Autonomous Security

Controllers Protect Themselves
Transportation Platforms’ Characteristics

• Autonomous computing
  • System-based decisions/commands
  • Not always externally connected

• Personal-safety above all
  • Must not risk lives

• Run on Electronic Control Units (ECUs)
  • Limited computing resources
  • Real-time performance constraints
The Sheer Magnitude of Security Vulnerabilities

- **F22 Jet Fighter**: 2M
  - 1,200
  - 100

- **Boeing 787 Dreamliner**: 15M
  - 9,000
  - 700

- **Midsize Car**: 10M
  - 6,000
  - 500

- **Premium Car**: 100M
  - 60,000
  - 5,000

Sources:  
- www.securityweek.com/secure-mobile-applications-considerations-developers
- www.informationisbeautiful.net/visualizations/million-lines-of-code
Hackers Exploit Security Bugs

1. Hidden security software bug
2. Bug exploited to run malware
3. Malware compromises the system
Automotive Cybersecurity Enabler

- Unauthorized change to factory settings $\iff$ malware
- Designated “gates” in the car
Karamba’s Autonomous Security

Seal
Harden Factory Settings

Detect
Exploit Attempts

Prevent
The Attack

Malware
Autonomous Security

- Standalone security
  - Host based: does not require external connectivity
  - No malware signature updates required

- Zero false positives
  - Deterministic algorithms

- Any ECU support
  - Hardware and OS agnostic