Application Note AN2011-01

SNMPv3 Security Features

Ken Fodero

INTRODUCTION

The SEL ICON™ Integrated Communications Optical Network and network management software use traditional Simple Network Management Protocol (SNMP) to securely manage settings and access to the ICON network. The ICON is also capable of interacting with third-party SNMP management software products.

This application note provides information on how Simple Network Management Protocol Version 3 (SNMPv3) operates securely over a network connection. SNMPv3 over Ethernet or USB operates differently from traditional command line or web-based interfaces. This application note explains the secure flow of data between the network management software and the ICON. The ICON does not support command line or Hypertext Transfer Protocol (HTTP) web interface.

SNMPV3 SECURITY DESCRIPTION

All SNMPv3 messages are encrypted using either Data Encryption Standard (DES) or 128-bit Advanced Encryption Standard (AES). In addition to encryption, each message is also authenticated using either Message-Digest Algorithm 5 (MD5) or Secure Hash Algorithm 1 (SHA-1). The SNMPv3 standard requires MD5 with DES, while SHA-1 with 128-bit AES is optional. In the ICON, these are user-configurable options. The default setting for the ICON is 128-bit AES and SHA-1, which is the strongest combination of options.

The ICON supports up to 30 user accounts, each with its own unique username and passwords. Each account can also have a unique level of privileges at each node. For example, a user may have read and test privileges but not settings privileges. Each ICON node in the system has a list of authorized users, their passwords, and their access rights.

The following sections explain the process for each command or request for information between the user and the ICON node.

Authentication Process: Manager to ICON

Step 1. The session between the user and the SNMP manager starts when the user logs in to the management software using a username and password.

Step 2. The user enters a request or command to one or more of the nodes in the system. This is shown as "Get Data" in Figure 1. Each of these requests or commands is processed individually between the network management software and each node.

Step 3. The SNMP manager sends a "Discover SNMP Engine ID" request to the ICON node. The SNMP engine ID (SID) is unique for every ICON node.

Step 4. The ICON responds with its SID.

Step 5. The SNMP manager hashes the SID and the user password (PW) to create a localized password (LPW).

Step 6. The SNMP manager creates the get message (GM).

Step 7. The SNMP manager hashes the GM using the LPW, creating a Hash Message Authentication Code (HMAC) from the SNMP manager (S-HMAC).

Step 8. The SNMP manager sends the GM and S-HMAC to the ICON.

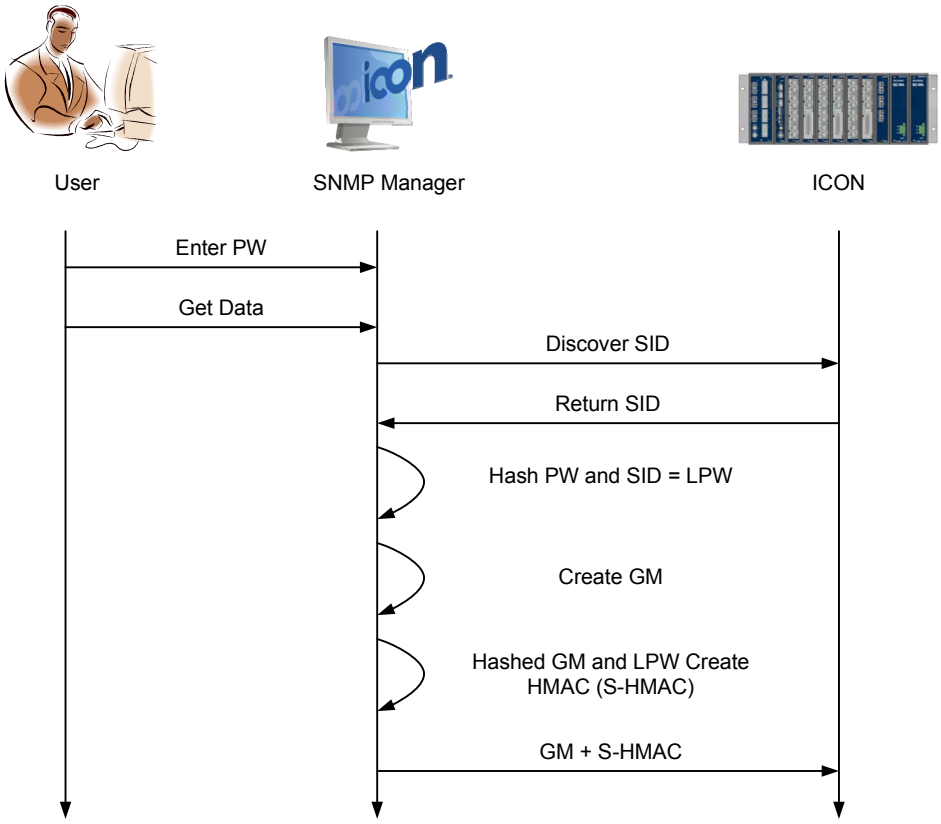

Figure 1 Authentication Process: Manager to ICON

Authentication Process: ICON to Manager

Step 1. The ICON receives the encrypted GM (GM + S-HMAC).

Step 2. The ICON hashes the GM and local stored password (SPW), creating an HMAC from the ICON (C-HMAC).

Step 3. The ICON compares the S-HMAC and the C-HMAC. If they match, authentication is confirmed. It is important to note that the user password is known by both devices and is never transmitted between the two.

Step 4. The ICON generates the response message (RM).

Step 5. The ICON hashes the RM using the SPW, creating a C-HMAC2.

Step 6. The ICON sends the encrypted RM back to the SNMP manager.

Step 7. The SNMP manager completes a similar authentication procedure and then pushes the data to the user or application. Each message is also time-synchronized to prevent replay attacks.

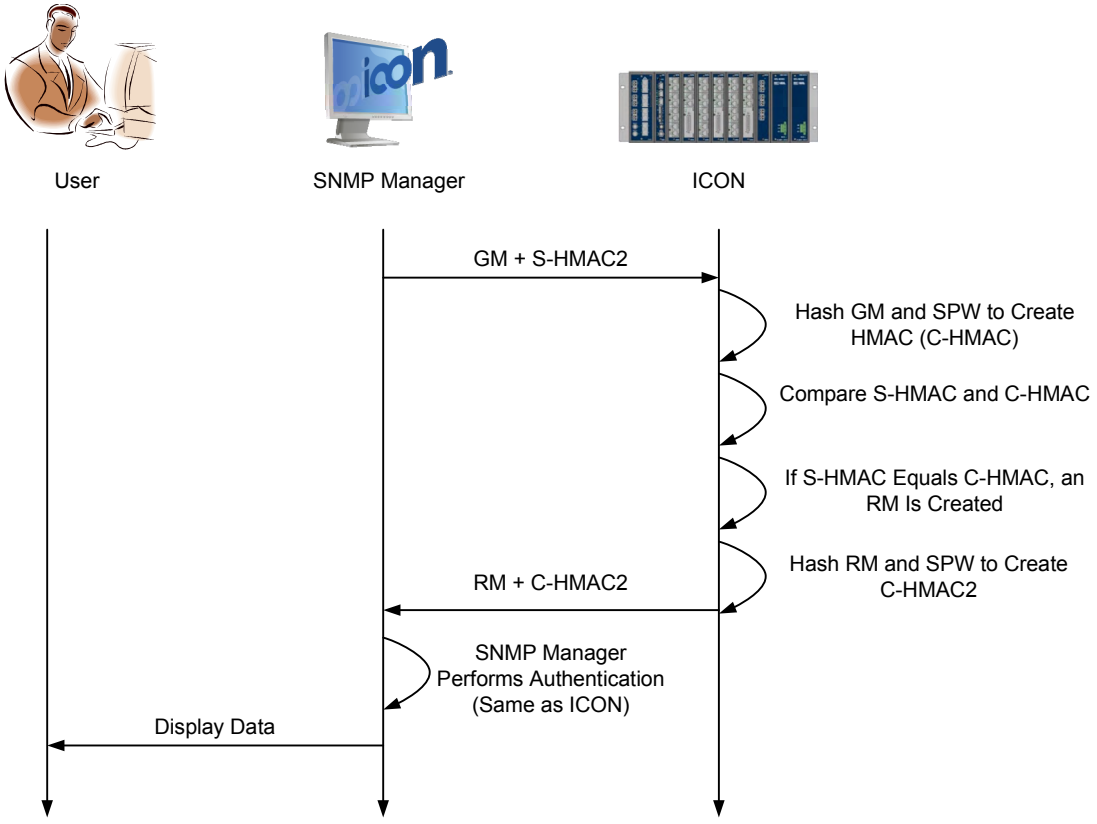

Figure 2 Authentication Process: ICON to Manager

LAN2011-01

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com