Cambium Networks™

Security in HCMP

INTRODUCTION

Information security failures are regularly in the news, with stolen information used to defraud or blackmail victims, to gain unfair advantages through industrial espionage, to influence political processes at home or in foreign countries, to embarrass or discredit individuals, or as the basis of sensational or intrusive media coverage. Furthermore, there is good reason to believe that the most successful attacks are not widely reported, since high-profile victims have little to gain by advertising vulnerabilities. The failures we know about are probably just the tip of the cyber-attack iceberg.

Cambium Networks takes a special interest in the wireless part of our customers' networks. Wireless technology has many of the same security issues as other data networking products, but faces some unique challenges. An attacker attempting to connect an unauthorized device to a wireless network, or simply to monitor wireless data traffic, could be at an unknown location anywhere within range of the wireless network. Attacks on wireless systems can be mounted without needing physical access to a rack or a cable duct.

Our existing PTP 650, PTP 670 and PTP 700 products, provide effective defense against cyber-attacks on the wireless link using optional FIPS-validated 128-bit and 256-bit AES encryption in hardware. The AES encryption ensures that unauthorized devices cannot be connected to the network, and ensures that attackers cannot decipher any data intercepted from wireless transmissions. Further, the use of an AES stream cipher at the wireless interface prevents an attacker from discovering details of the network (for example IP or Ethernet MAC addresses) or even from finding out if the link is actually carrying data traffic.

In this White Paper, we describe how we have delivered world-class wireless security in High Capacity Multipoint (HCMP) applications of PTP 670, with a choice of security models that minimize the impact of configuring for secure operation. All PTP 670 users benefit from this development, because the same security features are also available in the traditional PTP applications using PTP 670.

SECURITY OPTIONS FOR HIGH-CAPACITY MULTIPOINT

PTP 670 and PTP 700 can be used to create point-to-multipoint wireless sectors using HCMP with up to eight slave outdoor units (ODU) connected to one master ODU. The HCMP sector effectively operates like a number of point-to-point (PTP) links in a star topology, sharing a single channel.

While developing HCMP, we considered extending the existing security solution for HCMP by using a single AES encryption key for all of the ODUs in a sector. We rejected this option because compromise of one Slave ODU undermines the security of the remaining Slave ODUs. We also considered using a different AES key for each link so that the Master ODU must be configured with up to eight different 128-bit or 256-bit keys. We rejected this second option because an operator should not have to enter eight 32-character hexadecimal strings, particularly if that operator has a security policy that mandates monthly key changes.

We were conscious that the existing design requires a re-start in the ODUs to activate a new encryption key, and while this might be tolerable in a PTP link, it would be far from convenient in an HCMP sector with multiple ODUs.

AUTHENTICATION, AUTHORIZATION AND ENCRYPTION

Authentication refers to how an ODU securely verifies the identity of the remote unit that is attempting connection.

Authorization refers to the process of confirmation that the remote unit with the authenticated identity is actually one that the operator will allow to connect. For example, a genuine ODU might be authenticated (because it legitimately is the unit with the MAC address that it claims to have), but not be authorized (because it is not in the operator's inventory, or not part of the sector).

Encryption refers to how traffic in the wireless link is protected against eavesdropping.

ENCRYPTION ALGORITHMS IN HCMP

The wireless security solution for HCMP has to provide authentication, authorization and encryption with the minimum of configuration. Effective security generally includes some element of inconvenience, and wireless security in HCMP is no exception, so inevitably there is some work for an operator to do. We provide a choice of two different basic approaches:

- TLS-RSA
- TLS-PSK

The optimum security model will depend on the type of network, so operators should select the scheme that best suits their system and its applications. We now have some information to help with that selection.

TLS-RSA

For this option, device authentication is handled by the exchange of factory-installed RSA security certificates. The subject of the certificate is the ODU MAC address. Each Master or Slave ODU verifies the certificate offered by the remote unit and rejects the attempt to connect if the certificate is not valid. If the certificate is valid, the ODU knows with certainty the MAC address of the remote unit.

Authorization consists of configuring the MAC address of ODUs in a so-called Whitelist. The Whitelist holds up to 32 MAC addresses. This is the inconvenient bit; the operator has to compile both a list of MAC addresses for all the Slave ODUs that might need to connect to a particular Master ODU, and a list of the MAC address of all the Master ODUs available to a particular Slave ODU. This step is not so onerous if PTP 670 ODUs are used as part of a planned deployment in the network infrastructure, where the population of ODUs does not normally change unless an ODU is added or replaced. Configuring the Whitelist might be a more tedious task in a fast-moving deployment such as a disaster recovery mission where the network cannot be not planned in advance.

With TLS-RSA, the encryption keys are derived automatically from a master secret exchanged between Master and Slave ODUs. Each link in a sector has a different master secret and different encryption keys in the wireless link.

The TLS-RSA option automatically selects the largest key size supported by the Master and Slave in any particular link. For example, if one end of the link has a 128-bit AES license, and the other end of the link has a 256-bit AES license, the link will be encrypted using 128-bit encryption. TLS-RSA can even be used without the PTP 670 AES license; in this case, authentication and authorization are available, but encryption is disabled.

OPERATOR-SUPPLIED DEVICE CERTIFICATES AND THE BLACKLIST

PTP 670 provides an option for operator-supplied RSA security certificates as an alternative to the standard factory-installed device certificates. These must be generated as RSA certificates with 2048-bit key size and SHA-256, with the ODU MAC address as the subject.

The operator-supplied certificates provide higher security than the factory certificates, which are based on 1024-bit key size and SHA-1. Also, the operator-supplied certificates can be erased by the Zeroize CSPs action, unlike the permanent factory certificates.

Operator-supplied certificates can be used to establish a closed group of ODUs in one network, or one organization. When TLS-RSA is used with operator-supplied certificates, it makes sense to use the Blacklist option for authorization. The ODU will only connect to remote devices where the certificate is signed by the same Certificate Authority (CA). The Blacklist is the reverse of the Whitelist, containing the list of ODUs that is not allowed to connect. This means that the Blacklist contains only the small number of ODUs lost or otherwise compromised. Ideally, the Blacklist will be empty.

The Blacklist approach clearly requires minimal configuration – which appears most convenient – but the unavoidable drawback in this case is the need to generate device certificates. However, the certificate generation needs only to be done once, perhaps when ODUs are received and put into inventory, which saves effort during each subsequent deployment or redeployment.

TLS-PSK

For this option, each ODU is configured with a 128-bit or 256-bit pre-shared key (PSK). As with earlier PTP 650/670/700 releases, the wireless link will not connect unless the Master and Slave ODUs are configured with the same PSK. Use of the PSK effectively provides authentication and authorization in a single step. In an HCMP sector, all of the Slave ODUs must be configured with the same PSK. All ODUs must have an AES license for the selected key-size, bearing in mind that the 256-bit AES license allows a choice of 128-bit or 256-bit keys.

Encryption in TLS-PSK uses encryption keys automatically derived from the PSK, ensuring that data in each link is encrypted using a different key. This approach has the advantage that compromise of one Slave ODU does not undermine the security of the remaining Slave ODUs, satisfying one of the objectives identified earlier.

The inconvenient complexity of TLS-PSK is that the operator has to generate one or more PSKs (ideally in an approved random number generator) and must configure the same PSK in every ODU.

In an infrastructure deployment, it is a good practice to use a different PSK in every sector. In an ad-hoc deployment, it might make sense to configure the same PSK in all ODUs, to allow any Slave to be installed on any Master ODU.

SUMMARY OF WIRELESS ENCRYPTION OPTIONS

ENCRYPTION ALGORITHM	AES LICENSE	RSA CERTIFICATES	CONFIGURATION TASK	AUTHENTICATION AUTHORIZATION	ENCRYPTION	KEY-SIZE
None	—	—	None	No	No	—
TLS-RSA	No	Factory	MAC addresses in Whitelist	Yes	No	—
	Yes	Factory	MAC addresses in Whitelist	Yes	Yes	Auto
		User	Device certificates MAC addresses in Blacklist	Yes	Yes	Auto
TLS-PSK 128-bit	Yes	—	128-bit PSK in each ODU	Yes	Yes	128 bits
TLS-PSK 256-bit	Yes	—	256-bit PSK in each ODU	Yes	Yes	256 bits

REKEYING

TLS-RSA and TLS-PSK both provide an optional upgrade for automatic over-the-air rekeying (OTAR) for wireless encryption. Rekeying is completely transparent and does not interrupt normal wireless operation.

The rekeying interval can be configured with a minimum interval of one hour. Automatic rekeying is a valid response for security policies of some operators who require keys to be changed at periodic intervals. Automatic rekeying potentially offers significant cost savings by eliminating regular site visits.

Rekeying is activated by purchasing an upgrade.

AES LICENSES

TLS-PSK cannot be used without the optional AES license. To use TLS-PSK 256-bit, all ODUs must have the 256-bit license.

TLS-RSA can be used with authentication and authorization without the optional AES license. Encryption is automatically selected at the largest key size supported by the Master and Slave ODUs. The link can still be authorized if either the Master or Slave ODU lacks the AES license, but will be unencrypted.

USE OF STANDARD CRYPTOGRAPHIC ALGORITHMS

Wireless security in HCMP is based on standard secure cryptographic algorithms and protocols. The same algorithms are used in PTP 700, where Cambium is validating the product to FIPS 140-2. Operators can be confident that the HCMP security solution is robust and meets current best practice.

CONCLUSION

Existing PTP 650/670/700 products have provided class-leading wireless security for PTP links. We have overhauled the wireless security features in PTP 670/700 to provide a flexible set of options for HCMP networks, addressing the needs of different users. These options deliver easily configurable security that provides robust and effective protection for operators' valuable information in wireless networks. For further information about the security features in PTP 670, please refer to the PTP 670 Series User Guide.

Cambium Networks™

Cambium Networks, Ltd.
3800 Golf Road, Suite 360,
Rolling Meadows, IL 60008