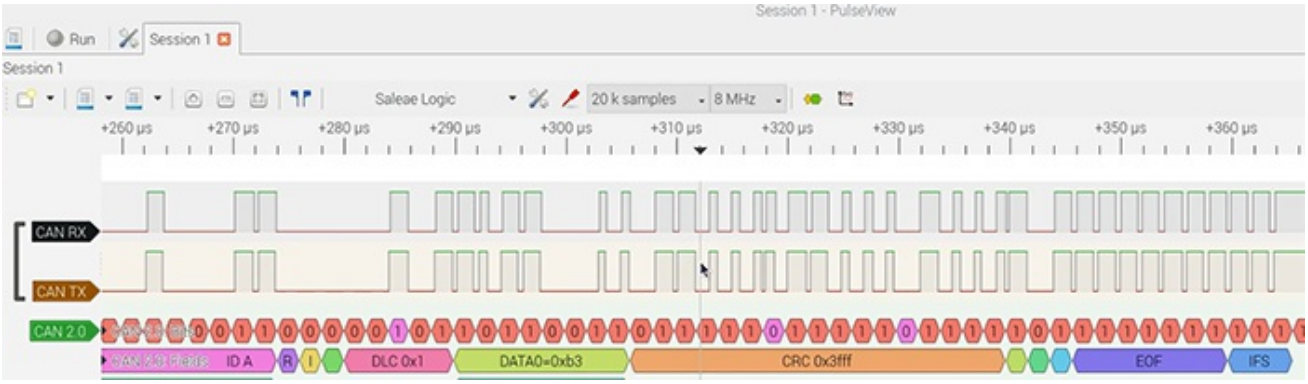
CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

The Janus attack

The Janus attack is a low-level CAN protocol attack where a single CAN frame contains two different payload contents.



Logic analyzer trace of a Janus frame (Source: Canis Automotive Labs)

The complete article is published in the December issue of the CAN Newsletter magazine 2021. This is just an excerpt.

With the Janus Attack, a targeted device sees a different payload than other devices. This attack could be used to transmit a frame to evade an intrusion detection system (IDS), or it could put two different actuators into inconsistent states (e.g. moving a pair of motors in different directions). It breaks the atomic multicast feature of CAN (where every device sees the same frame) - an important property that lots of systems rely on (often implicitly). The attack works by exploiting the CAN protocol synchronization rules and targets devices that have different sample points. The CAN specification defines the following rules:

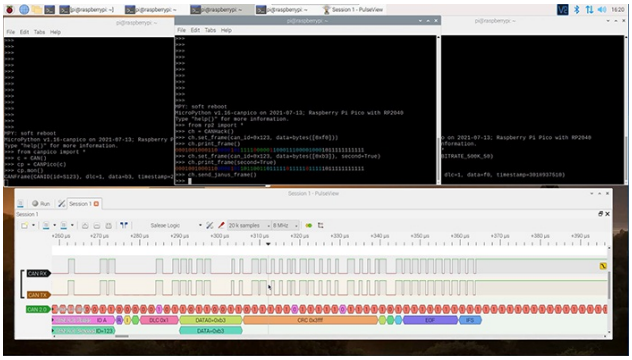
a. Only one synchronization within one bit-time (between two sample points) shall be allowed. After an edge was detected, synchronizations shall be disabled until the next time the bus state, detected at the sample point, is recessive.
b. An edge shall cause synchronization only if the bus state detected at the previous sample point (previous read bus state) was recessive.

The attack can be mounted purely in software that takes control of the GPIO port connected to the CAN Tx pin of a CAN transceiver, so a hijacked device using a remote code execution vulnerability could be used to mount the attack.

In a demonstration video of the attack, two CANPico boards (that contain the Microchip MCP2517/18FD CAN controller) are attacked by a CANHack board. The latter is a cut-down version of the CANPico that does not have a CAN controller, neatly proving that the attack can be mounted in pure software. The logic analyzer is running the Sigrok Pulseview CAN2 protocol decoder to show how the Janus signal is decoded into a CAN frame.

How does the attack work?

The attack forces CAN controllers to synchronize at the same time and then changes the CAN bus level after one controller has sampled the bus but before another. The bit sequences are set so that each device sees a valid frame, but the frames can have different payloads. The logic analyzer trace (Figure 1) shows how a Janus frame is made up of many more transitions than CAN bits but that form a valid CAN frame. There are two restrictions on the bit sequences. First, the first and second CAN frame have to have the same length, so there must be the same number of stuff bits. The CANHack tool kit has a function to show the bit patterns of both halves of a Janus frame (Photo 2). Second, if the Janus bit is ***10*** (i.e. the first sampled value in a CAN bit is a ***1*** but the second sampled value is a ***0***) then all controllers have to see the same subsequent bits (***00*** or ***11***) until they are brought back into sync (which happens after a ***11***).



Setup of the two CANPico boards and the CANHack board in the middle. The CANHack tool kit has a function to show the bit patterns of both halves of a Janus frame. (Source: Canis Automotive Labs)

If you would like to read the full article, you can download it free of charge or you download the entire magazine.

cw