Datensicherheit und Verschlüsselung bei Geräten der MRX-Serie von AZG Tech

Arbeitsweise der Geräte der MRX-Serie

Die Geräte der MRX-Serie (Mesh-Knoten) sind dazu gedacht, eine sichere und zuverlässige Netzwerk-Infrastrukur dort zu errichten, wo das Verlegen von Kabeln oder Glasfaser unmöglich, zu teuer oder nicht sinnvoll ist. Die Geräte etablieren untereinander ein Funk-Netzwerk auf Basis der AZG Mesh Technologie und verhalten sich im Wesentlichen wie ein Netzwerk-Switch, der die Daten von einem Port eines Knotens auf jeden anderen Port eines anderen Knotens im Mesh-Netzwerk weiterleiten kann und somit die Kommunikation von Geräten ermöglicht, die an einen der Mesh-Knoten im selben Netzwerk angeschlossen sind. Zur Verbesserung des Funktionsumfangs sind zusätzliche Features lieferbar, etwa ein Mobile Uplink (über 4G/5G-Mobilfunk) oder ein Wi-Fi Access Point (AP) für den drahtlosen Zugang zum Netzwerk. In der Standard-Konfiguration sind für angeschlossene Geräte ebenfalls ein DHCP- und DNS-Server aktiviert, um die Vergabe der IP-Adressen zu vereinfachen.

Die Geräte der MRX-Serie verfügen über eine moderne Web-GUI zur Konfiguration aller Funktionen des Geräts und sprechen außerdem SNMP zur Konfiguration und Überwachung der Gerätefunktion.

Verfügbare Netzwerk-Dienste

Mesh

Im Mesh werden die Kundendaten übertragen, die den Geräten über die Ethernet- oder Wi-Fi AP Schnittstellen eingespeist und an einem anderen Ethernet- Wi-Fi AP oder Mobilfunk-Uplink ausgekoppelt werden. Damit unterliegen die im Mesh übertragenen Daten besonderem Schutz.

Die Geräte der MRX-Serie implementieren den sicheren Mesh-Standard der Norm IEEE-802.11. Zur Authentifizierung der einzelnen Mesh-Knoten dient das SAE-Protokoll (siehe unten) mit einem pre-shared key (PSK, eine Passphrase), der auf allen Mesh-Knoten im selben Netzwerk bekannt sein muss. Während der paarweisen Authentifizierung der Mesh-Knoten untereinander werden verschiedene zufällige kryptographische Schlüssel vereinbart (unterschiedliche Master- und transiente Schlüssel für jedes Knotenpaar, pro Knoten ein Schlüssel für Broad- und Multicastpakete). Die Masterschlüssel werden nur zur Generierung und zum Austausch der transienten Schlüssel benutzt, die transienten Schlüssel selbst dienen der symmetrischen Verschlüsselung der Daten selbst. Dabei werden die transienten Schlüssel nach einer bestimmten maximalen Datenmenge oder einer bestimmten Zeit ausgetauscht, um die Sicherheit zu erhöhen. Zur eigentlichen Verschlüsselung wird das CCMP-Verfahren (siehe unten) benutzt.

Damit Angreifer die Funktionsweise des Mesh-Netzwerks nicht stören können, werden Protected Management Frames (PMF, verschlüsselte Kontrollnachrichten) benutzt.

Der Name des Mesh-Netzwerks (Mesh ID) sowie der gemeinsame PSK lassen sich vom Administrator der Geräte frei konfigurieren. Bei der Auslieferung vorkonfigurierter Geräte achtet die AZG-Tech auf die Vergabe sicherer PSKs.

Wi-Fi AP

Einige Geräte der MRX-Serie können mit einer zusätzlichen Funkschnittstelle ausgeliefert werden, die einen Wi-Fi Access Point bereitstellen, über den auf das Netzwerk drahtlos zugegriffen werden kann. Auf diesen Schnittstellen ist das bekannte WPA-2 mit Passwort-Authentifizierung WPA2-PSK) implementiert.

Es ist ebenfalls möglich, externe Access Points anderer Hersteller an die Mesh-Knoten anzuschließen.

Mobile Uplink

Die Geräte der MRX-Serie können mit einem LTE- oder 5G-Funkmodul ausgestattet werden, um einen Internetzugang für das gesamte Netzwerk zur Verfügung zu stellen. Dabei wird das Mesh-Netzwerk zu einem NAT-Router, der Verbindungen von innerhalb des Netzwerks nach außen zulässt, von außen kommende Verbindungen in das Netzwerk aber unterbindet.

Für die Sicherheit der über das Mobilfunknetzwerk übertragenen Daten ist der Kunde verantwortlich und muss dafür eine geeignete Ende-zu-Ende-Verschlüsselung wählen.

Web-GUI

Die Web-GUI eines Mesh-Knotens ist über die Ethernet-Schnittstellen oder den Wi-Fi AP des Geräts erreichbar. Es kann auch auf die Web-GUIs anderer Mesh-Knoten zugrgriffen werden, sofern sie im selben Mesh-Netzwerk erreichbar sind. Für als nicht vertrauenswürdig eingestufte Ethernet-Ports oder Wi-Fi APs (etwa an „öffentlichen“ Netzwerken) kann der Zugang zu allen Management-Funktionen der Mesh-Knoten abgeschaltet werden.

Die Web-GUI ist über HTTP sowie HTTPS (siehe unten) erreichbar. Für optimale Sicherheit ist der HTTP-Zugang abschaltbar, allerdings ist für die Einrichtung des Geräts der Zugang über HTTP aktiviert, damit der HTTPS-Server konfiguriert werden kann.

Der Zugang zur Web-Oberfläche ist nur mittels Username/Passwort-Authentifizierung möglich. Dafür lassen sich Benutzer mit unterschiedlichen Nutzernamen, Passwörtern und Berechtigungen (admin / user / guest) anlegen. Gängige Sicherheitsrichtlinien bei der Festlegung von sicheren Passwörtern (Länge, Ziffern, Sonderzeichen) werden beachtet und unsichere Passwörter vom System abgelehnt.

Zur Einrichtung des HTTPS-Servers ist der Kunde dafür zuständig, ein sicheres X.509-Serverzertifikat zu erzeugen und zusammen mit dem dazu gehörigen privaten Schlüssel auf dem Gerät zu hinterlegen. Das Serverzertifikat beinhaltet vom Kunden zu konfigurierende Aspekte (z.B. die IP-Adresse oder den DNS-Servernamen) sowie ein Ablaufdatum und muss in eine

Vertrauenskette eingebunden werden (Stammzertifikate). Deshalb kann nur der Kunde selbst die Erstellung und den regelmäßigen Austausch eines passenden Zertifikats vornehmen.

SNMP-Zugang

Die Geräte der MRX-Serie bieten einen Konfigurations- und Monitoring-Zugang per SNMP. Die notwendigen MIBs (Management Infomation Base, also Schnittstellenbeschreibungen des SNMP-Zugangs) sind über die Web-GUI des Geräts abrufbar.

Der SNMP-Dienst kann komplett deaktiviert werden. Wenn er aktiviert ist, kann zwischen den Protokollen SNMP V2c, SNMP V3 sowie SNMP V2c + V3 gewählt werden.

Das SNMP V2c-Protokoll gilt als unsicher und sollte nur in bereits abgesicherten internen Netzwerken verwendet werden. Dabei gibt es weder Verschlüsselung von Nachrichten noch Authentisierung von deren Sendern. Lediglich ein im Klartext übertragener „Community Name“ wählt einen konfigurierten Benutzer und die damit verbundenen Zugriffsrechte aus.

Das SNMP V3-Protokoll gilt als sicherer und behebt die Schwachstellen des SNMP V2c-Protokolls. Es beinhaltet ein User-based Security Module (USM), das die Funktionen der Nachrichtenverschlüsselung und -authentisierung beinhaltet. Beide Funktionen können getrennt ein- bzw. ausgeschaltet werden. Das USM spezifiziert HMAC-MD5 sowie HMAC-SHA1 als Authentisierungsverfahren sowie DES und AES als Verschlüsselungsverfahren an. Für beide Funktionen können separate Passwörter hinterlegt werden, die jeweils zur Ableitung eines kryptographischen Schlüssels benutzt werden.

Übersicht über kryptographische Protokolle

SAE – Simultaneous Authentication of Equals

Das SAE-Protokoll ist eine Variante der Dragonfly-Schlüsselaustauch-Variante und wurde zuerst im Jahr 2011 von der IEEE in den Standard IEEE-802.11s aufgenommen, der dann in den Haupttext der Norm IEEE-802.11-2012 aufging. Im Jahr 2018 spezifizierte die Wi-Fi Alliance dann den WPA3 Standard, der auf SAE beruht.

SAE basiert auf dem Diffie-Hellman-Schlüsselaustauschverfahren (DH) zur Vereinbarung eines gemeinsamen Master-Schlüssels für ein Paar von Kommunikationspartnern. Dem DH-Verfahren fehlt allerdings ein Bestandteil zur Bestimmung der Authentizität der Kommunikationsteilnehmen (und ist damit anfällig für Man-in-the-middle-Attacken, wo ein Angreifer im Kommunkationspfad Nachrichten manipuliert und zu jeder Seite selbst Verbindungen aufbaut), weshalb SAE zusätzlich den PSK und die MAC-Adressen der Kommunikationspartner in die Schlüsselberechnung einbezieht und das Authentizitätsproblem löst. Wenn das Authentifizierungsverfahren erfolgreich abgeschlossen wurde, wissen beide Geräte, dass das andere Gerät den richtigen PSK kennt und haben den einen gemeinsamen Master-Key (PMK, pairwise master key) ausgehandelt.

Mit dem PMK wird durch das AMPE-Protokoll (Authenticated Mesh Peering Protocol) eine sichere Verbindung beider Knoten hergestellt und gleichzeitig werden darüber transiente Schlüssel (PTK, pairwise transient key) abgeleitet, um die Datenkommunikation zu verschlüsseln.

Die Sicherheitsgarantien des Verfahrens sind:

- Der erfolgreiche Abschluss des Protokolls resultiert in einem gemeinsamen PMK zwischen zwei Mesh-Knoten.
- Ein Angreifer ist weder durch passives Mithören oder einfaches Weiterleiten der Kommunikation nicht in der Lage, das Passwort oder den PMK herauszufinden.
- Ein Angreifer ist nicht in der Lage, das Passwort oder den PMK durch Manipulation, Einschleusen oder erneutes Senden abgefangener Nachrichten herauszufinden.
- SAE ist resistent gegenüber Wörterbuchattacken.
- Ein kompromittierter PMK einer früheren Sitzung hilft nicht dabei, das Passwort oder den PMK einer aktuellen Sitzung herauszufinden.
- Ein kompromittiertes Passwort hilft nicht dabei, den PMK einer früheren Sitzung zu rekonstruieren.

Das CCMP-Protokoll

CCMP steht für Counter Mode CBC-MAC Protocol und ist ein kryptographisches Verfahren basierend auf AES für Datensicherheit, -integrität und -authentizität. Es kombiniert den AES CTR-Modus (Counter Mode) für sichere Datenverschlüsselung und dem Cipher Block Chaining (CBC) Message Authenticity Code (MAC).

Der CTR-Mode von AES fügt zusätzlich zum Key einen Zähler in die Berechnung der verschlüsselten Nachricht mit ein, der für jeden einzelnen AES-Block geändert wird. Damit wird aus einem Block Cipher (wiederholtes Verschlüsseln derselben Daten liefert dasselbe Ergebnis) zu einem Stream Cipher (wiederholtes Verschlüsseln derselben Daten liefert jedesmal ein anderes Ergebnis) und macht Brute Force-Attacken auf die Verschlüsselung extrem schwierig.

CBC-MAC ist ein Verfahren ähnlich zur Generierung einer digitalen Signatur: Es wird eine „Checksumme“ über die Nachricht gebildet, die sicherstellt, dass die Nachricht nicht verändert wurde und der Erzeuger im Besitz des Schlüssels ist. Dazu werden die Daten mit einem Block Cipher (z.B. AES) in verketteten Blöcken so verschlüsselt, dass das Verschlüsselungsergebnis eines Blocks vom verschlüsselten vorhergehenden Block abhängt. Der letzte Block wird als MAC mit an die Nachricht angehängt. Wird der falsche Schlüssel benutzt oder die Nachricht auf dem Weg verändert, so kann der Empfänger das durch Wiederholen der Berechnung feststellen, indem er zu einem anderen Ergebnis kommt.

Das HTTPS-Protokoll

HTTPS steht für HTTP über SSL (in aktuellen Versionen wird ausschließlich TLS, der Nachfolger von SSL verwendet). SSL und TLS stellen eine kryptografisch gesicherte Verbindung zwischen einem Client (der die Anfrage stellt) und einem Server (der die Anfrage beantwortet) her. Das Protokoll läuft wie folgt ab:

- Der Client startet das SSL/TLS-Protokoll entweder durch Verbindungsanfrage auf einem dedizierten Port des Servers oder durch das STARTTLS-Kommando in der laufenden Sitzung.
- Client und Server einigen sich auf einen Satz von Verschlüsselungsalgorithmen und Hash-Funktionen.
- Der Server präsentiert dem Client das digitale X.509-Serverzertifikat, das der Client prüfen muss. Dabei ist sowohl die Überprüfung der Sicherheitskette (Kette der Certificate Authorities) als auch der Besitz des zum Zertifikat gehörenden privaten Schlüssels und des Server-Namens (öffentlicher DNS-Name, IP-Adresse) notwendig.
- Es wird ein Key Exchange-Protokoll benutzt (normalerweise DH), um einen gemeinsamen, zufälligen und geheimen Schlüssel für eine symmetrische Datenverschlüsselung auszuhandeln.

In diesem Falle wird das Authentizitätsproblem des DH-Algorithmus durch die Authentifizierung des Servers mittels asymmetrischer Kryptografie (Public/Private Key Kryptografie) sichergestellt. In seltenen Fällen wird als Zugangsberechtigung zusätzlich eine Client-Authentifizierung über ein X.509-Zertifikat des Clients durchgeführt.

Die Sicherheitsgarantien sind hierbei:

- Der erfolgreiche Abschluss des Protokolls resultiert in einem gemeinsamen symmetrischen Kryptografieschlüssel (Session Key) zwischen Server und Client.
- Ein Angreifer ist weder durch passives Mithören noch einfaches Weiterleiten der Kommunikation nicht in der Lage, den Session Key herauszufinden.
- Ein Angreifer ist nicht in der Lage, den Session Key durch Manipulation, Einschleusen oder erneutes Senden abgefangener Nachrichten herauszufinden.
- Die Identität des Servers (ggf. auch des Clients) wird über Public-Key-Cryptography sichergestellt.
- Die Daten sind durch einen Message Authenticity Code (MAC) geschützt vor unerkannter Veränderung oder unerkanntem Verlust von Daten.