CHESS

CENTER FOR HYBRID & EMBEDDED SOFTWARE SYSTEMS

COLLEGE OF ENGINEERING, UC BERKELEY

Automotive Intrusion Detection

Armin Wasicek

http://chess.eecs.berkeley.edu/

Abstract

Combatting the modification of automotive control systems is a current and future challenge for OEMs and suppliers. 'Chip-tuning' is a manifestation of manipulation of a vehicle's original setup and calibration. With the increase in automotive functions implemented in software and corresponding business models, chip tuning will become a major concern. Recognizing tuned control units in a vehicle is required to report that circumstance for technical as well as legal reasons.

Chip Tuning

Modify control algorithm parameters

- Parameters are stored in a table in flash memory
- Reprogram ECU with new values
- Debug interface, 3rd party device

Messages emitted by ECU seem original!

Power Boxing

Modify commands to ECU

- Replace the ECU in the communication system
- Insert device between the ECU and actuators

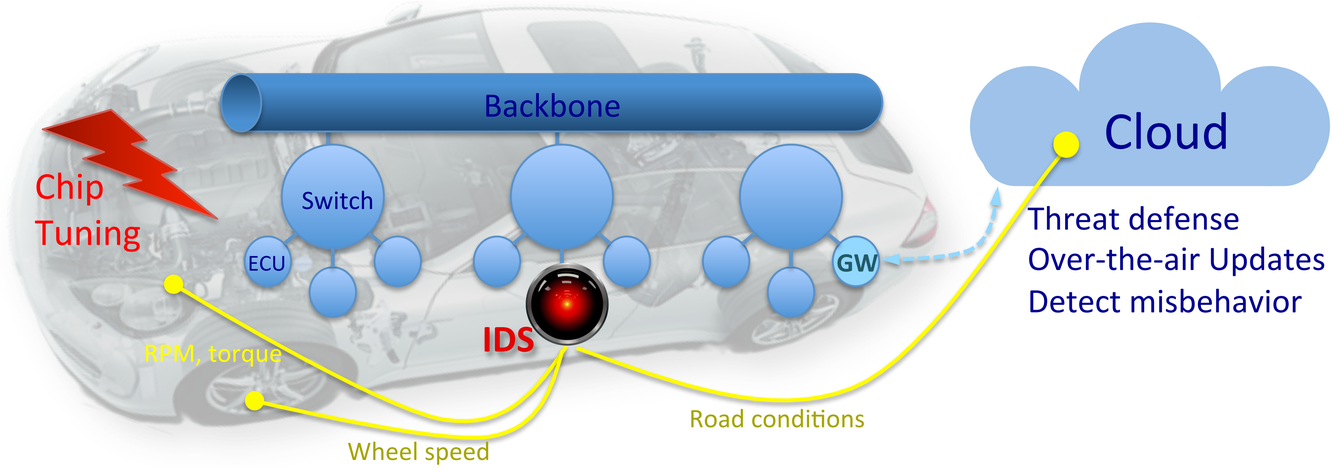
Communication pattern does not change!

Contact:
Dr. Armin Wasicek 545N Cory Hall
arminw@berkeley.edu 510-542-7718

Cyber-Physical Attacks

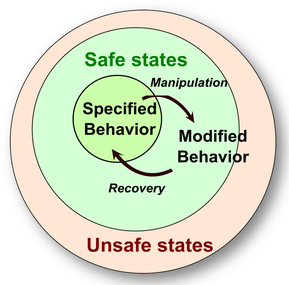
"A cyber-physical system (CPS) integrates computing and communication capabilities with monitoring and / or control of entities in the physical world dependably, safely, securely, efficiently and in real-time." - S. Shankar Sastry

"Cyber-Physical attack vectors include intrusions that cross the interface between the cyber and the physical worlds. Particularly safety-critical systems have to ensure that cyber-physical attacks are appropriately prevented and recognized, such that an intrusion might not propagate from the security to the safety domain." – A. R. Wasicek



Mission

Recognize manipulations in form of subtle changes within the space of safe states. For instance, chip tuning aims to modify but not to damage a system. It causes a deviation from the specified behavior to a modified behavior that might not be in compliance with warranty, legal regulations, etc.



Technical approach

Compare behavior to reference model enabling misbehavior detection. The technical approach uses neural networks to store the typical behavior of the vehicle. During operation, telematics data is gathered and continuously compared to the typcial behavior.

Types of IDS

Knowledge-based IDS

- Patterns/Signatures of malicious activities
- Low false positive rate, needs frequent updates

Heuristic-based IDS

- Look for abnormal behavior, e.g., higher entropy
- Detect new attack patterns

Context-aware IDS

- Compare to reference model, include semantics
- Check against specifications and regulations

Results

Evaluate using the racing car simulation TORCS. Car model 'p406' simulating a Peugeot 406 was tuned by increase engine torque by 10 Nm and 30 Nm, resulting in a better lap time.

Neural network was used to distinguish between original and modified behavior.