oMAC : Open Model for Automotive Cybersecurity

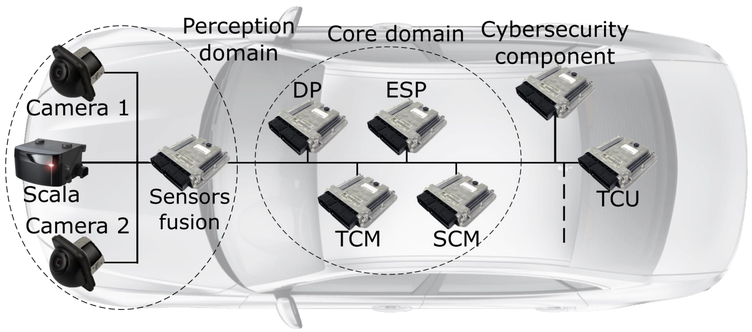
Vincent Hugot, Adrien Jousse, Christian Toinard, Benjamin Venelle

17th escar Europe – The World's Leading Automotive Cyber Security Conference
November 19 and 20, 2019, Stuttgart, Germany

oMAC : Open Model for Automotive Cybersecurity

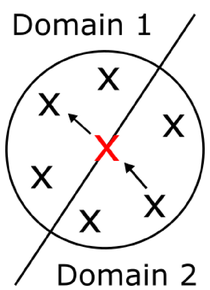
Vincent Hugot, Adrien Jousse, Christian Toinard, Benjamin Venelle

Cybersecurity has become mandatory to preserve safety. Mandatory Access Control (MAC) is needed to provide defense-in-depth to automotive architectures.

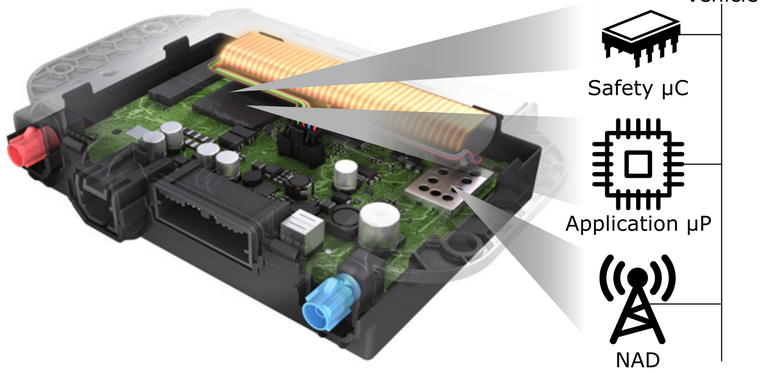


DP: Decisional Pilot
ESP: Electronic Stability Program
TCU: Telematics and Communication Unit
TCM: Transmission Control Module
SCM: Steering Control Module

The access control policy shall be enforced in the middleware. SOME/IP is used as a proof-of-concept. Effective access control mechanisms require enforcing the least privilege principle.



- Privilege separation: An entity with a fixed set of privileges shall not obtain further privileges.
- Duties separation: An entity can legitimately require new privileges through a mediating entity.



The following example is focused on a Telematics and Communication Unit (TCU), a privileged attack point.
For the above TCU, two use cases are considered: a remote diagnostic (RD) and a remote control (RC).

$$Allow\ NAD \xrightarrow{4G\ invoke\ RD} \mu P \xrightarrow{RD\ invoke\ Diag} \mu C \quad (1)$$

$$Allow\ NAD \xrightarrow{4G\ invoke\ RC} \mu P \xrightarrow{RC\ invoke\ Ctrl} \mu C \quad (2)$$

With the following ruleset and without rules sequencing, duties and privileges separation are not guaranteed. The TCU cannot guarantee these cybersecurity properties.

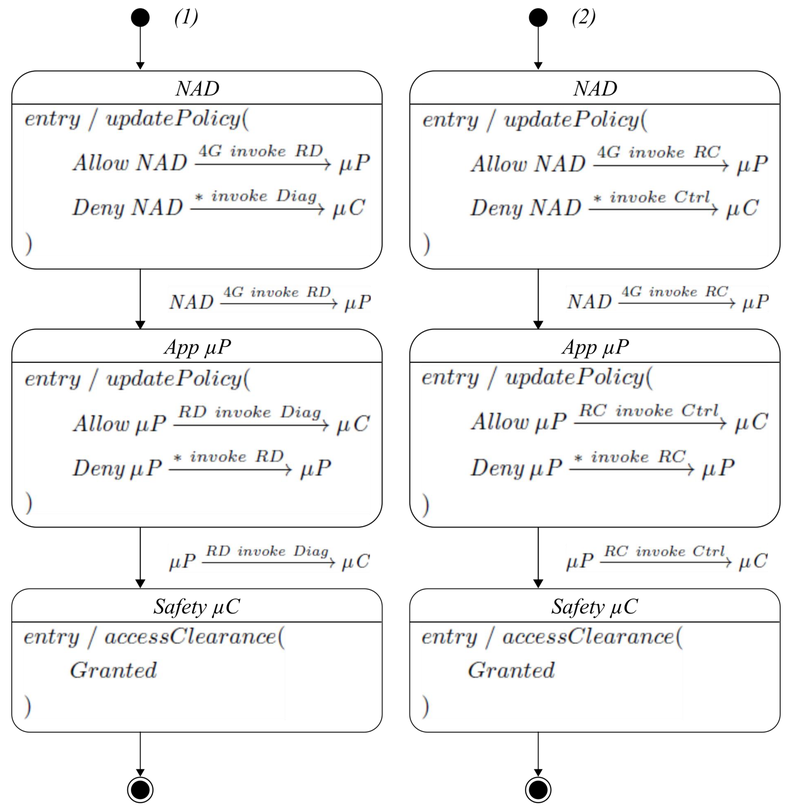
$$Allow\ NAD \longrightarrow \mu P \qquad Allow\ \mu P \longrightarrow \mu C$$

$$\Downarrow \text{ Refined access control policy } \Downarrow$$

$$Allow\ NAD \xrightarrow{4G\ invoke\ RD} \mu P \qquad Allow\ \mu P \xrightarrow{RD\ invoke\ Diag} \mu C$$

$$Allow\ NAD \xrightarrow{4G\ invoke\ RC} \mu P \qquad Allow\ \mu P \xrightarrow{RC\ invoke\ Ctrl} \mu C$$

Access control rules must be activated according to previous access decisions. Access control automata can implement this behavior by describing the evolution of the access control policy.



The automaton changes state according to observed relations, leading to a dynamic evolution of the access control policy.