Automotive IoT Security

Countering the most common forms of attack

AUTOMOTIVE IOT SECURITY

COUNTERING THE MOST COMMON FORMS OF ATTACK

FOREWORD BY 5GAA

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of companies from the automotive, technology, and telecommunications industries, working together to develop end-to-end solutions for future mobility and transportation services.

Connected vehicles that share information to make transportation safer, greener and more enjoyable are at our doorstep and strong cybersecurity will underpin these new connected services – overcoming the cybersecurity challenges associated with connected vehicles and the Internet of Things.

The 5GAA endorses the work the GSMA has done to drive the development and adoption of strong automotive IoT security solutions as described here in this document and in the GSMA IoT Security Guidelines.

THE EVOLVING ATTACKER

Over the past several decades, a pattern has emerged in information security: the attackers are winning, and they are winning faster. Today, there are more tools, information and technology available for breaking into computer systems than ever before. At the same time, the defence of computer systems, which requires constant diligence, resilient hardware architecture and skilled engineers, is often inadequate.

In 2011, Don A. Bailey of Lab Mouse Security presented the first ever remote car hack at Black Hat Briefings in Las Vegas. Today DEF CON, one of the world's largest hacker conventions, offers workshops devoted to car hacking that provide hardware tools, free software technologies and canned strategies for bypassing complex security controls.

As interest in hacking grows, not everyone will adhere to the ethical boundaries required of the professional information security researcher. Some individuals will choose to cross the line. Where there are significant weaknesses, criminals will gather to subvert controls in their favour.

Some attackers are employing a new flavour of malware, called “ransomware”, designed to disable a critical system until the victim pays a fee. Many such attacks can cause serious damage. In December 2015, for example, a three-week power blackout was caused by malware installed at electrical facilities operating the power grid for a small district in Ukraine. This malware has been active on the Internet since 2007, but was recently updated to subvert controls and damage hardware in industrial control systems. This is the first known power failure intentionally caused by hackers.

As the Internet of Things (IoT) evolves, and industrial systems become better connected, such attacks are likely to increase. Engineers and executives need to ask themselves *when*, not *if*, an attack will occur against their IoT solution. The only way to guard against such attacks effectively, and ensure the overall technology is resilient, is by building security into the solution at its inception.

This document provides an overview of how to counter the common threats to connected automotive services. Detailed guidance can be found in the GSMA IoT Security Guidelines.

THE ATTACK PATTERN

Attackers tend to target IoT solutions using a conglomeration of methods that stem from the industries and technologies that underpin the IoT. The IoT is essentially a combination of cloud, network persistence, and embedded technologies that enables physically connected computing systems to provide innovative new services.

In other words, the IoT employs existing technologies to enable interactivity and automation.

Thus, attackers can use well-defined strategies and existing tools to seek out vulnerabilities in IoT solutions.

Figure 1 shows some of the components that might comprise an automotive IoT solution.

Figure 1 - Common automotive IoT components and capabilities.

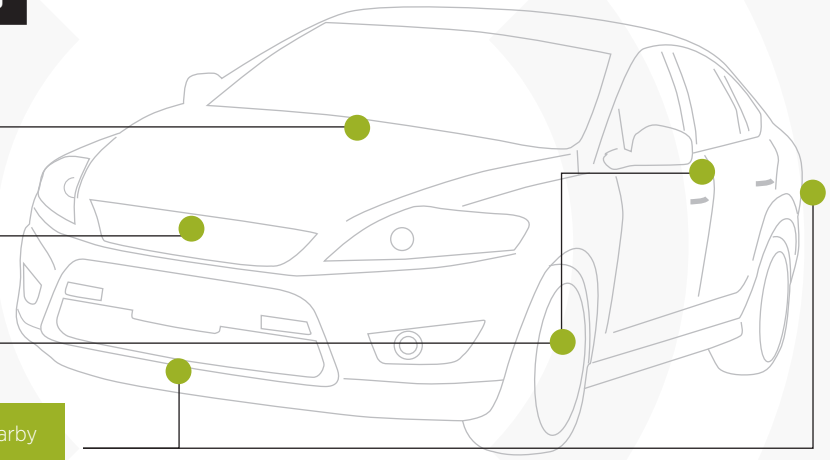
MODERN AUTOMOTIVE IoT CAPABILITIES

Modern telematics systems aggregate data, entertain, and visualize diagnostics

A central computing system guides real-time decision making

Sensors guide drivers toward the safe negotiation of the road conditions

Wireless communication systems interact with nearby peers to relay safety critical metrics and alerts



The common strategies used to attack IoT solutions are:

- Weaknesses in peer authentication
- Practical cryptographic tampering
- Gaps in endpoint integrity
- A lack of segmentation between critical and non-critical applications
- Flaws in software applications
- Business logic weaknesses

Every knowledgeable attacker knows a physical device will be the weakest point of entry into any isolated communications network. Since physical device security is challenging, the easiest way to subvert an IoT ecosystem is by either abusing weaknesses in network communications or weaknesses in the physical endpoint.

Although the core telematics systems might be secured by exceptional engineering, the sensor or ECU (electronic control unit) endpoints that compose the rest of a vehicle's computing network can be difficult to secure because of cost and complexity.

Figure 2 shows some of the ways in which an automotive IoT solution might be attacked.

Figure 2 - Common adversarial strategies in automotive environments.

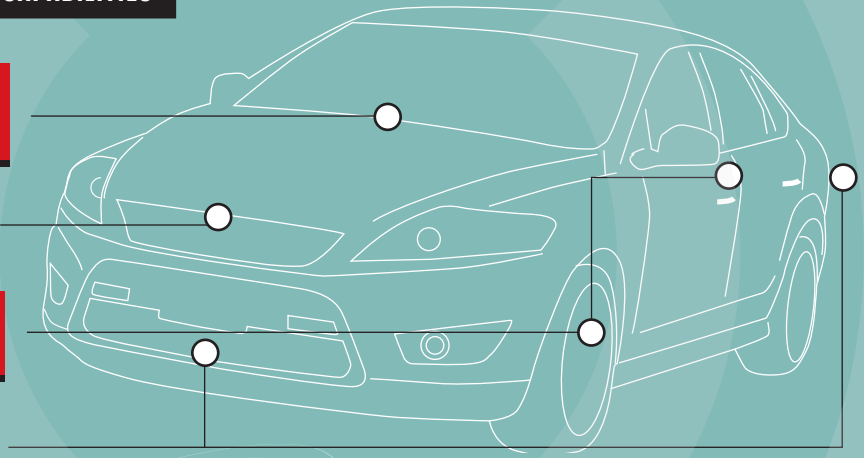
ATTACK PATTERNS AGAINST AUTOMOTIVE IoT CAPABILITIES

Telematics back-end service impersonation, firmware update manipulation, communication security flaws, and third-party application "jailbreaks"

Local or remote CANbus instrumentation to control ECU decision making

Remote code execution or sensor data impersonation via standard wireless protocol weaknesses

Manipulation of critical communication channels by abuse of security certificate or key hierarchies



COST-EFFECTIVE RESOLUTIONS

The issues outlined above are neither systemic nor unsolvable. In fact, there are very cost-effective ways to deter attacks on IoT solutions.

While administrative interface security must largely be addressed separately from the product or service architecture, the following four measures can secure the administrative interfaces made available on the endpoint device.

- **Require the use of a Trusted Computing Base for network and application security**
- **Ensure all network communications are confidential and have integrity**
- **Restrict application behaviour**
- **Enforce tamper resistance**

1. Use a Trusted Computing Base

A Trusted Computing Base (TCB) is a collection of policies, procedures, and technologies that enforce the use and security of critical cryptographic and application-based tokens. It is the foundation upon which a platform's trustworthiness can be defined. If a well-engineered TCB is used at the core of a product, the product will be trustworthy in the field. The use of a TCB can:

- **Diminish or even eliminate the potential for hardware cloning or spoofing**
- **Enforce the use of authentic components within the service**
- **Improve the cost-effectiveness of in-field or remote over-the-air application updates**
- **Increase interoperability and trust between the different components of a service**
- **Improve the longevity of a product**

The GSMA IoT Security Guidelines provide more information on the Trusted Computing Base and can be downloaded from: **www.gsma.com/iotsecurity**

2. Secure Network Communications

The second most important attribute of IoT security is network communications. All components within a network must be able to authenticate one another, and, where applicable, communicate data confidentially, and with verifiable integrity, to ensure data cannot be intercepted, altered, or impersonated.

Without a well-engineered TCB, securing network communications can be problematic and often results in unexpected behaviour in production environments.

For example, many new IoT products use personal area network (PAN) communications technologies, such as Bluetooth Low Energy (BLE), Zigbee, and Thread. These protocols include new security features that allow secure sessions to be created between networked peers on an untrusted network.

Although the cryptographic algorithms these updated protocols use (such as Elliptic Curve Diffie-Hellman) to secure a session are mathematically correct, guarantees about data confidentiality and integrity cannot be assured.

That's because these technologies have no root of trust, don't store keys in tamper-resistant areas of memory and may not have certain processing capabilities required for full session security.

Since the first goal of any would-be attacker is the analysis of network communications, it is imperative the security of network communications is considered a critical aspect of any IoT product or service.

3. Restrict Application Behaviour

Application security is exceptionally challenging, even for battle-hardened companies. While core applications designed by a manufacturer's engineering team can be thoroughly audited, modern architectures often allow third-party applications to be loaded on to IoT endpoints. As app stores enable users to access potentially hundreds of thousands of third-party apps, it is almost impossible for all of them to be thoroughly audited.

The correct way to secure applications is by isolating them in jails, virtual machines, containers, or another abstraction that limits both their functionality and their access to critical system devices or resources.

This way, flaws in the software will not result in an attacker breaking out of the application and accessing critical resources, such as the CANbus. In particular, it is crucial to ensure the application:

- **Cannot elevate its privileges to affect the host operating system**
- **Has no ability to gain access to low-level drivers or devices**
- **Cannot influence the behaviour of other critical applications**
- **Has no ability to write to, or read from, the memory or resources of other applications**

Where these rules are enforced, even if an attacker gains code-execution by exploiting a third-party application, or if the application has a subtle backdoor, the effects are quantifiable and limited to the compromised application. No other application, subsystem, or host operating system should be affected in any way.

4. Enforce Tamper Resistance

As most IoT attacks are channelled through a physical device, obstructing the analysis of these devices can be a practical way to decrease the likelihood of an attack.

Although a physical device in the hands of an attacker will always be at risk of compromise, physical tamper resistance can be used to complicate the attack process and increase the expense to a point where an attack is no longer practical or cost-effective.

For example, light-sensitive fuses can erase memory if a device's case is opened. Similarly, circuits can be embedded in the device's casing, which disconnect a coin-cell battery and cause critical memory components to be erased, if the device is opened. Other methodologies are also available to create cost-effective measures that significantly increase the amount of time, expertise and equipment the attacker must use to succeed in reverse engineering or subverting the device's security.

Figure 3: Cost-effective and practical strategies for securing automotive IoT systems.

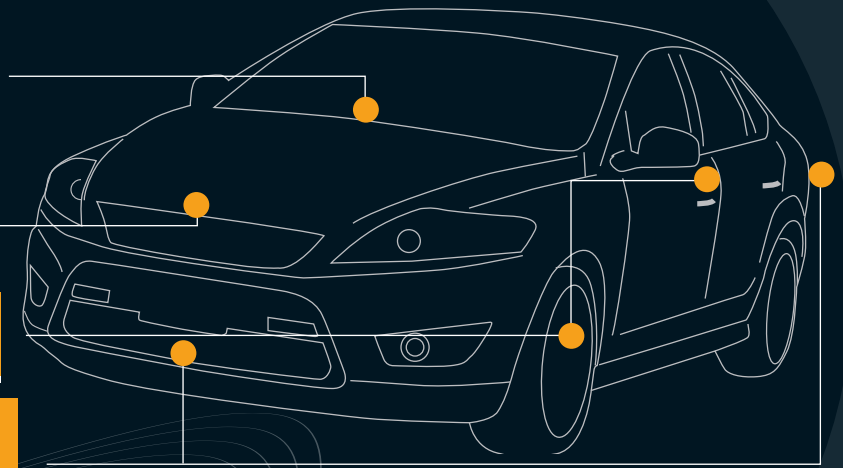
PRACTICAL AUTOMOTIVE IoT SECURITY STRATEGIES

Enforce application level communications security to ensure the highest degree of confidentiality and integrity even when mobile network security is uncertain due to roaming or protocol downgrades

Build trust into the core architecture to decrease long-term engineering cost and improve device longevity

Deploy peer authentication, data confidentiality, and message integrity even on lightweight sensor endpoints

Segment critical and non-critical applications from each other as this diminishes an attacker's ability to affect critical components, if a custom app is compromised



SECURITY ASSESSMENT

It is essential that all connected services are subjected to a rigorous security assessment both during their development and periodically after deployment.

The GSMA IoT Security Assessment provides a flexible framework that addresses the diversity of the IoT market, enabling companies to build secure IoT devices and solutions as laid out in the GSMA IoT Security Guidelines.

Completing a GSMA IoT security assessment will allow an automotive OEM, Tier 1 or Tier 2 supplier to demonstrate the security measures they have taken to protect their products, services and components from cybersecurity risks.

More details on the assessment scheme can be found here: **www.gsma.com/iotsa**

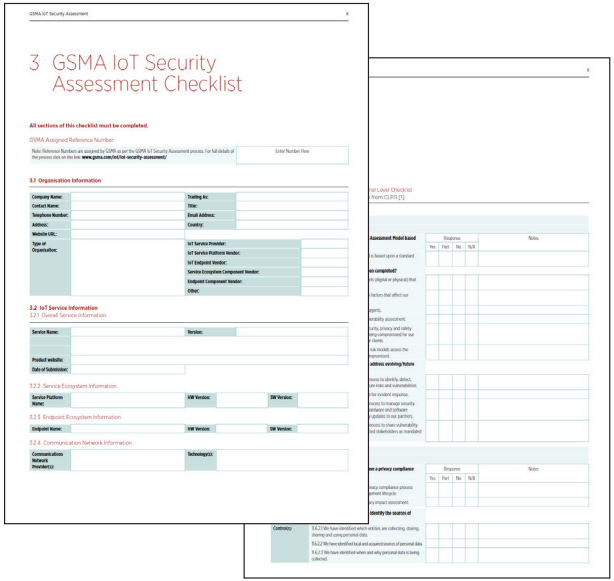


Figure 4 – GSMA IoT Security Assessment Template

SUMMARY

Despite the media hype, IoT solutions can be secured. Cost-effective security starts at the architectural level. Small changes can ensure the entire IoT product or service ecosystem is safe from abuse. But, in order to achieve this, the engineering team must take the time to build in security from the ground up: Security in IoT solutions cannot be implemented as an add-on. It must be a foundation.

Consult the GSMA IoT Security Guidelines for more recommendations on how to remediate common IoT risks.
www.gsma.com/iotsecurity

WORKED EXAMPLE - VEHICLE SENSOR NETWORK

Introduction

Cybersecurity starts with an organisational level agreement of cybersecurity principles. For the automotive sector, the European Automobile Manufacturers' Association (ACEA) have defined a set of Principles of Automobile Cybersecurity to enhance the protection of connected and automated vehicles against cyber threats:

- **Cultivating a cybersecurity culture**
- **Adopting a cybersecurity life cycle for vehicle development**
- **Assessing security functions through testing phases: self-auditing & testing**
- **Managing a security update policy**
- **Providing incident response and recovery**
- **Improving information sharing amongst industry actors**

ACEA's cybersecurity principles dictate the need for 'security by design' and 'security assessment' as described in the GSMA IoT Security Guidelines and IoT Security Assessment.

In this worked example, the design of a vehicle sensor network deployed in a new class of automobile will be evaluated using the guidance provided within the GSMA IoT Security Guidelines. The endpoint design will be evaluated using the GSMA IoT Security Guidelines for Endpoint Ecosystems document (CLP.13), while the service side of the design will be evaluated using the GSMA IoT Security Guidelines for Service Ecosystems document (CLP.12).

The overall design will then be assessed using the GSMA IoT Security Assessment.

1. Evaluate the Design of the Endpoint

In this step we use the GSMA IoT Security Guidelines for Endpoint Ecosystems to evaluate the design of the endpoint.

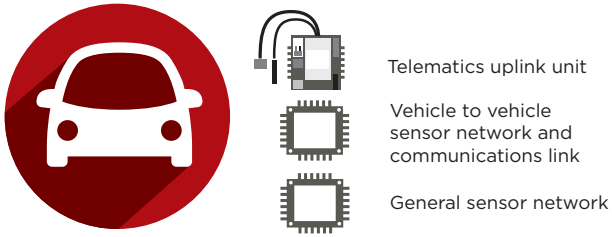


Figure 1 – Full Vehicle Sensor Network and Communications System

While the above model is too complex to properly depict in a simple diagram, the three high-level components involved are:

- **A telematics uplink unit that manages the sensor network, makes complex decisions on behalf of the driver, and maintains a connection to the back-end system**
- **A vehicle-to-vehicle (V2V) system that detects and reacts to V2V events**
- **A general sensor network that provides metrics to the telematics uplink unit**

In modern automotive systems, the telematics unit is a part of the automobile's computer network and makes decisions based on sensor data and back-end communications. This unit will make decisions with, or on behalf of, the consumer driving the vehicle. The unit ensures that the vehicle is operating properly, attempts to make intelligent decisions during emergencies, and takes commands from the back-end network.

The V2V sensor network identifies vehicles in the vicinity and makes decisions based on metrics gathered from sensors. While the telematics unit primarily makes decisions based on the state of components (such as brakes or tire pressure monitors), the V2V system makes decisions based on the presence of other vehicles, or sends out alerts to nearby vehicles in the case of a critical event.

The general sensor network is a series of components that provide data to the telematics unit, and sometimes the V2V unit. These units use the information gathered from the general sensor network to make accurate decisions during critical events.

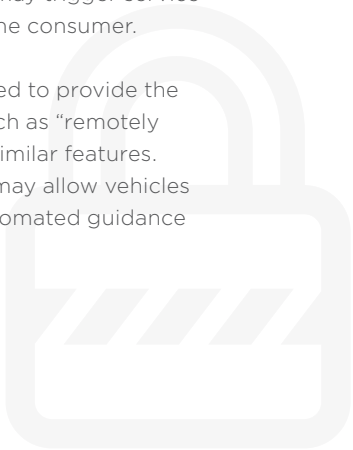
According to the GSMA IoT Security Guidelines for Endpoint Ecosystems, this system has components that fit into every IoT endpoint class. The telematics uplink unit acts as a gateway. The V2V unit acts as a complex endpoint. The general sensor devices are effectively all lightweight endpoints.

2. Evaluate the Design of the Service

In this step we use the GSMA IoT Security Guidelines for Service Ecosystems to evaluate the design of the service.

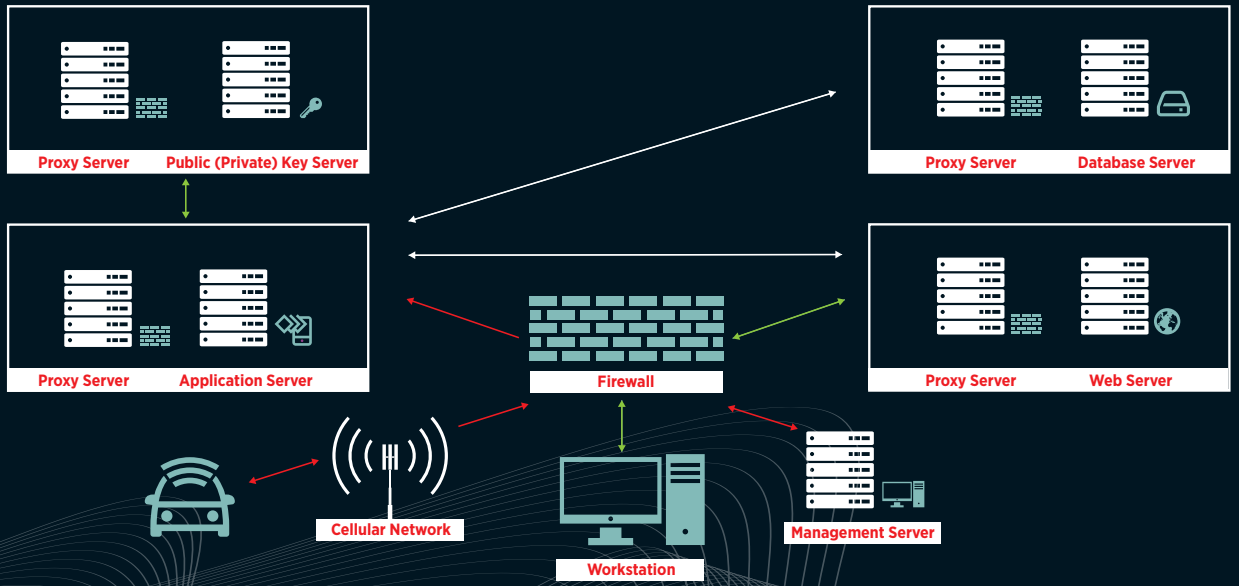
From a service perspective, the vehicle sensor network will provide metrics to the back-end environment. This data may or may not be provided to the consumer. Rather, the data could be stored by the manufacturer to observe or identify potential problems with components. This may trigger service warnings that are then issued to the consumer.

The system may also be augmented to provide the consumer with useful services, such as “remotely unlock door”, “start engine”, and similar features. In the near future, these systems may allow vehicles to be driven remotely through automated guidance systems.



While most critical decisions will be made in the processing units on the vehicle itself, it is reasonable to conjecture that some decisions will be made in the cloud, where more machine learning (ML) and artificial intelligence (AI) along with behavioural or statistical models can be leveraged to make more complex decisions.

Figure 2 – Flow of Data to Back End Services



3. Review the Use Case

The use case of this technology is obvious: to build smarter vehicles that can make complex decisions in safety-critical scenarios. The goal is to leverage the intelligence of as many sensors as possible to make critical decisions in very small windows of time. Automatic breaking, tire blow-out broadcast alerts, temporarily disabled operator warnings, and other critical scenarios can potentially be resolved through the use of sensors and well designed computer systems.

One interesting feature of this technology is that it may be entirely transparent to the user. The user would not need to configure these computers to act in a certain fashion. Instead, they should be capable of negotiating the current landscape through the use of sensor metrics. This will allow the computers to behave correctly regardless of the environment.

4. Define the Security Model

The engineering team at this example business leveraged the Frequently Asked Security Question sections of the GSMA IoT Security Guidelines to determine what issues are most relevant to their product and service.

From an endpoint perspective, the team learned the following issues are of concern:

- **Endpoint impersonation**
- **Service or Peer impersonation**
- **Side-channel attacks**
- **Detecting compromised endpoints**
- **Ensuring safety at the risk of security**

From a service perspective, the team decided the following issues are of concern:

- **Identifying anomalous endpoint behaviour**
- **Managing user privacy**

The biggest risk to this environment that hasn't been discussed in previous examples is the risk of impersonation with regard to peers. One concern that engineers have in this type of environment is the risk that a computer will make critical decisions using data that is not properly authenticated.

Since sensor data in critical scenarios requires exceptionally fast processing times, it is theorized that it may not always be feasible to implement asymmetric cryptography or PKI based communications. However, this may not be an accurate assertion. Instead, an accurate security model should account ahead of time for time-critical scenarios and cache session keys for nearby Endpoints.

For example, if two objects are approaching each other at a known rate, security applications in the Service Ecosystem can prepare session keys specific to these two Endpoints before they reach a distance where they can physically impact one another. This would ensure that secure communication between Endpoints and sensors can still be used in the event that there is no time to renegotiate an instantaneous secure session when the potential for a critical scenario (like an impending automotive crash) is detected.

Thus, an augmentation to the TCB implementation is required. One interesting solution is GBA, where the UICC used in the telematics uplink unit can distribute keys securely to endpoints throughout the system. This protocol will allow even rudimentary endpoints to be seeded with secure session keys that can be used in multiple critical scenarios. This way, the environment can always be seeded from a root of trust, even if lightweight endpoints are not capable of critical maths for public key session initialization.

This is just an illustrative example; other methods (and other roots of trust which do not necessarily require use of the UICC) are available.

Another critical issue in these environments is detecting compromised endpoints. For example, how can the environment recognize whether a simple sensor, such as a tire pressure monitor has been compromised? If the computer makes a critical

decision based on the tire pressure monitor signalling a tire has blown, a safety issue may arise. As a result, the behaviour of devices, and their trustworthiness, must be reassessed at every boot-up phase.

All devices should have tamper resistance, and must be able to notify the network if there is a compromise. Inversely, there should be a way that other devices in the sensor network can evaluate the trustworthiness of peers in the network.

5. Review and Assess the Result

After implementing the recommendations, the vehicle sensor network is well guarded against attacks on the vehicle communications network. GBA is used to distribute keys to all endpoints in the system, and does so on every boot-up, ensuring that old keys are not reused. This, along with tamper resistance, a strong TCB in every endpoint, and an organizational root of trust, allows the environment to function with far less risk.

Yet, regardless of these changes, safety is still a critical factor. The engineering team and business leadership, along with the company's legal team and insurance brokers, should evaluate safety critical technology and determine whether security can be implemented without risking safety of the users. While security can often be implemented, even in safety-critical scenarios, with some architectural adjustments, there are times when safety must come before all other concerns.

The engineering team should ensure the resultant design is fully assessed using tools such as the GSMA IoT Security Assessment. Issues found during the assessment should be resolved and the final assessment recorded.

WORKED EXAMPLE CONCLUSION

Systems like the one described in this example are often well engineered and as a result it can take a large amount of effort to attack the ecosystem. However, subtle flaws in the communications architecture can lead to a compromised environment. In walled gardens, such as some CANbus networks, a single flawed endpoint can cause the entire system to become vulnerable. Such issues, in safety-critical environments, are unacceptable thus necessitating the need for the principles and processes described in this example to be followed.

To keep up with all the latest GSMA IoT news:

Visit our website: **www.gsma.com/IoT**
Sign up for our newsletter: **www.gsma.com/IoT/sign-up-for-newsletter/**
Follow us on LinkedIn: **www.gsma.at/IoT**