M2M Cyber Security

Solution Brief

M2M Intelligence® - Essential platform for the M2M and IoT Economy

M2Mi™
Machine-to-Machine Intelligence Corporation

Table of contents

M2M Cyber Security Solution Brief

As more and more sensors and devices connect to Machine-to-Machine (M2M) and Internet of Things (IoT) infrastructures to share data, the implications of a security compromise can be serious.

Delivering security for both physical sensors/devices as well as digital information thus becomes a critical requirement for success. Cyber Security, which includes both secure exchange of digital information and cyber-physical critical infrastructure protection, is therefore the appropriate context for security in the M2M and IoT environment.

As the M2M and IoT ecosystem complexity increases with an ever growing number of devices, protocols, networks, applications, and services, it is important to design cyber security mechanisms with simplicity in mind. This also means an intelligent mechanism designed to grow organically as the resources to protect and the network to cover grow as well. This approach reduces the probability of introducing unwarranted traps or loopholes.

M2Mi addresses M2M and IoT Cyber Security with a holistic, simple and elegant solution. M2M Cyber Security, combined with M2M Automation, is M2M Intelligence®, the essential platform for the M2M and IoT economy. At the heart of M2Mi's Cyber Security technology efforts lies the Lockbox, an abstracted Cyber Security framework that controls access to resources. Granting access to a resource can depend on multiple and changing factors defined by the state of the requesting entity as well as pre-defined security rules. These factors range from access control policies to the physical state of the requesting device. When the right conditions are met, the Lockbox grants temporary access to the resource by configuring the adequate network and connection. Abstracting Cyber Security components allows security solutions such as the LockBox the flexibility to integrate various M2M and IoT topologies as well as meet the most stringent standards.

The LockBox was designed to support private and public standards as organizations become increasingly over-whelmed by governance and compliance standards. Of particular importance is the National Institute of Standards and Technology (NIST) Cyber Security Framework, a voluntary framework developed in response to the Obama administration executive order in 2013 for reducing cyber risks to critical infrastructure. The Framework consists of standards, guidelines, and best practices to promote the protection of critical infrastructure. It also provides a common language and mechanism for organizations to describe their target state for Cyber Security. The LockBox solution is an accelerator to attain the target state. The LockBox achieves this by defining universal terminology, policy and instructions that organizations can easily translate into their own Cyber Security protection efforts.

The following document is divided in three sections. The first section defines the fundamental components that characterize the LockBox solution. The second section describes LockBox implementations for cyber critical infrastructure protection and secure information exchange. These implementations align with the NIST Cyber Security Framework recommendations to improve an organization's Cyber Security state. The last section describes two use cases that put into practice the aforementioned LockBox implementations.

Defining Cyber Security Critical Components

In order to correctly design a Cyber Security solution, it is necessary to define the components that make up the universal cyber-critical environment to protect. The components defined below serve as the M2M and IoT Cyber Security backbone. These components persist regardless of the infrastructure, topology, or data to protect. Moreover the LockBox should apply the same set of universal instructions to ensure exhaustive protection. The components consider all aspects of an organization's Cyber Security environment thus allowing easy assessment of an organization's level of compliance with any standard it may be subjected to.

Resource

At its core, cyber security revolves around protecting resources from malevolent activity. A resource not only embodies data but also physical devices. A resource is located anywhere on the network whether it is out on the field in an end-device, on a data-center server, or transiting between these points. Typical resource examples include:

- Data at rest
- Applications
- Cryptographic keys
- Critical Infrastructure

Requestor

The requestor is the entity requesting access to a resource. The requestor may manifest itself through different forms: human, node, or application. Depending on its state, the requestor may be refused, gain partial, or full access to the resource. Once access is granted, certain conditions may apply on the requestor for the duration of the access.

Action

An action is defined as any operation that may be performed on a resource by the requestor. For example this can be read and write privileges on a data file or execution privileges on an application. Privileges can vary depending on the requestor's pre-determined rights and its current state.

Context

The requestor's state at the moment it requests access to a resource is defined as the "context". The context may determine whether the requestor will be granted authorization to access the resource. Context may be static or evolve dynamically in time. Static context defines the requestor's software and hardware features such as brand, model, operating, and memory. Dynamic context defines constraints of five types: temporal, spatial, prerequisites depending on the requestor's action history, requestor-declared goals, and provisions. They range from device geo-location to currently running applications.

Policy

Policies determine what actions a requestor can perform on a resource and under which constraints and monitoring conditions authorization may be granted. Authorization is granted depending on a requestor's context and whether it complies with the policies.

Access Control

Access control defines which entity may have permission to access a resource. More specifically the owner of a resource requires that the requestor authenticate itself (i.e. provide proof that it is what it claims to be) and carries the authorization to access the resource. Access controllers include Single-Sign-On (SSO) mechanisms, Access Control List (ACL), and Certificate Authority (CA).

Keys

Keys are at the heart of most cryptographic services: authentication, encryption, integrity, and non-repudiation. Any Cyber Security infrastructure must have the means to generate cryptographically secure keys, store them in a secure medium, and protect their access. Resources are typically protected with keys but may be temporarily shared with authorized

requestors that meet the appropriate conditions. The ability to correctly manage Keys is a crucial component of a successful Cyber Security infrastructure.

Connection

If a requestor meets the conditions required to access the resource, a connection is generated between the two in the form of a secure communication channel. This connection is composed of network configurations (such as firewall rules) and transport security (such as TLS). To establish the connection, the requestor must detain all necessary cryptographic Keys.

Compliance

Compliance refers to any standards, regulations, or guidelines an organization must conform to. These may be imposed by the organization's internal policies, by local and international laws, or a specific industry. Organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls such as the NIST Cyber Security Framework.

LockBox

The LockBox is a secure information exchange mechanism. It orchestrates all of the security requirements in an M2M implementation. By enforcing policies it ensures that a requestor is in the right context before allowing access to a resource. The LockBox configures the connection between the requestor and the resource and ensures that all required keys are securely delivered to the requestor such that it may access the resource.

LockBox Technology

The Lockbox is a foundational technology within the M2M Cyber Security product. In this section we describe the LockBox solution and provide two LockBox implementations. The first implementation, the Cyber Critical infrastructure Protection is designed to protect hardware assets of an organization whether located within the datacenter's firewalls and DMZ or outside in the field. These assets range from sensors and network equipment to the CPUs.

The second implementation, the Secure Information Exchange, is designed to protect resources belonging to an organization. This can be data-at-rest stored in the datacenter, data produced by field sensors, or data in transit over a network. We show how the LockBox leverages dynamic context of the requesting device and its surrounding ecosystem to determine under which monitoring constraints access to resources may be granted.

In both implementations we show how the LockBox determines what actions an end-device can perform on infrastructure resources, the allowed parameters of use as well as changes to environment to meet policies and Quality of Service (QoS) guidelines. This fine-grained ability to control information flow has significant advantages over less sophisticated, binary yes/no approaches to access.

We conclude this section by expanding on the subject of privacy and how any organization requires a secure key generation and management system.

LockBox as a Cyber Security Solution

The LockBox solution is a Cyber-critical Security engine aimed at protecting M2M and IoT critical infrastructures and resources. The LockBox Solution is part of the M2Mi Network Virtualization Suite that creates the seamless network environment required for M2M and IoT service delivery, security and application development. At its core, the LockBox Solution enforces policies that determine what actions a requestor can perform on datacenter resources and under which constraints and monitoring conditions authorization may be granted. Authorization is granted depending on a requestor's context and whether it complies with the policies. A unique "LockBox" key, securely stored on both ends, binds the requestor, or a group of users, with a list of policies.

In the most general use case the requestor is an end-device requesting an action on a datacenter resource. A device is defined broadly as a general-purpose hardware equipment capable of executing certain tasks and is connected to, e.g., cellular or IP networks. They range from smartphones to remote sensors. Each is associated with a user that may or may not interact with it. Together, the device and user form the requestor.

The Lockbox solution is composed of distributed Lockbox Nodes and a centralized Lockbox Core. The LockBox Nodes are distributed components that connect networks of end-devices with the cloud datacenter. The LockBox Node is the remote arm of the LockBox Core and together they control the access to the cloud datacenter. The Node is typically deployed on an application server somewhere in the network, but can also be running on the end-devices themselves. The LockBox Core normally runs in the cloud datacenter and/or telecommunications network.

The LockBox Node manages requests to the resource and provides contextual information to the LockBox Core. If a device cannot support the node (e.g. a smart meter with insufficient computational resources) it is instead loaded on another nearby device. Whenever a device is granted authorization the LockBox Core subsequently secures a route between the device and the resource.

The LockBox Core divides in three distinct components: Profile Manager, Policy Engine, and Key Manager. The Profile Manager authenticates in-coming requests while the Policy Engine authorizes them. The Key Manager handles cryptography. To fulfill its duty the LockBox Core seamlessly integrates with third party applications such as identity managers, secure storage, Public Key Infrastructure PKI certificate authorities, and single sign-on platform.

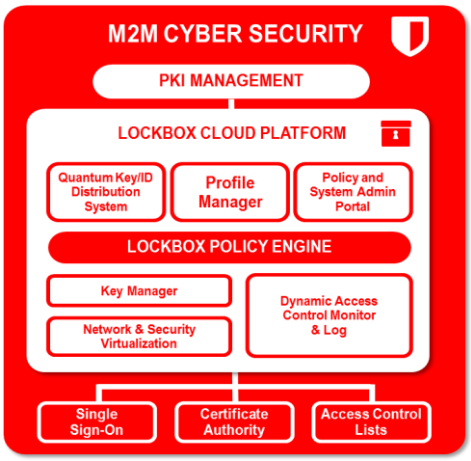

Figure 1: LockBox Core

The next sections describe how a new device integrates a PKI, how policies are created and managed, how requests are handled, and finally how a secure connection is established with a resource.

Initialization

Device Integration

The LockBox components are members of a centralized trust model and as such integrates a PKI. The Key Manager leverages the PKI by brokering X.509 certificates from the Certificate Authority (CA) to the end-devices. A Node must be a member of the PKI to access the organization's datacenter and LockBox components.

In the initialization phase the LockBox Nodes are bootstrapped with the LockBox Core's public key. This allows the establishment of a secure communication channel between the Nodes and the Core. To become a trusted member of the PKI a Node must obtain an RSA private key and an X.509 certificate binding it to the CA. In this phase the Key Manager acts as a broker between the Node and the CA endorsing an end-device's authenticity. It manages key generation and distribution, provides the CA with the necessary information, and securely sends the private key and the certificate in a PKSC#12 key store file format back to the device. The Key Manager also automates all other necessary PKI related tasks such as certificate renewal and revocation or user suppression.

Next the Node must obtain a LockBox key in order to access a datacenter resource. A LockBox Key binds a Node (and therefore its surrounding end-devices) with a list of policies. In this phase the Key Manager generates the unique LockBox Key and, with the input of a LockBox Administrator, lists the resources a Node can access and the policies it must comply with. The LockBox Key and the list of policy ID's are added to a database for this Node. The Key Manager subsequently sends the LockBox Key to the device via the secure communication channel. Upon receipt the device securely stores the Key. With it the Node and/or the device it is managing can now perform actions on resources within the limits dictated by its associated policies.

Policy Generation

Policies are divided in two categories: device specific and contextual. Device specific policies enforce rules for static characteristics of a device such as software and hardware features. They range from brand, model, and operating system to processor, memory and network capabilities. Contextual policies enforce rules for dynamic states of a device and/or user. Such policies typically define contextual constraints of five types: temporal, spatial, prerequisites depending on the user's action history, user-declared goals, and provisions. They range from device geo-location to currently running applications. A policy includes a requestor, resource, action, and condition. The requestor's context must meet the condition in order to perform the action.

Resource owners define the rules by which devices and users (the requestors) must conform to be granted access and perform actions. The M2Mi Policy Portal converts these rules into policies. Policies are stored in the Policy Engine database and are assigned to requestors via the LockBox Key.

Secure Resource Connection

Authentication Control

The Profile Manager authenticates users and devices using a whitelist mechanism. It enforces several security checkpoints on the connecting device and user before it can access the LockBox and eventually the resource. First the end-device must provide proof that it belongs to the PKI. It succeeds only if the device proves ownership of a certificate linked to the root of trust. This instantiates a secure communication channel to the LockBox using, e.g., the transport security layer (TLS) protocol or web-service (WSS) security depending on the use case. Next, the device must provide user login credentials to prove that the entitled user is commanding the device. As the LockBox allows for broad degrees of abstraction the Profile Manager can look up the credentials in the organization's directory, or locally on the LockBox. Finally, the device must provide a valid context that can be interpreted by the Policy Engine.

These three forms of whitelisting guarantee that only organization accredited devices and users will be granted access to the LockBox. This mechanism reduces spamming or flooding attacks against the environment. If authentication is successful, the Profile Manager passes the context and the LockBox Key to the Policy Engine and the Key Manager for checking and action response.

Authorization Control

The Policy Engine authorizes requests. The Key Manager, via the user's LockBox Key, provides The Policy Engine with a list of relevant policy ID's. The Policy Engine retrieves the policies from its database and confronts the device specifications and context with the policies. The selected tolerance level will determine if all or part of the policies must be met and under which constraints and monitoring conditions authorization may be granted. In case of validation, the LockBox logs the flow of the request including results, parameters, users and times. The Policy Engine instructs the M2Mi Network Virtualization Engine to prepare a secure communication channel between the device and the resource. Otherwise an error is issued to the device with useful information on the conditions not met or with a reference number to be retrieved by the LockBox Administrator for data on conditions not met.

Secure Connection

The M2M Automation: Network Virtualization Engine establishes the connection to the resource. First, it provides the device with a unique session token generated by the Key Manager. The token is a reference to the current request and context. The M2M Automation: Network Virtualization Engine subsequently composes the necessary network and firewall rules and extends the secure communication channel to the resource. If appropriate it can also request the Key Manager for cryptographic keys. They range from session keys that protect data in transit to database keys that encrypt or decrypt data at rest. Finally the M2M Automation: Network Virtualization Engine may also broker a single-sign-on (SSO) platform to log the user in the relevant resource environment.

Throughout the connection, the device provides constant context updates to the LockBox. This allows the Policy Engine to monitor compliance dynamically and ensures continued security of the granted access. In case of a policy breach the LockBox has the ability to disconnect the device from the resource.

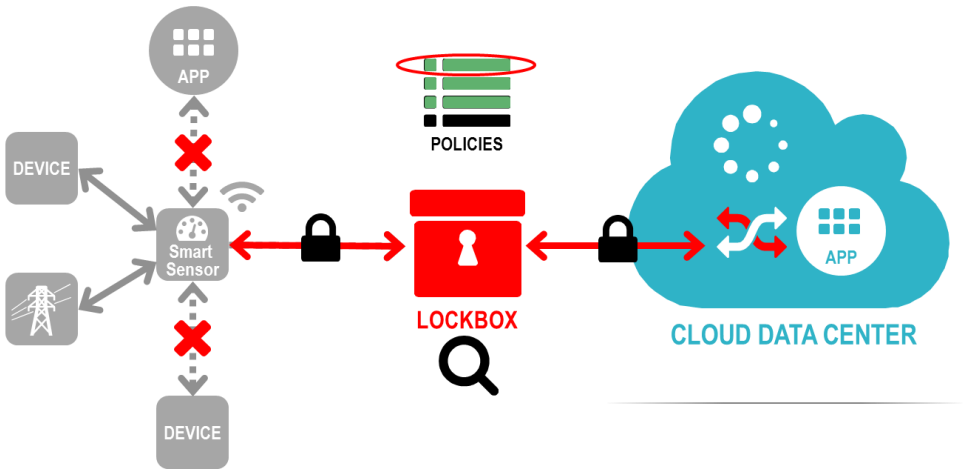

Figure 2: LockBox Example Implementation

Critical Infrastructure Protection

The LockBox for Critical Infrastructure Protection focuses on the cyber-physical world of sensors, processors and controls. The goal of this implementation is to protect an organization's infrastructure against cyber-attacks. They range from passive attacks such as wiretapping and port scanning to active attacks such as orchestrated Distributed Denial-of-Service (DDOS) and flooding attacks.

In this implementation the LockBox engine is configured to defend the hardware components that constitute an M2M and IoT critical infrastructure. As such, the Profile Manager, Policy Engine, and Key Manager focus on the following functions:

- Intelligent discovery of hardware components and surrounding ecosystem
- White listing of all native hardware components
- Multi-protocol and multi-level encryption
- Single-Sign-On
- PKI integration
- Two way authentication
- Scalable Certificate Authority and Registration Authority
- Control flow to and from hardware components
- Cryptographic keys provisioning
- Third party integration such as Intel® Corporation's Trusted execution CPU optimizations

Secure Information Exchange

The Lockbox Secure Information Exchange determines what actions a requestor can perform on an organization's resources and under which constraints and monitoring conditions authorization may be granted. It also determines the requestor's context, allowed parameters of use, and orchestrates the changes to the M2M and IoT ecosystem to meet policies and QoS guidelines. Indeed the LockBox Secure Information Exchange determines the dynamic nature of any end point or asset within the infrastructure, by intelligent analysis of the real-time surrounding context. This enables intelligent decisions and enforcement of dynamic policies instead of using static rules that do not reflect the true current state.

The LockBox Secure Information Exchange has the ability to seamlessly connect end points to the backend cloud via cellular or IP networks. Ensure performance, QoS, security policies are adhered to – from end to end. Includes bundled global connectivity for your devices through partner telecom networks, with the ability to provide seamless service in over 200 countries over 250 carrier networks.

The LockBox Secure Information Exchange focuses on the following functions:

- Request management
- Access Control
- Multi-protocol and multi-level encryption
- Mutual Authentication
- Dynamic discovery of the requestor's surrounding ecosystem
- Network reconfiguration based on policies and requestor's context
- Cloud and data center network reconfiguration to ensure an optimal connection
- Secure connection from the device to the data center application

Lockbox and the NIST Cyber Security Framework

The LockBox for Critical Infrastructure Protection and Secure Information Exchange in conjunction with the NIST Cyber Security Framework accelerate an organization's compliance requirements. Because the LockBox solution covers the full Cyber Security spectrum it thereby addresses a broad number of policies belonging to the most prevalent standards.

To help support organizations securely adopt M2M and IoT implementations, various governments and standards bodies have recently published regulations and recommendations addressing a variety of new cybersecurity challenges. However these regulations and recommendations can create confusion within an organization as those charged with designing breach prevention and incident response plans try to determine which regulations apply to their organization and how to maintain compliance.

Figure 3: Critical infrastructure components

To ease this difficulty the US government has introduced a Cybersecurity Framework that enables a consistent and iterative approach to identify, assess, and manage cybersecurity risk. The American National Institute of Standards and Technology (NIST) standards body has the

mandate of publishing what is called the “Cyber Security Framework”. It was ordered by the Obama administration in 2013 for reducing cyber risks to critical infrastructure. This document is now available here.

The Framework helps an organization, from a structural point of view, determine the steps required to reach a desired level of compliance. As organizations learn to do this, they become better and more efficient at managing the cost of a data breach. The Framework consists of standards, guidelines, and best practices to promote the protection of critical infrastructure. It also provides a common language and mechanism for organizations to describe their desired target state for cybersecurity.

Alignment between the LockBox and NIST Cyber Security Framework

Using the NIST Cyber Security Framework, organizations can examine what capabilities they have implemented in the five high-level Functions identified in the Framework’s Core: Identify, Protect, Detect, Respond, and Recover. The Framework introduces the concept of a “Framework Profile”. It represents the outcomes that a particular organization has achieved or is expected to achieve as specified in the Framework Categories and Subcategories. The Framework Profile can be characterized as the alignment of Preliminary Cybersecurity Framework industry standards and best practices to the Framework Core in a particular implementation scenario.

Profiles are also used to identify opportunities for improving cybersecurity by comparing a “Current” Profile with a “Target” Profile. The Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-effectiveness and innovation. In this sense, Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

An organization therefore produces a “Comparison Profile” which identifies the gap to fulfill between the Current and Target Profiles. The LockBox is the ideal security solution that can assist an organization to seamlessly implement the prioritized technical requirements raised through the Comparison Profile. Indeed a natural one-to-one correspondence exists between the LockBox components and the NIST Cyber Security Framework Core Functions.

Identify

The LockBox facilitates the institutional understanding of organizational systems, assets, data, and capabilities requiring protection. The LockBox keeps track of all of the infrastructure’s hardware devices, provides an exhaustive software inventory and network map. It maintains real-time information on data-flows, internal as well as external communications, and cryptographic suites and versioning. Finally the LockBox provides environmental awareness such as the location of all infrastructure assets ranging from data center devices to field sensors.

Protect

The LockBox implements the appropriate Cyber Security safeguards, prioritized through the organization's risk management process, to ensure delivery of critical M2M infrastructure services. Identity, Credential, and Access Management of assets and resources are protected by the LockBox using standardized processes supported by state of the art technologies. They include:

- Unique LockBox Keys to protect each infrastructure resource.
- Public Key Infrastructures
- Certificate Authorities
- Two-Factor Authentication
- NIST recommended cryptographic suites
- Privacy, Integrity, and Non-Repudiation of Data at rest and in transit
- Secure Random Number Generation for all involved devices
- Dynamic Access Control Listing
- Rate limiting
- Data Analytics

Detect

The LockBox provides the appropriate components required to identify the occurrence of a Cyber Security event. They include network monitoring components that scan for repeated connection attempts, abnormal termination of device connections, and repeated authentication attempts. The LockBox offers granular detection mechanisms due to the delocalization of LockBox Nodes. Nodes can be placed anywhere on the network thus allowing proximity to sensors and M2M devices as well as the networks on which they connect. This front row seat exposure allows the LockBox to gain maximum insight on organizational assets located beyond the datacenter firewall.

Respond

The LockBox implements the appropriate emergency response flows, prioritized through the organization's risk management process, to take action regarding a detected Cyber Security event. Possible actions include:

- Revocation and/or suppression of LockBox Keys
- Revocation of lost or compromised certificates
- Revocation of lost or compromised authentication credentials
- Disconnection of suspicious or compromised devices
- Blocking of compromised networks or channels
- Intelligent Firewall policy modification
- Interruption of compromised datacenter devices
- Log and monitor activities of suspicion target device

Recover

The LockBox implements the appropriate actions, prioritized through the organization's risk management process, to restore the appropriate network capabilities that were impaired through a Cyber Security event. Possible actions include:

- Generate and distribute new LockBox Keys
- Perform information system recovery
- Perform reconstitution activities
- Intelligent Firewall policy recommendation
- Certificate and authentication credentials reissue
- Automatic System backups

The LockBox for Critical Infrastructure Protection and Secure Information Exchange in conjunction with the NIST Cyber Security Framework accelerate an organization's compliance requirements. Because the LockBox solution covers the full cyber security spectrum it thereby addresses a broad number of policies belonging to the most prevalent standards. The LockBox and the NIST Cyber Security Framework naturally interlock together as both offer consolidated and harmonized sets of compliance and security controls. This enables the necessary governance requirements to be met without the unnecessary duplication of effort and activity from the organization's resources.

LockBox Privacy Manager

A fundamental goal of the LockBox Solution is the ability to deliver privacy to an organization's resources. With the ability to share confidential data among multiple authorized participants who can remain anonymous, the Lockbox can provide multiple levels of privacy. Policy can also dictate that each lockbox requires two keys to access the contents, in this way the depositor and consumer of information are completely segregated and can even remain anonymous to each other.

Cryptography and Key Management

To achieve this multi-level privacy, the Key Manager must employ cryptographic techniques that guarantee the confidentiality of all keys generated inside the critical infrastructure as well as outside on the network and end-devices. A compromised key can enable malevolent perpetrators access to large amounts of confidential data or control of critical infrastructure. This is widely considered to be one of the top threats for an organization's Cyber Security.

Many key management systems are available on the market. They range from open source API projects to commercial proprietary solutions. They typically take the form of a hardware security module (HSM). An HSM traditionally consists of an external security device that can be attached directly to a server or general purpose computer through a network or USB connection.

Each module contains one or more secure cryptoprocessor chips to prevent tampering and probing. An HSM's primary purpose is to securely store and manage keys exclusively within the datacenter omitting end-devices. Also the method by which keys are generated is often left to the implementer's responsibility.

The most widely used cryptographic key types are asymmetric keys for PKI and symmetric keys for encryption. The primary property of cryptographic keys is that they should remain unpredictable to any unauthorized party. This is typically hard to achieve in servers and devices since software applications and operating systems are limited by their deterministic nature and cannot produce unpredictable events that yield the keys. Instead, they are sought from physical random phenomena. Peripheral activity such as mouse movements, keyboard strokes, and hard disk motion are typical examples of randomness sources.

In many cases however there is a flagrant lack of peripherals. Datacenter servers, for instance, are rarely connected to mice or keyboards. To make matters worse, these same servers often perform virtualization in an effort to reduce costs thereby increasing the demand for the server's

different resources including the available randomness. This lack of peripherals affects even more M2M and IoT sensors and end-devices.

The LockBox Key Manager fills the technological gap by offering a Key generation and distribution system that can not only generate cryptographically secure keys for datacenter devices but also reach out to end-devices.

Lockbox Use Cases

In this section we present two use cases that leverage the LockBox solution. The first use case utilizes the LockBox to protect an M2M and IoT environment within a Message Queue Telemetry Transport protocol (MQTT) context and the second use case showcases a Smart City scenario where multiple entities (cars, public transport, emergency vehicles, and city support staff) exchange data to efficiently manage the city traffic infrastructures and minimize security risks.

LockBox and MQTT

The Message Queue Telemetry Transport (MQTT) is a publish/subscribe and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. These principles also turn out to make the protocol ideal for M2M and IoT connected devices, and for mobile applications and sensors where bandwidth and battery power are at a premium.

To provide more flexibility, MQTT supports a hierarchical topic namespace. This allows application designers to organize topics to simplify their management. Levels in the hierarchy are delimited by the '/' character, such as SENSOR/1/HUMIDITY.

The MQTT protocol defines 2 entities: a client and a broker. A client can publish and subscribe to topics while the broker dispatches messages between clients. A topic therefore binds publishing and subscribing clients into a Community of Interest (CoI). Here the resource is the payload published by a client to a subscribing client, the requestor. To protect the resources exchanged between the clients, the CoI must not only protect data in transit but also protect the topic from unwarranted subscribers. The former is typically solved using traditional cryptographic suites such as SSL. The latter is more complex as it requires white listing each member of the CoI and results in a scaling problem when a broker is required to handle millions of different topics.

To efficiently protect resources within an MQTT CoI, the LockBox appends a top-level topic name composed of random characters called a LockBox Topic Key. More precisely, clients publish and subscribe to 'private' topics starting with a lockbox key (a string of random characters). For example, a client with (publication) LockBox Topic Key “1A46HGT” publishes under the topic “/1A46HGT/House/Room1/Temp”. This implies that the published data will only be available to subscribing clients in possession of that key. As a result, the clients in possession of the same LockBox Topic Key now share a 'Private Virtual Broker' on which only they can publish and

subscribe (analogous to a VLAN in networking terms). In other words the LockBox acts as a dynamic ACL where it is dynamically decided who can access a given topic.

In this implementation the LockBox is configured as an extra software layer running atop the MQTT broker and does not require any modification of the MQTT protocol itself. Essentially it is composed of a three components. The Key Manager distributes a unique (publish and subscribe) LockBox Topic Key to the clients of a CoI thus limiting who can access the messages exchanged in the CoI. The Topic Mapper allows to safely map messages between different topics locally on the same broker or on another broker. The Topic Filter allows for fast analytics of the data contained in MQTT messages.

LockBox Topic Keys

The distribution of the LockBox Topic Keys is done by publishing the key to each of the CoI client's private topic (e.g. ClientId/LockboxKeys/subscription or ClientId/LockboxKeys/publication). For example publishing and subscribing clients of a CoI would each obtain the corresponding LockBox Topic Key from a private topic unique to every client. It is through this topic that all of the client's LockBox Topic Key can be accessed. Once every client of the CoI is in possession of the key, messages can be published with the certainty that an unauthorized client subscribes to CoI's topic.

Topic Mapper

In some cases it is useful for two CoI's to share a common topic. For example two distinct organizations working on a common project or service may wish to publish data that both organizations can access. The LockBox Topic Mapper functionality does exactly this.

The basic principle is to have the Lockbox of both organization create a CoI for the clients connected to the broker each manage. To exchange data, both organization's LockBox are themselves part of a CoI managed by a third party broker called an aggregation broker. From the Aggregation broker's point of view, the two LockBox are two subscribing/publishing clients of a CoI. The two Lockbox can then exchange messages through the aggregator by forwarding/importing topics to/from the aggregation broker.

The Topic Mapper can also be used locally on a single broker where clients may not have the capacity to obtain a LockBox Topic Key. This is simply done by creating a LockBox local mapping that forwards messages from keyless clients to the appropriate LockBox topic.

Topic Filter

The LockBox Topic Filter is a real-time analytical service that scans for key words, tags, and topics. It is useful to locate important events and trends that can be published to other topics or forwarded to other brokers. Consider a natural gas pipeline infrastructure where sensors monitor the pressure along the gas line. These sensors publish the pressure under a specific topic that is subscribed by the gas company's datacenter applications. The LockBox Topic Filter is configured to monitor messages that contain abnormal gas pressures. Whenever such an event occurs and

is intercepted by the LockBox Topic Filer, the LockBox Mapper forwards the message to emergency topics that automatically reach out to the company's crisis unit, emergency response teams located near the publishing sensor, and any other entity that may quickly require the alert.

NIST Cyber Security Framework

The upcoming OASIS MQTT specification 3.1.1 is accompanied by a supplemental security document "MQTT Supplemental Publication Version 1.0 Part 1: NIST Cyber Security Framework". M2Mi contributed support for NIST Cyber Security Framework into the OASIS MQTT version. It has the mission to bridge the OASIS MQTT protocol with the NIST Cyber Security Framework. The supplemental document is a compilation of OASIS MQTT and M2M and IoT Cyber Security guidelines and references that are common across critical infrastructure sectors. The MQTT Framework Core consists of five Functions - Identify, Protect, Detect, Respond, Recover - which can provide a high-level, strategic view of an organization's management of MQTT and M2M and IoT related Cyber Security risk. The Framework then identifies underlying key Categories and Subcategories for each of these Functions, and matches them with Informative References such as existing standards, guidelines, and practices.

The LockBox Critical Infrastructure Protection and LockBox Secure Information Exchange are the perfect security implementations that fulfill the recommendations found in the OASIS MQTT supplemental document. Indeed, the LockBox solution can leverage all of the recommendations:

- Use of PKI (e.g. TLS, VPN)
- Certificate Authority
- Mutual Authentication
- Use of cryptographic suites (e.g. TLS, VPN)
- Integrity of Application Messages and Control Packets
- Privacy of Application Messages and Control Packets
- Non-repudiation of message transmission
- Secure Random Number Generation for all involved devices
- Automatic Client disconnect mechanisms
- Suspicious behavior detection
- Dynamic Access Control Listing
- Rate limiting and/or blocking (e.g. IP address)
- Data-at-rest encryption
- Proper storage of the client certificate (key management considerations)

LockBox and City Traffic Flows

In this use case the LockBox secures a city's traffic infrastructure where multiple entities (cars, public transport, emergency vehicles, and city support staff) exchange data to efficiently manage the city traffic infrastructures and minimize traffic security risks. As the data is potentially shared between several entities, the ability to secure and accurately apportion data and trends to the authorized members is important. Here the LockBox enforces dynamic boundaries between entities and groups while intelligently routing data to the authorized parties.

A smart city has vehicles equipped with sensors that provide real-time data such as geo-location, speed, or heading. Public transit vehicles and emergency vehicles are also equipped with such sensors. The data is forwarded to the city's traffic management center where it monitors traffic trends and responds to incidents. The data is transported via a publish/subscribe protocol such as OASIS MQTT.

Figure 4: LockBox and city traffic flows

To protect its citizens, increase public security, and reduce emergency response times the city implements a series of security measures and optimization on its IT infrastructure. For example city officials decide to

- Limit the entities that can subscribe to certain message topics (e.g. police vehicle location)
- Protect the city's private IT resources from unauthorized access
- Efficiently dispatch messages to emergency response vehicles
- Locate and warn vehicles that are near an incident
- Create on-the-fly communities that can communicate traffic information privately and efficiently
- Grant access to city resources based on a requestor's context

The LockBox solution is the ideal service to implement the city's security requirements seamlessly. The LockBox Secure Information Exchange is used to access the city's IT resources by imposing a spectrum of policies that dynamically monitor the context of any requesting entity. For example a police officer may not access the city's emergency traffic information console whenever she/he is not located in a registered police vehicle. Whenever an accident occurs, the LockBox will automatically generate temporary private topics and CoIs that include the closest emergency response vehicles and all other vicinity vehicles. The vehicles are dynamically added and removed from the CoI's as they approach and leave the accident location within a certain radius. Each of these changes has the LockBox Critical Infrastructure Protection orchestrate the required network modifications enabling protection within the city's datacenters and between the members of the CoIs.

Quantum Random Number Generation

The Lockbox leverages an optional centralized ultra-fast Quantum Random Number Generator (QRNG). This QRNG find its randomness in the quantum fluctuations of a special type of laser light and can deliver up to 4 Billion cryptographically secure random bits per second (4 Gbps).

In the absence of sufficient peripherals it is common practice to use a pseudo random number generator (PRNG) to produce keys. A PRNG is a deterministic software program for generating a sequence of numbers that only approximates the properties of genuine random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial parameters and eventually repeats due to the finiteness of the device on which it is running. To initialize a sequence, the algorithm employs an internal state of the device (called a seed) such as the device's current time. The algorithm will always produce the same sequence thereafter when initialized with the same seed. This resource becomes meaningless in a cryptographic context if an unauthorized user can correctly guess the PRNG algorithm as well as the initial seed used to generate the random numbers.

A cryptographically safer alternative in producing random numbers is to use a hardware random number generator (HRNG). A HRNG is an apparatus that generates random numbers from a physical process. Such devices are often based on physical systems such as thermal noise, avalanche noise, or time drift. Depending on the generation rate of the HRNG and the requirements of a given device, the HRNG can either feed the device locally (e.g. the HRNG is installed on the mother board or connected via USB) or at a distance (e.g. through a network). The former method is equivalent, from the device's perspective, to having access to peripherals producing good quality randomness. The latter is equivalent, from the device's perspective, to having access to a virtual peripheral connected to a delocalized source of good quality randomness distributing random numbers over a network. In this case a device requests random numbers over the said network whenever its operating system or applications are in need of random numbers.

Delocalizing and distributing random numbers through a single (or several) HRNG(s) deployed within a network to provision a number of devices is a recent idea that offers many advantages. Most importantly this centralized approach reduces the cost of ownership and management of resources. Indeed, given the size of modern datacenters, which can host tens of thousands of servers, installing, running and maintaining a HRNG such as a USB key on every server can rapidly become a daunting and expensive task.

To solve this problem, M2Mi leverages an optional centralized ultra-fast Quantum Random Number Generator (QRNG). This QRNG find its randomness in the quantum fluctuations of a special type of laser light and can deliver up to 4 Billion cryptographically secure random bits per second (4 Gbps). This incredible bandwidth offers the opportunity to produce a centralized QRNG that can simultaneously address many physical and virtual devices. With a maximum throughput of 4Gbps, this QRNG can distribute random numbers on a datacenter's LAN, providing up to 4000 devices with 1Mbps of random numbers.

The random numbers produced by the QRNG are transported securely through the network using a novel cryptographic protocol that limits the required computational resources to guarantee authentication, integrity, privacy and uniqueness of every random sequence. This is especially useful for M2M and IoT devices that are limited in their processing capacity. A device can thus expect to receive its own sequence of secure random numbers in the same fashion as if it was done locally.

The Centralized QRNG is thus an ideal companion for traditional HSMs as it produces the keys HSMs manage within the datacenter and enables to reach external end-devices. Finally the QRNG's large throughput enables an extremely low cost per generated key.

Founded – 2006 at NASA Research Park

Trusted production solutions

- Fortune 500 customers
- Installed on thousands of network and compute cloud data center assets

Intellectual property and trademarks

- “Personal portal and secure information exchange”. Patent US7376652 granted 2003.
- Global Trademark “M2M Intelligence®”

Industry leadership

- Founding member of OASIS MQTT
- Member of Smart Grid Interoperability Panel

Machine-to-Machine Intelligence (M2Mi) Corporation

NASA Research Park
Building 19, Suite 2063
Moffett Field, CA 94035
USA

General Enquiries: info@M2Mi.com

1-(650)-961-5376 phone

1-(650)-961-5934 fax

M2Mi™
Machine-to-Machine Intelligence Corporation