Partnerships- the C2A way

Partnerships could be a good way to create value for your customers. It’s a tool that allows you to create something new that combines two different approaches / IP portfolios / strategies / source of funds.

Sometimes, successful partnerships can even define an ecosystem. In automotive we can actually see many of them in our days, especially with OEMs chasing the autonomous or electric dream.
From my point of view, the way to achieve successful partnership must coherent with the Win-Win-Win approach - if all parties, including the customers, enjoy something that you do, it will be successful.

It’s quite common to see partnerships PRs announcing collaboration between one of the market’s top organizations and a young startup.

The neighborhood veteran keeps his position as a market leader that attracts and supports new technologies, and the young startup enjoys the fame of the veteran. As Michael likes to say about such fame: An elephant and a mouse stand together and kick the dirt with their feet, and the mouse says “look how much dirt **we** throw into the air”.

When two giants do such collaboration, it could be indeed a big thing. Imagine Apple and Google announcing a collaboration enabling Iphones to support Android out of the box.

However, when a small startup announces a collaboration in which he “support” one of the major players environment, then there isn’t really much excitement around it, usually rightly so.

Partnership between a startup and a giant should aim to provide the market a unique value**.**

At C2A, we understand that we’re not the Apple nor the Check Point of the automotive industry (yet ;) ). If we want to create impact in such collaboration, we have to find unique synergies that provide our clients unique value proposition that couldn’t otherwise be available.

The CAN bus security gaps are a well known issue in automotive. They were discussed many times, chewed to tiny bits and pieces, and proved by many hackers with many variations, and on multiple platforms.

Yet, there wasn’t (until today) any practical solution available in the market to solve those issues. A solution that on one side is easy to integrate and maintain, and on the other side is comprehensive enough to provide the required security layer.

CAN bus is here, and it is not leaving us anywhere soon.

Although everyone is tired of talking about CAN bus security problems, and it not being sexy anymore, **we have to provide a solution that will vehicles safe until the risk will be completely out of the car.**

When we sat together with the NXP team, the goal was clear - provide our clients iron-clad CAN bus cybersecurity protection, that will finally give them a unique edge over attackers.

We understood that such outstanding edge might be achieved by combining two different paradigms into one holistic solution In this case, combining both companies Software and Hardware cybersecurity capabilities.

Together, we have listed various possible CAN bus attack vectors, ranging from the lowest OSI layer, through basic medium attacks up to sophisticated application level attacks. Accordingly, we devised a defence strategy and required mechanism, also taking into account the much needed elaborated reporting mechanism, connecting the solution to be an integral part of OEMs security lifecycle.

Then, we carefully meshed our solutions together to create a unique synergy between C2A software and NXP hardware.

Finally, we managed to create the first of its kind solution, that provides our clients the much needed CAN bus security layer that they have long been waiting for. The Win-Win-Win has been achieved - SW IP, combined with HW IP, resulting in a fantastic value for our clients.

It was a real pleasure teaming up the NXP team, and having the fruitful and educating discussions leading to the concrete solution that we revealed today.

I must admit having a diverse team led by a VP R&D with more than 20 years experience handling embedded security definitely helped the process, but it also allowed us to gain deep insights from the process, and mature as a company as well.

I look forward to having more collaborations like these in the future, allowing us to learn, contribute and evolve in this great ecosystem, while enhancing our clients security posture.