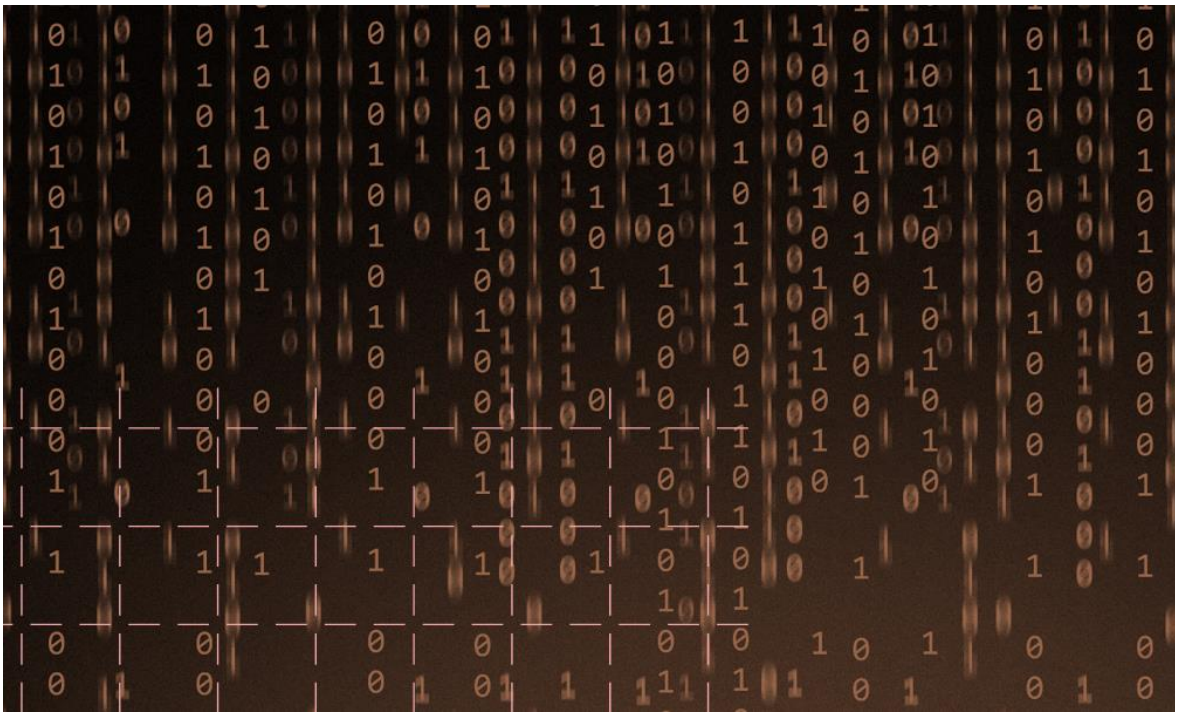
AutoSec-resultatspridning och omvärldsbevakning för cybersäkerhetsprojekt. Slutrapport.



Författare: Fredrik Cederstav
Datum: 2023-05-29
Projekt inom Elektronik, mjukvara och kommunikation, DNr: 2019-05883

FFI Fordonsstrategisk Forskning och Innovation
VINNOVA Energimyndigheten TRAFIKVERKET
FKG VOLVO SCANIA VOLVO

1 Sammanfattning

Projektet har bidragit till kunskapsutbyte mellan befintliga Vinnovaprojekt inom området cybersäkerhet. Genom projektet har fordonsindustrin även avlastats genom att dissemineringen av aktuella forskningsresultat från befintliga forskningsprojekt inom cybersäkerhet har samordnats, varpå kapaciteten i svensk fordonsindustri har stärkts. Kommersiella aktörer har bjudits in för att tala vid flera konferenser. Projektet har genomfört både lunchseminarier och heldagskonferenser. Förutom fordonsföretagen Scania, Volvo Cars och AB Volvo har akademin med Chalmers och ytterligare fordonsaktörer bjudits in och deltagit i projektets nätverk, exempelvis Polestar, Einride och Wireless car. Projektet har stärkt samarbetet mellan fordonsföretagen, akademien, externa företag och forskningsinstitut. Chalmers har stöttat med omvärldsanalys och en sammanfattning av kommande konferenser. RISE har koordinerat projektet, kallat till projektmöten och drivit konferenserna. Projektet har även stärkt samarbetet med RISE interna satsning *Centrum för Cybersäkerhet*. Projektet har starkt påverkats av pandemins premisser vilket resulterade i fler digitala möten och konferenser än just fysiska.

2 Executive summary in English

This project was started as a next step to the Dex-project. Before these two projects, there was an insufficient coordination among cyber security projects for the vehicle industry in Sweden. The project has contributed by organizing and bringing together researchers and product developers within cyber security and has thus freed up time for own product development within the vehicle industry. The project has also linked the automotive industry to academia and research institutes, which in turn have generated new projects. The complexity of the vehicle system increases over time and the requirement for cyber security will be tightened, which increases the need for knowledge exchange and national efforts to strengthen collaborations within vehicle cyber security. Next step will be to form a national arena for cyber security and discussions are ongoing to find a solution to this.

3 Bakgrund

Disseminering av forskningsresultat har tidigare inom detta område varit spretigt, dvs spritt på enskilda artiklar och ej väl organiserat, vilket har gjort det svårt att förstå den samlade kunskapsbasen. Vid den tid då Jeep Cherokee hackades (2015) inleddes FFI:s satsning inom området. Insikten om att fordon kunde hackas på distans ledde till ökade industriella satsningar och forskningsinsatser som resulterade i ett mer holistiskt perspektiv på säkerhetsutveckling, hotmodellering och arbetsprocesser. Idag är det väl känt att det förekommit många attacker mot fordon. Med en förståelse av att vi inte kan förutse alla möjliga sårbarheter har projekten börjat fokusera mer på motståndskraft, vilket innebär att ansträngningarna också ligger på att upptäcka intrångsförsök och säkra fordonets vidare funktion efter att ett intrång redan skett. Beräkningar pekar mot att runt 2030 kommer varje fordon innehålla cirka 300 miljoner programrader, vilket innebär att ett stort antal fel redan smugit sig in från början. På grund av detta och den ökade hastigheten i produktutvecklingen och de påtryckningar som orsakas av en ökad sårbarhet i fordons programvara måste kunskapen inom området öka snabbt. För att uppnå detta är både

utbildningsinsatser och strukturerad kunskapsöverföring av största vikt. Något som detta projekt bidragit till.

4 Syfte, forskningsfrågor och metod

Syftet med projektet har varit att sprida forskningsresultat på ett mer systematiskt sätt än tidigare. Arbetet organiserades i fyra olika arbetspaket där AP1 innefattade projektledning, AP2 omvärldsanalys och AP3 fysiska resultatsammankomster. AP3 inskränktes på grund av pandemin till enbart tre tillfällen. AP4 innebar digital informationsspridning, vilket innefattade både lunchseminarier och social media samt uppdaterad information på hemsidan. Projektet använde samma informationskanaler som utvecklades i Dex-projektet under åren före 2020. En heldagskonferens genomfördes även helt online.

5 Mål

Målen med projektet var att bidra till:

- Digital resultatspridning av resultat från Vinnovafinansierade forskningsprojekt i ämnet cybersäkerhet för fordonsindustrin. Detta har gjorts via sex stycken konferenser, AutoSec's hemsida, nyhetsbrev, Twitter och LinkedIn.

- Fysiska konferenser, forum och träffar för branschen för att utbyta resultat och kunskap från Vinnovas övriga pågående projekt. På grund av pandemin under 2020 och delar av 2021 har endast tre fysiska träffar organiserats. Resten har organiserats online.

- Uppföljning och sammanfattning av kommande och genomförda konferenser, resultatsammanfattningar och affärsinsikter. Flera av konferenserna har haft fokus på projektresultat från specifika Vinnovaprojekt.

AutoSec har bidragit med kunskapsutbyte i befintliga projekt. Projektet anordnade totalt sex olika seminarier och konferenser under tre år med deltagarantal mellan 30-75 personer. Kapaciteten i svensk fordonsindustri har stärkts genom att kommersiella aktörer har bjudits in för att tala vid flera konferenser och att konferenserna har inbjudit till samtal och nätverkande. Projektet har genomfört både lunchseminarier och heldagskonferenser. Nu under 2023 har även fler fordonsaktörer bjudits in till detta forum. Projektet har stärkt samarbetet mellan fordonsföretagen, underleverantörer, akademien, externa företag och forskningsinstitut. Projektet har även stärkt samarbetet med RISE interna satsning *Centrum för Cybersäkerhet*.

6 Resultat och måluppfyllelse

Genom att organisera och sammanföra forskare och produktutvecklare inom cybersäkerhet har projektet bidraget med att frigöra tid för företagens egen produktutveckling inom fordonsutveckling och andra åtaganden inom cybersäkerhetsområdet. Projektet har även knutit fordonsbranschen till både akademien och forskningsinstitut som i sin tur har genererat nya projekt för att lösa flera av de utmaningar branschen står inför. Då komplexiteten i fordonssystemen ökar över tid kommer även kraven på cybersäkerhet att skärpas. Detta kommer att öka behovet av ett organiserat och samordnat kunskapsutbyte samt nationella insatser som stärker samarbeten och därmed cybersäkerheten i framtidens fordon över lag. Projektet organiserade tre lunchseminarier och tre heldagskonferenser varav två var fysiska sammankomster. Projektet har även haft en egen hemsida och skrivit nyhetsbrev varannan vecka. Feedback från parterna ger vid handen att delar av innehållet i projektet hade varit möjliga att lyftas ut och ersättas av exempelvis fysiska träffar. Något vi tar med oss vid en eventuell fortsättning. Förslaget framgent är att skapa en nationell arena med fysiska möten och konferenser men utan formella krav på nyhetsbrev.

7 Spridning och publicering

7.1 Kunskaps- och resultatspridning

Hur har/planeras projektresultatet att användas och spridas?	Markera med X	Kommentar
Öka kunskapen inom området	x	Genom nätverkande och träffar
Föras vidare till andra avancerade tekniska utvecklingsprojekt		Inte projektet i sig utan associerade forskningsprojekt
Föras vidare till produktutvecklingsprojekt		Nej.
Introduceras på marknaden		Nej.
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		Nej.

7.2 Publikationer

Inga egna forskningsresultat har tagits fram i projektet.

8 Slutsatser och fortsatt forskning

Det finns som nämnts ett behov av att driva detta samarbete vidare i form av ett fortsättningsprojekt eller en nationell arena likt exempelvis CLOSERS *Urban Logistics Round Table*. En diskussion bör föras med Vinnova om innehåll, omfattning, drivningsansvarig, samt möjlig finansiering. Viljan finns från fordonsföretagen. Kontakten är nu sedan april tagen och diskussion pågår.

Den snabba elektrifiering som nu pågår i branschen inkl. utbyggnad av laddinfrastruktur gör att riskytorna för angrepp ökar. Transportsystemet som helhet blir mer sårbart när fordonen gör sig beroende av laddning på både privata och publika laddstationer och där ytterligare aktörer som laddoperatörer och andra tjänsteföretag levererar IT-lösningar inom detta kluster. Cybersäkerheten blir då ännu viktigare i systemet.

9 Deltagande parter och kontaktpersoner

Företag	**Kontaktperson**	**Mail**
RISE AB	Fredrik Cederstav	fredrik.cederstav@ri.se
Chalmers	Tomas Olovsson	tomas.olovsson@chalmers.se
Scania	Niklas Wiberg	niklas.wiberg@scania.com
AB Volvo	Christian Sandberg	christian.sandberg@volvo.com
Volvo Cars	Magnus Eek	magnus.eek@volvocars.com