The world’s first on-chip monitoring solution to rapidly detect cyber security threats in Connected and Autonomous Vehicles (CAVs)

Professor Mark Zwolinski, University of Southampton
The Internet of Things faces major security challenges.

Connected and autonomous vehicles, as part of the digital home, present many potential attack vectors, increasing cyber security risk.

The socio-economic impacts of cyber security attacks are tremendous, with the automotive industry estimated to lose £20 billion annually by 2023 [Upstream Security].
Example capabilities of proposed solution

**Safety**
HW “stuck pixel” detect

**Security**
HW-based attack detect

**Performance Measurement**
eg preventative failure

- **Non-intrusive**: No performance impact or “warning”
- **Hardware**: Fast, react at HW timescale; invisible to software
- **Visibility**: Analyze software and system everywhere in SoC, see any problem

These “proof of concept” analytics and anomaly detection examples with key customers will move towards full licensable product with investment.
UltraSoC will create new in-silicon modules including:

- Analytics sub-system – on-chip platform ML algorithms and code will run on
- Bus Filter – detect and filter certain events and transactions
- Bus Guardian – filter and “smart” response to detected events and transactions
- Lockstep Monitor – check that redundant systems are functioning correctly
- Forensic Trace – cycle-accurate record of what has happened on-chip (on chip “black box”)
Anomaly detection

• University of Southampton School of Electronics and Computer Science will develop leading edge ML algorithms and code to analyse data produced by UltraSoC monitors and identify threats and hazards, using techniques such as:

  • One-Step Ahead Prediction
    • Minimal computational overhead (to complement the on-chip analytics subsystem). Potential approaches:
      • Single Exponential Smoothing (SES)
      • Autoregressive Moving Average (ARMA)
      • Single-Layer Linear Network Predictor (LN)
  • Anomaly Classification
    • Real-time
      • Residual Distribution (RD)
      • Prediction Interval (PI)
  • Technique demonstrated for natural anomalies:
    • ARMA + RD

3 July 2019
Threat analysis and security testing

- Copper Horse will use its expertise to create a comprehensive threat analysis, informing “security by design” in the system and then use security testing to validate the detection, monitoring and defence techniques:

  - **Threat landscaping** - Explore the existing, known and relevant threat landscape of attacks against vehicular, mobile, IoT and embedded systems.
  - **Develop threat models** - using formal OCTAVE or STRIDE methodology to inform the project.
  - **Use real world attack techniques** - with experts who have vast experience in the embedded hacking world.
  - **Security test** - using the team’s knowledge perform penetration testing against the system demonstrator and evaluate real-world performance against a determined, skilled attacker.
Automotive security functional testbed

- Full-scale automotive functional testbed would ensure an environment which:
  - Supports multi-bus, multi-component configurations;
  - Provide a plug-and-play ECU interface for telematics, sensors, infotainment, in-cabin and body modules as part of test configurations;
  - Underpinned by a high-powered multi-core computing platform for scalable and parallel data processing and analysis, with a cloud-supported interface at the backend to allow for elastic storage and computation.

3 July 2019

Commercial in Confidence
Hardware-based Security

• Mark Zwolinski
• Basel Halak

• PhD Students
  • Dongyao Zhai
  • Haibo Su
  • Miao Yu
  • Xiao Liu