White Paper

Schutz für Interaktionen im Industrial Internet of Things (IIoT)

Autoren: Anthony Fitze, Carl Fenger, LEGIC Identsysteme AG

In der Welt von heute sind IIoT-Geräte besonders anfällig für Angriffe. Der Schlüssel zur Vermeidung dieser Bedrohung liegt in dem Sicherheitssystem, das den Benutzern am Netzwerkrand den Gerätezugriff gestattet und diesen verwaltet.

Zusammenfassung

Bisher konzentrierte sich die Internetsicherheit auf den Diebstahl von Informationen – den Schutz von Vermögenswerten persönlichen Daten, die in der Cloud bewirtschaftet werden. Mit dem schnell wachsenden Industrial Internet of Things (IIoT) entstehen neue Herausforderungen, während wertvolle, geschäftskritische Maschinen und Infrastrukturen vom gefährdeten Internet abhängig werden.

Das Industrial Internet of Things absichern

Schutz für Interaktionen am Übergang zum Netzwerk

Im Gegensatz zu Daten werden IIoT-Geräte und -Assets nicht in der Cloud gespeichert, sondern befinden sich am Netzwerkrand (Edge), das heisst am Übergang zum Netzwerk. Der Schlüssel zum Schutz dieser Assets liegt beim Gatekeeper – dem Sicherheitssystem, das die Benutzer authentifiziert und ihre Rechte für den Zugriff und die Nutzung von IIoT-Edge-Geräten wie Gebäudezutrittsytemen, öffentlicher Infrastruktur, vernetzten Fahrzeugen und Industriemaschinen verwaltet.

Erhebliche Anstrengungen gegen Hackerangriffe sorgen dafür, dass internetbasierte Dienste weiterhin funktionieren. Hacker arbeiten unermüdlich daran, die Sicherheitsmaßnahmen zu umgehen. So setzt man alles daran, den Hackern einen Schritt voraus zu sein. Die derzeit weltweit gebräuchliche Verteidigungslinie besteht hauptsächlich aus dem asymmetrischen, kryptografischen Protokoll Transport Layer Security, kurz TLS. Es handelt sich um die am weitesten verbreitete Technologie für die Sicherheit von Datenübertragungen im Internet. Es wird durch das Kürzel HTTPS (HTTP over TLS) in der Adressleiste Ihres Webbrowsers angezeigt. Allerdings ist TLS angreifbar. TLS ist seit 1995 im Einsatz und liegt inzwischen in der siebten Version vor. So scheint es nur eine Frage der Zeit, bis jedes „sichere" Internet-Transportprotokoll gefährdet ist.

Der Kampf zwischen Hackern und Sicherheitsprotokollen geht also unvermindert weiter. Wie lassen sich Daten so schützen, dass sie nicht unbefugt abgefangen werden können? Der beste Weg besteht darin, die Verschlüsselungscodes außerhalb des Internets und in einem sicheren, physischen Secure Element offline zu speichern. So ist zumindest das allgemeine Verständnis. Es ist eine bekannte Tatsache, die den Erfolg von Bitcoin und anderen Kryptowährungen untermauert.

Schutz des „Internet of Things to Steal"

Die Anzahl der vernetzten Geräte übertrifft bereits die Anzahl der menschlichen Nutzer. Wertvolle geschäftskritische und lebenswichtige Edge-Geräte sind von Internetverbindungen abhängig. Zu den geschäftskritischen und lebenswichtigen Zielscheiben gehören öffentliche Verkehrssysteme, (fahrerlose) Fahrzeuge, Geräte im Gesundheitswesen, Industrieroboter, Staudämme und Kernkraftwerke sowie Zutrittskontrollsysteme für Büros, Schulen, Flughäfen, Regierungsgebäude und Krankenhäuser. Daher werden bald ganz andere Probleme die Schlagzeilen beherrschen. Der von Hackern verursachte Schaden, die in kritische Infrastrukturen eindringen können, fällt in eine andere, bedrohlichere Kategorie als der Diebstahl von einigen Millionen Facebook-Nutzerprofilen oder Kreditkartennummern, der uns bisher beschäftigt hat.

Schutz kritischer IIoT-Assets: ein Plattform-basierter Ansatz

Die teuersten und geschäftskritischsten vernetzten Geräte sind diejenigen, auf die regelmäßig zugegriffen wird und die von mehreren Benutzern gemeinsam genutzt werden. Dazu gehören Industrieanlagen, Fahrzeuge beim Carsharing, Diagnosegeräte in Krankenhäusern, Baumaschinen und Hotelzimmer, die in der Regel mit Kosten in Höhe von Hunderttausenden bzw. Millionen von Euros einhergehen.

Abbildung 1: IIoT Geräte bieten eine große Angriffsfläche. Die Lösung dieser Problematik liegt in der Verwaltung des Zugangs zu und der Nutzung von Geräten am Netzwerkrand.

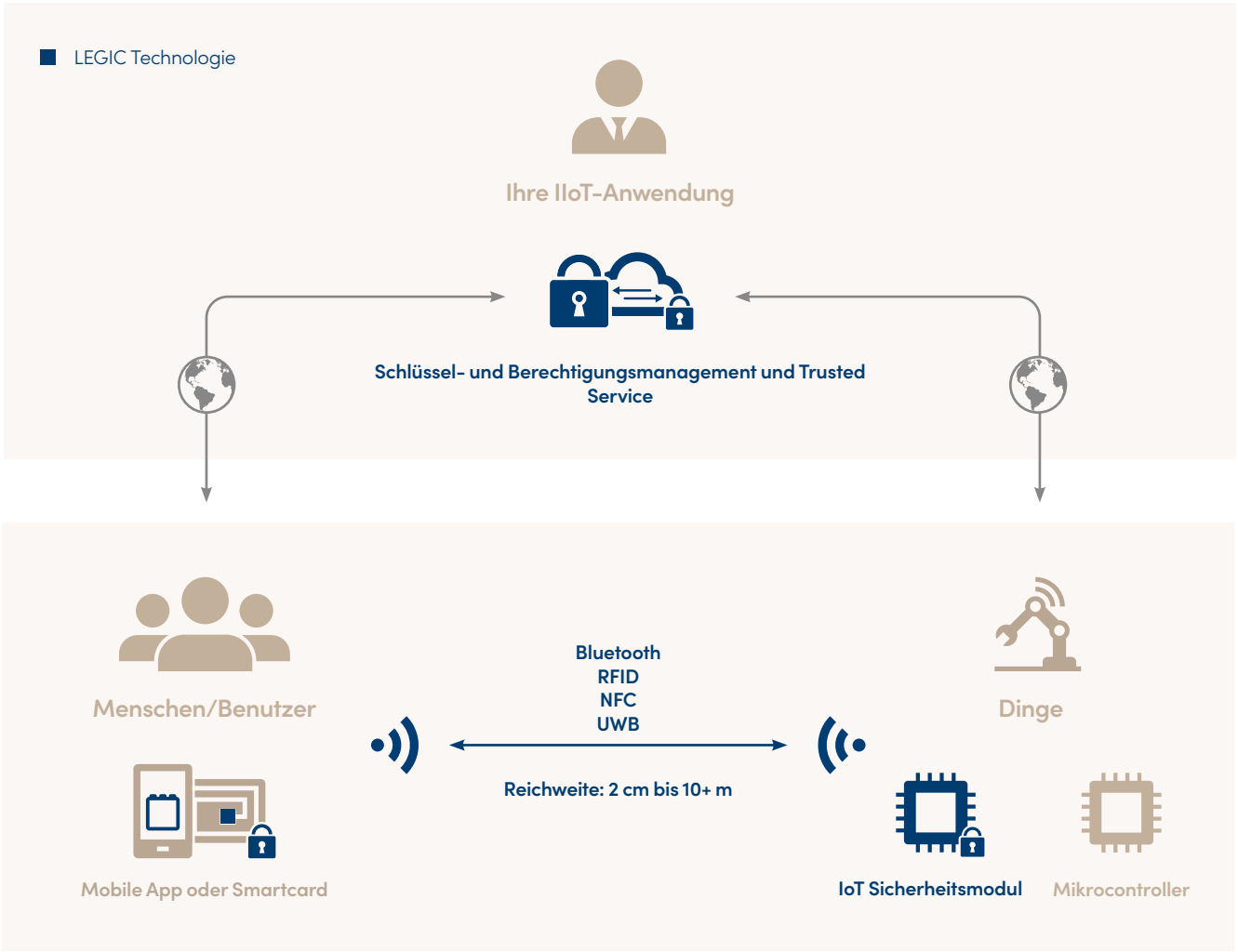

Abbildung 2: LEGIC bietet Systemintegratoren eine kryptografisch sichere Authentifizierungs- und Credential-Management-Plattform für den kontaktlosen, autorisierten Zugang zu Daten, Geräten, Assets und Infrastruktur.

Die Authentifizierung einer großen Nutzerpopulation und die Verwaltung ihrer Berechtigungen für den Zugriff auf wertvolle IIoT-Ressourcen in großem Umfang und in Echtzeit erfordern eine ordentlich verwaltete Beziehung zwischen Menschen, Geräten und dazugehörigen Funktionen (Abb. 3).

Zu den wichtigsten Anforderungen an das System gehört eine automatisierte End-to-End-Plattform, die eine sichere und bei Bedarf biometrische Authentifizierung der Nutzer ermöglicht. Sie muss selbstständig Nutzungsrechte gewähren, die von den Credentials einer Person abhängen: was darf diese Person nutzen, wie, wann, wo und mit welchen Funktionen? Auch persönliche Einstellungen können berücksichtigt werden.

Eine Internetverbindung ist oft nicht verfügbar und kann, selbst wenn sie verfügbar ist, unzuverlässig und kostspielig sein. Außerdem erfordert sie IT-Unterstützung wie Benutzeranmeldung. Deshalb muss das System auch dann funktionieren, wenn das IIoT-Asset offline ist, z. B. wenn eine gemeinsam genutzte Maschine oder ein Fahrzeug sich in einem abgeschirmten Bereich befindet.

Die Prozesse, ob ein Benutzer den Zugriff erhält oder nicht und ob die Nutzung auf der Grundlage der Credentials eines Benutzers erlaubt wird, müssen autonom und unmittelbar am IIoT-Asset ausgeführt werden. Die sichere Authentifizierungsintelligenz muss am Netzwerkrand in Form eines Sicherheitsmoduls mit integriertem RF-Transceiver und einem Secure Element zur Speicherung der Verschlüsselungscodes bereitgestellt werden (Abb. 3). Secure Element Storage kann auch zur sicheren Speicherung vertraulicher, anwendungsspezifischer Daten wie Nutzungsdaten, Audit Trails, Zertifikaten, Whitelists und E-Payment-Daten verwendet werden.

Ein End-to-End-Authentifzierungssystem auf der Grundlage der Secure-Element-Technologie

Um die Sicherheits- und Nutzungsanforderungen zu erfüllen, sollte die Schnittstelle zwischen Nutzer und IIoT-Asset mit kostengünstigen, bereits vorhandenen Komponenten realisiert werden. Wie die jüngsten Ereignisse verdeutlicht haben, ist die kontaktlose Kommunikation zwischen Nutzern und Infrastruktur vorzuziehen: Sie ist nicht mehr nur

Abbildung 3: Integriert in IoT-Edge-Geräte: LEGIC SM-6310, programmierbares IoT-Sicherheitsmodul mit integriertem NFC, RFID und Bluetooth plus Secure Element

	Datenzugriff				Zugriff auf Infrastruktur								Gerätezugriff			
	Logistiksystem	Verwaltungsakten	Steuerung der Fertigungslinie	Abrechnungs-/Finanzsystem	Haupteingang des Werks	Produktionsbereiche	Fertigungsmaschinen	Logistik-/Lagerbereiche	Kantine	Verwaltungsbüro	Versorgungsraum	Serverraum	Produktionskontrolle	Logistikmaschinen	Überwachungsgeräte	Lager-/Versandbehälter
Betriebsleitung	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					
Bedienung	(x)		x		(x)	x	x		x	x			(x)	(x)	(x)	
Service/IT	x		(x)	(x)	x	(x)	(x)	(x)	x		(x)	x	(x)			(x)
Qualitätskontrolle	(x)		(x)		x	(x)	(x)	x	x		x	(x)	(x)	(x)	x	
Audits*	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)		(x)	(x)	(x)	(x)	(x)	(x)
Reinigung*					(x)	(x)	(x)	(x)	(x)	(x)	(x)	(x)				(x)

(x) = Bedingter Zugriff (z. B. abhängig von Tageszeit, verfügbarer Funktionalität)
* = Externe Dienstanbieter

Abbildung 4: Verwaltung des Zugangs der Mitarbeitenden zu Daten und Infrastruktur

eine Frage der Bequemlichkeit. Transponder auf der Basis von Smartcards oder Smartphone-Apps, die drahtlose Kommunikation über Kurzstrecke, wie Bluetooth®, RFID, NFC und UWB implementieren, sind die bequemste, kostengünstigste und sauberste Methode für die Interaktion von Menschen mit IIoT-Geräten zu Authentifizierungs- und Credentialing-Zwecken.

Zusätzliche Sicherheit kann durch die Anforderung eines PIN-Codes oder durch die Verwendung der integrierten Smartphone-Apps zur Fingerabdruck- oder Gesichtserkennung erreicht werden. Auf Grundlage der in der Cloud verwalteten Credentials der Benutzer wird der Zugang zu den Geräten, zu spezifischen Funktionen und physischen Nutzungsbereichen automatisch zugewiesen und von den Smart-Edge-Geräten verwaltet.

Verschlüsselungscodes im Internet? Undenkbar

Der Schlüssel zum Schutz hochwertiger oder lebenswichtiger IIoT-Ressourcen ist eigentlich ganz einfach. Man darf niemals zulassen, dass Benutzerauthentifizierungs- oder Credential-Daten unverschlüsselt im Internet im Umlauf sind oder unverschlüsselt auf einem Smartdevice gespeichert werden. Darüber hinaus sollte bei der Inbetriebnahme des Systems eine praktische Methode zur sicheren Initialisierung von Edge-Geräten mit Verschlüsselungs- und Entschlüsselungscodes per Smartcard oder Smartphone möglich sein. Die Schlüssel sollten während des Vorgangs für menschliche Augen unsichtbar sein, auch für die Person, die die Installation durchführt.

Die beiden oberen Verbindungen in Abbildung 2 werden vom öffentlich zugänglichen Internet unterstützt, wo Transport Layer Security (TLS) heute als minimale Sicherheitsstufe für den meisten Webverkehr gilt. Da IIoT-Apps lebenswichtig oder geschäftskritisch sein können, ist eine zusätzliche Sicherheitsebene unter der direkten Kontrolle des Dienstanbieters wünschenswert, z. B. eine symmetrische End-to-End-Verschlüsselung nach AES (Verschlüsselung nach Militärstandard). Hierbei sollten die Schlüssel durch ein Hardware-Sicherheitsmodul zusammen mit der Secure-Element-Technologie geschützt und verwaltet werden, die in einer vertrauenswürdigen Umgebung läuft. Diese etablierten, in der Branche bewährten Techniken bieten den stärksten Schutz gegen Hackerangriffe, das Abfangen von Daten oder das Spoofing von Infrastruktur.
Die drahtlose Kommunikation über Kurzstrecken zwischen Smartphone/Smartcard und Infrastruktur muss ebenfalls durch wechselseitig gehaltene, sitzungsabhängige Verschlüsselungscodes, die temporär in einem Hardware-Secure-Element gespeichert sind, gegen Replay-Angriffe geschützt werden.

Anwendungsfall Fertigung – Verwaltung der Interaktionen zwischen Mitarbeitenden, Daten, Infrastruktur und Maschinen

Ein Beispiel aus der chemischen Industrie veranschaulicht die Notwendigkeit einer verwalteten Authentifizierung und Autorisierung von Werksangehörigen sowie externen Auftragnehmenden (Abb. 4). In einem typischen Chemiewerk ist eine Vielzahl von Mitarbeitenden beschäftigt, darunter in der Betriebsleitung, Maschinenbedienung, Servicetechnik, Qualitätsprüfung, sowie in der Prüfung (bei Audits) durch Externe und in der Reinigung. Jede Funktion hat spezifische Aufgaben, die eine Erlaubnis für den Zugang zu Gebäuden, Anlagenbereichen, Maschinen, Verwaltungs-, Sicherheits- und Logistiksystemen usw. erfordern. Der Zugang muss auf autorisiertes Personal beschränkt werden und kann sowohl zeitlich begrenzt sein und von den verfügbaren Funktionen abhängen. So darf beispielsweise bei Schichtarbeit das Personal bestimmte Maschinen und Funktionen in bestimmten Bereichen zu bestimmten Zeiten bedienen. Externe Auftragnehmende wie in der Prüfung und Reinigung müssen ebenfalls kontrollierten Zugang zu physischen Bereichen und Geräten haben, wobei die besuchten Innenbereiche protokolliert werden müssen.

Zu den wichtigen Systemanforderungen gehören die Integration biometrischer Verifizierungen wie Fingerabdruck- oder Gesichtserken-

nung, die Echtzeitaktualisierung von Credentials sowie das Hinzufügen und Entfernen von Mitarbeitenden per Knopfdruck. Der On- und Offline-Betrieb wird sichergestellt, um die operative Kontinuität bei einem Netzwerkausfall zu gewährleisten. Jedes Edge-Gerät ist mit einem Bluetooth®/NFC/UWB-fähigen Sicherheitsmodul ausgestattet, das mit einem Verschlüsselungscode initialisiert wird, welcher in einem integrierten Secure Element gespeichert ist. Das Secure Element ist von außerhalb des Moduls weder elektrisch noch physisch zugänglich.

Ein vertrauenswürdiger Gatekeeper am IIoT-Netzwerkrand

Mit einem kryptografisch sicheren, End-to-End-IIoT-Managementsystem können elektronische Benutzer-Credentials in Kombination mit anderen persönlichen Authentifizierungsmerkmalen wie PIN-Code oder biometrischen Daten zur Authentifizierung von Benutzern eingesetzt werden. Benutzer-Credentials können mit standort- oder anderen kontextbezogenen Informationen wie Sensordaten kombiniert werden, um Aufgaben einfacher, effizienter und sicherer zu machen und gleichzeitig die Prozessqualität und den Komfort zu verbessern.

Einige spezifische Anwendungsfälle:

- **Warentransport in Innenbereichen:** Die Plattform ermöglicht die Sicherheit und Protokollierung von Waren, die innerhalb einer Produktions-/Logistikanlage transportiert werden, indem sie die Autorisierung von Mitarbeitenden oder Robotern per Badge oder Smartphone-Authentifizierung implementiert. Der autorisierte Transport von Waren innerhalb der Einrichtung wird durch Indoor-Navigation auf der Grundlage von Ultrabreitband-Positionierung erleichtert (siehe Anwendungsfall „Kombination eines UWB-RTLS (Real Time Locating System) mit sicherer Transporteur-Authentifizierung").

- **Verwaltung von Carsharing-Fahrzeugen:** Die Plattform kann das Carsharing erleichtern, indem sie autorisierten Nutzern (Mietern) Over-the-Air virtuelle Schlüssel zur Verfügung stellt. Die Fahrer können ein Fahrzeug über eine Smartphone-App buchen. Sie erhalten dann digitale Schlüssel und Credentials auf ihr Smartphone, die für ein bestimmtes Fahrzeug für einen bestimmten Zeitraum gültig sind. Auf der Grundlage der Credentials werden automatisch personalisierte Fahrereinstellungen wie Sitz-, Licht-, Klima-, Navigations- und Radioeinstellungen vorgenommen.

- **Virtuelle Hotelschlüssel:** Die Plattform ermöglicht die Buchung von Hotelzimmern und das Einchecken per Smartphone. Die Gäste laden virtuelle Schlüssel herunter und haben an der Rezeption keinen Zeitaufwand mehr, sondern gehen direkt auf ihr Zimmer. Indoor-Navigation mittels UWB führt die Gäste an ihr Ziel. Mit dem Schlüssel werden digitale Credentials heruntergeladen. Auf der Grundlage der darin gespeicherten Präferenzen können maßgeschneiderte Angebote auf das Smartphone der Gäste gesendet werden.

Die sichere, symmetrische Kryptografie in Kombination mit Secure-Element-Technologie und Funkkommunikation über Kurzstrecken, die als Sicherheitsplattform implementiert ist, welche in jede Anwendung integriert werden kann, bietet die besten Aussichten, um den sicheren Betrieb von lebenswichtigen und geschäftskritischen IIoT-Systemen zu ermöglichen.

Weitere Informationen finden Sie unter www.legic.com/de/iot

Über LEGIC

Seit über 25 Jahren ermöglicht LEGIC Unternehmen aus aller Welt die Implementierung von Lösungen mit anspruchsvollen Sicherheitsanforderungen. Auf der Grundlage von Schlüsselverwaltung, Trusted Services und sicheren, kontaktlosen Halbleitern bietet die LEGIC-Sicherheitsplattform End-to-End-Sicherheit für Smartphone- und Smartcard-basierten Zugriff, Mobilität, gemeinsam genutzte Ressourcen und industrielle IoT-Anwendungen.