Homeland Security
Science and Technology

Side-Channel Causal Analysis for Design of Cyber-Physical Security

HRL Laboratories, LLC.
David Payton

Team Profile

HRL LABORATORIES
Prime Contractor

Mr. Dave Payton KEY (PI)
Dr. Connie Ni KEY

Unique Capabilities:
- Side-channel analysis
- Network Information Dynamics
- Automotive cyber defense

Task Responsibilities:
- Task 1: Side-channel monitoring
- Task 2: Causal Analytics
- Task 5: Platform SW & Integration
- Task 6: Program Management

Dr. Gernot Heiser
Subcontractor

DATA 61 CSIRO

Unique Capabilities:
- seL4 microkernel developer

Task Responsibilities:
- Task 3. Real-Time Secure microkernel

Dr. Gene Tsudik
Subcontractor

Unique Capabilities:
- Provably secure remote attestation

Task Responsibilities:
- Task 4. Attestation & Secure Updates

Automotive Cyber Insecurity

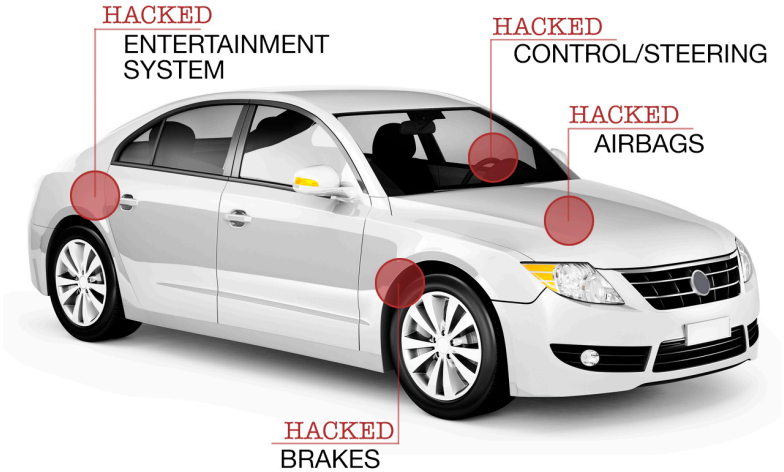
What will be the consequences of the next vehicle cyber hack?

Customer Need

- Remote hacking of vehicles is now a proven possibility.
- As vehicles gain more advanced autonomy, vulnerabilities will increase.
- Cyber intrusion detection is needed, but added cost must be minimal.

Fiat Chrysler recalling unprecedented 1.4m cars due to hacking threat

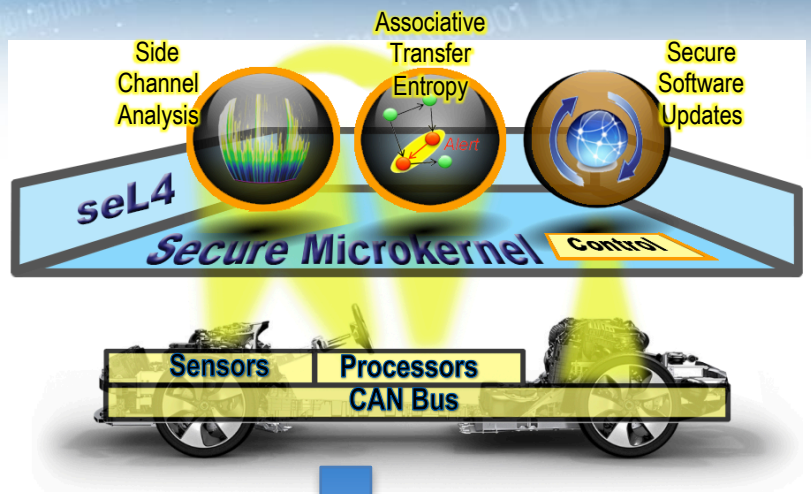
By Brad Reed on Jul 24, 2015 at 10:46 AM



Technical Goals

Analyze side-channel data to reveal causal inconsistencies during system operation.

Provide software-only secure updates using process isolation of seL4.



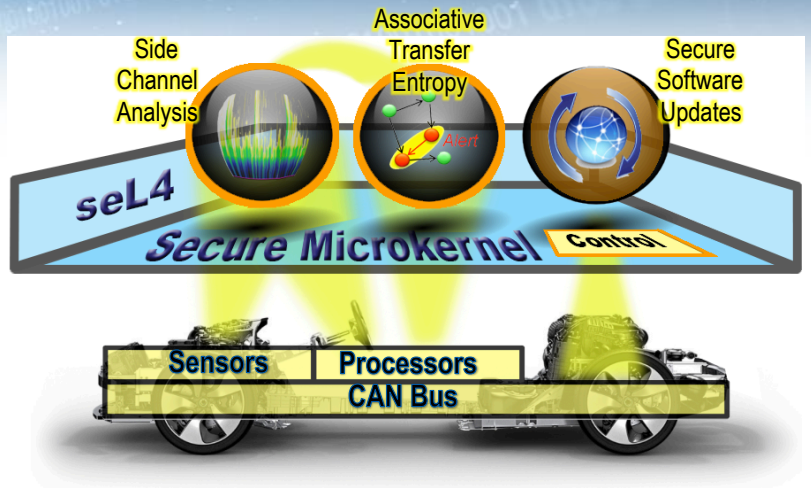
Provide seamless integration into existing infotainment system architectures.

Enable a single component to monitor the entire vehicle without having to know internal details about other supplier's products.

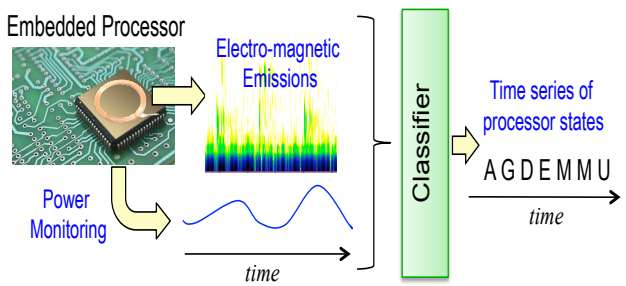
Approach

Analyze side-channel data to reveal causal inconsistencies during system operation.

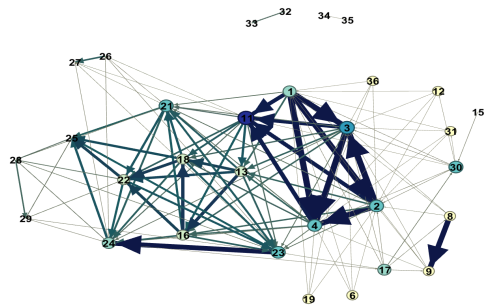
Provide software-only secure updates using process isolation of seL4.



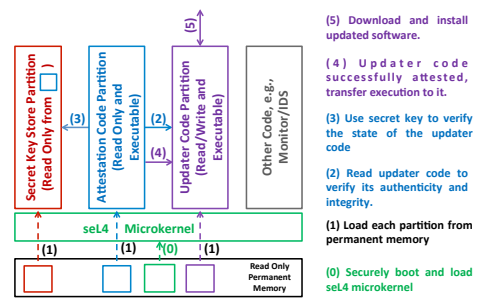
Innovations:



Side-channel defense monitors causal couplings between cyber and physical realms that are beyond the control of an attacker.



Associative transfer-entropy detects when observed interactions deviate from known physical causal structure.

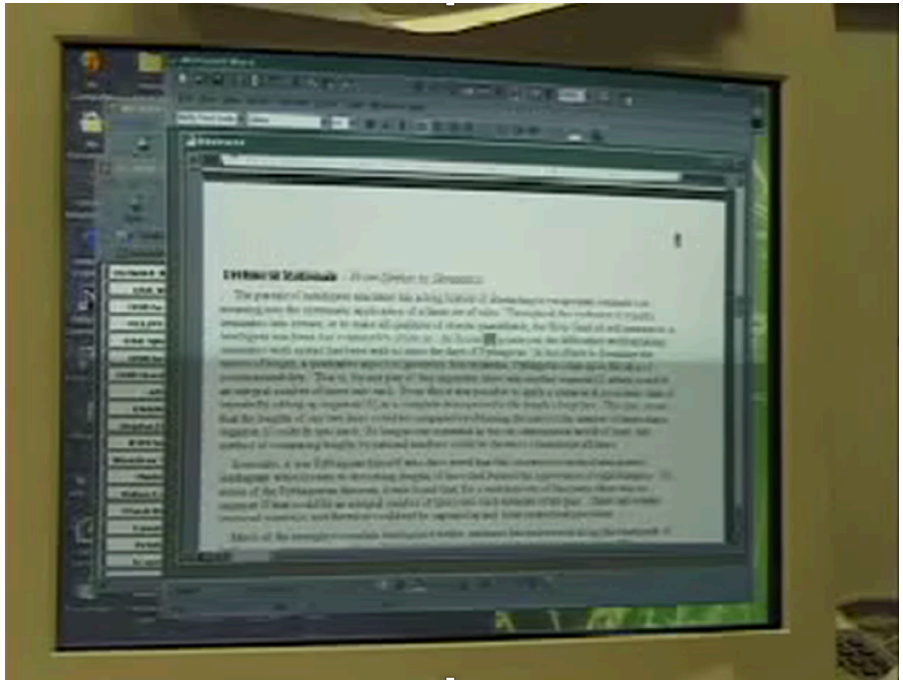


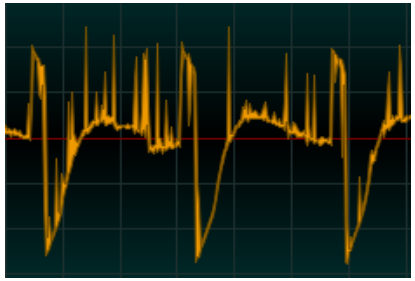
The first provably secure software-only attestation scheme is enabled by proven process isolation within seL4.

Side-channels can be as much a means for cyber defense as they are for cyber attack.

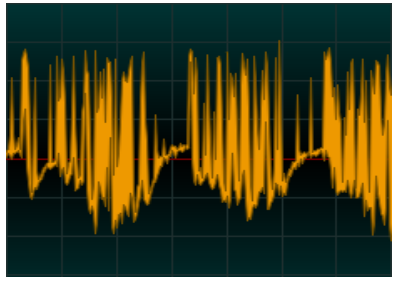
Side-Channel Analysis

- **Side-channel signals are commonly used by attackers to reveal secret keys**
  - **ex: RF emissions, Acoustic emissions, Power fluctuations**
- **Our strategy is to use these same sources to detect system compromise**
  - **An attacker will have difficulty altering functionality without altering observable side-channel behavior**

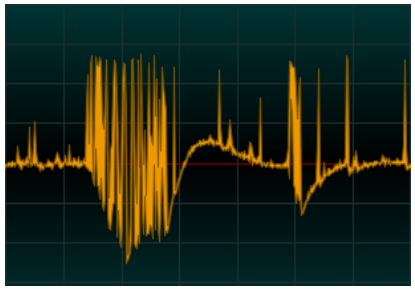




Move mouse over text



Drag window

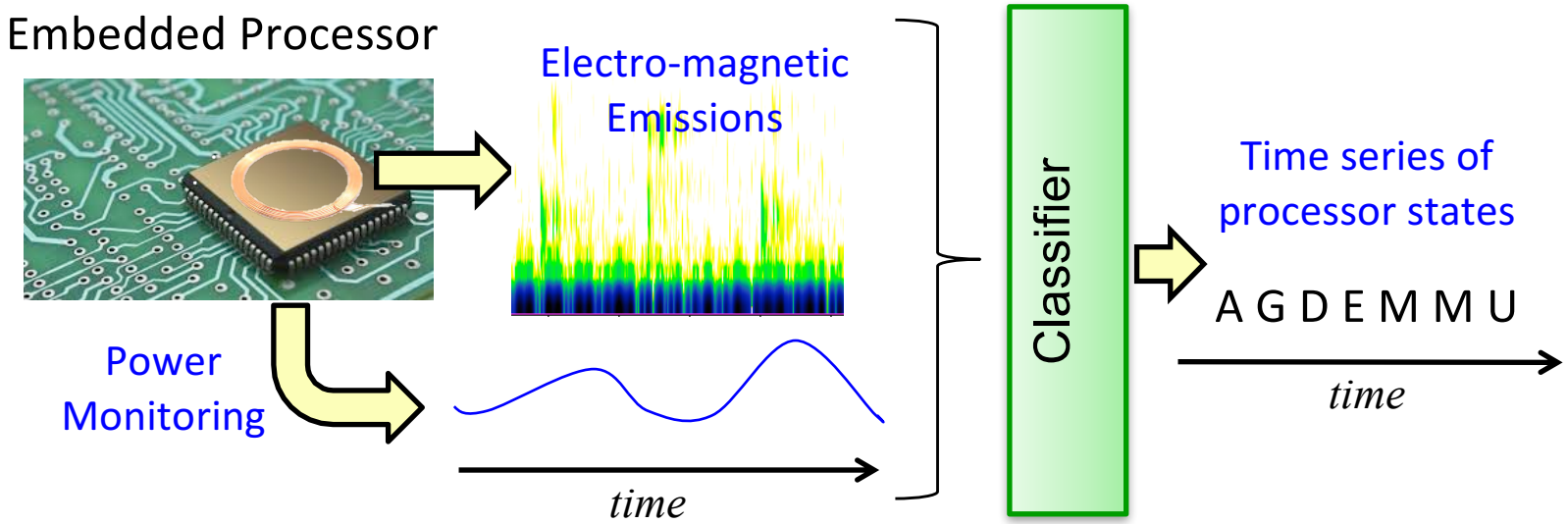


Select text

Just as side channels from a PC can reveal what the computer is doing, so can side-channels from vehicle control modules.

Vehicle State from Side-Channels

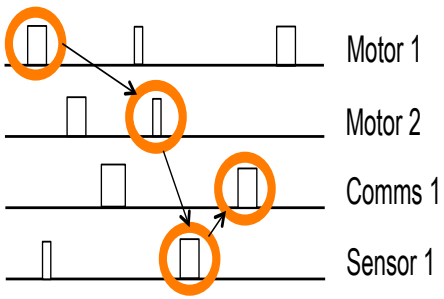
- A classifier will decode analog side-channel emissions into a time series of processor states.
- Anomalous sequences of states within a single processor can be one indication of compromise.
- Statistical relationships between states of different processors will be an even more powerful tool for detecting compromise.



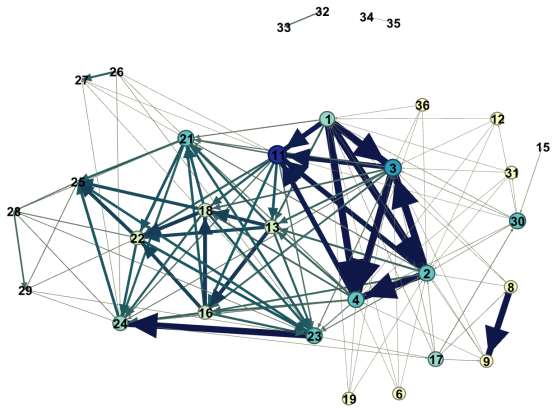
Side-channels can provide an indication of vehicle activity that is unalterable by and inaccessible to hackers.

ATE Analysis

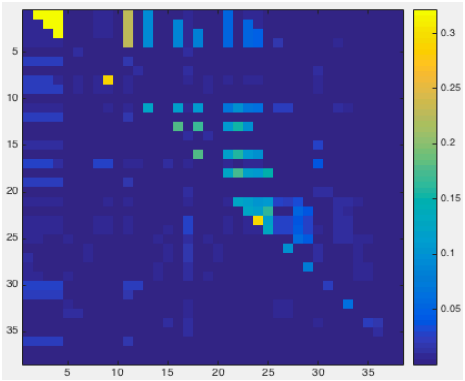
- **Our Associative Transfer Entropy (ATE) algorithms detect directional influences between related time series**
  - **derived from side-channel data and CAN bus data**
  - **intrusion is detected when the normal influences are altered**



Distinct activity patterns between system components



ATE directed graph – nodes represent different message types on CAN bus



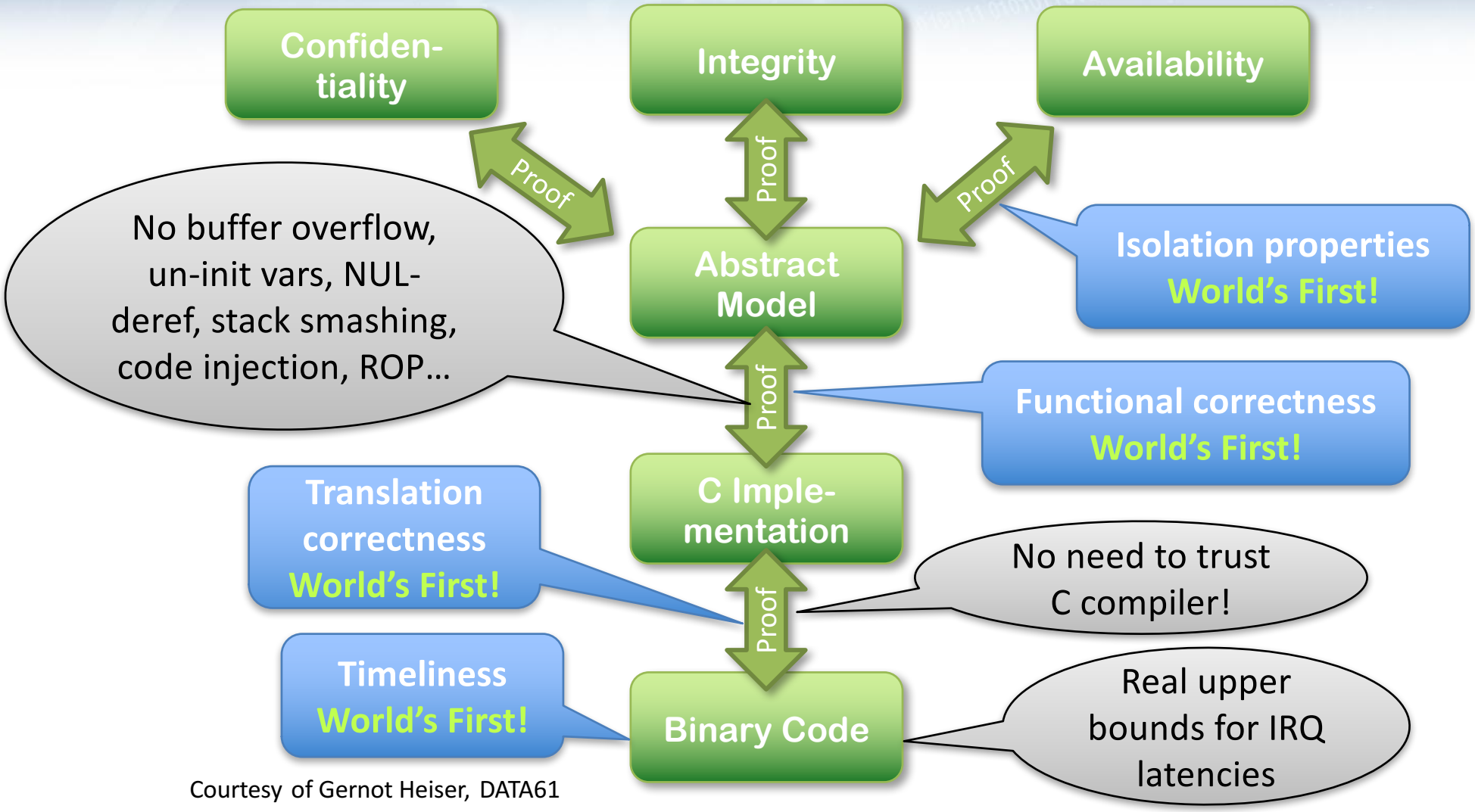
ATE Matrix

- **Example: CAN Bus transmissions originating from an improper source may be detected by the change in relationship between message timing and EM emissions.**

ATE captures aspects of causal structure that a hacker cannot avoid altering if they want to change vehicle behavior.

seL4 Provable Isolation

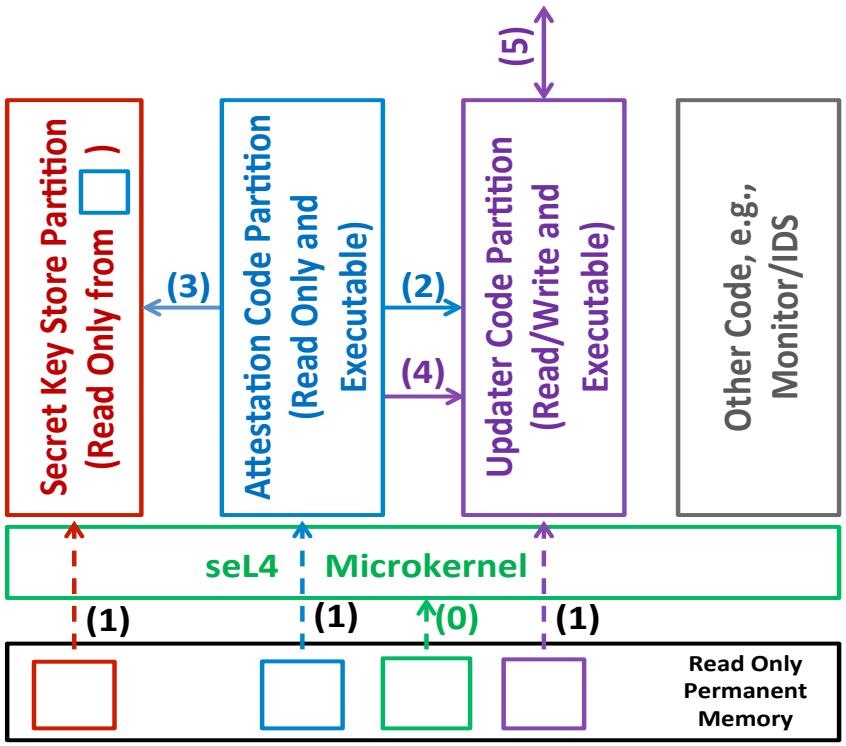
seL4: Provides Mathematical *Proof* of Security and Safety



Courtesy of Gernot Heiser, DATA61

Secure Attestation

- **Using seL4 isolation properties, we will be able to replace dedicated hardware to provide a software-only* solution to attestation and secure updates.**



(5) Download and install updated software.

(4) Updater code successfully attested, transfer execution to it.

(3) Use secret key to verify the state of the updater code

(2) Read updater code to verify its authenticity and integrity.

(1) Load each partition from permanent memory

(0) Securely boot and load seL4 microkernel

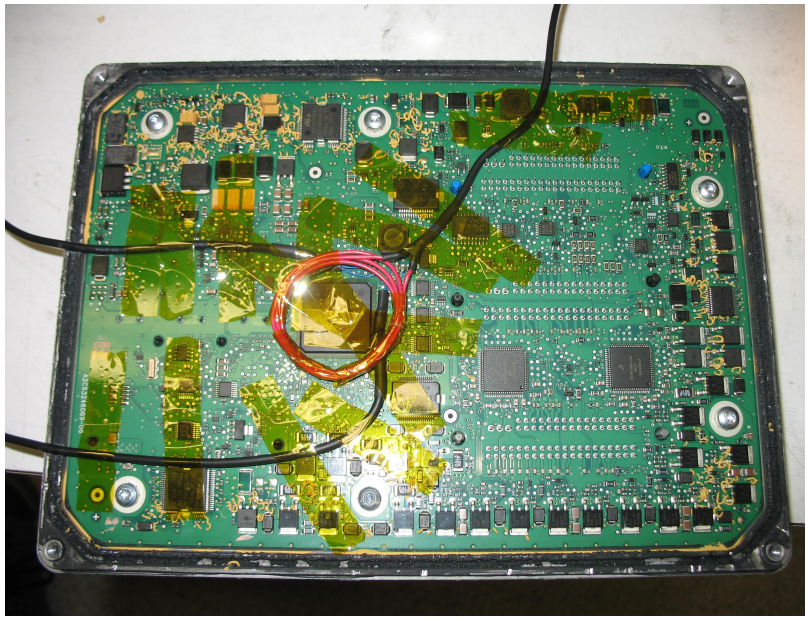
* We rely only on existing hardware such as TrustZone for secure boot-up.

Benefits

Challenge	Innovation	Benefit
Detect covert intrusion.	**Side-channel defense** monitors physical signatures that are beyond the control of an attacker	Detect stealthy attacks from the way they alter physical signatures.
Distinguish anomalous behavior	**Associative transfer-entropy** analysis detects deviations from known physical causal structure	Sensitive to the subtle causal changes related to attacks.
Minimize added cost	**Real-time seL4 microkernel**: processes securely coexist on the same hardware.	Ensures isolation to limit possibility of corruption on existing hardware.
Secure software updates	**The first provably-secure software-only attestation scheme**	Easy integration with any cyber-physical system.

Side-Channel Data Acquisition

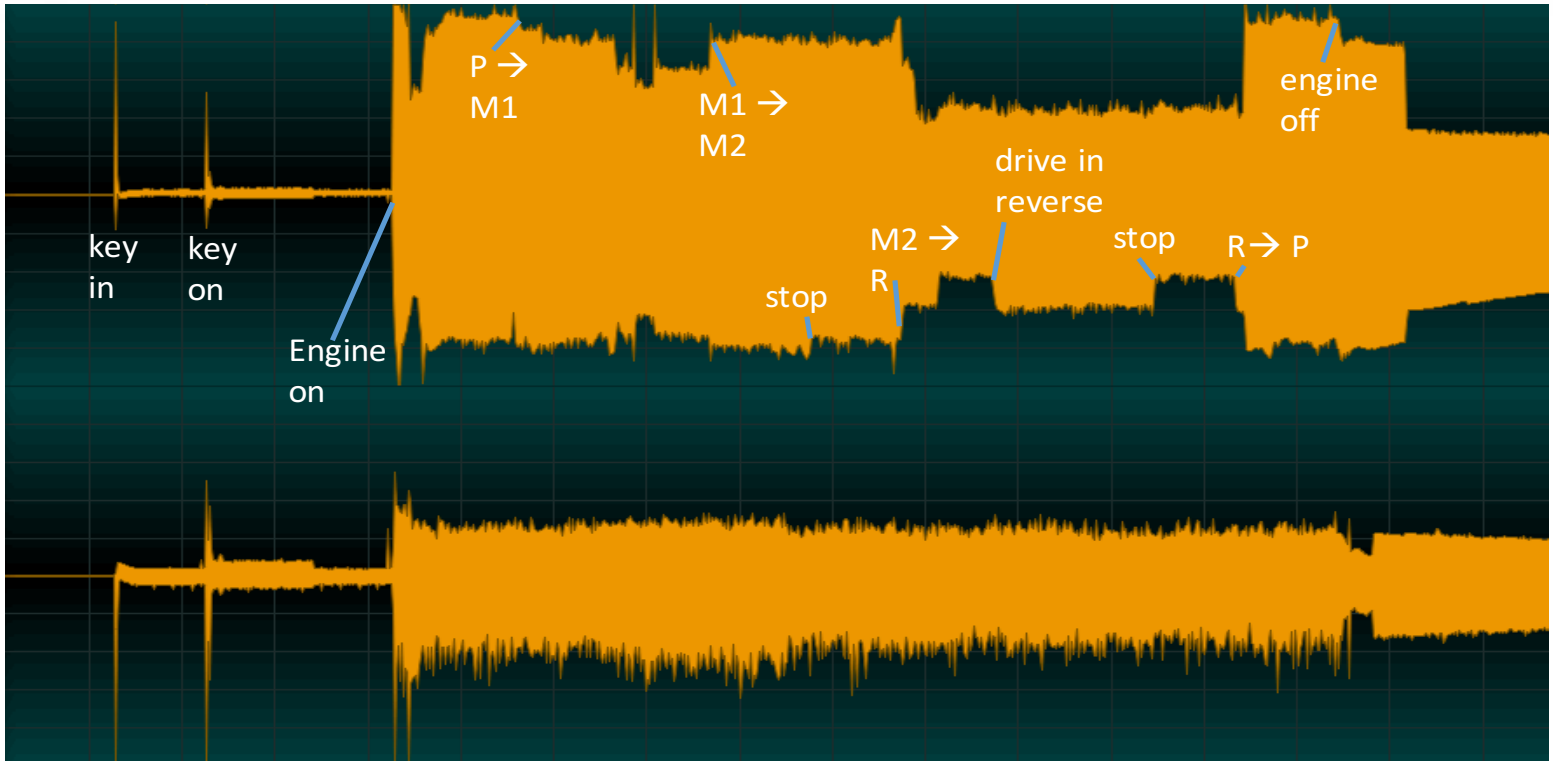
- **Side-channel signals are available from a number of sources**
- **Capturing fluctuations in power consumption is our primary goal**
  - **An RF loop or a probe on various voltage tap points provides useful data for analyzing any control module activity.**



Acquisition of clean side-channel data from within a noisy vehicle environment is possible.

Sample Side-Channel Data

- **Sample data from a vehicle transmission control module shows distinct states corresponding to various driving modes.**

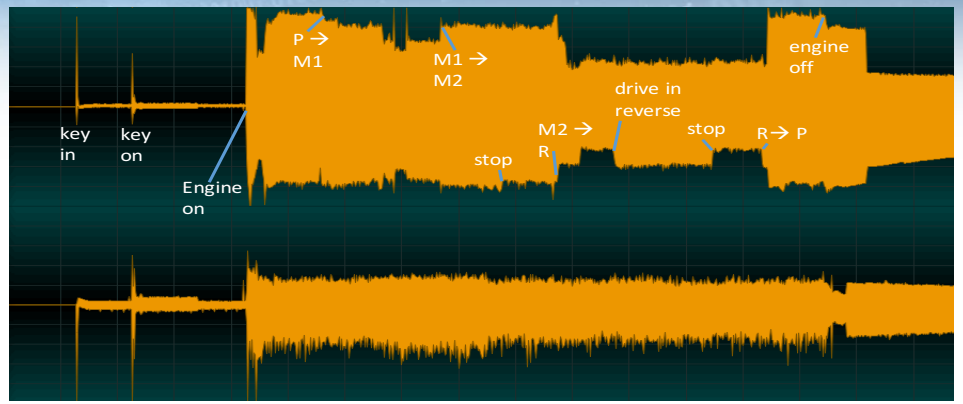


Results from simultaneous capture of side-channel data for two controllers.

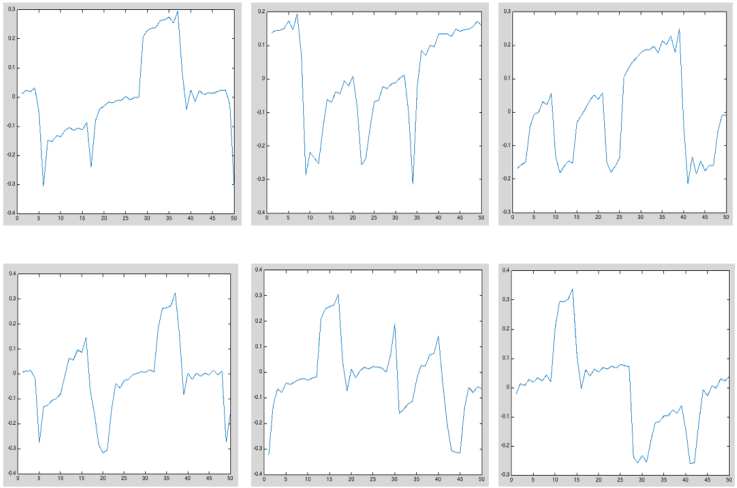
Captured side-channel data reveals strong link to physical system events.

Side-Channel Signal Processing

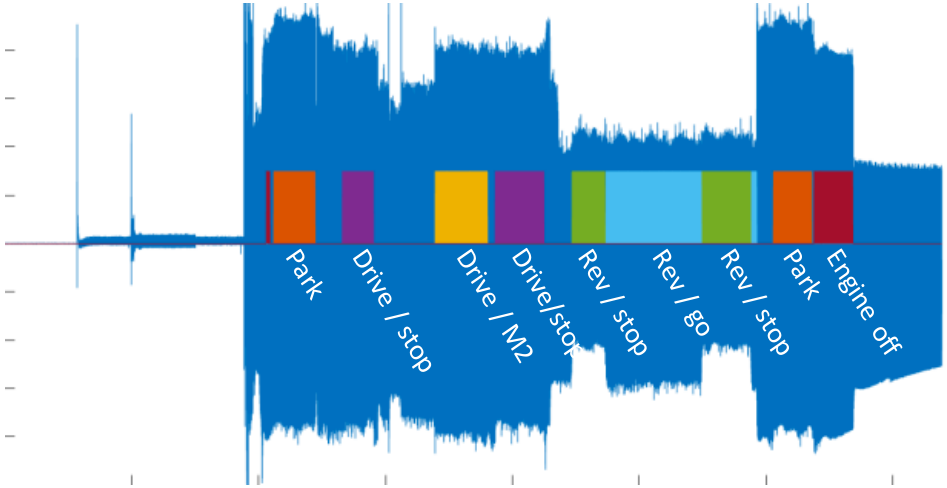
- **Automated analysis of side-channel signals provides a reliable identification of system states that can make spoofing by hackers easily detectable.**



Feature Templates Extracted from Data



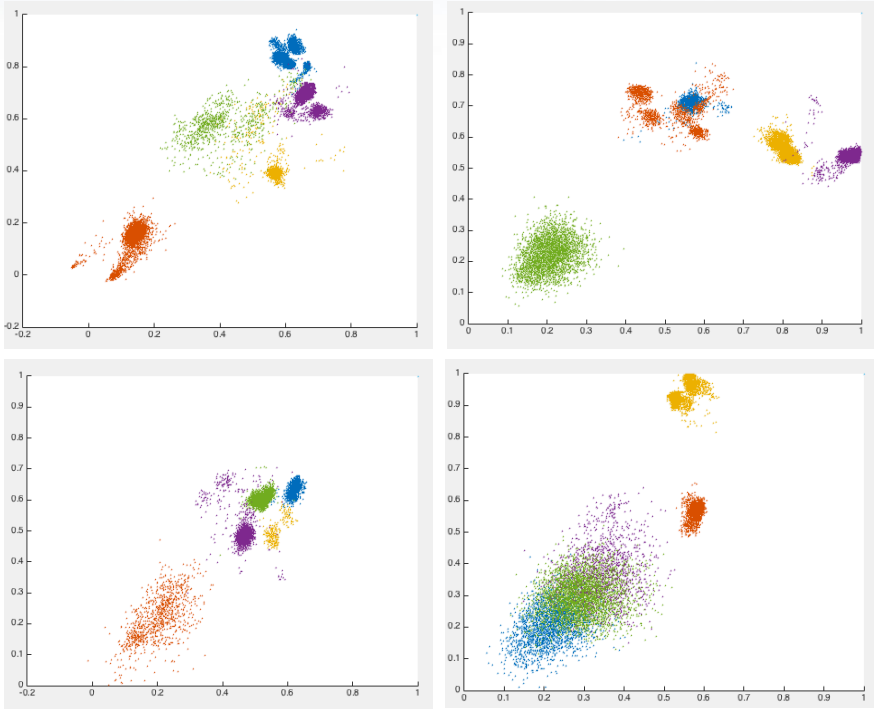
Convolved templates over data reveals matching states



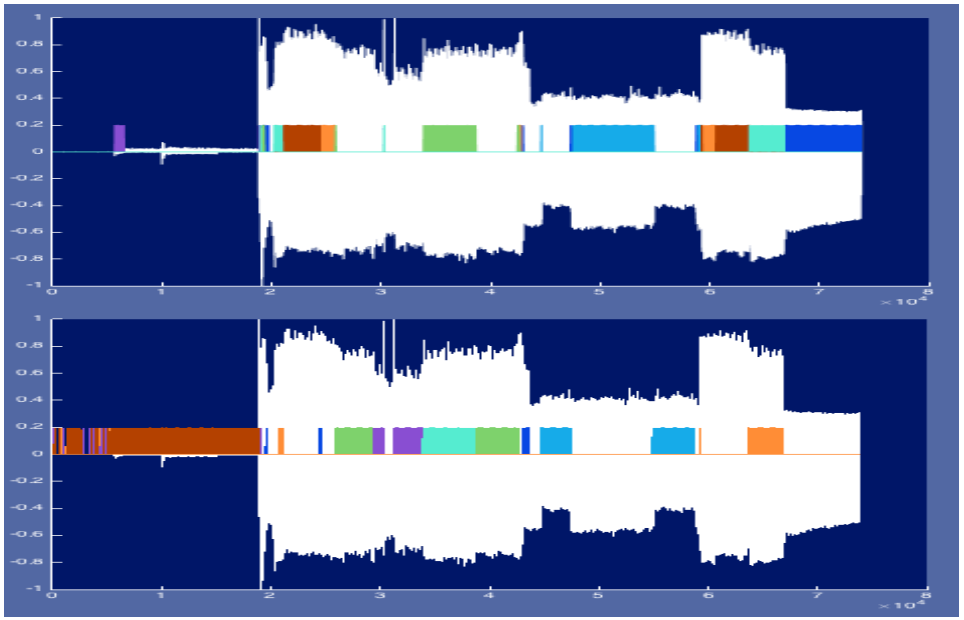
Convolving templates over the data reveals distinct states.

Side-Channel Signal Analysis

K-Means Clustering Of Data Using Templates as Features



Clusters Displayed on Data Shows Good Match to Observed States



These states will be difficult for an attacker to spoof, providing a physical reference of true state for verification against cyber sources.

Clustering reveals a richer set of distinct system states that can be used both for detecting hackers and for diagnostics.

Analyzing CAN Bus Data

Time Code → Bus ID → Message ID → Message Contents

(1446592470.674673)	can0	188	000000010024
(1446592470.674917)	can0	3C5	0000000000000031
(1446592470.675163)	can0	3C6	0000000000000030
(1446592470.678278)	can0	1EB	003B
(1446592470.678517)	can0	097	7FC0081400000018
(1446592470.678954)	can0	039	00001B
(1446592470.679196)	can0	164	041000603D000020
(1446592470.679787)	can0	1A4	0000000000000018
(1446592470.680028)	can0	1AA	7FFF00000000891D
(1446592470.680258)	can0	1B0	8040000000001F
(1446592470.680506)	can0	1D0	000000000000000A
(1446592470.683024)	can0	0E5	00000005

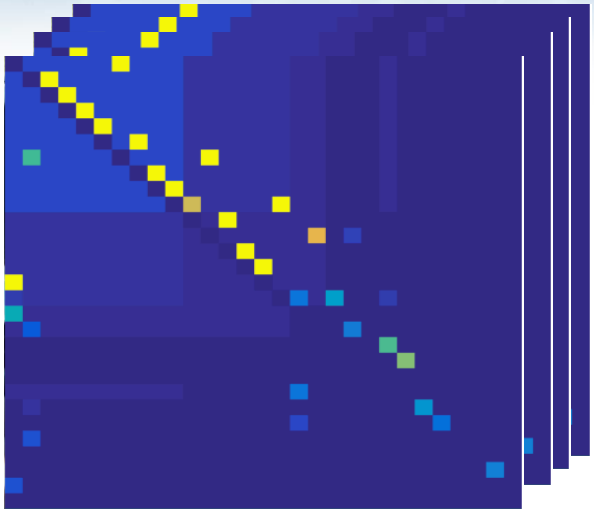
Analyzing timing of vehicle CAN bus messages can potentially reveal signs of hacking.

Detecting Hacking Activity

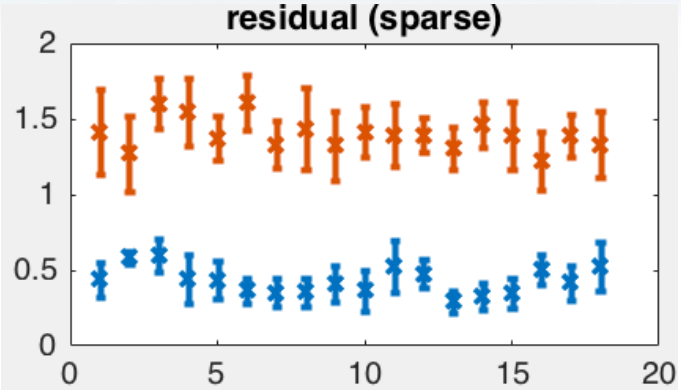
CAN Bus Data

(1446592470.674673)	can0	188	000000010024
(1446592470.674917)	can0	3C5	0000000000000031
(1446592470.675163)	can0	3C6	0000000000000030
(1446592470.678278)	can0	1EB	003B
(1446592470.678517)	can0	097	7FC0081400000018
(1446592470.678954)	can0	039	00001B
(1446592470.679196)	can0	164	0410006030000020
(1446592470.679787)	can0	1A4	0000000000000018
(1446592470.680028)	can0	1AA	7FFF00000000891D
(1446592470.680258)	can0	1B0	8040000000001F
(1446592470.680506)	can0	1D0	000000000000000A
(1446592470.683024)	can0	0E5	00000005

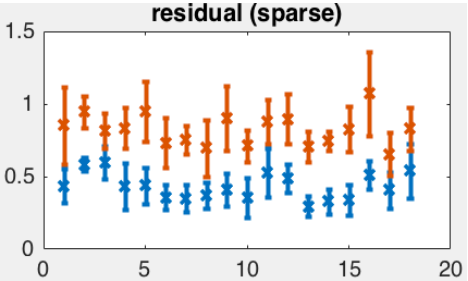
Sequence of TE Matrices



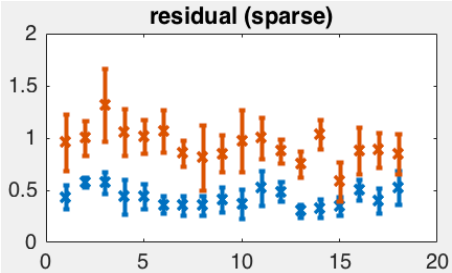
Residual Magnitude from TE Analysis



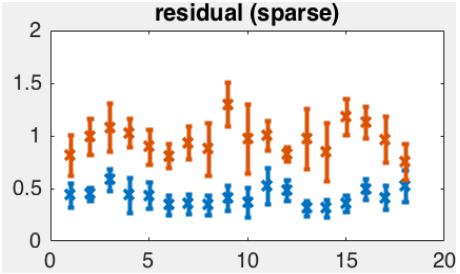
Normal Hacked



Message Delayed



1st to Follow Removed

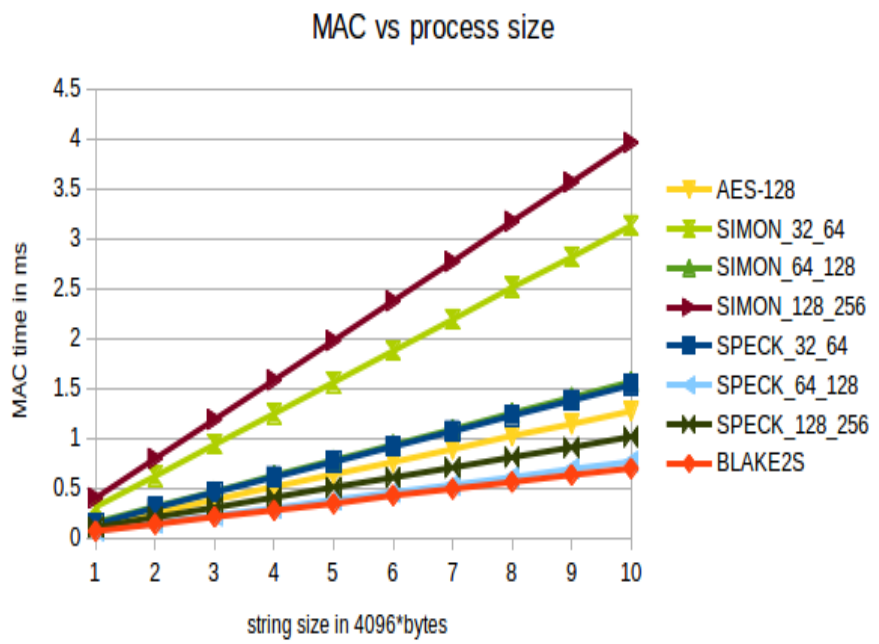


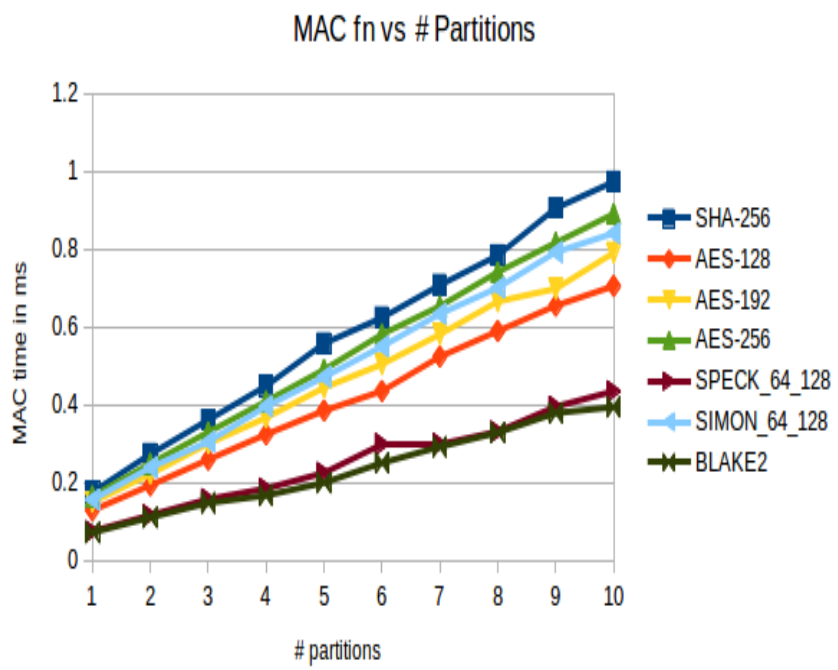
2nd to Follow Removed

Analysis of TE matrices gives promising capability to detect subtle anomalies in CAN Data

Attestation Within seL4

Attestation software is now running in a protected seL4 partition and is able to run checks on other isolated partitions.





Comparison of different MAC algorithms shows that BLAKE2s provides the best performance for attestation in seL4.

Our tests of hash functions for attestation show desired linear scaling

Competition

- PFP Cybersecurity – has demonstrated spectral fingerprinting of signals from processor power bus, claiming to detect anomalous behavior in embedded devices.
- Virta Lab – has product that monitors a device AC power consumption to detect anomalies and malware.
- DARPA HACMS – developing tools to enable high-assurance software for vehicles to make systems more resistant to hackers

- Our solution looks not only at side-channels of individual processors but also at interactions between processors to provide a systems-level view of potential intrusions.
- Our secure update method can work with existing hardware and yet provides provable isolation that specialized hardware does not.

Potential Transition Activities

- Participated in workshops on secure over-the-air software updates for vehicles.
- Outreach to SAE standards group – Vehicle Electrical System Security Committee, with participating members from many automakers.
- NICTA provides all enhancements to seL4 as open source
  - Potentially broad application for seL4 in many other programs
- We have a unique relationship with our LLC members, General Motors (GM) and Boeing that has the potential to accelerate transition to transportation applications.

Contact Information

David W. Payton
HRL Laboratories, LLC
Payton<at>hrl.com
(310) 317-5685

This material is based on research sponsored by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) BAA HSHQDC-14-R-B00016, and the Government of United Kingdom of Great Britain and the Government of Canada via contract number D15PC00223.