

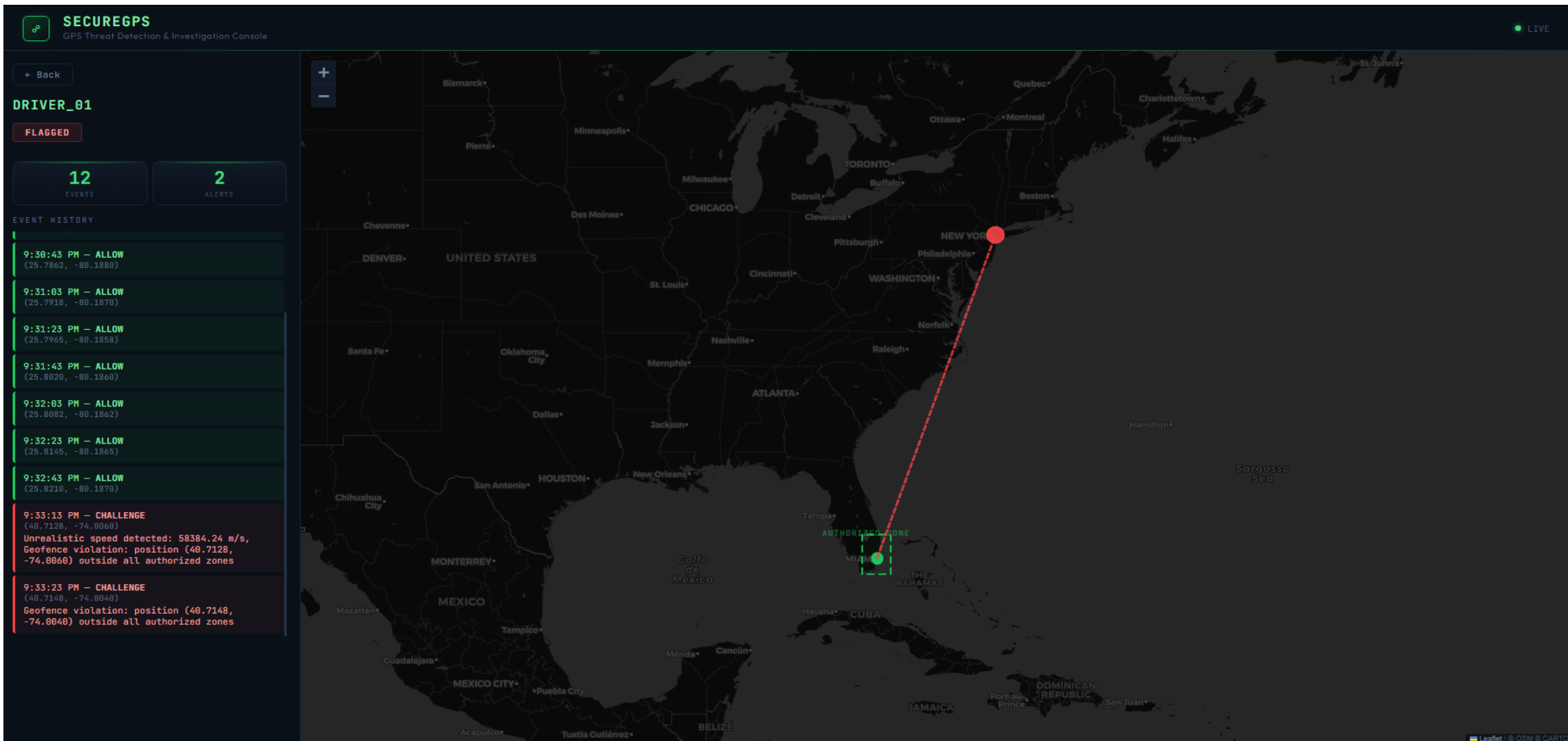
Secure GPS

Students: Daniel Bikowicz, Helen Gomez, Nahahme Bar ‘Ysrael, Omar Adel Alali, Matthew Clayton
Instructor/Faculty: Professor Masoud Sadjadi, Florida International University



PROBLEM

GPS spoofing is a growing cybersecurity threat in which attackers broadcast fake GPS spoofing is a cybersecurity attack where adversaries broadcast falsified satellite signals to manipulate a device’s perceived location, velocity, and time. Because civilian GPS systems do not include authentication mechanisms, receivers cannot distinguish legitimate satellite signals from malicious ones. This makes spoofing highly accessible, as it can be executed using low-cost hardware and software-defined radios. The impact is significant across logistics, transportation, autonomous systems, and fleet management, where incorrect positioning can lead to safety risks, operational disruption, and financial loss. Existing mitigation techniques are often hardware-dependent or expensive, creating a need for a scalable, software-based detection approach.



SYSTEM DESIGN

SecureGPS is a real-time, server-side GPS spoofing detection system designed to analyze telemetry as it is received. GPS-enabled devices transmit structured JSON payloads containing device ID, timestamp, latitude, longitude, speed, and HDOP via HTTP requests to a FastAPI backend. Each incoming event is processed through a detection pipeline that evaluates spatial and behavioral consistency using multiple independent checks. The system assigns a severity classification (Allow, Low, Medium, High, Critical) based on combined results. After evaluation, each event is cryptographically signed using HMAC-SHA256 to ensure data integrity before being stored in a SQLite database. A real-time dashboard built with Leaflet.js visualizes device movement, alerts, and geofence boundaries, enabling live monitoring of system behavior.



VERIFICATION

System verification was performed using controlled test scenarios with known ground-truth outcomes. Each simulated GPS event was labeled as either normal or attack-based, including teleportation, geofence violations, bearing anomalies, and HDOP manipulation. Detection outputs were compared directly against expected classifications to evaluate correctness. In addition, data integrity was tested by modifying stored database entries after ingestion and validating HMAC-SHA256 signatures. Any modification resulted in a failed verification check, confirming that the system reliably detects post-processing tampering. These tests validate both the accuracy of the detection pipeline and the robustness of the forensic integrity mechanism.

SUMMARY

SecureGPS presents a software-only approach to real-time GPS spoofing detection that does not require modifications to existing hardware or GPS receivers. By combining multiple independent detection methods with cryptographic verification, the system is able to identify a wide range of spoofing behaviors while maintaining high accuracy and low latency. Experimental results demonstrate strong performance under simulated attack conditions, including perfect detection rates and no false positives. The system also introduces a forensic layer through HMAC-based integrity verification, ensuring that stored telemetry can be trusted even after ingestion. Overall, SecureGPS provides a scalable foundation for improving GPS security in real-world, connected environments.

CURRENT SYSTEM

In most GPS-dependent applications today, incoming location data is assumed to be accurate and trustworthy. Fleet tracking systems, navigation platforms, and IoT devices typically consume GPS telemetry without performing validation beyond basic sanity checks. As a result, malicious or synthetic GPS data is treated as legitimate if it appears structurally valid. This creates a critical vulnerability where spoofed movement—such as impossible travel speeds or location jumps—is not inherently detected. The lack of built-in authentication in civilian GPS signals means most systems rely on external safeguards, which are often minimal or absent.

REQUIREMENTS

The system was designed to meet both functional and non-functional requirements for real-time spoofing detection. Functionally, it must ingest GPS telemetry in real time, evaluate each reading using multiple detection methods, classify severity levels accurately, and present results through a live monitoring interface. It must also support cryptographic verification of stored data to detect tampering. Non-functionally, the system must maintain low latency (under 50 milliseconds per event), minimize false positives under normal driving conditions, and remain scalable for multiple concurrent devices. Additionally, it must provide consistent performance without relying on external hardware modifications or specialized GPS receivers.

OBJECT DESIGN

The system is structured around four primary object types that support both real-time detection and forensic analysis. The **Device object** maintains state information, including the most recent GPS reading, which is required for computing speed and bearing changes. The **Event object** represents each incoming GPS reading along with its computed detection results and assigned severity level. Each event is paired with a **Signature object**, which stores the HMAC-SHA256 hash used to verify data integrity and detect post-ingestion tampering. Finally, the **Alert object** represents flagged events within the monitoring interface and includes metadata such as severity, status (Pending or Acknowledged), and analyst notes. This structure allows the system to maintain both operational and forensic perspectives of the data.



IMPLEMENTATION

SecureGPS is implemented using a Python-based FastAPI backend, SQLite for lightweight storage, and Leaflet.js for real-time geospatial visualization. The detection engine consists of four core methods: speed anomaly detection using the Haversine distance formula, geofence validation against predefined geographic boundaries, HDOP anomaly detection based on signal quality metrics, and bearing reversal detection for identifying physically impossible directional changes. These methods operate independently and contribute to an aggregated severity score. The system was evaluated using 85 simulated GPS readings across 8 devices, achieving 100% detection accuracy with zero false positives. Average processing latency remained below 50 milliseconds per event due to in-memory computation and elimination of database queries in the critical processing path. All events are cryptographically signed at ingestion, allowing any post-storage modification to be detected through signature mismatch validation.