Secure Autonomous Systems

CSCI 6907/3907 88

Fall 2022

Prof. Sibin Mohan

https://bit.ly/secureauto-fall22

Security Classification

How do you define **security**?

Security Classification | Attacks

Passive (stealing data) vs active (causing physical harm)

Sensors hacks

- tags on stop signs, reflective paint on vehicles
- Jamming RADARs
- Physical damage to sensor

Attacks by other vehicles/V2X system hacks

Software hacks

- Operating system
- Entire software stack: Kalman filter, planning algorithms, vision algorithms, sensor fusion, etc.

Attacks on actuation subsystem

- Prevent actuation commands from executing
- Change commands in flight

Denial of service

- Cause wear and tear on devices, e.g., engine/brakes

Security Classification | Attacks

Passive (stealing data) vs active (causing physical harm)

Sensors hacks

- tags on stop signs, reflective paint on vehicles
- Jamming RADARs
- Physical damage to sensor

Malware injection is one way to enter system

Attacks by other vehicles/V2X system hacks

Software hacks

- Operating system
- Entire software stack: Kalman filter, planning algorithms, vision algorithms, sensor fusion, etc.

Attacks on actuation subsystem

- Prevent actuation commands from executing
- Change commands in flight

Denial of service

- Cause wear and tear on devices, e.g., engine/brakes

Security Classification | Attacks [contd.]

Hardware

- Trojan horses in chips
- Hidden backdoors in chips/hardware units

Data attacks

- Maps/other data could be tampered with

Security Classification | Defenses

Passive [only detect/raise alarms] vs active [take action on detection]

- intrusion detection and prevention

Reactive [take action on detection] vs proactive [action without detection]

Use existing (additional) sensors/functions

- To detect anomalous sensor behavior

Warnings

- How to design warnings that will be noticed/heeded?

Security Classification | Defenses [contd.]

Buy cheap chips/supply chains

Few communication end points + encrypt/authenticate

- Other vehicles/traffic signs, sensors (GPS)
- Network updates (OS)
- Entertainment systems
- Computation and memory overheads
- Power consumption

Hardware verification to detect attacks at startup

- Additional chips (ROM)

History of correct behavior → use to check

- Vehicular level, software behavior

Security Classification | Defenses [contd.]

Sensor fusion

- use multiple sensors to verify each other

Use hardware signature

Human input to verify

- humans as failsafe

Security as a first principle

Hide systems design (security through obscurity)

Software security (isolation, VMs, etc.s)

Better systems design/product design