TECHNICAL NOTE

REFERENCE DOCUMENT

Improving Security for Axis Products

Created: 4 October 2007

Last updated: 15 May 2009

Rev: 1.1

TABLE OF CONTENTS

1 Introduction

This technical note provides the following security information to assist you in reducing the risk of unauthorized access to your Axis products:

- Best-practice security policies
- General security features of Axis products
- Wireless network security

It is also a good idea to routinely check the support page for your Axis product for information about firmware releases that contain the latest security updates.

Using the security features of network video products should also be seen in a wider scope. This includes the definition of procedures as to how and by whom the surveillance system should be used, and what physical protection of the surveillance system is to be used. And, most importantly, it is vital to constantly monitor the effectiveness of these procedures.

2 Best-Practice Security Policies

Follow the steps below to reduce the risk of unauthorized access to your Axis products:

- Use only one window in your Internet browser, and do not use tabbed browsing.
- When you are finished using your Axis product, close your Internet browser.
- Do not save any passwords or user names in your Internet browser. For example, do not use **AutoComplete** in Internet Explorer, and delete **Form data** and **Passwords** under **Tools** > **General** > **Browsing history** > **Delete**.
- Use different user credentials for each Axis product.
- Use strong passwords.
- Use notification functionalities from H/W switches and software applications to send an alarm when video products are disconnected.
- If a camera gets disconnected from the network, check all configuration information, passwords, encryption keys, etc. that were in the camera. An intruder could access this information.
- Deactivate all protocols that you do not use.

The US-CERT also encourages users to implement the following best-practice security policies to reduce the risk of cross-site scripting vulnerabilities:

- Do not save passwords for the affected devices.
- Use NoScript to allow only trusted sites to execute JavaScript.
- Restrict device access to only private, trusted networks.
- Do not navigate to other websites while logged into the device.
- Filter known cross-site scripting vulnerabilities with an application firewall, intrusion prevention system or reverse proxy.

3 General Security Features of Axis Products

Most Axis products include support for one or more of the following security features. For specific information about your Axis product, please visit http://www.axis.com/ .

3.1 IP Address Filtering

Using IP Address Filtering provides a function similar to using a built in firewall. Once enabled, the IP addresses you enter into the list can be allowed or denied access to your product according to the choice made in the drop-down list **Allow/Deny the following IP addresses**.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses). The users from these IP addresses need to be specified in the user list with the appropriate access rights. This is done from **Setup** > **System Options** > **Security** > **Users**.

3.2 Virtual Private Network (VPN)

An alternative that is even more secure than IP Address Filtering is using a Virtual Private Network (VPN). A VPN uses an encryption protocol to provide a secure tunnel between networks through which data can more safely travel. A VPN provides secure communication across a public network, such as the Internet, because only devices with the correct “key” will be able to work within the VPN itself.

A VPN typically encrypts the packets on the IP or TCP/UDP layers and above. The IP Security Protocol (IPSec) is the most commonly used VPN encryption protocol.

3.3 HTTPS

Enable HTTPS to protect your Axis product from eavesdroppers and man-in-the-middle attacks. Hyper Text Transfer Protocol Secure (HTTPS) is the most common data encryption protocol used in applications like online banking to provide the requisite security for financial transactions performed over the Internet. HTTPS is identical to HTTP, but with one key difference: the data transferred is encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). A higher level of privacy is achieved through encrypting data rather than the transport. Follow the instructions under **System Options** > **HTTPS**.

We recommend that for protection against man-in-the-middle attacks, that you create a request for a certificate from a Certificate Authority (CA) **System Options** > **HTTPS** > **Create & Install** > **Create Certificate Request...**.

A **self-signed certificate** can be used until a Certificate Authority-issued certificate has been obtained. Click the **Create self-signed Certificate** button to install a self-signed certificate. Although self-signed certificates are free and offer some protection, true security will only be implemented after the installation of a signed certificate issued by a certificate authority.

A signed certificate can be obtained from an issuing Certificate Authority by clicking the **Create Certificate Request** button. When the signed certificate is returned, click the **Install signed certificate** button to import the certificate. The properties of any certificate request currently resident in the camera or installed can also be viewed by clicking the **Properties...** button. The HTTPS Connection Policy must also be set in the drop-down lists to enable HTTPS in the camera. Additional setup information is also available from the product’s online help pages.

3.4 Digest Authentication

Basically, HTTP authentication user credentials are sent in plain text. It is, therefore, possible to find out the password that was used through network tracing. With HTTP digest access authentication it is possible to establish user identity more securely since not the password itself is sent over the network but an encrypted string.

It is recommended to use digest authentication when HTTPS cannot be used. Basic authentication should only be used in non-critical applications.

The type of authentication to be used is configured in **Setup > Basic Configuration > Users**. Choose encrypted passwords in HTTP/RTSP Password Settings.

3.5 IEEE 802.1x

IEEE 802.1x is an IEEE standard for port-based Network Admission Control. It provides authentication to devices attached to a network port (wired or wireless), establishing a point-to-point connection. If authentication fails, access is prevented on that port. 802.1x is based on EAP (Extensible Authentication Protocol).

In an 802.1x enabled network switch, clients equipped with the correct software can be authenticated and allowed or denied network access at the Ethernet level.

Clients and servers in an 802.1x network may need to authenticate each other by some means. In the Axis implementation, this is done with the help of digital certificates provided by a Certification Authority. These are then validated by a third-party entity, such as a RADIUS server, examples of which are Free Radius and Microsoft Internet Authentication Service.

To perform the authentication, the RADIUS server uses various EAP methods/protocols, of which there are many. The one used in the Axis implementation is EAP-TLS (EAP-Transport Layer Security).

The Axis product presents its certificate to the network switch, which in turn forwards this to the RADIUS server. The RADIUS server validates or rejects the certificate and responds to the switch, and sends its own certificate to the client for validation. The switch then allows or denies network access accordingly, on a pre-configured port.

4 Wireless Network Security

Axis strives to provide the highest level of security and continual improvement for all its products including its wireless products. But wireless products, and wireless networks in general, are more vulnerable than wired networks and products.

So if a wireless network is to be used, you need to understand what its vulnerabilities are, and take precautions to make your wireless network and your wireless Axis products as secure as possible.

4.1 Protocol and Physical Layer Attacks

First, wireless products using the IEEE 802.11 standard are susceptible to DoS attacks using weaknesses in the IEEE 802.11 standard and any wireless system.

In other words, someone with the right software and hardware can disconnect your wireless product from the network and keep it off-line by abusing the IEEE 802.11 control and management mechanisms, or by flooding the IEEE 802.11 channel with traffic.

Currently, there is no way to prevent these kinds of attacks on wireless products if they are located on an external network. But, it is possible to detect and receive notification of a DoS attack by deploying systems to monitor IEEE 802.11 traffic for rogue management and control traffic or traffic flooding.

4.2 Wireless Interception and Substitution

Secondly, it is also possible to intercept the information a wireless product sends across the network and even substitute false information in its place. Someone can gain unauthorized access to the video stream of your wireless product, and they can even substitute a false image in its place. But the risk of interception and substitution can be reduced if you take security precautions such as using WPA.

4.3 WPA and WEP

Axis wireless products have one or more of the following security options:

- WPA-/WPA2-PSK
- WPA-/WPA2-Enterprise
- WEP

WPA-/WPA2-Enterprise is more secure than WPA-/WPA2-PSK, which in turn is more secure than WEP. For detailed instructions for setting up Wireless security in your Axis product, refer to its *Installation Guide*.

4.3.1 WPA-/WPA2-PSK (Wi-Fi Protected Access - Pre-Shared Key)

If your Axis wireless product can use WPA-/WPA2-PSK, one effective way to make it more secure is to enable WPA and set a good passkey. Do not set your wireless product to **No security** or **WEP**. Instead, set your wireless Axis product to **Basic Configuration > Wireless > WPA**, or **System Options > Network > Wireless > WPA**. Your Axis product will then use a pre-shared key (PSK) to initiate WPA security. The pre-shared key is entered on the access point and on each device on the wireless network. The key can be entered either as Manual hex, as 64 hexadecimal (0-9, A-F) characters, or as a passphrase, using 25 to 63 ASCII characters. The access point keeps out unauthorized users by requiring the key for communication.

4.3.1.1 WPA and Passphrases

It is important to set a good passphrase or key. When you have set your wireless product to **WPA**, the **Passphrase:** field will appear. Do not enter a short easy to guess passphrase, especially any kind of name or word that could be looked up in a dictionary.

Instead, although the standard is to use a passphrase that is 8 to 63 characters, Axis recommends that you use a passphrase that is at least 25 to 63 characters. It should include both small and capital letters, and numbers. If you need help, there are online, freeware and shareware programs that will help you generate a long difficult to guess passphrase. Another good resource is www.diceware.com.

4.3.2 WPA-/WPA2-Enterprise (Wi-Fi Protected Access - Enterprise)

WPA-/WPA2-Enterprise is a security method that provides strong data protection for multiple users and large networks. It uses the 802.1X authentication framework with TKIP or AES encryption. Network users trying to gain access are verified through an authentication server.

4.3.2.1 Certificates

The client and server authenticate each other using digital certificates provided by a Certificate Authority. To gain access to the protected network, your wireless Axis product t presents its certificate to the network switch. If the certificate is approved, the switch allows access. You may need to contact your network administrator for information on certificates, user IDs and passwords. See 3.3 for more information about certificates.

4.3.3 WEP (Wired Equivalent Protection)

The original security standard used in wireless networks that provides a minimal level of security that can deter minor trespasses. While this standard is available for your wireless products, we still recommend that you use WPA for greater security.