Automotive RF Detection Logic: Event Types & Detection Methods

This document explains how each event type in the Automotive Security Capstone project is detected, both in real (SDR) and mock/demo modes. Use this as a script or reference for professor Q&A, demos, or technical documentation.

General Approach

- **RF packets** are analyzed for frequency, timing, payload patterns, and context (e.g., repeated unlocks, signal strength, etc.).
- **Mock/demo mode** simulates plausible packets and cycles through all event types for demonstration purposes, but uses the same logic structure.
- **Detection logic** is centralized in `backend/detection/event_logic.py` via the `analyze_event()` function.

Event Types & Detection Logic

1. **RF Unlock / RF Lock**

- **Definition:** Legitimate key fob unlock/lock command.
- **Detection:**
  - Recognized by expected RF frequency (e.g., 315/433/868 MHz).
  - Payload matches known unlock/lock command patterns (manufacturer-specific).
  - Signal strength (RSSI) is within normal range.
  - Not repeated in rapid succession (to avoid brute force/replay classification).
  - **Threat Level:** Benign (unless anomalous context is detected).

2. **Replay Attack**

- **Definition:** An attacker records a legitimate unlock/lock signal and replays it to gain unauthorized access.
- **Detection:**
  - Identical or highly similar RF packets detected more than once, outside of expected timing.
  - No rolling code progression (if rolling code is used, see Rolling code).
  - Unusual timing or context (e.g., unlock signal received when owner not present).
  - **Threat Level:** Always Malicious in demo; real logic would use rolling code analysis and timing.

3. **Jamming Attack**

- **Definition:** An attacker transmits noise or signals to block legitimate RF communication (e.g., prevent lock/unlock).
- **Detection:**
  - Sustained or repeated RF noise detected on the expected frequency bands.
  - High RSSI with no valid payloads.

  - Lock/unlock packets missing or failing during noise bursts.
  - **Threat Level:** Malicious.

4. **Brute Force Attack**

- **Definition:** Repeated attempts to unlock/lock by cycling through possible codes or sending many packets.
- **Detection:**
  - Multiple unlock/lock attempts detected in rapid succession.
  - Payloads differ slightly (code cycling) or repeat with invalid codes.
  - More attempts than normal user behavior would generate.
  - **Threat Level:** Malicious.

5. **Unknown**

- **Definition:** RF packet does not match any known pattern or event type.
- **Detection:**
  - Frequency is in automotive band but payload is unrecognized.
  - No match to unlock/lock, replay, brute force, or jamming signatures.
  - **Threat Level:** Always Suspicious (never Malicious or Benign in demo).

6. **NFC Scan / NFC Tag Present**

- **Definition:** Near-field communication event, e.g., key card or phone scanned.
- **Detection:**
  - Detected by NFC hardware interface.
  - Payload matches expected NFC tag or scan pattern.
  - **Threat Level:** Benign (unless anomalous context).

Summary Table

Event Type	Detection Method Highlights	Threat Level (Demo)
RF Unlock/Lock	Known RF pattern, normal timing, valid RSSI	Benign
Replay Attack	Duplicate packet, no rolling code, odd timing	Malicious
Jamming Attack	High noise, no valid payloads, comms blocked	Malicious
Brute Force	Rapid, repeated attempts, code cycling	Malicious
Unknown	No match to known patterns	Suspicious
NFC Scan/Tag	NFC interface, valid tag pattern	Benign

References & Further Reading

- Replay attack - Wikipedia
- Rolling code - Wikipedia
- Radio jamming - Wikipedia

- Brute-force attack - Wikipedia
- Automotive security - Wikipedia

Note:

- In demo/mock mode, events are cycled for visibility, but logic structure matches real detection code.
- For real deployments, detection can be enhanced with rolling code validation, anomaly detection, and context-aware analysis.