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

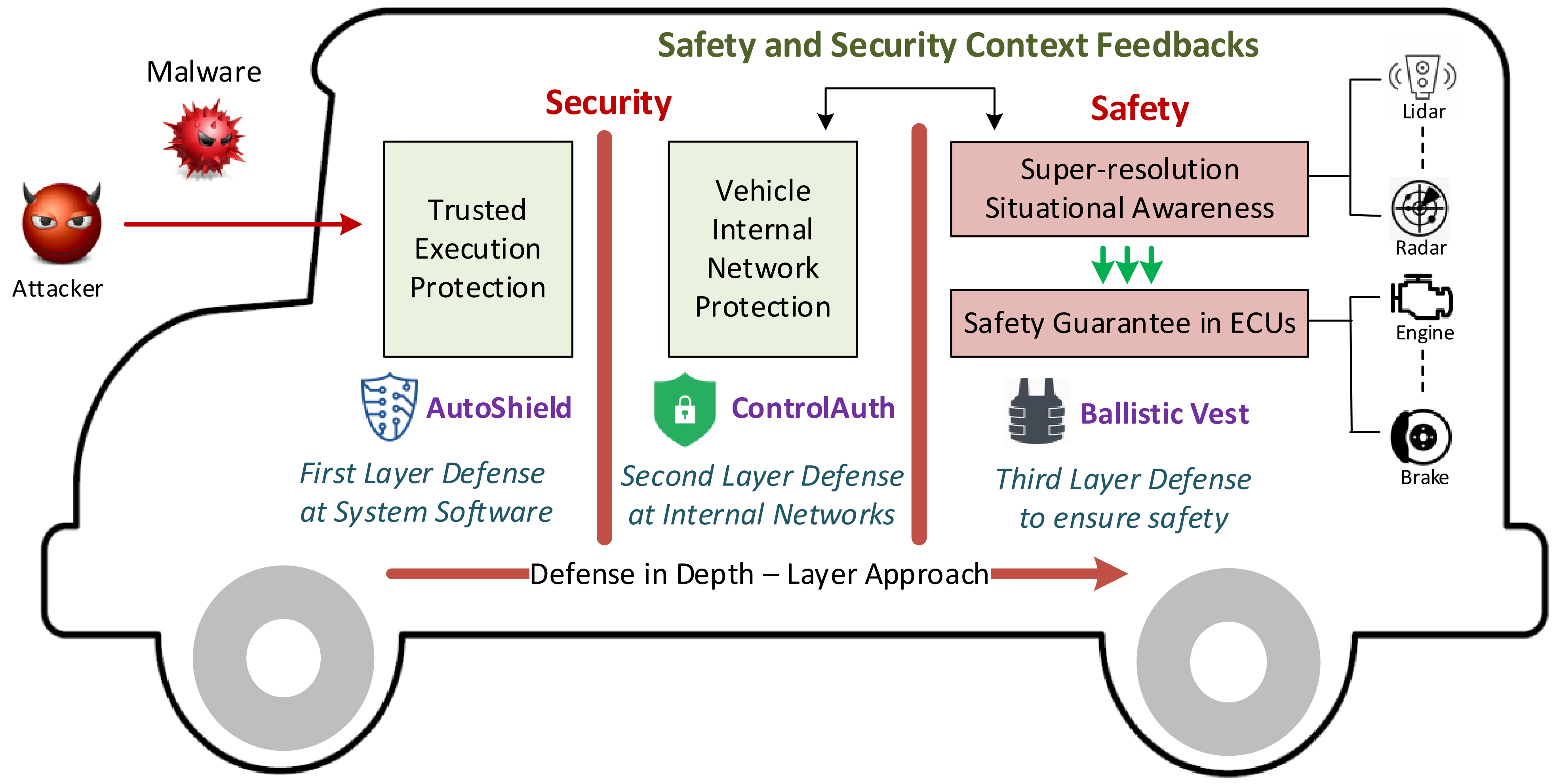
Wenjing Lou[†], Thomas Hou[†], Haibo Zeng[†], and Ning Zhang*

[†]Virginia Tech, *Washington University in St. Louis, https://cybersecurity.seas.wustl.edu/projects/S2Guard.html

Autonomy without assurance can negate its perceived benefits and hinders the deployment of autonomous systems for societal good.

Key Challenges:

- Bootstrapping trustworthiness in modern commodity autonomous vehicles
- Improving the cyber-resiliency when the system is under attack
- High resolution localization in real time
- When everything fails, how do we achieve fail-operational


Malware
Attacker
Safety and Security Context Feedbacks
Security
Safety
Trusted Execution Protection
Vehicle Internal Network Protection
Super-resolution Situational Awareness
Safety Guarantee in ECUs
Lidar
Radar
Engine
Brake
AutoShield
ControlAuth
Ballistic Vest
First Layer Defense at System Software
Second Layer Defense at Internal Networks
Third Layer Defense to ensure safety
Defense in Depth – Layer Approach

Technical Approach

- 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

Boarder Impact on Society

- Developed scientific foundation to bootstrap trust (safety and security) in emerging autonomous systems
- Catalyzed multiple open source projects on security protection of embedded system and network

Broader Impact on Education

- Led to the development of multiple courses on cyber-physical system security

- Supported participation of research from undergraduate students

Quantification of Broader Impact

- 3 newly developed undergraduate and graduate courses on CPS/IoT
- Supported the participation of more than 10 undergraduates
- Resulted in 5 papers at Usenix Security, NDSS, AAAI, ACSAC, RTSS

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: 1837519