SNMP Security Protocols

James M. Galvin
Trusted Information Systems, Inc.

Keith McCloghrie
Hughes LAN Systems, Inc.

James R. Davin
MIT Laboratory for Computer Science

April 8, 1991

Contents

1 Status of this Memo 1

2 Acknowledgements 1

3 Introduction 1

3.1 Threats 3

3.2 Goals and Constraints 5

3.3 Security Services 6

3.4 Mechanisms 6

4 SNMP Party 7

5 SNMP MD4 Authentication Protocol 10

5.1 Generating a Message 13

5.2 Receiving a Message 14

6 SNMP DES Privacy Protocol 16

6.1 Generating a Message 17

6.2 Receiving a Message 18

7 Clock and Secret Distribution 19

7.1 Initial Configuration 21

7.2 Clock Distribution 24

7.3 Secret Distribution 25

7.4 Crash Recovery 28

8 Security Considerations **30**

8.1 Conformance 31

8.2 Protocol Correctness 32

8.2.1 Clock Monotonicity Mechanism 33

8.2.2 Data Integrity Mechanism 33

8.2.3 Data Origin Authentication Mechanism 33

8.2.4 Restricted Administration Mechanism 34

8.2.5 Ordered Delivery Mechanism 35

8.2.6 Message Timeliness Mechanism 36

8.2.7 Confidentiality Mechanism 36

1 Status of this Memo

This draft document will be submitted to the RFC editor as a protocol specification. Distribution of this memo is unlimited. Please send comments to the authors: James M. Galvin <galvin@tis.com>, Keith McCloghrie <kzm@hls.com>, and James R. Davin <jrd@ptt.lcs.mit.edu>.

2 Acknowledgements

3 Introduction

The Simple Network Management Protocol (SNMP) specification [1] allows for the protection of network management operations by a variety of security protocols. The SNMP administrative model described in [2] provides a framework for securing SNMP network management. In the context of that framework, this memo defines protocols to support the following three security services:

- data integrity,
- data origin authentication, and
- data confidentiality.

In the model described in [2], each *SNMP party* is, by definition, associated with a single *authentication protocol.* The authentication protocol provides a mechanism by which SNMP management communications transmitted by the party may be reliably identified as having originated from that party. The authentication protocol defined in this memo also reliably determines that the message received is the message that was sent.

Similarly, each *SNMP party* is, by definition, associated with a single *privacy protocol.* The privacy protocol provides a

mechanism by which SNMP management communications transmitted to said party are protected from disclosure. The privacy protocol in this memo specifies that only authenticated messages may be protected from disclosure.

These protocols are secure alternatives to the so-called "trivial" protocol defined in [1].

USE OF THE TRIVIAL PROTOCOL ALONE DOES NOT CONSTITUTE SECURE NETWORK MANAGEMENT. THEREFORE, A NETWORK MANAGEMENT SYSTEM THAT IMPLEMENTS ONLY THE TRIVIAL PROTOCOL IS NOT CONFORMANT TO THIS SPECIFICATION.

The *SNMP MD4 authentication protocol* is described in Section 5. It provides a data integrity service by having the originator compute a digest over an appropriate portion of a message and sending that digest to the recipient, with the message, for verification. The data origin authentication service is supported by prefixing the message with a secret value known only to the originator and recipient, prior to computing the digest. Thus, data integrity is supported explicitly while data origin authentication is supported implicitly in the verification of the digest.

The *SNMP DES privacy protocol* is described in Section 6. This protocol protects messages from disclosure by encrypting their contents according to a secret cryptographic key known only to the originator and recipient. The additional functionality afforded by this protocol is assumed to justify its additional computational cost.

The SNMP MD4 authentication protocol depends on the existence of loosely synchronized clocks between the originator and recipient of a message. Maintaining such clocks may be accomplished by a variety of strategies. Section 7.2 presents one such strategy that is particularly suited to the demands of SNMP network management.