CRII: CPS: Design of Secure and Dependable Next Generation Automotive Cyber-Physical Systems

Award #1743490, Award Date: June 1, 2017

Arslan Munir (PI), Kansas State University, Email: amunir@ksu.edu

Abstract: This project aims at simultaneous integration of security and dependability while minimizing energy consumption and ensuring that real-time constraints of the application are not violated. We have proposed novel electronic control unit (ECU) architectures for real-time automotive CPS that incorporate security and dependability primitives with low resources and energy overhead. We have further proposed an evolving side-channel attacks resistant reconfigurable hardware for elliptic curve cryptography that can be used in cyber-transportation systems (CTS) and other CPS applications requiring asymmetric cryptography. We have also developed a true random number generator (TRNG) that is resistant to PVT variations and can be used for generating secure secret keys in automotive and other CPS.

Challenge:

- Simultaneous integration of security and dependability while ensuring that real-time constraints of the application are not violated

Solution:

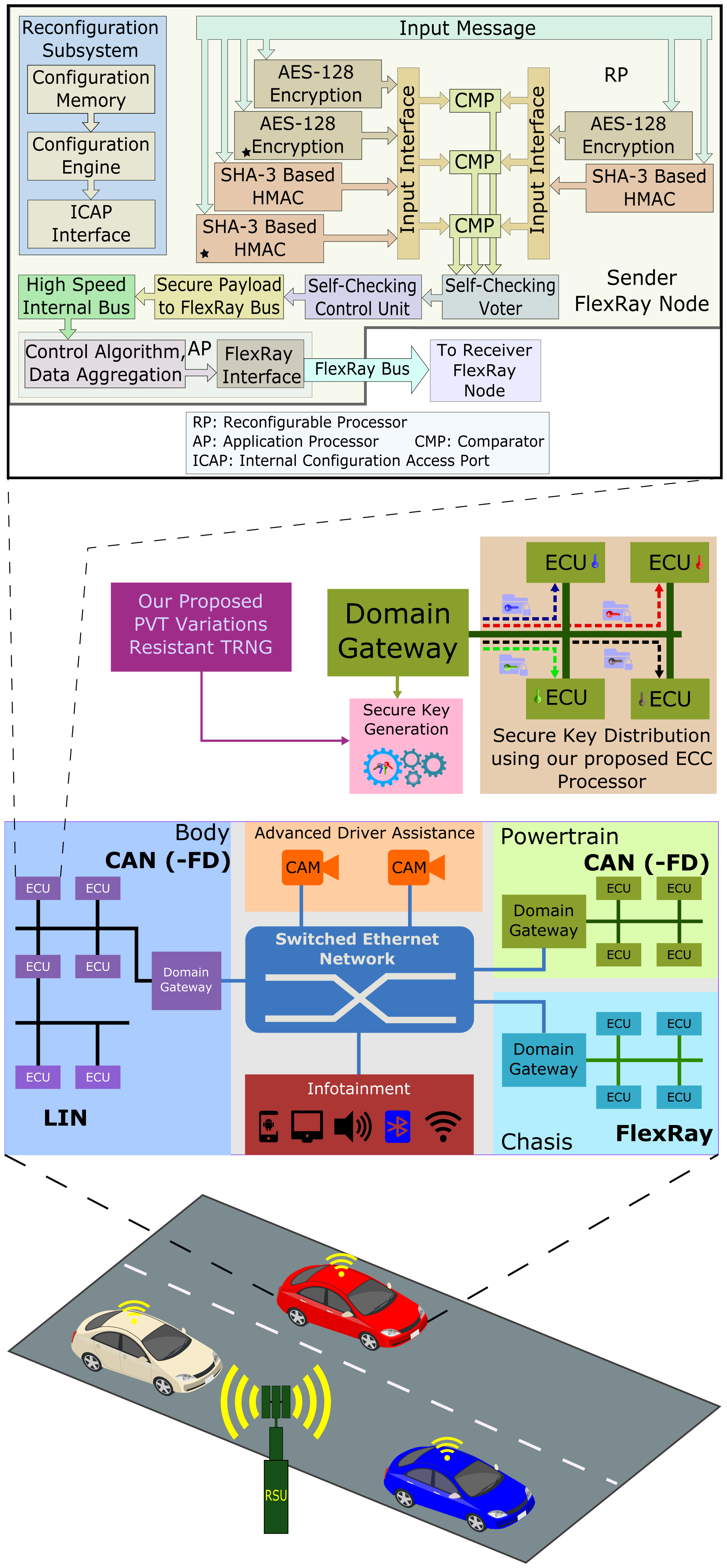
- Novel ECU architectures
  - ○ Reconfigurable ECU architecture
  - ○ GPGPU-based ECU architecture
- Side-channel attacks resistant asymmetric cryptography
  - ○ Evolving side-channel resistant reconfigurable hardware for elliptic curve cryptography
- TRNG
  - ○ PVT-variation resistant TRNG

Novel ECU Architectures:

- Proposed two novel secure and dependable ECU architectures
  - ○ Effectively meet security, dependability, and real-time requirements of automotive CPS
- Reconfigurable ECU architecture
  - ○ Attains a speed up of 31.7x while consuming 1.75x lesser energy then a state-of-the-art ECU (SABRE board)
- GPGPU-based ECU architecture
  - ○ Attains a speed up of 1.8x while consuming 2x lesser energy then state-of-the-art ECU (SABRE board)

Side-channel Attacks Resistant Asymmetric Cryptography:

- First work to use an artificial intelligence algorithm (multi-objective genetic algorithm (GA)) to generate a gate-level circuit that performs cryptographic function
- GA is able to generate side-channel attack resistant 8-bit elliptic curve cryptosystem (ECC)



PVT Variation-Resistant TRNG Circuit:

- Proposed TRNG is a generic circuit-level solution to design a PVT variation-resistant TRNG that can be used with any unreliable entropy source
- Proposed TRNG is simulated using TSMC 65nm and 28nm process technologies in PSpice
- Characteristics of our proposed TRNG
  - ○ Generates random numbers with bit-entropy that always lie in the range [0.998, 1]
  - ○ Data rate of 16 Mbps
  - ○ Resistant to noninvasive fault attacks like changing power supply values and operating temperature

Scientific Impact:

- Proposed ECU architectures are applicable to ground and aerial vehicles
- Proposed evolving side-channel resistant reconfigurable ECC processor can be used for secure asymmetric cryptography applications
- Proposed PVT-variation resistant TRNG can be used for high-reliability applications, such as automotive, military, aerospace, and UAVs

Broader Impacts:

- Societal impacts
  - ○ Alleviating problems with traditional transportation systems, such as energy expenditure, pollution, etc.
  - ○ Designing safe and secure CTS that will result in lesser number of traffic accidents
- Commercial and Defense impacts
  - ○ Proposed architectures and designs can benefit vehicle OEMs, third-party vendors, and military
- Educational impacts
  - ○ Techniques investigated in this project have been incorporated in undergraduate and graduate courses taught by the PI
  - ○ The PI has given lectures/tours of his research lab to high school teachers and students
  - ○ The work presented at various conferences