WeepingCAN

- The bus-off attack is easily detectable by a good intrusion detection system
- *WeepingCAN* is a variation of the original bus-off attack, stealthier than the original one
- Differences:
  - The attacker disables the transmission of the attack message with the same ID as the victim
  - The attacker causes *recessive bit errors*
  - The attacker does not fabricate preceded messages
  - The attacker randomizes bit errors

WeepingCAN

- The attack message has the victim’s ID, bit-time, and prefix bits until a random position where the victim is dominant but the attacker is recessive
- As for the original bus-off, both attacker and victim have TEC = 0 at the beginning
- The goal of weepingCAN is to avoid exhibiting temporal differences due to the error state transition

Attack Cycle

- The attacker synchronized with the victim using the same approach of the original bus-off
- The attacker however <u>disables the retransmission</u> of the attack packet
- The attacker injects the attack message
- The attacker' CAN controller sends an error-active flag due to the bit error in the attacker's packet, which increases both attacker's and victim's TEC by 8
- The victim retransmits the original packet and TEC=TEC-1
- Victim and attacker decrease TEC for other transmissions

Disable Retransmissions

- Disabling retransmission allows to remove an easily detectable feature, i.e., the consecutive retransmissions of the same packet
- The attack is now composed by an active error + successful retransmission
- Two ways to avoid retransmissions:
  - Disable automatic retransmission for all messages (via control register)
  - Abort transmission on transmit error (via interrupt)

Recessive Injection

- The attacker injects a recessive bit when the victim “contains” a dominant bit
- Both attacker and victim increase TEC by 8, however only the victim retransmits (TEC = TEC - 1)
- The attacker must identify additional messages it can transmit to keep its TEC lower than that of the victim
- The attacker needs to transmit at least 1 more message than the victim for each attack packet

Basic Attack Strategy

- Suppose that the attacker and victim both have a single message they can send
- Suppose A sends its packet with one fifth the period of V
- Thus, for every attack message, A transmits 5 messages while V transmits 1 → $TEC_A=3$, $TEC_V=7$
- V can be forced to error passive with 19 attack messages
- A needs to be careful not to reach error passive before V goes bus-off!
- A can decide to skip some injections

Randomized Bit Positions

- The second feature making bus-off identifiable is the presence of successive messages over the passive error flags of the victim
- Furthermore, the attacker may always use the same packet for the attack
- Therefore, it might be good for the attacker to have the possibility to randomize packets
- In particular, to randomize the position of the error bit

Randomized Bit Positions

- The DLC of most messages is a fixed constant that can be discovered by offline analysis of a CAN trace
- The number of dominant bits in DLCs vary between 1 and 3, so the entropy is low
- A clever attacker may inject recessive error in the data field
- The data field often encodes a number that does not change quickly because of physical constraints or an event identifier that comes from a limited set of event
- If A can identify a deterministic pattern → inject error in the data