EMiZON

Security

The Emizon network is capable of providing a secure monitored service using Internet Protocol (IP) over both fixed line and wireless networks such as GSM GPRS. The protocol used in the Emizon Network is inherently secure at all times, and thus can be used with public IP networks or private IP networks securely. The Abstract below taken from one of our product definition documents describes the mechanisms used to ensure that all data is secure, whatever network it may be transported over.

The use of public IP networks, including the internet provides no additional challenges to the Emizon Network itself. Emizon used across a public IP network provides equal cryptographic security to that when used over a private IP network. The Emizon TCD has an embedded firewall which prevents all traffic into the TCD and permits only connections out from the Emizon TCD application to the Emizon network, only on the IP ports permitted. This prevents any form of external IP attack.

All data between the Emizon TCD device and the Emizon Network is encrypted using the mechanisms below, preserving the integrity of the data across the internet or other IP networks at all times. Each IP message from or to the Emizon TCD is prefixed with an index identity. The Emizon security engine examines the index and attempts to decrypt the message using the cryptographic keys associated with the Emizon system using that identity. If the index is not valid, or the subsequent decryption attempt of the message fails, the message is simply discarded and no reply is sent to the invalid device. This provides an extremely high level of security and reliability, allowing the Emizon protocols to be used across all forms of digital communications networks securely.

Reliability

The Emizon TCD uses both fixed and wireless routes in combination to provide a very high level of availability. Messages are exchanged regularly and independently over both communications paths between the Emizon TCD and the Emizon network. The timing of these is designed to ensure that a TCD which detects that a path is suffering a poll 'failure' may attempt alternative paths within the timings required by standards result in a 'path failure' message at the monitoring centre.

The Emizon TCD operates from a fixed program system, which is immune to any form of virus, Trojan, worm or other program since the program which the TCD is running is not permitted to alter. The Emizon TCD IP stack has been exhaustively tested independently against vulnerabilities from malformed IP packets. The firewalling system within the Emizon systems and TCD ensure that only the essential connections from the TCD to the Emizon network are permitted, and no inbound connections are permitted at all. This ensures that the risk from any unknown malformed IP frame exploits which may be discovered in the future is kept to an absolute minimum. Any such exploit can have no

effect on the operation of the TCD other than causing the device to fail, resulting at worse case in a communications loss event to the monitoring centre.

It is possible for deliberate distributed denial of service attacks (DDOS) to be launched to any public IP address (any many 'private' IP networks since they normally share infrastructure including VPN links across public networks, whether provided by the customer or provided transparently by their network service provider) and, whilst such an attack will not penetrate the Emizon TCD defences, the flooding of the network links could result in a loss of connectivity to the Emizon network, resulting in a 'communications loss' signal being sent to the Monitoring Centre for the fixed line path. The GSM GPRS path from the TCD is entirely separated from the fixed line IP path, and thus would be unaffected by such an attack, ensuring that the TCD continues to signal reliably. Emizon also used a private IP address within the GSM GPRS network in order to provide physical redundancy with connections and Access Point Nodes. Measures are taken with the core Emizon networks to minimise the effects of any attempted denial of service attack, since the Emizon Network provides multiple ingress and egress network paths, provided by several differing service providers, with geographic separation also being used.

This redundant and resilience design also provides an IP network arrangement which is in many cases more reliable than private IP networks, since the Internet itself provides multiple routes and heals round most node failures seamlessly, whereas many private IP networks will suffer from single points of failure which can render the network inoperable, such as corporate firewalls, routers, switches and interconnecting links between the sites.

Abstract

This protocol was developed to provide a secure mechanism for the transport of critical messages between many disparate units connecting via the public internet and the GSM GPRS radio network to a centralised managed alarm transmission system, comprising several servers located in more than one geographical location. Each of the disparate units, termed TCD in this document has connectivity to the Emizon server network via various wired internet access technologies, including ADSL broadband, cable broadband and corporate IP networks along with alternate connectivity via long range wireless networks including GSM GPRS networks in multiple territories.

The requirements for security of such systems are such that the devices must be monitored securely and regularly for their connection status over all configured communications paths, with alerts being generated if communications is lost with a given TCD path for any reason, as this may be indicative of a malicious attack on the protected property. Such communications checks should be explicit between the device application and the server, and not reliant on a transport mechanism session close notification such as provided by TCP/IP, or rely on insecure checking messaging such as 'ping' type processes. The Poll / Poll Response cycle used within the Emizon TCD is secured using the maximum cryptographic mechanisms provided, and which TCP/IP may be used as a transport mechanism, the protocol herein does not use any of the TCP/IP session mechanisms for it's security, and every message is secured using this protocol.

A centrally managed alarm transmission system is necessary to provide the infrastructure scale necessary to allow geographical and system resilience and redundancy in a cost effective manner, and to permit comprehensive support infrastructures to be put in place shared across many customers, and hence provide true support at a cost effective level.

As the protocol is intended to operate over public IP networks, strong cryptographic measures are seen as essential in protecting the devices from intrusion or substitution. For this reason, the protocol uses peer-reviewed public domain cryptographic methods to ensure that the data is secure and cannot be impersonated. The protocol uses:

SHA-1	Secure Hash Algorithm producing a 160 bit secure hash value of a given data block
AES-128	encryption technology, which encrypts a 16 byte block using a 128 bit key strength algorithm
System Key	128 bit key used for encryption of all communications seen as non-secure, as the system key is shared across several units and must therefore be seen to be less secure than unique keys.
Master Key	128 bit key used for encryption of all security establishment messages between a single TCD and the Emizon service platform. Master Keys are unique across the entire TCD estate[1].
Session Key	128 bit key used for all secure communications. This key is changed at regular intervals by the Emizon Service Platform to deny any determined attack on the protocol.
TCD HardID	A SHA-1 hash of a copy protected unique identity located within the hardware of the TCD. In the Emizon TCD this is derived from the security protection registers on the flash memory chip which is hard programmed during the flash chip manufacture.

This protocol provides the mechanism for initial establishment of a secure communications session between a given TCD and the Emizon Service Platform, a secure mechanism for the exchange of information used to derive a session key, enhanced impersonation / substitution protection by the use of unique Master Key information combined with the use of secure Hardware Identity information. The ability to pass messages before the establishment of a session key is also provided using the System Key arrangement which, whilst encrypted using the normal mechanisms, is based on a shared key system where the key may be known to several units, and is therefore seen as less secure. This function is therefore restricted to non-critical diagnostic message processing and is not used for alarm or command messages.

The security protocol herein and the Emizon messaging protocol actually used for message communications are separate and have no interaction with each other, with the exception that the Emizon messaging protocol requires the secure protocol to be and remain established whilst the TCD is ACTIVATED. All Emizon Messaging protocol data frames are passed securely across the connection established by this protocol,

[1] Emizon Networks view is that Master Keys should be unique. If shared keys are used in more than one device, this will dramatically reduce the protection afforded by the cryptographic algorithms, permitting an attack to be performed by copying the static key to another hardware device and altering the device ID to impersonate another. Whilst the encrypted data may therefore be secure, a substitution attack becomes much more feasible as an attack vector on systems with common keys.

Abbreviations and Definitions

AES	Advanced Encryption Standard – an industry standard, peer reviewed cryptographic system, used in 128 bit key mode within the Emizon systems.
ESP	Emizon Service platform – The core alarm transmission network
CMP	Central Message Processor – The main computer system in the ESP
FLASH	non-volatile memory using flash programmable devices, these retain their contents for long periods and can be readily reprogrammed several thousand times, but do have a finite permitted reprogram cycle limit.
PIP	Peripheral Interface Processor – A front end for CMP connected subsystems
RAM	Random Access Memory – volatile storage which loses its contents on power down
SATCD	Stand Alone Telemetry Communications Device
SHA	Secure Hashing Algorithm – an industry standard, peer reviewed one way secure hash algorithm. Used in all Emizon systems.
SVR	Server – short for ESP in this document
TCD	Telemetry Communications Device (short for SATCD)

Cryptographic Keys

The Emizon protocol uses one of three possible keys for the encryption and hashing functions.

System Key

This is a unique single 128 bit key which is known to each TCD on the system, and is used only for non-secure operations such as initial unit announcements for a new TCD on the Emizon System, or for non-secure diagnostic exchanges with the TCD.

Master Key

This is a 128 bit key which is associated with each TCD on the ESP and passed to the TCD when it is first attached to the Emizon network. Once a master key has been assigned to a TCD it is never exchanged again, and the TCD will cease to function if the master key is changed or lost. This is used only for authentication exchanges, and in combination with unique hardware identifiers and securely exchanged random tokens (nuggets) is used to generate the session keys.

Session Key

This is a 128 bit key which is generated as part of the secure authentication command, and is used for all secure data exchanges throughout the TCD/ESP system, the same session key being used by all configured communications paths for a single TCD. It is changed at intervals by the ESP to further enhance the security.

Hardware Key - ID

This is a 160 bit hardware identifier which is used to prevent sophisticated substitution attempts, and is intended to be known only to the Emizon ESP and the TCD code itself. In the current SATCD design this is derived from a SHA-1 hash which incorporates the unique protection register identity from the flash memory chip, which makes it very difficult indeed to copy.