Satellite Security for Connected and Autonomous Automobiles

January 2016
# Contents

Satellite Security for Connected and Autonomous Automobiles .................................. 1  
Abstract .......................................................................................................................... 1  
Connected Car Security .................................................................................................. 2  
  Application Security ....................................................................................................... 3  
  Reducing Attack Vectors ............................................................................................... 5  
Benefits of Satellite Networks .......................................................................................... 6  
  High Security .................................................................................................................. 6  
  Robust Reliability and Terrestrial Independence ............................................................. 7  
  Global Scalability ............................................................................................................ 7  
  Ubiquitous coverage ......................................................................................................... 7  
  Cost Efficient - The Lowest Cost Method into the Car ..................................................... 8  
  Source System Integrity .................................................................................................. 9  
  Network-Based Authentication/Certification .................................................................. 10  
  Fast, Thorough, Global Reaction and Remediation ....................................................... 10  
Intelsat’s Information Assurance Program ......................................................................... 11  
  Information Security Framework .................................................................................... 11  
  Information Security Controls and Countermeasures ..................................................... 13  
Conclusion ....................................................................................................................... 14
Abstract

Safety is paramount for connected and autonomous automobiles. They demand failsafe and ubiquitous communication that is more than tamper-resistant – it must have the reliability and dependability of a technology on which human life depends.

Satellite systems provide an attractive solution. A satellite communications link offers a robust and reliable foundation for network architectures having critical security and availability requirements. Intelsat developed its Information Security framework utilizing security controls from the most stringent industry standards and government regulations. Intelsat incorporates the very best practices.

Governments today trust these networks when lives are at stake. And because satellites are removed from terrestrial adversities such as weather and strife it is possible to incorporate a level of redundancy and reliability that is impractical with other solutions.

In addition to the need for uncompromised connectivity it is important to protect from malicious acts. This can only be accomplished by layering security designs throughout the entire system development life cycle. For example, reducing attack vectors is a critical consideration.

Fortunately there are inherent factors in a satellite-based network that significantly reduce its attack surface compared to other approaches. The number of “entry points” and “exit points” in a well-designed satellite network are a small fraction of the possibilities in a network using technologies such as Wi-Fi or 4G/5G.

Satellite systems are uniquely suited to the demanding requirements of this application and offer advantages from the following standpoints, discussed herein:

- Authentication/certification
- Source system integrity
- Application security
- Reduced attack vectors
- Near instantaneous global attack response
- Fast-react to attack, globally, completely
- Configuration management
- Comprehensive Intelsat Information Assurance program

A satellite-based solution using Intelsat’s robust global network meets the security criteria important to today’s cars and offers the critical infrastructure for autonomous cars of tomorrow.
Connected Car Security

Automobiles today are internet-enabled computers with tires and steering – and they travel fast and far. But their speed and mobility do not protect them from remote access – from being hacked – since they are increasingly connected continuously via cellular networks. The benefit of a constant connection is enormous and further advances hold tremendous promise, but the very real threat of costly and even dangerous penetration has been demonstrated through highly publicized “white hat” software attacks on a number of vehicles.

With high end computer functionality already pervasive in automotive technology the industry is aware of the operational and maintenance benefits of enabled vehicles. But as the intelligence and connectivity of the automobile advances, so does its need to communicate beyond its physical boundaries. Activities such as software updates can be accomplished without necessitating a visit to the dealer for a cable-connected upload. While this type of functionality offers attractive flexibility for manufacturers, any connected system is vulnerable to compromise.

The concern over smart-car issues and vulnerabilities has become forefront. It is paramount that security be addressed continually throughout the system’s life cycle. A key component to minimizing risk is selecting a transport mechanism that is dynamic, reliable and secure.

Currently some vehicles use private home Wi-Fi networks for connectivity while others employ public-access cellular networks, which is an increasing concern for vulnerabilities. These unmanaged transport options introduce a new set of malicious vectors that bad actors can exploit in addition to multiple attack vectors in the vehicle itself. In most cases unmanaged transport is the weakest link in the security chain of the connected ecosystems.

Satellite technology provides reliable, secure and ubiquitous access possibilities for the automobile node. This paper discusses that although node security in the automobile is vitally important; the more

---

1 Publication of this paper predates release of the new standards recommendation for connected cars from SAE International (Automotive Recommended Practice, SAE J3061, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems") and so it cannot be specifically addressed herein. However, its progress and content are being tracked and the authors anticipate release by February 2016.
comprehensive solution involves the layering of security at every level of the solution hierarchy, and throughout its life-cycle.

Overall network security, and in the case of connected automobiles consumer safety, demands that every conceivable use-scenario is as robust and reliable as is normal operations. Important considerations over the life-cycle include planned and unplanned deviations from standard ops such as: deployment; maintenance; contingency; failure detection / recovery; and upgrade.

A discussion of network security for future mobility comprises the following elements:

- Application security
- Reducing attack vectors
- Source system integrity
- Network based Authentication/Certification
- Fast, thorough and global reaction/remediation.

**Application Security**

There is no such thing as ‘bullet proof’ software.

“Software will always have bugs. Whether you are looking at a defect density of one bug per 100, 1000, or 10000 lines of code, there will be always bugs, and a subset of those bugs will be security related. This is the reality of software for the foreseeable future, and it will remain a factor for any products or technologies that contain software.” (Greg Shipley, IQT)

Figure 1 is a simple depiction of the fundamental components of an application or a network’s attack vectors. In essence, exit or entry points or a breach of the channel can allow unauthorized access to important data points. Every application has some form of these components and the attack vectors increases proportionally with complexity. Even bug-free software can be vulnerable to threats. Any unauthorized access to important data points is a concern. The channel in this diagram can fall at any abstraction layer of a communications hierarchy. It can be a connection between firmware, subroutines, applications, operating systems, nodes, or networks, depending on the level of the application’s operation. Certainly an era of extreme interconnectivity is underway and the need for reliable, secure, high-quality global connectivity is increasing exponentially.
As the necessary infrastructures are rolled-out and advanced capabilities are enabled for vehicles, architects must of course be aware of the safety threats inherent in the vehicle itself and in its operation. There will also arise threats which may be only temporary as systems progress from early and intermediate designs to the more secure and robust solutions of the future.

Applications are inevitably vulnerable to attack. Regardless of the extent to which protections are incorporated they are still vulnerable in some measure. Therefore the importance of swift detection and rapid response is on par with that of design rigor. Important data points need to be monitored for suspicious activity just as closely as the most critical operational parameters. Architectures must incorporate a secure and nimble network that can react to breaches quickly and for every affected car in the fleet without waiting for a ‘recall’ trip to the shop.

Current automobiles are almost universally burdened with recall as their only viable option. An architecture having global reach and the capability to remotely access affected vehicles is much simpler and much less expensive. However the most important consideration can be timeliness. If a needed correction might impact safety, any delay is unacceptable.

There have been attempts to correct software glitches or other potentially dangerous problems via USB or dealer-installed software updates. However, implementation has proved to be challenging. Owners may be unaware of any required action or they might simply dismiss the action altogether because, “it’s just a little software glitch”.

Security is a vital requirement in today’s increasingly dynamic and complex threat environment and must be integrated into all phases of the software development life cycle (SDLC) from inception (Figure 2).

**Security in the SDLC Process**

![Security in the SDLC Process](image)

**Figure 2 - Security Integrated Throughout SDLC**

Application security programs and secure development processes are fundamental for securing communications, connections, and integrations between vehicle software, hardware, firmware, control units, control...
networks, etc. The application security program governs and defines policies, standards, and processes and sets the strategy, goals and organizational structure to support them. Program elements typically include: awareness and training, assessing program maturity and effectiveness, secure development life cycle, incorporating security requirements, vulnerability assessment and remediation procedures, and measuring established metrics.

Because risk management is ongoing, assessments should be conducted as recurring activities throughout the software development life cycle to, in part, identify security risks and emerging threats. For example, a security vulnerability might necessitate the need for a vehicle recall (along with the associated costs), but most importantly could lead to a loss of safety. Implementing security principles, secure coding best practices, and proactive controls are key to reduce vulnerabilities and the associated risk. Examples include, but are not limited to:

- Requirements definition, threat modeling, design reviews, code analysis
- Vulnerability testing, deployment, maintenance
- Security architecture, minimize attack vectors, establish secure defaults, principles of least privilege and defense in depth, don’t trust other services
- Fail securely, preparation of duties, thoroughly resolve security risks, manage the security disclosure process, consider offering a bug bounty / vulnerability reward program
- Parameterize queries, encode data, input validation, enforcement appropriate access controls
- Establish identity and authentication controls, protect data and privacy (including strong encryption in transit and at rest)
- Implement logging, error handling and intrusion detection, leverage security frameworks and security libraries

**Reducing Attack Vectors**

The ability to update a vehicle and efficiently distribute software updates over the air (SOTA) is critical in any connected car solution. Current implementation drawbacks with cellular solutions are difficult to scale and they introduce many points of entry (attack vectors). Alternatively to use owner-provided connectivity introduces additional unmanaged vectors that could compromise the vehicle and possibly the central managed system. Most important is the inherent vulnerability of the public nature of cellular and Wi-Fi networks.

An ideal approach would be to implement a private network. A dedicated private one-to-many multicast network ensures each receiving node is but a step removed from the sender. The attack vectors
are significantly reduced, while also diminishing the ability to ‘spoof’ the network. The entire management process from ingestion into the network to deployment to the node could be viewed, monitored and guarded from one location. Each car receives clean data directly from the source (Figure 3). Virtual private networks over public transit cannot offer the same level of segmentation and come with their own set weaknesses that need to be mitigated.

**Benefits of Satellite Networks**

A satellite-based network from Intelsat offers significant benefits to the connected car application:

- High security
- Robust reliability and terrestrial independence
- Global scalability
- Ubiquitous coverage
- Cost efficient
- Source System Integrity
- Network-Based Authentication/Certification
- Fast, Thorough, Global Reaction and Remediation

**High Security**

Satellites today provide the network of choice for today’s most secure communications built on government-grade security standards. When a military or diplomatic communication is critical it will almost certainly be a satellite communications link that is employed to provide assured connectivity – often with stringent requirements to reduce probability of detection or interception.
Satellite Security for Connected and Autonomous Automobiles

The attack vectors in a satellite network are much fewer than more easily accessed networks such as fiber or cellular. The number of entry and exit points in a satellite network is eight or nine orders-of-magnitude less than cellular (Figure 4). Those that remain are closely guarded and difficult to access. Regardless of end-market use, when a point-to-multipoint application requires cost efficient, ubiquitous multicasting, satellites remain the go-to solution.

**Robust Reliability and Terrestrial Independence**
Intelsat’s expansive satellite network offers in-orbit backup for most locations worldwide. The robust network attributes that result from a geostationary satellite’s distance from terrestrial adversities is further enhanced when in-orbit backup is available. Intelsat networks augment their on-board redundancy with backup by other space vehicles. This allows a failure or problem to be quickly remedied, often before any disruption of service can occur.

**Global Scalability**
The Intelsat network is well suited to worldwide expansion. A connected car service can easily begin as a beta service in a small area anywhere in the world and be incrementally grown as capabilities are rolled-out. Or when beta testing is completed the growth can be an explosive expansion into a worldwide service – or growth can be implemented at any pace in between. A global network such as that offered by Intelsat allows for a controlled scaling that can be slow or fast and has the flexibility to adapt quickly to a changing growth plan as evolving target markets dictate.

**Ubiquitous coverage**
Satellites can truly set the standard for ubiquitous coverage. In the case of Intelsat’s networks it is *globally* ubiquitous coverage. And limitations that naturally result from a geostationary satellite regarding coverage at

---

Figure 4 - Satellite-Based Systems Provide Protected Communications
latitudes approaching the poles will soon be remedied by Intelsat’s participation in the OneWeb low-earth orbit satellite constellation. Together Intelsat and OneWeb will cover 100% of the globe.

**Cost Efficient - The Lowest Cost Method into the Car**

The economic model is as compelling as the benefits in security, reliability and scalability. Satellite-based network implementations vary across fixed and mobile networks, with end-market use spanning the government, enterprise, transportation, and media sectors, all benefiting from greater efficiency, reliability and protection than terrestrial solutions.

Satellites today push terabytes of data into home theaters and digital audio radios for cars. The fastest of aircraft and most leisurely ocean liners get broadband connectivity via satellite, and the services are growing. Extending these capabilities to provide ubiquitous coverage for the connected car is an in-family application of satellite technology.

**Figure 5 - The Connected Car**

The satellite radio and satellite-to-home broadcasting business plans are services that exist today and have similarities to connected cars. In these businesses, the fixed cost structure, whether serving 100 or 1,000,000 subscribers, allows the service provider to achieve attractive cost efficiencies as the business scales, so investment can be funneled into content, not the delivery mechanism. And because the cost of content does not change with an increasing receiver-count, added subscribers will increase revenues but not expenses.\(^2\) This same economic model is applicable to the connected car (Figure 5).

\(^2\) Content providers of radio and television may in fact tie pricing to the number of viewers/listeners, but often in an inverse relationship. The price may decrease as subscribership grows to incentivize distributors toward more subscribers.
The full complement of automobile services, when assessed in aggregate, will represent a sizeable network/connectivity requirement. Existing and future services include: lost vehicle recovery; vehicle diagnosis; telematics; games; medical insurance fraud abatement; living room/car integration; news; sports; weather; entertainment; owners manuals; advanced driver assistance systems; usage based insurance; live television; movies; POIs; enhanced navigation and software/firmware updates over-the-air (SOTA/FOTA).

**Source System Integrity**

The business model of a satellite system is dependent upon integrity. Intelsat’s earth stations are designed to the highest international standards of customer data security. Data flow can be detected but not viewed or decoded by port personnel. The monitoring and control system that coordinates and monitors network traffic is unable to see the information flowing through the system, only the signature of its presence. The health and integrity of the entire network, from data ingestion to certification and return receipt, is visible to the operator. Attacks across the entire data-arc can be detected and abated.

Intelsat maintains the highest standards of Information Assurance by designing and continually assessing networks and infrastructure against the most stringent DoDI 8500.2 MAC Level I controls, NIST 800-53, and ISO 27000 standards. Intelsat teleports make an ideal place to house data center services for efficient distribution of content – “one hop away from the destination”.

**“One throat to choke”…or,**

**The Operational Efficiency of a Global Ubiquitous Solution**

Auto companies find it exasperating to deal separately with each of the more than 130 terrestrial cell carriers. The problems in this regard are significant. First, every software or firmware update should be compatible with the lowest common denominator of performance and throughput for the least capable terrestrial system. This necessitates a ‘dumbing-down’ of the optimal update procedure.

Conversely, if a software patch does exploit a more robust cellular carrier’s capabilities, an evolving and deepening configuration management problem may result for cars only accessible via less capable networks. A global automobile manufacturer might then confront different standards of safety and integrity in different parts of the world – easily becoming a nightmare for customer service and public relations.
An automobile executive recently expressed this frustration as follows: “I do not have the time or ability to manage 130 different cell carriers worldwide – none of whom act as a proper partner should act. Give me one throat to choke!” A critical process requires identifiable and discrete points of responsibility, action and authority. The inherent architecture of a satellite based distribution system is ideally suited for just such a structure because it can provide global service via one highly reliable solution. As the longest operating satellite services provider with the largest and most expansive global fleet, Intelsat has earned its gold standard reputation based upon the reliability, integrity and value of its system.

**Network-Based Authentication/Certification**

The exchange of certifications and authentications must not be vulnerable to ‘man-in-the-middle’ attacks. This means that the acknowledgement path for the reception of updates, the keys to unlock certificates and manage digital rights issues must be securely architected as part of the forward and return path into and out of the car. The Kymeta Ky Vault™ server in the car is an intelligent device that authenticates and certifies data in and out of the car. It holds media for future viewing and works in tandem with additional side-caching at the teleports. It can report location to monetize and enrich the location-based experience; provide for emergency services; cache software updates for later deployment and provide business insights. The authentication and certification protocols are linked to Intelsat’s private network for trusted operation worldwide.

**Fast, Thorough, Global Reaction and Remediation**

Cyclical security management of the connected car is essential, but the ability to react quickly in the event of an immediate issue is equally critical. Once threat exposures have been minimized through: reduced attack profiles; applications security; source systems integrity; and network-based authentication/certification, the system must remain capable to quickly and thoroughly repair, patch and replace.

No application is 100% secure so the ability to respond to a threat or an attack FAST is vital. On occasion it may be imperative to replace an entire software version rather than in a patch-upon-patch fashion, perhaps even at the exact moment software regression testing is completed. The ability to do so fast and globally may be vital to customer safety.

Fortunately speed and ubiquity are inherent characteristics offered in a satellite-based solution. For example, it is essential to have visibility into the entire communications path when identifying and responding to operational issues. A satellite network solution offers a single vendor – a partner – with
whom data can be shared and on which dependence can rest to assume whatever level of involvement or disassociation may be desired.

It is appropriate to acknowledge that Tesla and others have demonstrated automotive software maintenance via Wi-Fi and cellular networks. However, the scale of the problem is much different for a global automotive enterprise than it is for a limited distribution vehicle or a small boutique brand catering to affluent consumers. Architectures comprised of small and expensive terrestrial cellular channels will tend toward smaller, more incremental system patches that invariably lead to a diverging configuration management nightmare of disparate revisions and patch-upon-patch maintenance.

A solution supporting a small number of models in a narrow region may not scale globally or satisfy a price-sensitive worldwide consumer market. The stark difference in scale between the examples of Tesla and Toyota is exemplified by their respective production volumes: Tesla sold about 23,000 Model S units in 2015, whereas Toyota sold about 2.5 million vehicles in the US alone and over 10 million vehicles globally in 2015. An adequate solution for one may be entirely wrong when scaled by two orders of magnitude.

**Intelsat’s Information Assurance Program**

Intelsat’s Information Assurance program focuses on prevention and restoration by taking a systematic defense-in-depth approach to detect, prevent, and mitigate attacks, enhancing resilience and mission assurance in its satellite, ground, and network infrastructure. The program is centrally managed by Intelsat’s Information Security team, which is the authority for all Intelsat Information Assurance policies.

Further, Intelsat maintains a comprehensive Information Assurance assessment and remediation program, which includes recurring penetration assessments, organization-wide control assessments, and annual third-party Service Organization Control (SOC3) audits against Intelsat’s satellite and terrestrial service environments including Intelsat’s satellite commanding, teleport, terrestrial, and service management infrastructure and relevant service procedures.

**Information Security Framework**

Intelsat’s Information Security team maintains the enterprise-wide Information Security Policy and within the Policy, Information Security defines roles and responsibilities applicable to the entire company. The Policy is approved by management, published, communicated to employees, reviewed a minimum of twice per year, and it is updated as applicable. Employees are required to complete Information Security
awareness training during new hire training and on an annual basis thereafter.

Intelsat’s Information Security framework addresses continuously evolving threats and risks using a lifecycle approach (Figure 6) that consists of the following phases:

- Set security goals
- Identify assets, applications, networks, and services
- Assess risks (consequences, vulnerabilities, and threats)
- Prioritize
- Implement protective programs
- Measure effectiveness

Information Security implements its framework to address the following across its service and enterprise networks:

- Information security compliance
- Policy
- Access control
- Threat, vulnerability, and incident management
- Remote access
- Awareness and education
- Network management applications
- Secure design and configuration
- Security information and event management

Figure 6 - Intelsat's Lifecycle Security Approach
Information Security Controls and Countermeasures

Intelsat employs relevant and layered countermeasures to combat the most advanced threats against industry and government. Further, Intelsat continuously evaluates the threat landscape and the effectiveness of its countermeasures to adjust and adapt to the latest threat actors and attack methods. These controls and countermeasures are categorized as shown in Figure 7 below.

![Figure 7 - Intelsat Threat Controls and Countermeasures](image-url)
Conclusion

The car satisfies a wide diversity of human needs, from emotional, to functional, to aesthetic. Automobile technology and the improvements being made in every aspect of the driving experience are nothing short of extraordinary. That is not likely to change soon.

Today’s automobile has moved into a realm that is more akin to a personal computing device than simply a means of transportation. These are the developments that transform the experience from the distant memories of standing roadside with the hood up to what is today and will continue to be a truly luxurious experience.

These are also the developments that deliver the car into the lexicon of hacking, data theft, and cyber threats. But just as these threats are being addressed in the world of software development and IT infrastructure, they are also being addressed in the realm of automotive engineering. The threats are manageable when they are recognized and understood.

It is important to acknowledge that issues will inevitably arise and that it is the network’s ability to react quickly and accurately which becomes the failsafe. This is a long-learned expertise at Intelsat.

Of the many considerations that affect the ultimate security of an automotive system, the wireless access approach need not be a dominant risk. Intelsat has delivered satellite-based communications services for over 50 years and well understands how to make the connection to the connected car secure.