Network Management Card Security Implementation

OFFER AT A GLANCE

Offers Involved
Network Management Card, APC Security Wizard

Applications
Configuration and monitoring of network managed devices

Broad Customer Problem
Secure access to Network managed devices from Schneider Electric

CUSTOMER BENEFITS

• Compliance with Industry standard security level
• Secure access across multiple interfaces

SECURITY CERTIFICATION

• Certified TITANIUM level security 2012 by Tracesecurity™
• Assessment of Application with about 160 hours of testing

Abstract

This document highlights the industry-standard security implementation on the Network Management Card from Schneider Electric. The document should be used as a high-level overview of the Network Management Card functionality. More details on specific functionality can be referenced in the associated device's User Guide.

The described features apply to Network Management Cards, embedded in a network managed device or inserted into its SmartSlot, and running AOS version 2.x and above¹.

¹For how to identify the AOS version - Refer to Appendix A.

Make the most of your energy℠
Security Implementation Overview

The Network Management Card-based devices have four interfaces for remote configuration and control. Each of these interfaces has different methods of user authentication and data encryption. The interfaces are:

- Web (HTTP, HTTPS) interface
- Telnet, Secure SHeIl (SSH) interface
- File Transfer Protocol (FTP), Secure Copy (SCP) interface
- Simple Network Management Protocol (SNMP) interface

All devices produced by Schneider Electric that contain the Network Management platform have user authentication capabilities in the form of username and password. The user access can also be determined through the use of RADIUS. Additionally, the SNMP service fully supports SNMPv1 and SNMPv3. In addition to these features, the user has the ability to disable any or all interfaces, and can also change the standard access port on the Telnet/SSH, Web, FTP, Syslog interfaces.

To ensure that communication between the Schneider Electric device and the client interfaces cannot be interpreted in-stream, a greater level of security can be established by using one or more of the listed encryption algorithms. On the Network Management platform running AOS versions 2.x through 3.x, the user can select from a list of available encryption methods, with lower encryption complexity translating to faster information processing times. On the Network Management platform running AOS 5.x and above, all encryption is done through hardware and has no adverse effect on processing times.

Web Interface

SSL provides a secure mechanism to access a Web interface. The Network Management Card supports SSL version 3.0 and TLS version 1.0. Most Web browsers allow you to select the version of SSL to enable. When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen. Encryption methodologies supported by Schneider Electric devices are listed in Table 1 below.

Table 1 – SSL Security Options

<table>
<thead>
<tr>
<th>Encryption Algorithms</th>
<th>Public Key Algorithm</th>
<th>Message Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOS v2.x through AOS v3.x</td>
<td>56-bit DES</td>
<td>768- or 1024-bit RSA¹</td>
</tr>
<tr>
<td></td>
<td>168-bit 3DES</td>
<td>1024- or 2048-bit RSA²</td>
</tr>
<tr>
<td></td>
<td>128-bit RC4</td>
<td>1768-bit if generated by the Network Management Card; 1024-bit if generated by the APC Security Wizard</td>
</tr>
</tbody>
</table>

¹ 768-bit if generated by the Network Management Card; 1024-bit if generated by the APC Security Wizard
² 2048-bit if generated by the Network Management Card; 1024-bit or 2048-bit if generated by the APC Security Wizard
SSL Certificates for Server Authentication

There are many different methods of implementing specific security standards. Schneider Electric provides three different ways to manage certificates for SSL so that our products integrate with many different user environments. The Network Management Card devices allow you to:

- Use the Network Management Card auto-generated, unique default certificate
- Use the APC Security Wizard to create a Certificate Authority (CA) and server certificate
- Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate

Table 3 – SSH Security Parameters

<table>
<thead>
<tr>
<th>Encryption Algorithms</th>
<th>Public Key Algorithm</th>
<th>Message Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AOS v2.x through AOS v3.x</td>
<td>AOS v5.x and above</td>
</tr>
<tr>
<td>56-bit DES</td>
<td>768- or 1024-bit RSA¹</td>
<td>1024- or 2048-bit RSA²</td>
</tr>
<tr>
<td>128-bit Blowfish</td>
<td></td>
<td></td>
</tr>
<tr>
<td>168-bit 3DES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>128-bit AES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>256-bit AES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

¹ 768-bit if generated by the Network Management Card; 1024-bit if generated by the APC Security Wizard
² 2048-bit if generated by the Network Management Card; 1024-bit or 2048-bit if generated by the APC Security Wizard

Telnet Interface

SSH provides a secure mechanism for Telnet access. Various SSH clients that have been evaluated in conjunction with released products from Schneider Electric are listed in table 2 below. The corresponding SSH security parameters are listed in table 3 below.

FTP Interface

Secure Copy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords and files. SCP is automatically enabled when SSH is enabled, but FTP is not disabled automatically and should be disabled for secure applications. List of evaluated Schneider Electric SCP functionality with SSH clients are in table 4.

Table 2 – SSH Client Support Matrix SSH Security Parameters

<table>
<thead>
<tr>
<th>Client</th>
<th>Version 1</th>
<th>Version 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSSH</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PuTTY</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>F-Secure SSH Client</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SSH Secure Shell</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SecureCRT</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>TTSSH</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Key: ✓ = supported x = not supported

Table 4 – List of evaluated Schneider Electric SCP functionality with SSH clients
Table 4 – SCP Client Support Matrix

<table>
<thead>
<tr>
<th>Client</th>
<th>Version 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSSH</td>
<td>✓</td>
</tr>
<tr>
<td>PuTTY</td>
<td>✓</td>
</tr>
<tr>
<td>F-Secure SSH Client</td>
<td>✓</td>
</tr>
<tr>
<td>SSH Secure Shell</td>
<td>✓</td>
</tr>
<tr>
<td>SecureCRT</td>
<td>✗</td>
</tr>
<tr>
<td>TTSSH</td>
<td>✗</td>
</tr>
</tbody>
</table>

Key: ✓ = supported  ✗ = not supported

**SNMP Interface**

SNMPv1, SNMPv2 and SNMPv3 are supported on all Network Management platform devices.

SNMPv1 does not support encryption, but supports loose authentication in the form of community names and network management system (NMS) IP filtering.

SNMPv2 introduces new message formats incompatible with SNMPv1. New party based security system in SNMPv2 is not widely accepted and is not supported by Network Management platform devices. Of the options provided, SNMPv3 configuration is to be enabled in order to use SNMPv2.

SNMPv3 is more secure. It allows for authentication of traffic, prevents packet replay by utilizing engine time and system boot counts, and encrypts the payload of the packets (if desired). SNMPv3 is fully supported on platform running AOS v3.x and above.

**SMTP Interface**

In network management cards running AOS 6.0.6 or above, SMTP supports SSL/TLS encryption, for secure email.

**Conclusion**

The landscape of network security continues to grow and change in the fast paced IT industry. User requirements for security solutions are becoming a requirement for system delivery. The interfaces are implemented to allow user as much flexibility as possible. Industry standard security implementation coupled with flexibility of the Network Management Card enables products to exist in different user environments.
Appendix A

How to identify the AOS version of the Network Management Card firmware?

The Network Management Card is browser and command line interface accessible.

The 2 distinct browser interfaces that the user would experience based on the AOS version of the Network Management Card firmware are as below,

**User Interface 1**

In case of User Interface 1, please follow the below steps to identify the AOS version of the Network Management Card firmware,

- Navigate to the Network Management Card IP using a browser supporting HTTP protocol
- Login using the default user name & password (in case its not changed, else use the modified user name & password)
- Navigate to Administration -> General -> About
- AOS version is listed in the APC OS (AOS) section.
User Interface 2

In case of User Interface 2, please follow the below steps to identify the AOS version of the Network Management Card firmware,

- Navigate to the Network Management Card IP using a browser supporting HTTP protocol
- Login using the default user name & password (in case its not changed, else use the modified user name & password)
- Navigate to About -> Network
- AOS version is listed in the APC OS (AOS) section.
Command Line Interface

In case of Command line interface, please follow the below steps to identify the AOS version of the Network Management Card firmware,

- Login using the default user name (with either administrator or device level access) & password (in case its not changed, else use the modified user name & password)
- Execute “about” command at the prompt
- AOS version is listed in the APC OS (AOS) section.