**Partnerships –the C2A way**

Partnerships can be a good way to create value for your customers. They are a means of allowing you to create something new; something that can combine different approaches, IP portfolios, strategies, and perhaps sources of funding.

Successful partnerships can sometimes even define an ecosystem. In the automotive field, many exist at the present time, especially with OEMs chasing the autonomous or electric dream. From my point of view, the way to achieve a successful partnership must be consistent with the Win-Win-Win approach – if all parties, including one’s customers, benefit from something you do, then its success is ensured.

It is common to see press releases announcing different partnerships, or collaboration between one of the market’s leading players and a young startup.

The neighborhood veteran keeps their status as a market leader who both attracts and supports new technologies, while the young startup can benefit from the spillover of the veteran’s reputation. As Michael likes to say about such fame: an elephant and a mouse are standing next to one another kicking the dirt with their feet; the mouse remarks “look how much dirt *the two of us* are kicking into the air”.

When two giants join in such a collaboration, this can definitely be a significant event: 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 they “support” the environment of one of the major players, this does not generate much excitement, and usually rightly so.

Partnership between a startup and a giant should aim to provide unique value to the marketplace**.** At C2A, we understand that we are not (yet) the Apple or the Check Point of the automotive industry. If we want to create impact in such a collaboration, we must find one-of-a-kind synergies that provide our clients with a unique value proposition that wouldn’t otherwise be available.

Controller Area Network (CAN) bus security gaps are a well-known issue in the automotive sector. They have been discussed often, taken apart, and challenged in many instances by hackers, often on multiple platforms. But until now there hasn’t been any practical solution available in the market to solve these issues: a solution that, on the one hand, is easy to integrate and maintain, while, on the other hand, is comprehensive enough to provide the required layer of security.

CAN buses are here, and will be with us for the foreseeable future. Although everyone may be tired of talking about CAN bus security problems, and it might not be ‘sexy’, **we must work to provide a solution that will make vehicles safe.**

When we sat down with the NXP team, our goal was clear – to provide clients with ironclad CAN bus cybersecurity protection that will ultimately provide a unique edge over potential attackers. We understood that the way to achieve such an outstanding edge might be by combining two different paradigms into one holistic solution. In our case, this meant combining both companies’ software and hardware cybersecurity capabilities.

Together, we 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 the mechanisms required, also taking into account the much-needed elaborate reporting mechanism, connecting the solution so as to be an integral part of the OEM’s security lifecycle.

We then carefully meshed our solutions together to create a unique synergy between C2A’s software and NXP’s hardware.

In the end, we were able to create a solution, the first of its kind, that provides our clients with the much-needed CAN bus security layer for which they have long been waiting. We believe we have achieved a Win-Win-Win situation: – software IP, combined with hardware IP, and resulting in fantastic value for our clients.

It has been a real pleasure to cooperate with the NXP team, and to have the fruitful and illuminating discussions that led to the specific solution we can reveal today.

I must admit that having a diverse team led by an R&D VP who has over 20 years’ experience handling embedded security definitely helped the process, and allowed us to gain deep insights from the process and to mature as a company.

I look forward to future collaborations like this, enabling us to learn, contribute and evolve in this important ecosystem, while enhancing our clients’ security posture.