values for IP address version:
   In Section 4.3.8. "Address Tuple Attribute" IP version number is defined as 0x4 and 0x6 for IPv4 and IPv6. In Section 4.3.9. "PRR parameter set" IP version number is defined as 0x1 and 0x2 for IPv4 and IPv6. This difference is quite confusing and a remark was why not to unify them to a single meaning. SOLUTION: Unified notation for IPv4 and IPv6, for instance, 0x4 as IPv4 and 0x6 as IPv6.

The interoperability has shown that the MIDCOM semantics and the SIMCO protocol specification are technical sound and can be implemented by various parties without problems. Issues listed above are only minor issues to be solved within the SIMCO protocol specification and no changes to the MIDCOM semantics are needed.

6. Security Considerations

This memo documents the interoperability test results only and has not raised any new features for SIMCO. Therefore, no new security threads have been introduced.

7. Acknowledgments

We would like to thank UST/IKR for providing space and network equipment for interoperability testing and Juergen Quittek for his valuable comments.

8 Informative References

[1] Stiemerling, M., Quittek, J. and C. Cadar, "Simple Middlebox Configuration (SIMCO) Protocol Version 3.0", draft-stiemerling-midcom-simco-06.txt (work in progress), July 2004.

[2] Stiemerling, M., Quittek, J. and T. Taylor, "MIDCOM Protocol Semantics", draft-ietf-midcom-semantics-08.txt (work in progress), June 2004.

[3] Srisuresh, P., Kuthan, J., Rosenberg, J., Molitor, A. and A. Rayhan, "Middlebox communication architecture and framework", RFC 3303, August 2002.

[4] Swale, R., Mart, P., Sijben, P., Brim, S. and M. Shore, "Middlebox Communications (midcom) Protocol Requirements", RFC 3304, August 2002.

Authors' Addresses

Martin Stiemerling
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 6221 905 11 13
EMail: stiemerling@netlab.nec.de

Cristian Cadar
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 6221 905 11 21
EMail: cadar@netlab.nec.de

Sebastian Kiesel
University of Stuttgart, IKR
Pfaffenwaldring 47
Stuttgart 70569
Germany

Phone: +49 711 685 7992
EMail: kiesel@ikr.uni-stuttgart.de

Andreas Mueller

Germany

EMail: And.Mueller@gmx.de

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on−line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf−ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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