White paper

Securing interactions in the Industrial Internet of Things

Authors: Anthony Fitze, Carl Fenger, LEGIC Identsystems

IIoT devices are especially vulnerable to attack. The key to solving this looming problem lies with the security system that grants and manages device access to users at the network edge.

Summary

Until now, internet security has focused on information theft – protecting data hosted in the cloud. With the Industrial Internet of Things (IIoT), new challenges are emerging as mission-critical machines and infrastructure become dependent on the same vulnerable internet.

Securing the Industrial Internet of Things

Securing interactions on the edge

Unlike data, IIoT devices and assets are not stored in the cloud but are at the network edge. The key to protecting these assets lies with the gatekeeper – the security system at the edge that authenticates users and manages their rights to access and use IIoT edge devices such as building access systems, public infrastructure, connected vehicles, and industrial machines.

That internet-based services continue to function is the result of considerable efforts to stay one step ahead of hackers who work tirelessly to defeat security measures. Our current line of defense consists mainly of the asymmetric cryptographic protocol "Transport Layer Security" or "TLS" which is the most widely used technology for security of data traversing the internet. This is indicated by "HTTPS" ("HTTP over TLS") that you see in your web browser address bar. Yet, TLS is vulnerable. First released in 1995, the fact that TLS is now in its seventh release is evidence that it is only a matter of time before any "secure" internet transport protocol is compromised.

As the battle between hackers and security protocols continues, it is generally acknowledged that the best way to protect data from unauthorized interception is to keep encryption keys off the internet and stored in an offline hardware secure element. This is a well-known fact that underpins the success of Bitcoin and other cryptocurrencies.

Protecting the "Internet of Things to Steal"

The number of connected devices has already surpassed the number of human users. We will soon be reading very different headlines as valuable, mission- and life-critical edge devices become dependent on internet connections. Business and life-critical targets include public transportation systems, (driverless) vehicles, healthcare devices, industrial robots, power-grid equipment, dams and nuclear power plants, as well as access control systems for offices, schools, airports, government buildings and hospitals. The damage caused by hackers who are able to breach critical infrastructure will far exceed that of few million Facebook user profiles or stolen credit card numbers.

Securing critical IIoT assets: a platform approach

The most expensive and mission-critical connected devices are those that are regularly accessed and shared by multiple users. This includes industrial equipment, shared vehicles, hospital diagnostic machines, construction equipment and hotel rooms, all which typically cost hundreds of thousands, or even millions of dollars.

Authentication of a large user population and management of their permissions to access valuable IIoT assets at scale, and in real-time, requires a well-managed relationship between people, devices and required functionalities.

Key system requirements include an automated, end-to-end platform that can securely and, where necessary, biometrically authenticate users. It must autonomously grant usage permission dependent on a person's credentials: what he or she is allowed to access and use, how, when, where and which features. Personal preferences can also be included.

Figure 1: IIoT managed devices have a large attack surface. Solving this problem lies with managing access to, and usage of devices at the network edge.

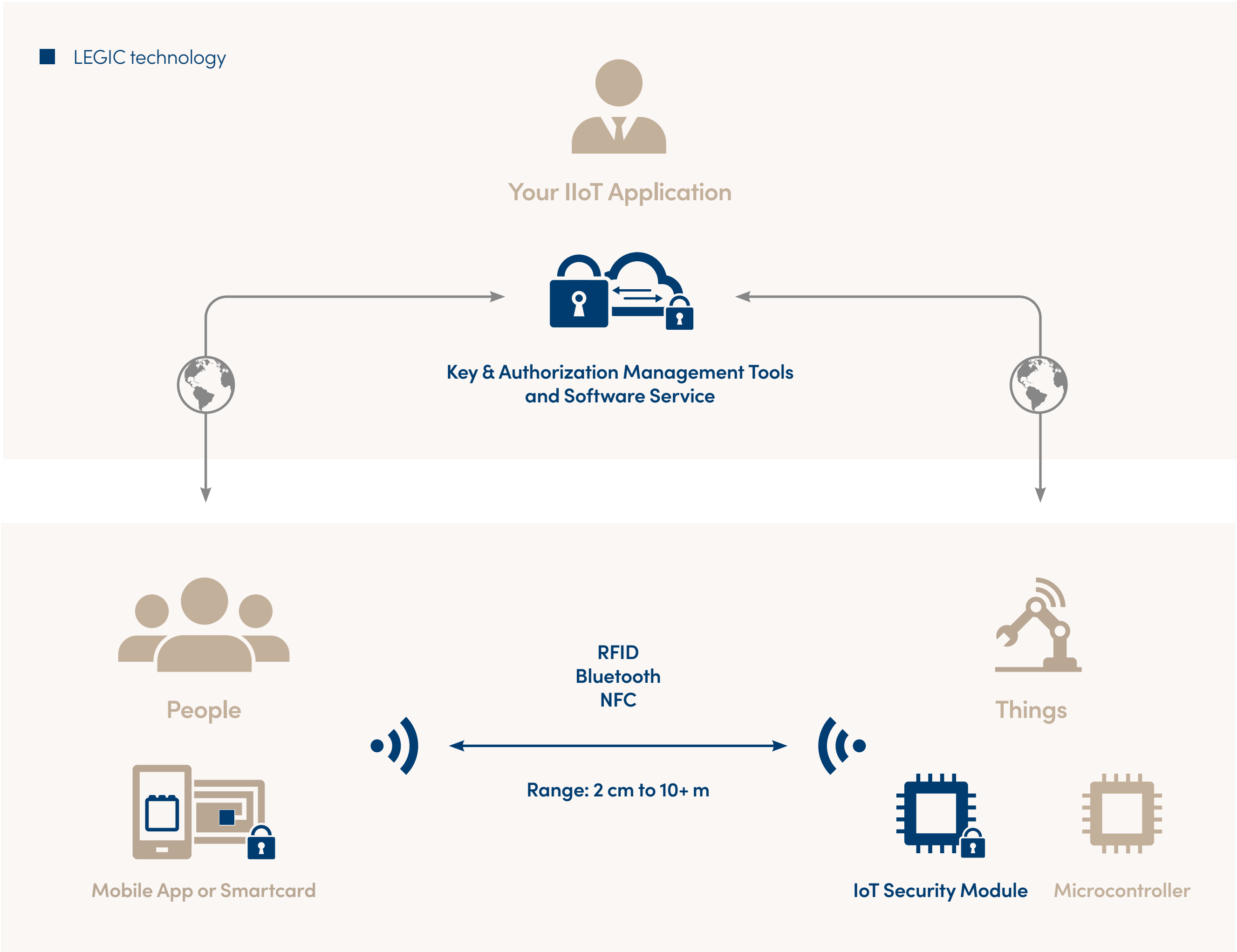

Figure 2: LEGIC provides system integrators with a cryptographically secure authentication and credential management platform used for contactless, permissioned access to devices, assets and infrastructure.

As an internet connection is often not available, and even when available can be unreliable, costly, and require IT support such as user log-in, the system also needs to function when the IIoT asset is offline, e.g., a shared machine or vehicle in a shielded area.

Approval or denial of a user, as well as usage permissioning based on a user's credential must be executed autonomously and immediately at the IIoT asset. Secure authentication intelligence must be provisioned at the network edge in the form of a Security Module with integrated RF transceiver and secure element for storage of encryption keys. Secure element storage can also be used to safely store sensitive application-specific information such as usage data, audit trails, certificates, whitelists and e-payment data.

An end-to-end authentication system based on secure element technology

To meet security and usage requirements, the interface between user and IIoT asset should be made using low-cost, existing devices. As recent events have underscored contactless communication between users and infrastructure is preferrable: it is no longer just a matter of convenience. Transponders based on smartcards or smartphone apps implementing short-range wireless communications such as Bluetooth®, RFID, or NFC and UWB are the most convenient, cost-effective and hygienic method for people to interact with IIoT devices for authentication and credentialing purposes.

Additional security can be implemented via PIN code requirement, or by employing the built-in smartphone fingerprint or facial recognition apps. Based on the user's cloud-managed credentials, access to equipment, specific functionalities and physical areas of usage are automatically assigned and managed by smart edge devices.

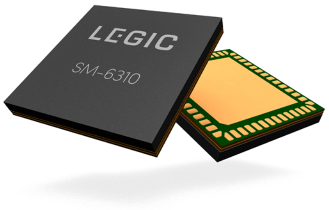

Figure 3: Embedded in IoT edge devices: LEGIC SM-6310 programmable IoT Security Module with integrated NFC, RFID and Bluetooth plus secure element.

	Information Access				Infrastructure Access								Device Access				
	Logistics system	Administration records	Production line controll	Billing / Finance system	Factory main entrance	Production areas	Manufacturing machiens	Logistics / storage areas	Cantine	Administration office	Supply room	Server room	Production control	Logistics machines	Monitoring devices	Storage / shipping containers	HVAC
Plant manager	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CFO	x	x		x	x	(x)		x	x	x	x						
Operators	(x)		x		(x)	x	x		x	x			(x)	(x)	(x)		
Service / IT Staff	x		(x)	(x)	x	(x)	(x)	(x)	x		(x)	x	(x)			(x)	x
Quality control	(x)		(x)		x	(x)	(x)	x	x		x	(x)	(x)	(x)	x		
Auditors*	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)		(x)	(x)	(x)	(x)	(x)	(x)	
Cleaning staff*					(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)				(x)	(x)

(x) = Conditional access (e.g. time of day, available functionality)

* = External service providers

Figure 4: Managing staff access to information and infrastructure

Keeping encryption keys off the internet

The key to protecting high-value or life-critical IIoT assets is to never allow user authentication or credential data to traverse the internet or be stored on a smart device in an unencrypted state. Additionally, during system commissioning, a practical method to securely initialize edge devices with encryption/decryption keys via smartcard or smartphone should be possible. Keys should be invisible to human eyes during the process, even to the person executing the installation.

Two links in Figure 2 are supported by the publicly available internet where Transport Layer Security (TLS) is considered today as the minimal security level for most web traffic. As IIoT apps can be life or business critical, an additional level of security under the service provider's direct control is desirable such as end-to-end AES ("Military Grade Encryption") symmetrical encryption where keys are protected and managed by a Hardware Security Module together with Secure Element technology running in a trusted environment (Figure 3). These well-established, industry-proven techniques provide the strongest protection against hacking, data interception or infrastructure spoofing.

Short-range wireless communication between smartphone / smartcard and infrastructure must also be protected against replay attacks by mutually held, session-dependent encryption keys stored temporarily in a hardware Secure Element.

Use case manufacturing – managing the interactions between employees, information, infrastructure and machines

An example based on the chemical manufacturing industry illustrates the need for managed authentication and permissioning of plant employees and external contractors (Figure 4). A typical chemical plant employs a wide range of staff including plant managers, machine operators, service technicians, quality controllers, external auditors and cleaning personnel.

Each staff function has specific responsibilities which require permission to access buildings, plant areas, machines, administrative, security and logistics systems, etc. Access must be restricted to authorized personnel and may be a function of time as well as available functionality. For example, shift workers are allowed to operate specific machines and functionalities in certain areas at certain times. External contractors such as auditors and cleaning firms must also have controlled access to physical areas and devices, including logging of indoor positions visited.

Important system requirements include integration of biometric verification such as fingerprint or facial recognition, real-time updating of credentials, as well as adding and removing staff at the touch of a button. On- and offline operation is ensured to guarantee operational continuity in the case of network outage. Each edge device is equipped with a Bluetooth®/NFC/UWB-enabled Security Module that is initialized with an encryption key stored in an integrated secure element which is not accessible from outside the module, either electrically or physically (Figure 3).

A trusted gatekeeper at the IIoT edge

With a cryptographically secure, end-to-end IIoT management system in place, electronic user credentials combined with other personal authenticators such as PIN code or biometric data can be employed to authenticate users. User credentials can be combined with location or other context-based information such as sensor data to make tasks easier, more efficient and safer while improving process quality and convenience.

Some specific use-cases:

- **Indoor goods transport:** the platform enables security and logging of goods transported within a production / logistics facility by implementing employee or robot authorization via badge or smartphone authentication. Authorized transport of goods within the facility is facilitated by indoor-navigation based on Ultra-Wideband positioning (see use case "Combining UWB Real-Time Locating System with secure transporter authentication".)

- **Management of shared vehicles:** the platform can facilitate car-sharing by provisioning virtual keys to authorized users (renters) over-the-air. Drivers can book a car via smartphone app, then receive digital keys and credentials to their phones which are valid for a specific vehicle for a specific time period. Based on user credentials, personalized driver settings are automatically applied such as seat, lighting, climate control, navigation, and radio settings.

- **Virtual hotel keys:** the platform enables hotel room booking and check-in via smartphone. Guests download virtual keys, bypass reception and go straight to their rooms. Indoor navigation via UWB guides guests to their destination. Customized offerings can be pushed to each guest's smartphone based on preferences stored in their digital credentials which are downloaded with the key.

Implemented as a security platform which can be integrated with any application, secure symmetrical cryptography combined with Secure Element technology and short-range radio communication is a strong candidate to ensure safe and secure operation of life- and business-critical IIoT systems.

For details, visit:
www.legic.com/iot

About LEGIC

LEGIC Identsystems AG provides system integrators with a cryptographically secure authentication and credential management platform used for contactless, permissioned access to devices, assets and infrastructure. Consisting of software services and semiconductors based on a Root-of-Trust security anchor, the platform is used worldwide for smartphone and smartcard-based access, Smart City and IoT applications.

Authors: Anthony Fitze, Carl Fenger

January 2022