Best Practices for Cybersecurity Management in Telematics

GEOTAB
management by measurement

Editors: Gleb Nikonov, Melanie Serr, Alex Sukhov, Scott Sutarik

About Geotab

Geotab connects commercial vehicles to the internet, providing advanced web-based analytics to better manage your fleet. Geotab's open platform and Marketplace, offering hundreds of third-party solution options, allows both small and large businesses to automate operations by integrating vehicle data with a company's other data assets. As an IoT hub, the in-vehicle device provides additional functionality through IOX Add-Ons. Processing more than 1 billion data points a day, Geotab leverages big data and machine learning to improve productivity, optimize fleets through the reduction of fuel consumption, enhance driver safety, and achieve stronger compliance to regulatory changes. The company's products are represented and sold worldwide through its Authorized Geotab Resellers. To learn more, please visit www.geotab.com and follow us @GEOTAB and on LinkedIn.

Comments or questions related to this white paper can be emailed to: testdrive@geotab.com

For more fleet tips and best practices, visit: www.geotab.com/blog

The Value of Telematics Data

Telematics generates a vast amount of data, including a detailed history of vehicle and driver activities and operations. This type of data is extremely useful within an organization for controlling fuel and maintenance costs, increasing productivity and safety, and minimizing risk. Using telematics for accident reconstruction or benchmarking can generate even greater insight.

Protecting that valuable data is essential. If accessed by a malicious party, there could be serious consequences, potentially jeopardizing customer accounts, schedules, shipments, location of assets, and personal information. Cybercrimes are committed because there is value to be gained from data, whether that data is a collection of usernames and passwords, credit card numbers, or social security numbers, or — as we'll see — telematics data.

Therefore, whether you are a small business owner, fleet manager, developer, CIO or CEO, it's critical that you understand how your telematics data is handled and protected.

What You Will Learn

In this white paper, you will learn about:

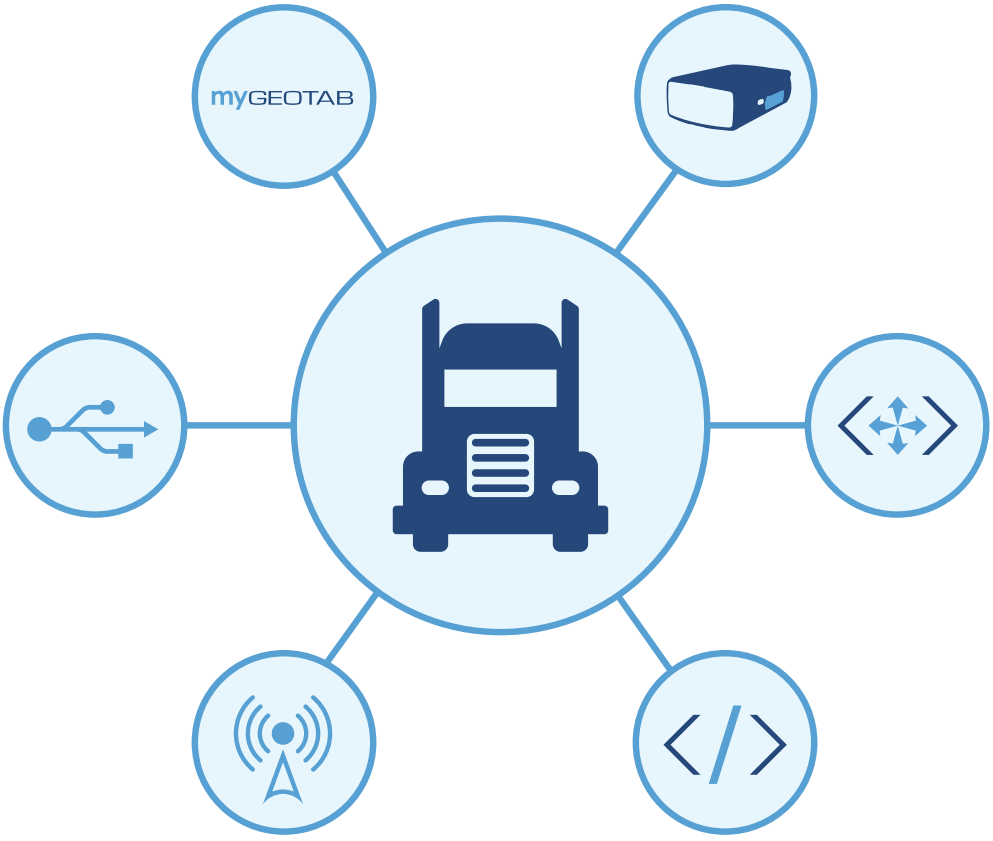
- Overview of the telematics ecosystem
- How Geotab secures telematics data at each level
- Best practices for telematics cybersecurity
- Key questions to ask your telematics provider about security

Overview of the Telematics Ecosystem

Open platform telematics can be viewed as the Internet of Things (IoT) hub of the vehicle, connecting multiple devices to the vehicle through one centralized communications system. An expanding list of third-party devices can be integrated with telematics, such as these solutions from the Geotab Marketplace:

- Bluetooth beacons
- Temperature sensors
- Tire pressure sensors
- Salt and sand spreading monitors
- In-vehicle verbal feedback
- Collision avoidance systems
- Cameras

Open Platform Telematics: The IoT Hub of the Vehicle



The telematics ecosystem includes both hardware and also the software responsible for collecting and analyzing the vehicle data.

The Telematics Ecosystem

Area	Description
Geotab GO Telematics Device GO RUGGED Ruggedized Telematics Device	The Geotab GO is a small telematics device with GPS technology and auto-calibrating accelerometer that plugs into the OBD II port of the vehicle (from passenger vehicles up to Heavy Duty trucks). The device collects data on vehicle position, speed (relative to posted), harsh braking, harsh driving, seatbelt, fuel consumption, odometer, vehicle fault codes, battery voltage, air temp, and other engine data, sending it to the cloud hosted environment for processing and analysis.
MyGeotab Fleet Management Software	Flexible, scalable, web-based software for fleet management. Key features include GPS vehicle tracking, advanced reporting, driver behavior management, engine data reporting, route optimization, engine health and maintenance, accident reconstruction, open data integration, and custom mapping.
Input/Output Expanders	Third-party hardware that connects to the expander port of the Geotab telematics device that performs specific task and relays information to and/or from the device. Examples: driver identification via Near Field Communication (NFC), GO TALK in-vehicle verbal feedback, salt and sand spreader monitoring, and device communication over the Iridium satellite network for remote workers.
Marketplace Solutions	Online center of fleet management solutions that integrate with the Geotab open telematics platform, including software Add-Ins, hardware accessories and Add-Ons, mobile apps, general software solutions, and custom reports. Examples: driver's camera and in-cab video, Bluetooth asset tracking, Mobileye advanced collision prevention, Geotab Drive app for Hours of Service, Driver Vehicle Inspection Reporting and Driver ID, paperless gamification apps.
Software Development Kit (SDK) Application Programming Interfaces (APIs)	The Geotab software development kit (SDK) and Application Programming Interfaces (APIs) are a set of tools for automating tasks, building third-party hardware Add-Ons for the Geotab GO device, and integrating business systems such as accounting, payroll, CRM, maintenance, route planning, risk management and safety compliance.

Best Practices for Telematics Cybersecurity

As businesses gravitate towards software-based systems and working in the cloud, telematics data security will become an even bigger challenge. Telematics systems are expansive and multi-tiered: they are a combination of physical hardware, radio systems, software servers, and human agents. Because there are many components involved, the potential threats[1,2] are numerous and can include theft, GPS jamming, cellular sniffing, firmware manipulation, server exploits, and phishing.

General Strategies for Cybersecurity

Protecting telematics data requires a comprehensive, proactive approach. The integrity of the system relies on the upkeep of many sub-systems, each with its distinct set of potential vulnerabilities. Therefore, in addition to strong policies and processes, creating a culture of security across the organization is the best way to protect data and create resiliency against malicious attacks.

In general, telematics security can be strengthened with these principles from IoT security:[3,4]

Leadership

Establish a dedicated team of security specialists and management who believe in security.

Policies

Set comprehensive and transparent policies on security and privacy.

Design

Implement security best practices in product and software development.

Education

Regular training of employees, partners, and end users on security policies and procedures.

15 Key Recommendations for a Resilient Telematics Platform

The call has gone out for stronger security for the connected vehicle. The FBI has recommended that "vehicle owners should check with the security and privacy policies of the third-party device manufacturers and service providers, and they should not connect any unknown or untrusted devices to the OBD II port."[5] In a similar vein, NAFA Fleet Management Association recommends that "fleet managers should have policies in place to ensure that only secure devices are connected to the port."[6]

Geotab has proposed the following 15 security recommendations for building a telematics platform resilient to cyber threats. For further details, please consult the full article (available at https://www.geotab.com/blog/telematics-cybersecurity-recommendations/).[7]

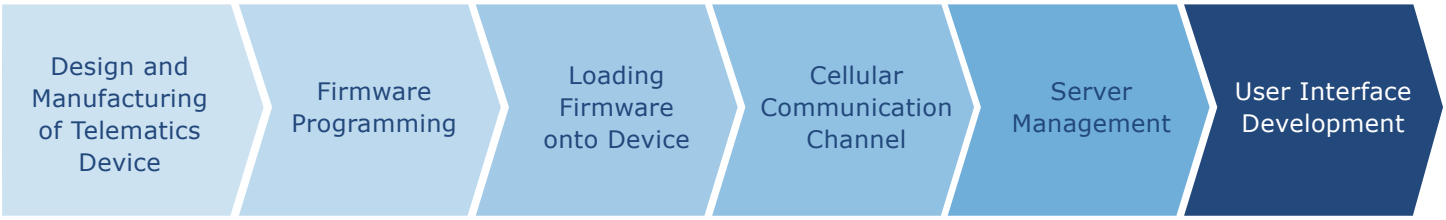
1. Implement secure data transfer
2. Digitally sign updates
3. Enable hardware code protection
4. Assume your code is public so you do not rely on secrets
5. Use cryptographically strong random numbers that cannot be reverse engineered
6. Individualize security-critical data
7. Use different keys for different roles
8. Monitor metadata to detect hacks
9. Do not forget to disable debug features
10. Perform third-party auditing
11. Limit server access
12. Apply secure design practices
13. Implement support for software/firmware updates
14. Verify and test
15. Develop a security culture

Geotab Telematics Platform Security

Geotab takes a rigorous approach to data security following the principle of continuous improvement. To protect our customers and partners, Geotab is constantly reviewing, improving and validating our security mechanisms and processes so our systems remain resilient to intrusion and disaster. Geotab provides customers with comprehensive documentation regarding the technical and organizational data security measures implemented throughout our ecosystem. We also collaborate with leading stakeholders to advance security across the industry.

As a vertically-integrated telematics provider, Geotab is directly involved in every stage of its telematics ecosystem.

Strength Through Vertical Integration



Geotab platform security is designed for end-to-end protection of your data. Key implementations include:

- GO device and network interfaces use authentication, encryption, and message integrity verification to ensure that telematics data cannot be read or forged by malicious parties.
- Over-the-air updates use digitally-signed firmware to verify that updates comes from a trusted source.
- Geotab uses independent third-party experts to validate the platform from end to end.

The following explains in more detail how telematics systems are secured.

Security in Design and Manufacturing

The microelectronic modules on each Geotab GO device are manufactured in fabrication facilities across the globe. The pieces return to Geotab's facilities where the final assembly by Geotab employees completes the GO device hardware. The electronics of each device are tested and then prepared to receive the firmware programming.

Since Geotab does not purchase the device hardware from any other entity and has full control of design, manufacturing, assembly, and testing, we can quickly and efficiently respond to manufacturing defects or potential hardware vulnerabilities internally, without being reliant on any other party.

Firmware Security

Firmware is the specialized software that programs the microcontroller and electronics modules in the device — including communicating with the engine computer and auxiliary systems, receiving GPS coordinates, and coordinating cellular communication.

Because a telematics device attaches itself to a complex and interconnected system, the firmware that issues the orders to the device is an exceptionally important part of the connected car.

A telematics device will receive many updates to its firmware over the course of its life. These updates introduce new features or resolve issues with the device after it has been installed in a vehicle. The device automatically receives over-the-air (OTA) updates and performs the update process in a way that is invisible to the user.

This leaves a potential opening for attackers to attempt to replace the firmware on a telematics device with malicious firmware of their own.

To prevent compromised firmware, the following methods are used to secure the device:

- Controlling firmware installation on the device at the manufacturing stage.
- Digitally-signing over-the-air updates to verify that the updates come from a trusted source.

Without both steps to verify that every firmware update is authentic, it is impossible to know if the device is under your control or the control of a malicious party interested in getting your data.

Secure Data Transfer

The telematics device sends data from the vehicle to the central server over a cellular connection. Although varying by territory, provider, and infrastructure, cellular communication is commonly done over 2G, 3G and 4/5G networks, which can have their own unique vulnerabilities.[8]

A secure communication channel can be established with the use of encryption. Encryption is the process of encoding a message such that only the sender and recipient would be able to view the message. To an outside party, like an attacker, this encoded message would appear as a meaningless collection of symbols. The intended recipient of the message, using a special key, can turn this collection of symbols into intelligible information.

As such, a normally potentially vulnerable channel like a cellular network can be made secure by encrypting the messages sent from a telematics device to the destination server. Because of its mathematical properties, strong encryption cannot be decrypted trivially even by powerful computers. Geotab devices use industry-leading encryption.

Security in the Cloud

Telematics devices relay their data to storage and processing servers, which can be thought of as vaults containing valuable information. The physical servers can be protected by restricting physical access only to authorized personnel. The data inside, on the other hand, can be protected by securing the cloud environment through industry-standard firewalls, access control, and activity monitoring.

It is critical to understand that even the most secure systems are not perfect. In the event of a security breach, it is important to be capable of mitigating the damage caused by any unauthorized access.

Mitigation is the act of minimizing the potential impact from a threat. Effective mitigation can be done by never storing user passwords for the attacker to steal. This is a process known as hashing and salting a password — storing a hash and salt value of a password instead of the actual password. This process impedes the progress of an attacker if they gain unauthorized entry, thus buying precious time to respond to the security compromise and mitigate damage.

Hashing and salting extends the metaphor of the vault: if a robber breaks into a bank vault, instead of having direct access to pile of treasure, they would have to break into every single individual personal vault one at a time in order to steal the valuables.

Corporate Culture of Security

Data security is a practice rather than an act. New security threats are bound to arise as technology develops and the complexity of a system grows. An organization that is serious about security will continuously engage with security issues through updating their systems, training employees, refining processes, and finding vulnerabilities.

At the very core of the telematics system is the team of engineers and support staff that keep everything running smoothly. Resilient organizations should address the fact that an employee might go against the best interest of the company — whether leaking data because of payments from competitors, malfeasance, or simply accidental errors.

So it becomes essential that an organization maintain vigilance at all levels. This can be accomplished by controlling and monitoring access privileges, making log records of important operations, and making sure all employees are aware of the risks related to their actions. A strong culture of security should instill confidence in employees of their ability to respond to security threats, but without creating anxiety about attacks that may or may not come.

One way of building security confidence and safely exposing a telematics system to threats is by performing penetration tests, which are authorized hacking attempts performed by a company specializing in computer security. In a penetration test, the security company will attempt to find vulnerabilities in your hardware and software and — instead of exploiting these vulnerabilities like an actual hacker might — they will document their attack methodology and report their findings to you. The results of the penetration test should then acted upon accordingly — whether that is fixing security holes or changing internal procedures — before malicious agents can exploit those very same vulnerabilities.

Ultimately, data security is an ongoing, corporation-wide effort aimed at safeguarding the data of all users.

Five Key Questions to Ask Your Telematics Provider

Security is a complex topic that deals with every part of a telematics system. Simply asking "is our data secure?" isn't enough. With valuable data on the line, your questions should aim deeper. Look for specific implementations and strategies that form the very basis of modern security standards. The following questions are intended to serve as a primer to help you engage telematics providers about the security of your telematics data.

1 Who manufacturers the telematics hardware? Will the device be the same across my entire fleet?

Why It Is Important To Ask: If your telematics provider does not manufacture their own hardware, they may not have good insight into the security of the hardware. Similarly, if your provider does not have direct control over their hardware and software security, they may take longer to respond to threats or vulnerabilities because they will need to coordinate with third parties.

Moreover, electronics are updated frequently. Different hardware models can introduce different sets of vulnerabilities for each model, meaning that more work will need to be done to patch these security holes across the entire product line. With more hardware variants, there is a higher demand on the engineers to maintain and fix security flaws — in this way resources may not be evenly spread and attention might waver because of product complexity, which can lead to omissions and unfound vulnerabilities. Manufacturers must be the ones responsible for security for the life of the product.

2 Do you encrypt the data as it is sent over the cellular network?

Why It Is Important To Ask: Cellular carriers should not be exclusively relied upon to secure the delivery of your telematics data over the air. It is important that your telematics providers takes additional steps to encrypt your data so that even if the cellular communication channel is compromised, your data will not be.

3 Is the firmware signed to prevent outside parties from changing the code on the device?

Why It Is Important To Ask: The firmware is the brain behind the device — it decides where the data is sent, what data is captured, and how it is stored. If a malicious firmware were installed on your device, it would no longer be possible to know where your data is being sent or what is happening to it. Your telematics provider should sign every firmware update with a digital signature that indicates the update came from a trusted source.

4 Do you have security documentation that covers your hardware, your servers, the transmission of data, as well as policies for employees?

Why It Is Important To Ask: Security documentation shows a baseline commitment to a culture of security. A telematics provider should be able to provide details on their security measures, as well as their mitigation and disaster recovery strategies in case something unexpected occurs.

A security process outline document — like Geotab's Technical and Organizational Data Security Measures Statement — goes a long way towards helping you understand what happens to your data.

5 In the event that your servers are compromised, what sort of mitigation strategy do you use to protect the account information of your users?

Why It Is Important To Ask: If a security breach does occur, the system should contain as little personal information as possible. Passwords should never be stored directly in the system of your telematics provider; rather, passwords should be transformed into hashes and further strengthened through salting.

Summary

The security of your telematics data should not be overlooked. Like any other critical business data, it should be protected with comprehensive security mechanisms and processes that are continuously reviewed and updated. Following industry best practices is essential.

Cybersecurity is a shared responsibility. We can all play a role in keeping security systems strong. Getting informed and asking questions is a great first step on the path to effective cybersecurity management.

To learn more about telematics security, please visit: security.geotab.com

References

1. S. Kilcarr, "Telematics hacking: Three things you need to know," Sep. 3, 2015. Retrieved from: http://fleetowner.com/technology/telematics-hacking-three-things-you-need-know

2. H. Williams, "Top five biggest threats to IoT security," Oct. 24, 2016. Retrieved from: http://www.cbronline.com/news/cybersecurity/breaches/top-five-biggest-threats-iot-security/

3. M. Turner, "How to secure the internet of things," June 2015. Retrieved from: http://www.computerweekly.com/opinion/How-to-secure-the-internet-of-things

4. Accenture, "Securing the Internet of Things: Executive Summary," 2015. Retrieved from: https://www.accenture.com/t00010101T000000__w__/jp-ja/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents22/Accenture-Security-Call-to-Action-IoT-ExecSummary-FINAL.pdf

5. Federal Bureau of Investigation, "Alert Number I-031716-PSA: Motor Vehicles Increasingly Vulnerable to Remote Exploits," Mar. 17, 2016. [Online] Available: https://www.ic3.gov/media/2016/160317.aspx.

6. NAFA Fleet Management Association, "Fleet Management and the Connected Vehicle," Oct. 2016. [Online] Available: www.nafa.org/download.php?f=832

7. A. Sukhov, "15 Security Recommendations for Building a Telematics Platform Resilient to Cyber Threats," Nov. 14, 2016. Retrieved from: https://www.geotab.com/blog/telematics-cybersecurity-recommendations/

8. D. Perez and J. Pico, "A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications," 2011. Retrieved from: https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf

GEOTAB

management by measurement

www.geotab.com