

Security Features of APC's NetBotz Appliances

By Peter Kokolski

Abstract

APC's NetBotz appliances provide environmental and security monitoring. Many customers have questions concerning the safety and privacy of the data collected by these appliances. This paper outlines the security features of the NetBotz appliances which ensure the security and privacy of the information collected and monitored.

Introduction

All NetBotz appliances utilize both authentication and encryption services to ensure the security and privacy of the information collected and monitored. When securing a digital system, both authentication and encryption must be used together to ensure both the security and privacy of the transacted data. Authentication is defined as the process of verifying the identity of a user or system. Encryption is defined as the process of putting data into a secret code / format so that it is unreadable by everyone except its intended recipients. Using both in concert assure the data is being protected by industry standard methods used around the world to secure sensitive data.

Authentication

The NetBotz appliances utilize HTTP Basic Authentication based on a user ID and password to enable users and administrators to login to the device via the Basic View or Advanced View user interfaces. HTTP stands for HyperText Transfer protocol. This is a widely used authentication process defined in the HTTP protocol itself. User ID and passwords used for the authentication by the Advanced View and Basic View are stored on the NetBotz appliances themselves. Default configuration of the appliances requires users who wish to view or retrieve information from the NetBotz appliance to log into the appliance with the correct User ID and password. Once authenticated, there are five tiered privilege levels that can be associated with User IDs defined on NetBotz appliances, as indicated by the chart below.

Privilege Level	Capabilities
Administrator	Gives user access to all information and configuration tasks available on the appliance.
Application (with Alert Update)	Gives user access to only the Navigation, Sensor Data and selected portions of the Information / Action panes. User accounts configured with the Application Privilege Set can view the Camera, Graphs, Alerts, and About panes. The user can also resolve alert conditions for thresholds that have been configured with the Return-To-Normal Requires User Input setting in their Advanced Settings. However, this Privilege Set does not permit access to the Configuration pane.
Application	Gives user access to only the Navigation, Sensor Data and selected portions of the Information / Action panes. User accounts configured with the Application Privilege Set can view the Camera, Graphs, Alerts, and About panes. However, this Privilege Set does not permit access to the Configuration pane and the user cannot resolve alert conditions for thresholds that have been configured with the Return-To-Normal Requires User Input setting in their Advanced Settings.
Sensor	Gives user access to only the Navigation, Sensor Data and selected portions of the Information / Action panes. User accounts configured with the Sensor Privilege Set can view the Camera, Graphs, and About panes. However, this Privilege Set does not permit access to the Alerts or Configuration panes.
Sensor (No Camera)	Gives user access to only the Navigation, Sensor Data and selected portions of the Information / Action panes. User accounts configured with the Sensor (No Camera) Privilege Set can view the Graphs and About panes. However, this Privilege Set does not permit access to the Cameras, Alerts, or Configuration panes.

The HTTP Basic Authentication is utilized by both HTTP and HTTPS protocols. HTTPS stands for HyperText Transfer Protocol Secure. In a security conscience environment, HTTP Basic Authentication should not be used with the HTTP protocol. When HTTP Basic Authentication is used with the HTTP protocol, all information passed between the Advanced View and Basic View (including user IDs and passwords) and the appliance is sent as clear text. When HTTP Basic Authentication is used with HTTPS protocol, all information passed between the Advanced View and Basic View (including all user IDs and passwords) is encrypted and secure.

NOTE: Authentication alone does not secure the NetBotz appliance. Authentication only ensures that the user is entitled to access the appliance. To ensure the greatest level of security, authentication should always be used with high level encryption, such as that available on the NetBotz appliance.

Encryption

The NetBotz appliances utilize Secure Socket Layer (SSL) to encrypt communications to and from the Basic View and Advanced View. By default the appliance is configured with TCP/IP ports 80 and 443 open and usable for this transacted data. Port 80 is by default used for non-encrypted HTTP protocol traffic. Port 443 is by default used for encrypted HTTPS protocol traffic. The HTTP and HTTPS ports can be disabled as well as the port number may be changed per customer requirements to provide custom configurations or as an additional security provision.

NOTE: Encryption alone does not secure the NetBotz appliance. Encryption should always be used in conjunction with authentication to ensure the greatest level of security, such as that available on the NetBotz appliance.

Secure Socket Layer (SSL)

Overview

SSL is a protocol that is used to securely exchange information between a server and a client. SSL is a widely used and highly accepted solution for securing transactions over TCP/IP. SSL is NOT an encryption algorithm; it is a transaction based protocol for exchanging data securely. SSL supports multiple types of ciphers or encryption algorithms that are utilized to encrypt the data.

How It Works

SSL uses public-key encryption to exchange a session key between the client and server. In the case of the NetBotz appliance, the key exchange occurs between the Advanced View or Basic View and the appliance itself. This session key is used to encrypt the HTTP transaction (both request and response). The length of the keys used by SSL may vary. However, most security experts agree that any key length less than 128 bits is not secure. Each transaction uses a different session key so that even if someone did manage to decrypt a transaction that would not mean that they would have found the server's secret key. This means that if they wanted to decrypt another transaction, they'd need to spend as much time and effort on the second transaction as they did on the first.

SSL Certificates

SSL also utilizes the concept of Certificates to prove server validity. An SSL Certificate is analogous to a digital identification card. SSL Certificates are digitally signed and trusted. SSL protocol incorporates a facility for validating SSL Certificates to ensure that the server in question really is who it says it is. There are two types of SSL Certificates:

- Signed certificates which are signed by a trusted third party Certificate Authority (CA) such as Verisign or Thawte. These signed certificates or “real certificates” allow the SSL protocol to test the validity of the certificate.
- Self-signed certificates are NOT signed by a trusted Certificate Authority. Self-signed certificates do not “authenticate” that the server is who it says it is.

NOTE: The type of certificate or certification authority (if any) does not affect encryption of the data. The difference between the signed and unsigned certificates is the fact that the server can not be verified against its certificate since it was not signed by a trusted Certificate Authority. In other words, the client system can not authenticate that the server system is who it says it is. The purpose of the SSL Certificates is to provide a way for a server system to prove its identity to a client system.

Ciphers and Keys

Ciphers or encryption algorithms are the mathematical routines used to transform data in order to conceal its meaning. There are various types of ciphers available. SSL itself is not a cipher, but uses ciphers to perform encryption. SSL has the capability and flexibility to use many different types of ciphers. Some ciphers are more secure than others and a discussion of the relative strength of various encryption techniques is beyond the scope of this application note. Ciphers have many characteristics to differentiate themselves such as security, speed, efficiency, and required system resources. Some of the more commonly used ciphers used by SSL are:

- RC4
- RC2
- Triple DES
- DES
- AES

When an SSL client establishes a session with an SSL server, during the session initiation the client and server determine the highest level or most secure cipher supported by both systems, and then utilize that cipher from that point forward. The key used to encrypt the data is an important factor in the “strength” of the encryption along with the algorithm itself. The longer the key, the more difficult it is to “crack” the encryption, or in other words, to determine the correct mathematical key required to decrypt the data. The key length determines the number of possible key combinations. For example:

- 16 bit keys have 65536 or 2^{16} possible key combinations
- 128 bit keys have 339,000,000,000,000,000,000,000,000,000 or 2^{128} possible key combinations

Uses of SSL

The NetBotz appliances utilize SSL transactions in a variety of ways:

- Interactive communications with the NetBotz appliance via the Basic View or Advanced View can be handled entirely by an SSL connection (HTTPS)
- Interactive communications from the NetBotz appliance and the Infrastructure Central management platform can be handled entirely by an SSL connection (HTTPS)
- Alert actions and periodic report information sent from the appliance can utilize SSL as well. The following actions are capable of using SSL:
 - HTTP Post alert action
 - Email alert action (primary, secondary, and short messages)
 - Periodic reports sent via email and HTTP Post

- SNMP V3 Informational Message

Simple Network Management Protocol (SNMP)

SNMP is a protocol that is available on NetBotz appliance that allows the appliance itself to be monitored and controlled via SNMP commands such as GET, SET, and TRAP. Further, information and warning messages can be sent to devices that are expecting such information, such as InfrastruXure Central[®], where active management and event processing can occur on a near real time basis. Note that SNMP itself does not define what variables are available for management. This information is provided for in a Management Information Base (MIB) which describes the NetBotz appliance in a way that SNMP can be utilized.

Today, there are multiple versions of SNMP. Each subsequent version is an evolution of the former. As of this writing, SNMP v1, v2 and v3 exist. For practical purposes of this application note, only version 1 and version 3 are relevant to the NetBotz appliance. Further, while there are many differences between the versions of protocol that can be explored via the relevant standards, the germane point to take away is that SNMP v1 transmits information in clear text, and SNMP v3 has the ability to securely transmit the information.

Both versions of SNMP are available on all NetBotz devices and are configurable via Advanced View. SNMP v3 should be utilized in all cases to assure secure transfer of any data.

Frequently Asked Questions (FAQ)

Q1. Can communications to and from the NetBotz appliance be fully secured with high level encryption?

A1. Yes. However, some alert actions and periodic report capabilities do NOT utilize SSL such as SNMP Traps and FTP transfers. These would have to be disabled as well as disabling standard HTTP requests. Note, however that SNMP v3 does allow for secure transaction of data.

Q2. What is the maximum strength of the cryptography algorithms used by the NetBotz appliance?

A2. The NetBotz appliances utilize OpenSSL (open source SSL technology) for all SSL transactions. The maximum strength cryptography algorithm utilized by the OpenSSL is 256 bit, yet offers a wide variety of ciphers, hashes, and public key cryptography.

Q3. Is my SNMP traffic secure?

A3. If the SNMP v1 protocol is utilized for traffic, similar to HTTP, any network traffic is transferred in clear text. However, if SNMP v3 is used, and the security features of that protocol are correctly configured on your network, it does provide secure transfer of data.

Q4. Are the NetBotz appliances vulnerable to internet viruses and worms?

A4. Most viruses and worms are targeted at the Windows operating system. The NetBotz appliance runs Linux, making it immune to these types of Windows viruses. However, all relevant precautions should be taken to protect both the physical assets, and their data transmission from unauthorized access.

Q5. How are the NetBotz appliances secured against hacking?

A5. The NetBotz appliance TCP/IP ports can be configured to use only port 443 for encrypted SSL (HTTPS) traffic. All other ports and daemons can be disabled. Further, the NetBotz appliances can be configured to deliver alerts via alert actions that only use SSL to ensure the security of the information.

About the Author:

Peter Kokolski is the director of engineering for embedded technologies in the data center solutions group at APC by Schneider Electric. Peter is a 17 year veteran of the electronics industry and has worked in commercial, semiconductor, medical and military fields as an engineer and consultant. He received his Bachelor's degree in Electrical Engineering from Northeastern University in 1991, and is completing his JD coursework currently at Concord University School of Law. Peter is a member in good standing of IEEE and ASTQB.