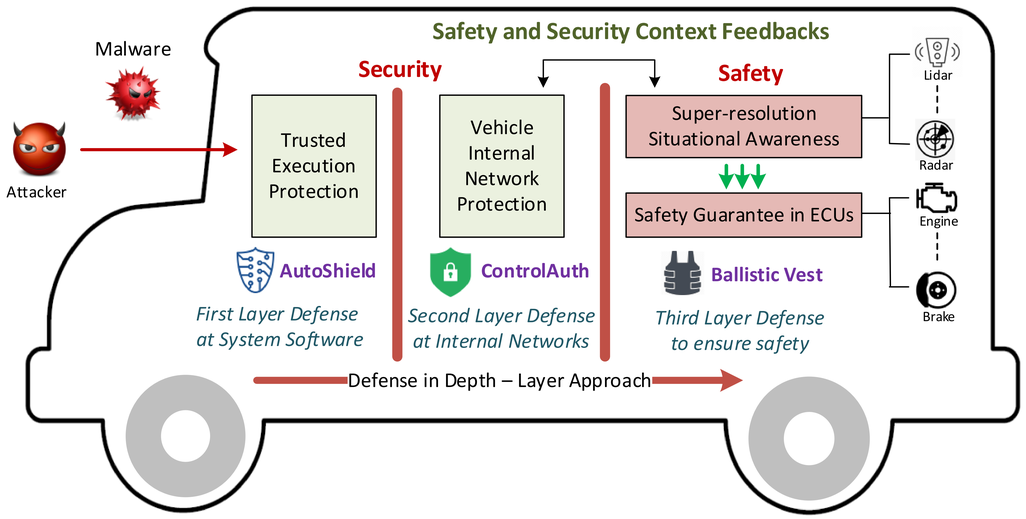
2021 NSF CYBER-PHYSICAL SYSTEMS PRINCIPAL INVESTIGATORS' MEETING

CPS: Medium:
S2Guard: Building Security and Safety in Autonomous Vehicles via Multi-Layer Protection

Wenjing Lou, Thomas Hou , Haibo Zeng — Virginia Tech
Ning Zhang — Washington University in St. Louis

Challenge:

- Bootstrapping trustworthiness in modern commodity autonomous vehicles
- Improving the cyber-resiliency when the system is under attack
- High resolution localization in real time
- Fail-operational when previous security layers fail



Scientific Impact:

- Developed scientific foundation to bootstrap trust (safety and security) in emerging autonomous systems
- Resulted in 5 papers at Usenix Security, NDSS, AAAI, ACSAC, RTSS

Solution:

- Defense-in-Depth: Building multiple layers of defense to improve resiliency
- Building root of trust at each layer: Enabling trustworthiness in the autonomous system
- Novel GPU-based real-time super-resolution algorithm for direction of arrival
- Formal safety guarantee at critical control units: Fail-operational (minimal functionality) as the last line of defense

Broader Impact:

- Catalyzed multiple open source projects on security protection of embedded system and network
- Developed multiple courses and course modules on CPS/IoT security
- Supported the participation of research of more than 10 undergraduates

CNS -1837519
10/1/2019 ~ 9/30/2022