CPS Attacks

Soumyajit Dey, Assistant Professor,
CSE, IIT Kharagpur

October 17, 2019

Section 1

Secure n Dependable Automotive CPS

Steer By Wire (SBW) case study - Munir et. al.'18

- Dependable Implementation choices - FT-RMT-QED-TMR
- Can use advanced encryption standard (AES) for providing message confidentiality and hash-based message authentication code (HMAC) for ensuring message authenticity and integrity.
- Need to use security and dependability primitives together
- Possible error/fault sources - communication/computation medium

Architectures

- For dual-core ECUs, the FT configuration can be either FT-RMT or FT-RMT-QED.
- FT-RMT executes safety-critical computations on redundant threads and detects an error at the end of computation if there is a mismatch between the two threads' output.
- In FT-RMT- QED, the main thread executes original instructions and the check instructions, which are inserted at different points in the program/computation, whereas another thread executes duplicated instructions.
- Triple-core ECUs can be configured as either FT-RMT- TMR or FT-RMT-TMR-QED
- The FT-RMT-TMR executes the computations on three redundant threads and the correct output is determined by majority voting of the threads' outputs.

FT-RMT-TMR-QED

- The FT-RMT-TMR-QED inserts check instructions at different points in the program/computation to enable early detection of errors via majority voting.
- The FT-RMT- TMR-QED copies the correct output, which is determined by majority voting, to an additional buffer.
- the output of the faulty thread is replaced by the correct output so that the approach can provide single error detection and correction for the remaining computation.
- by using additional comparison and copy instructions, the FT-RMT-TMR-QED can detect and correct multiple single errors at different points in the program
- the number of errors tolerated depends upon the granularity of check instructions - at the expense of additional performance overhead.

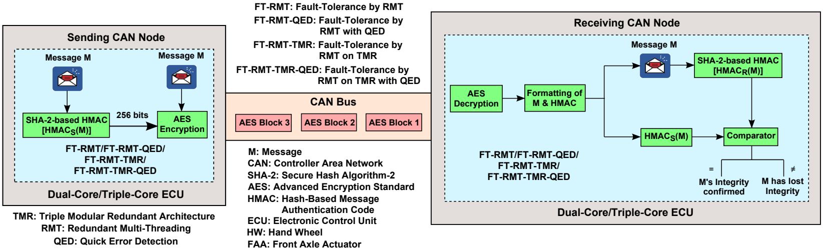
FT-RMT: Fault-Tolerance by RMT
FT-RMT-QED: Fault-Tolerance by RMT with QED
FT-RMT-TMR: Fault-Tolerance by RMT on TMR
FT-RMT-TMR-QED: Fault-Tolerance by RMT on TMR with QED
Sending CAN Node
Message M
Message M
SHA-2-based HMAC [HMAC_S(M)]
256 bits
AES Encryption
FT-RMT/FT-RMT-QED/ FT-RMT-TMR/ FT-RMT-TMR-QED
Dual-Core/Triple-Core ECU
TMR: Triple Modular Redundant Architecture
RMT: Redundant Multi-Threading
QED: Quick Error Detection
CAN Bus
AES Block 3
AES Block 2
AES Block 1
M: Message
CAN: Controller Area Network
SHA-2: Secure Hash Algorithm-2
AES: Advanced Encryption Standard
HMAC: Hash-Based Message Authentication Code
ECU: Electronic Control Unit
HW: Hand Wheel
FAA: Front Axle Actuator
Receiving CAN Node
Message M
SHA-2-based HMAC [HMAC_R(M)]
AES Decryption
Formatting of M & HMAC
HMAC_S(M)
Comparator
=
≠
M's Integrity confirmed
M has lost Integrity
FT-RMT/FT-RMT-QED/ FT-RMT-TMR/ FT-RMT-TMR-QED
Dual-Core/Triple-Core ECU

Figure: Example CPS Implementation

Section 2

Automotive Threat Model

Passive Eavesdropping & Traffic Analysis: Need for Confidentiality

- Modern automotive in-vehicle networks carry a mix of operational and personally identifiable information,
- e.g. current location, previous destinations, navigation history, call history, microphone recordings, financial transactions, etc
- An adversary invading an in-vehicle network could perform passive eavesdropping (i.e., sniff and store all the traffic in an automobile's internal network)
- Do traffic analysis, thus, obtaining critical information about the driver and the vehicle.
- by eavesdropping and traffic analysis of the steering angle, accelerator, and braking values, the adversary could track the car

Passive Eavesdropping & Traffic Analysis: Need for Confidentiality

- an adversary can have the capability to request generation of encrypted messages
- Recorded packets and/or knowledge of the plain-text can be leveraged to reveal the encryption key, decrypt complete packets, or gather other useful information through traffic analysis.

Active Eavesdropping & Message Injection: Need for authentication and integrity:

- An attacker may perform spoofing attacks by actively injecting and/or modifying messages in the in-vehicle network.
- an adversary might inject malicious messages by encoding the messages on a CD as a song file and convincing the user to play the CD using social engineering.
- The adversary can also insert a replayed packet.
- the attacker's device may impersonate a valid ECU or gateway for malicious activities

CIA for Automotive CPS with CAN

- AES-128 (128-bit) encryption provides confidentiality
- HMAC based on SHA-2/SHA-256 (Secure Hash Algorithm-2) render integrity and authenticity
- In the example, we have a SHA-2 habsed HMAC module and an AES module
- Msg $M \Rightarrow SHA-2\, HMAC \Rightarrow$ msg digest $HMAC_S(M)$
- $M + HMAC_S(M) \Rightarrow AES \Rightarrow Final\ O/P$

Key storage Overhead $\mathcal{O}_{M,S}$

$$\begin{aligned} \mathcal{O}_{M,S} &= \text{calc}\,[HMAC_S(M)] \\ &\quad + \text{Encrypt}_{AES}\,[M + HMAC_S(M)] \end{aligned} \tag{1}$$

- AES, HMAC keys need storage in tamper resistant memories
- Keys need to refreshed over time by participating ECUs
- Ex, Car starts ⇒ one ECU from every safety critical domain broadcasts AES, HMAC keys ⇒ prevents replay attacks

Storage and communication for $\mathcal{O}_{M,S}$

- 8 byte CAN msg, $M + HMAC(M) = 64 + 256 = 320\,bits$
- Encrypting 320 bits require three 128-bit AES blocks ($\lfloor \frac{320}{128} \rfloor$)
- The third AES block encrypts 64 bits padded by 1 and then all 0s creating a 128 bit block
- $128 \times 3 = 324$ bits generated, 324/64=6 CAN msg frames
- Hence, One unprotected CAN msg $\equiv$ 6 protected ones

FT requirements

$$\begin{aligned}
\mathcal{O}_{M,S}^{FT-RMT-TMR-QED} \quad &= \quad \text{calc}^{\forall i=1,2,3}\left[HMAC_S^{T_i}(M)\right] \\
&+ \text{copy}\left[HMAC_S^{c}(M), \mathcal{V}_{mj}^{i=1,2,3}\{HMAC_S^{T_i}(M)\}\right] \\
&+ \text{copy}\left[HMAC_S^{T_f}(M), HMAC_S^{c}(M)\right] \\
&+ \text{Encrypt}_{\text{AES block}_j}^{\forall j=1,2,3}\left[M + HMAC_S^{T_i\ \forall\ i=1,2,3}(M)\right] \\
&+ \text{copy}^{\forall j=1,2,3}\left[\text{AES block}_j^{c}, \mathcal{V}_{mj}^{i=1,2,3}\{\text{AES block}_j^{T_i}\}\right] \\
&+ \text{copy}^{\forall j=1,2,3}\left[\text{AES block}_j^{T_f}, \text{AES block}_j^{c}\right] \qquad (2)
\end{aligned}$$

- calculate HMAC - three parallel threads
- Majority voting, to get correct HMAC (additional buffer required); copy correct HMAC to faulty core o/p-s
- AES - three parallel threads, majority vote, copy to buffer
- copy back to faulty compute node o/p-s

Receiving side

$$\begin{aligned} \mathcal{O}_{M,R} &= \text{Decrypt}_{AES}\left[M + HMAC_S(M)\right] \\ &\quad + \text{format}\left[M + HMAC_S(M)\right] + HMAC_R(M) \\ &\quad + \text{comp}\left[HMAC_S, HMAC_R\right] \end{aligned} \tag{3}$$

- Decrypt
- Separate out *M*
- compute HMAC in receiving side
- compare

Receiving side with redundancy

$$\begin{aligned}
\mathcal{O}_{M,R}^{FT-RMT-TMR-QED} \quad &= \\
&\text{Decrypt}_{\text{AES block}_j}^{\forall j=1,2,3}\left[M + HMAC_S^{T_i\ \forall\ i=1,2,3}(M)\right] \\
&+ \text{copy}^{\forall j=1,2,3}\left[\text{AES block}_j^c, \mathcal{V}_{mj}^{i=1,2,3}\{\text{AES block}_j^{T_i}\}\right] \\
&+ \text{copy}^{\forall j=1,2,3}\left[\text{AES block}_j^{T_f}, \text{AES block}_j^c\right] \\
&+ \text{format}^{i=1,2,3}\left[M + HMAC_S^{T_i}(M)\right] \\
&+ \text{calc}^{\forall i=1,2,3}\left[HMAC_R^{T_i}(M)\right] \\
&+ \text{copy}\left[HMAC_R^c(M), \mathcal{V}_{mj}^{i=1,2,3}\{HMAC_R^{T_i}(M)\}\right] \\
&+ \text{comp}\left[HMAC_S(M), HMAC_R^c(M)\right] \qquad (4)
\end{aligned}$$

Receiving side with redundancy

- decrypt - 3 parallel threads
- copy correct after voting
- copy correct result to faulty o/p-s
- separate *M*
- calculate HMAC (3 - threads), vote, copy
- and compare

SBW system

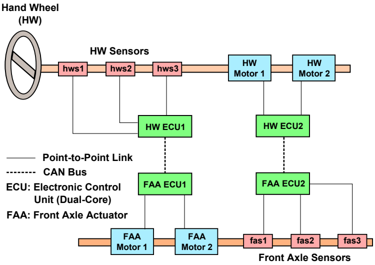

Figure: SBW system - eliminates steering column

Two main functionalities -

- Front axle control (FAC) that controls the wheel direction in accordance with the driver's request;
- Hand wheel force feedback (HWF) that provides a mechanical-like force feedback to the hand wheel.

SBW

- removing the steering column reduces the weight of the vehicle and therefore reduces fuel consumption.
- SBW system enhances driver comfort by providing a variable steering ratio, that is, the steering ratio between the handwheel and the road wheels can be adapted according to the driving conditions (e.g., smaller steering ratio in parking and urban driving as compared to the driving on freeways).

QoS and Behavioral Reliability

- This end-to-end delay/response time T_{res} is perceived as the QoS - can be effected by other CAN bus loads
- The behavioral reliability is defined as the probability that the worst-case response time is less than some critical threshold T_{max}
- Automotive OEMs determine T_{max} by various means, such as Matlab/Simulink simulations, vehicular network simulations, vehicle system simulations, and vehicle tests, etc.

Brake Anomaly Detection (BAD)

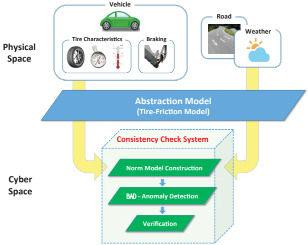

Figure: CPS approach, norm check

Tire-slip

$$\sigma = \frac{r_{eff}\, w_w - V}{max(r_{eff}\, w_w, V)}$$

where r_{eff} is the rolling tire radius, w_w the wheel angular velocity, and V the vehicle speed.

- During acceleration, $\sigma > 0$, during braking, $\sigma < 0$

The normalized longitudinal force $\rho_x = F_x/F_z$,

1

[1] "CPS Approach to Checking Norm Operation of a Brake-by-Wire System" - Cho et. al.

BAD

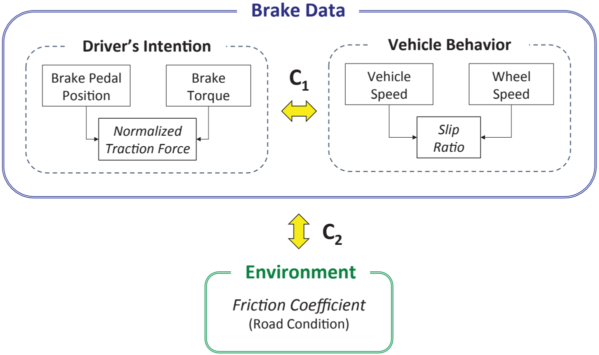

Figure: Checking consistency between the driver's intention and vehicle braking behavior, and brake data and environment

Section 3

Industrial Control Systems

-
-
-

-
-
-

-

-

-

-

-

-