
Security
Whitepaper
mymesh
by Chess

Mymesh -Connect any light, anywhere.

Smart business for the Internet of Things powered by Mymesh.
An overview of the Mymesh security architecture

Technical White Paper concerning the security architecture of Mymesh, a self-organizing network with distributed processing capabilities.

Version 2.2
April, 2019

Ashley Bateup
Director Chess UK
Email: ashley@getmymesh.com

Paul Bingham
Strategic Advisor, Mymesh
Email: paul@getmymesh.com

Company Address: The Old Rectory, Springhead Road,
Northfleet, Kent, DA11 8HN
Company Phone: +44 7701 411308
Website: www.getmymesh.com

Table of Content

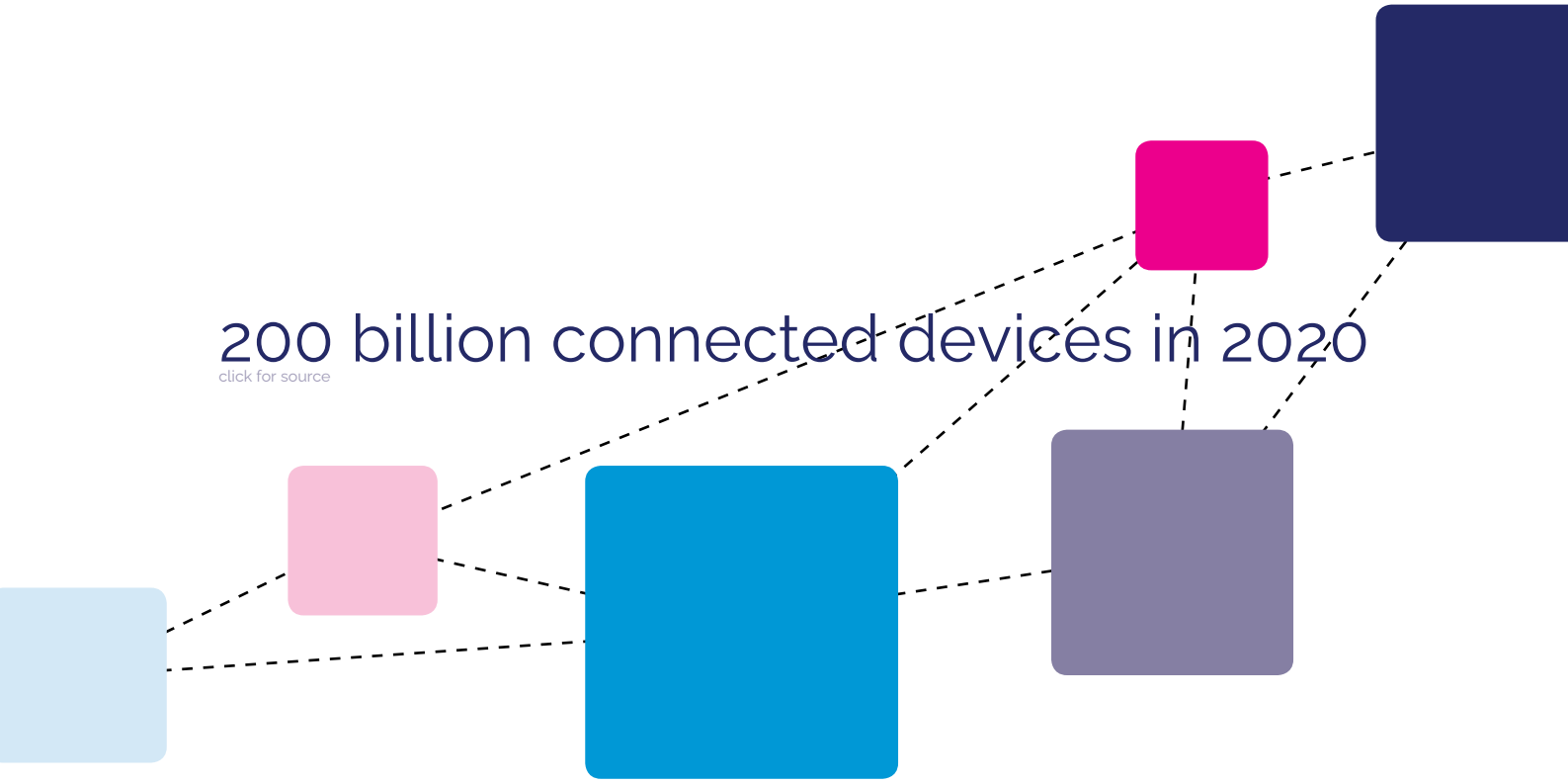
Management Summary

Meshed networks are the future for Internet of Things (IoT) applications. Chess already has this future-proof solution today. With Mymesh we deliver an IoT platform that optimizes the feasibility of any IoT business case and is ultra-scalable in support of future growth.

Mymesh solves the traditional challenges for wireless sensing and actuation: the data model for distributed sensor data, localization of sensors and actuators, time synchronization for coordinated sleep and wake-up times, and time-stamping of sensor data with globally-usable timestamps. Mymesh networks automatically reconfigure themselves according to the availability and proximity of bandwidth or storage. This makes them resistant to interference and other poten- tial problems. Dynamic connections between nodes enable messages from nodes to use multiple routes to travel through the network, which makes the network robust and agile even when oper- ating at large scale.

About this whitepaper

In this whitepaper, we look at the Mymesh security archi- tecture. This technical white paper is for CTOs and decision makers in IT, working at companies and organizations that are looking into an Internet of Things solution that is robust, reliable, easy to manage and very secure.



Creating smart businesses in a connected world

Data is at the heart of the enablement of businesses around the world to make the right decisions to use resources and assets effectively and optimize their business models. In the era of IoT, smart and connected assets play a key role in providing the distinctive data that will determine the competitive advantage of a business in a hyper-connected world, for example, energy usage, location, life-cycle information. Security of these IOT systems is a major requirement and has been constantly top of mind within Chess.

Chess

In 1988, Chess started as a design and development studio to create hard-and software solutions for the professional market.

"As engineers at heart, we firmly believe that technology makes the world more safe, efficient and sustainable."

After almost two decades of active development, our founders foresaw the immense potential of having wireless infrastructures in 2003. Back then, there was one major problem; scalability. No network protocol could connect thousands of devices. It was the start of Mymesh's development.

Mymesh

Mymesh easily lets you connect, monitor and analyze large wireless networks. Derived from decades of experience, the robust, scalable and secure characteristics make Mymesh the best lighting control application for the public, work, and industrial space.

Secure by design

Mymesh is developed with security in the core of its architecture. Each Mymesh node is personalized with a unique ID and keys, enabling it to participate in the network and allowing it to obtain authenticated software updates. For personalization and general key management, Chess Wise uses Hardware Security Modules (HSM), similar to those used in the banking industry. The Nordic Semiconductors chip is initially programmed in the production facility before it becomes part of a Mymesh network. The crypto keys are stored in a protected area of the chip, which makes it nearly impossible to read. When the Mymesh network is running autonomous, this architecture provides optimal protection of the communication with a 128 bit AES encryption standard.

Introduction

Chess has implemented a series of procedures and mechanisms to safeguard the security of the Mymesh network and the Mymesh nodes.

Keys used in Mymesh

Each node receives, during manufacturing, a set of cryptographic keys. Currently, all keys are 128 bit AES keys.

Key	Shared/derived	Specific to	Usage
Network key	Shared between all nodes in the same network	A single customer or a single installation	Encryption and authentication of network messages
Node authentication keys	Derived key in node, master key in uploader	Master key specific to a single customer, derived key specific to single node	Mutual authentication between node and uploader
Node encryption key	Derived key in node, master key in uploader	Master key specific to a single customer, derived key specific to single node	Derivation of secure channel session key for firmware upload (point-to-point).
Blob decryption key	Shared between Chess and gateway nodes	A single customer	Decryption of the encrypted firmware image, loaded into a gateway for distribution over the network
Blob verification key	Shared between Chess and all nodes	A single customer	Verification of a firmware image (blob) loaded into a gateway or distributed over the network.

Hardware security modules

Chess uses hardware security modules for the generation, storage, and operations of all cryptographic keys outside the nodes. These HSMs are mechanically and electronically protected against tampering, intrusion, and unauthorized use. When tampered with, the cryptographic keys contained in the HSM are securely wiped.

Chess has added firmware to these HSMs to implement the specific operations needed. At Chess, HSMs are used to generate and store keys and to encrypt and electronically sign firmware imag- es for manufacturing and for software distribution. At the manufacturing sites, HSMs are used to generate the derived keys, decrypt and verify firmware images, and inject the keys and firmware into the Mymesh nodes.

The used HSMs are certified to FIPS 140-2 level 3

Network

The network communication is protected using AES CCM encryption according to NIST SP 800- 38C. For this purpose, all nodes in a Mymesh network share a 128-bit AES key.

The CCM encryption combines the encryption of the network messages with authentication by the means of a message authentication code (MAC). Thus, the network communication is protected against eavesdropping, modification ,and forgery of messages.

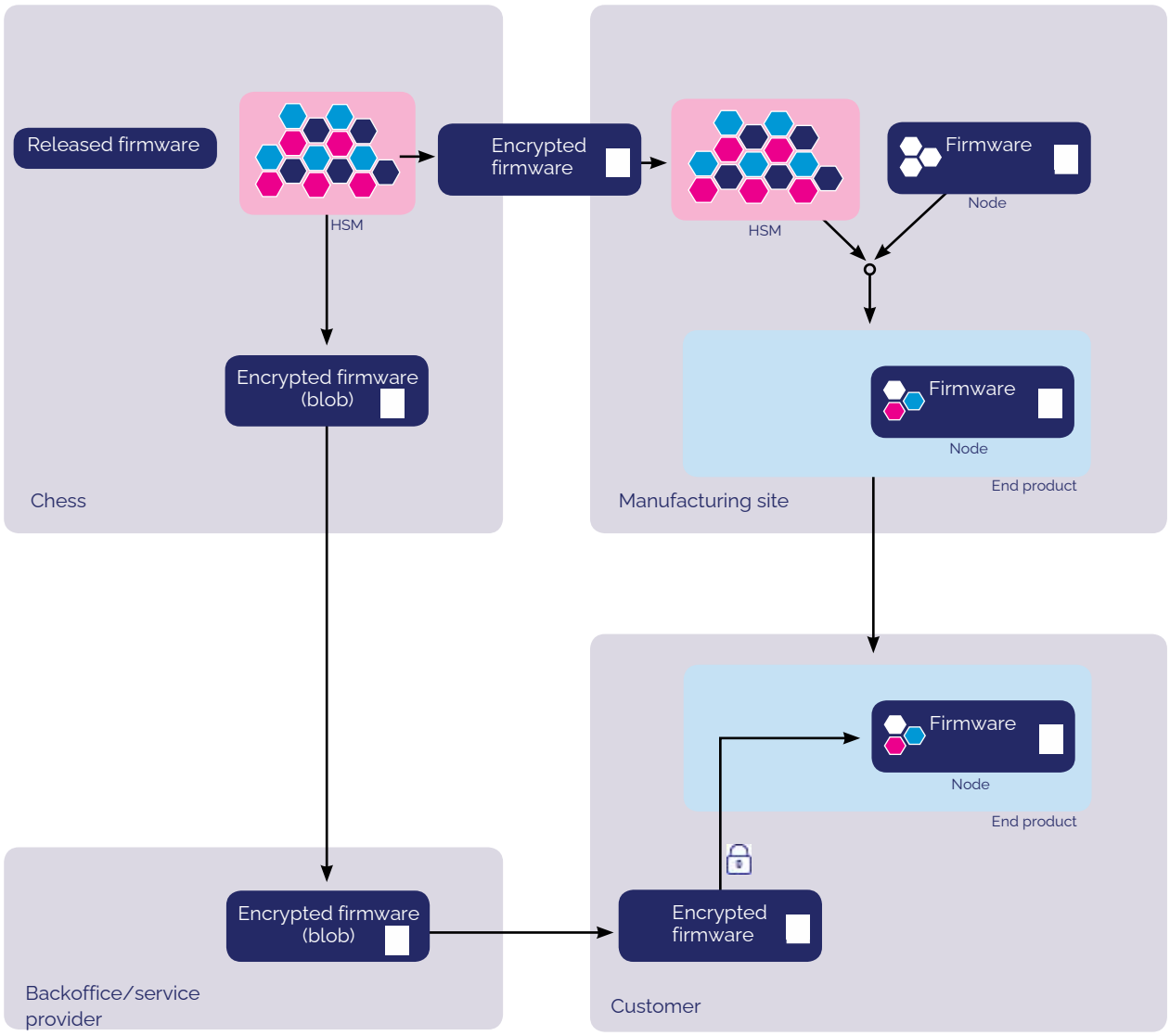
All nodes in a connected Mymesh network share a counter: the global time. This counter is included in the nonce of the CCM encryption and messages with a global time that lies in the past are silently discarded by the receiving node. This provides protection against replay attacks.

Firmware Programming and Updates

The Mymesh nodes support three methods for updating the node firmware:

- Flash programming using the single wire debug interface of the NRF51.
- Point-to-point over the air update.
- Over the air firmware distribution using Mymesh Blob (the secure distribution format used for Mymesh).

The overall software distribution process (except for the point-to-point mode) can be depicted as follows:



SWD Flash Programming

This is used during the production of a Mymesh Node. At this stage, all flash memory is being erased and Mymesh Boot (the bootloader), MymeshAm (the second stage bootloader), the application firmware, the initial properties, and the security keys
are programmed into flash. After programming, the flash is “locked”: it is no longer possible to read-back flash memory, RAM, or peripheral registers over the SWD interface.

The combined firmware image (Mymesh Boot, MymeshAm, application, initial properties) is available at each production location in encrypted and cryptographically signed form. A hardware security module (HSM) is used during production to:

- Verify the firmware signature
- Decrypt the firmware image
- Inject the device specific security keys into the image

This is all done inside the HSM. The resulting image is then injected into the Mymesh Node over the SWD interface and the flash is locked.
The whole production process is organized in this way to:

- Prevent injection of keys into non-authentic firmware.
- Prevent any access to the cryptographic security keys being generated/used.
- Protect the Chess Wise IP

Point-to-Point over the Air Updates

The Mymesh Boot provides a mechanism to upload a new firmware image to a Mymesh Node over a point-to-point wireless link. A special "upload" node establishes a secure link with the node and then uploads a new firmware image.

The process uses an ISO 9798 compliant mutual authentication mechanism for authentication and session key establishment. After successful completion of the authentication protocol, both the uploader and the downloader share a AES session key used for CCM encryption of the secure link.

Firmware Distribution using Mymesh Blob

For firmware updates in the field, the Mymesh network implements a torrent-like mechanism to distribute (amongst other things) a new firmware image. The image originates at a gateway node and is gradually distributed over the entire network where all nodes participate in the distribution.
To protect this process against interference and tampering, the whole process is cryptographically secured:

- The firmware image is generated by Chess Wise and, using an HSM, injected with any necessary keys, encrypted, and authenticated (using a MAC).
- Gateway nodes contain a key that enables them to decrypt the image.
- All nodes (including the gateway node) contain a key that enables them to verify the authenticity of the new image.

Only authentic images will be accepted and distributed by the gateway node.
Only authentic images will be activated by the receiving nodes.

Security Enhancing Mechanisms

Each MymeshNode implements various mechanisms to enhance the security and stability of the network:

- Corrupted messages (detected by CRC errors at the radio level) are discarded.
- Only messages in the current network channel and domain are considered for processing.
- Messages with a global time in the past are discarded.
- Messages that fail authentication (incorrect MAC) are discarded.
- Only tokens present on a configurable white list are considered for processing.
- None-white listed tokens in a message end the processing of a message.
- The Mymesh token processing time is monitored to prevent token processing from (unintentionally) exceeding the network round time.
- A global watchdog timer guards the node firmware and resets the node when necessary.

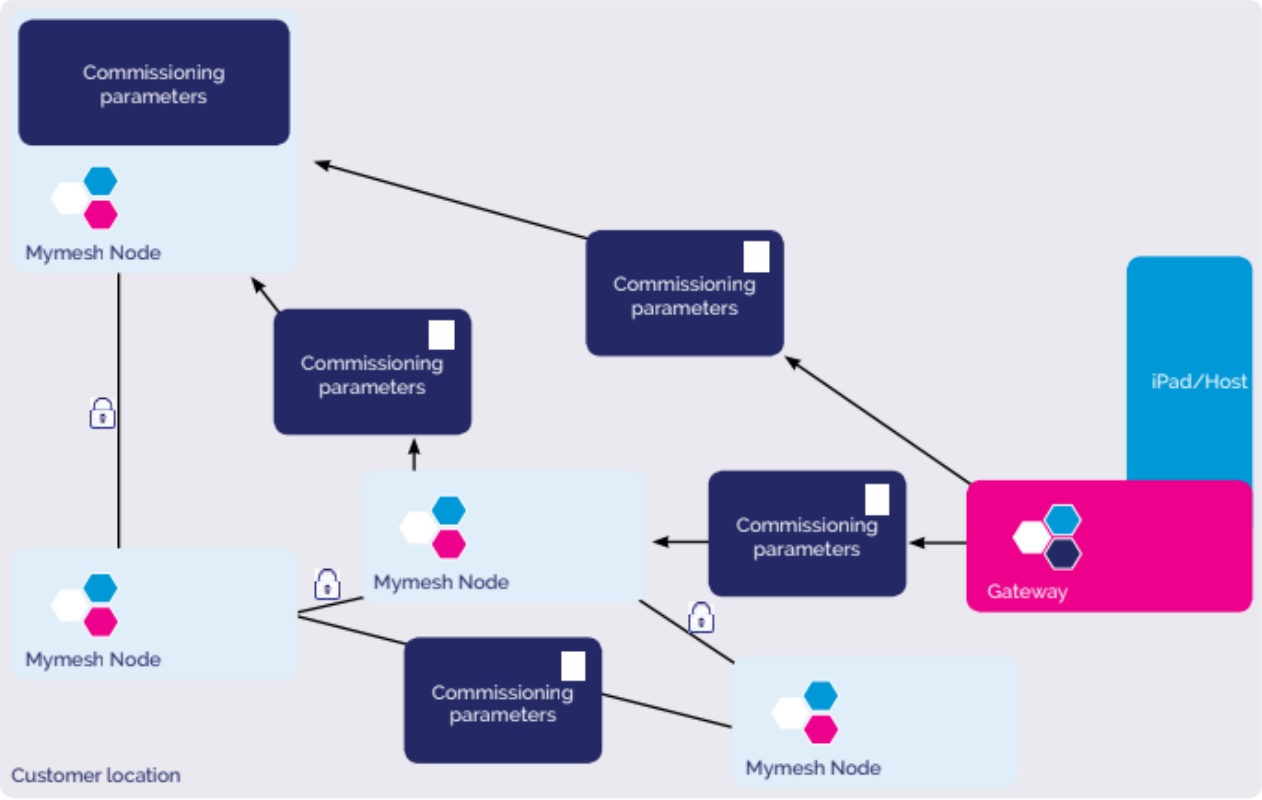
Node Lifecycle

Manufacturing

During manufacturing, node firmware, initial properties, and node keys are programmed
into the nodes. This is done after rigorous testing of the product, incorporating the node.

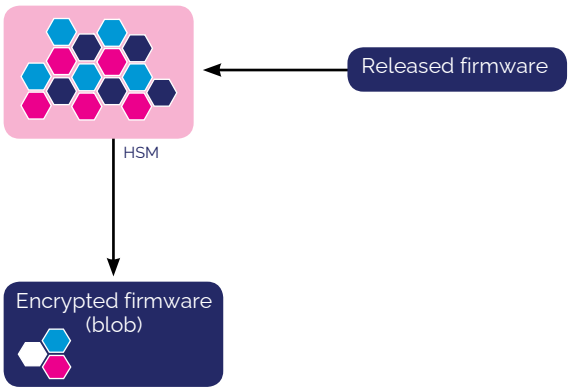
Installation

During node installation, an iPad with Bluetooth gateway or a back office host (with Ethernet or 3G Gateway) is able to commission nodes by setting node specific commissioning parameters over the Mymesh network. New nodes can join the network because they have been pro- grammed with the appropriate network key during production.



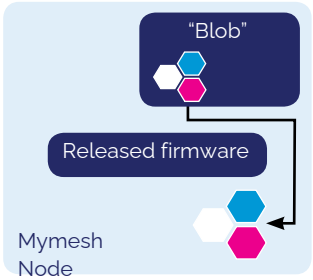
Operation and Maintenance

During the operation/maintenance phases, MymeshNodes may receive new firmware updates using MymeshBlob. “Blobs” for firmware updates are generated by Chess Wise:



A back office host or an iPad presents the encrypted and authenticated blob to a gateway in the network that needs a firmware update, after which the gateway decrypts and authenticates the blob:

The blob is then securely distributed over the network to all nodes and, when authenticated on the nodes, installed on request:



Mymesh Glossary

gMAC
De dedicated MAC-layer in a MymeshMesh Network

MymeshDTM
The Distributed Token Machine (DTM) used by MymeshMesh

MymeshMesh
The Internet of Things meshed network platform from Chess Wise

MymeshMesh Boot
The boot layer of MymeshMesh to commission, provision, configure and re-configure nodes

MymeshMesh Core
The core layer of MymeshMesh, the embedded operating system of the Mymesh-Mesh
platform.

MymeshModule(s)
Ready-to-go hardware nodes from Chess Wise

MymeshNode(s) or just nodes
Nodes in a meshed network based on MymeshMesh

Contact

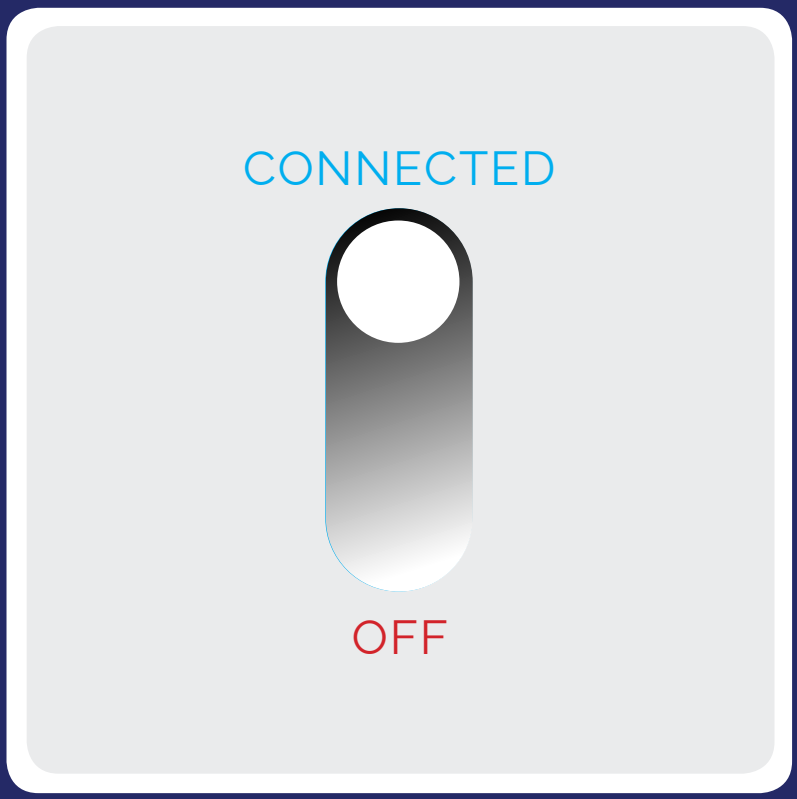
Ashley Bateup
Director Chess UK
Email: ashley@getmymesh.com

Paul Bingham
Strategic Advisor, Mymesh
Email: paul@getmymesh.com

Company Address: The Old Rectory, Springhead Road,
Northfleet, Kent, DA11 8HN
Company Phone: +44 7701 411308
Website: www.getmymesh.com

Switch

Connected is the new on.



Find out more at getmymesh.com