CASUS

Publik rapport

Författare: Henrik Broberg
Datum: 2023-05-08
Projekt inom Fordons IT-säkerhet och Integritet

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

Innehållsförteckning

1 Sammanfattning

Målet med projektet var att förse projektledare med "särskild försäkran" att en produkt har tillräcklig cybersäkerhet för att kunna släppas till konsumenter. Projektet har undersökt vad en sådan ”särskild försäkran” behöver bestå av och hur den ska struktureras så att den lätt kan skapas, förstås och underhållas. En studie av det nuvarande forskningsläget har utförts för att förstå olika förhållningssätt till säkerhetsbevisning (”cybersecurity assurance cases") som redan fanns när projektet startade. Utöver detta genomfördes intervjuer vid företag för att förstå affärsintresset för ”cybersecurity assurance cases” för att komplettera produktperspektivet.

Studierna av det nuvarande forskningsläget samt utforskande testning av olika koncept ledde fram till en struktur för säkerhetsbevisning (”cybersecurity assurance cases") centrerad på skyddsvärda tillgångar. Tillämpning av strukturen i ett säkerhetsbevisning (”cybersecurity assurance cases") innebär argumentation för varje del av produkten, men också knyter ihop alla delar till en övergripande argumentation att fordonet är säkert på komplettfodonsnivå. Säkerhetsbevisning (”cybersecurity assurance cases") knyter även de bevis som behövs för att produkten är tillräckligt cybersäker för att släppas till marknaden. Dessutom kan säkerhetsbevisning (”cybersecurity assurance cases") användas för att planera det cybersäkerhetsarbete som krävs, underlättar säkerhet per design och dokumentation kan extraheras för typgodkännande med avseende på cybersäkerhet enligt R155*.

*UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

2 Executive summary in English

The aim with the project was to provide project managers with “specific assurance” that a product is cybersecure before releasing it. Therefore, this project has investigated what this “specific assurance” needs to contain and how it shall be structured so that it can easily be created, understood, and maintained. A state-of-the-art study was performed in order to understand which different approaches to assurance cases that already existed. Furthermore, interviews at a company were performed in order to understand the complete business interest for a cybersecurity assurance case, not only from a product release point-of-view.

Based on these findings and exploratory testing of different concepts, an asset centric structure of a cybersecurity case was developed. This structure has been the starting part for the implementation of a cybersecurity case at a company. The implemented cybersecurity case provides argumentation for each part of the product, but also connects everything to an overall argumentation that the complete vehicle is secure. The cybersecurity case also connects the evidence needed to claim that the complete product is sufficient cybersecure for release. Moreover, the cybersecurity case can be used to plan the cybersecurity work needed, to guide the design to build in cybersecurity from the beginning into the product, and documentation can be extracted from it to support Product CyberSecurity vehicle type approval for R155*.

*UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

3 Bakgrund

Från ungefär 2010 har medvetenhet hos tillverkare och myndigheter om risker mot individer och samhälle från cybersäkerhet i bilar ökat. Sedan 2015 har myndigheter i olika regioner börjat mer eller mindre formell certifiering av fordon med avseende på cybersäkerhet där till exempel EU

kräver uppfyllande av UNECE reg 155 krav med avseende på cybersäkerhet för att få typgodkännande av fordon.

Under de senaste 20 åren har tekniker för säkerhetsbevisning (”security assurance”) utvecklas mycket. Flera approacher har mognat för varje del av utvecklingscykeln:

- Upprätta säkerhetskrav (KAOS, Secure i-star, secure problem frames)
- Definiera säkerhetsarkitektur (UMLsec, Secure SysML, security patterns, security design principles)
- Implementera ett säkert system (säkerhets bibliotek, ramverk)
- Analys av system (fuzz test, statisk kodanalys)
- Övervakning av system i fält (system för intrångsdetektering)

För att kunna dra nytta av teknikerna ovan behöver även organisationen en strukturerad approach för säker utveckling av produkter och tjänster. Flera processer finns för säker utveckling (som Microsoft SDL och CLASP från OWASP) och modeller för att mäta mognadsgrad (som BSIMM).

En syntes av process aktiviteter och tekniker kan ge en organisation stöd med generisk argumentation för viktiga åtgärder i projekt. Effektivitet är en nödvändighet för effektiv kommunikation internt och extern där i slutändan typgodkännande av produkter och tjänster, d.v.s. själva verksamheten är på spel.

4 Syfte, forskningsfrågor och metod

CASUS syftar till att gynna fordonsindustrin på följande sätt:

- Öka effektivitet för ”assurance aktiviteter”
- Reducera ledtider, från osäkerhet, i beslutsprocessen genom bättre systematik
- Minska risken för krav på rättsligt ansvar från incidenter

Den främsta forskningsfrågan för detta projekt är hur en projektledare kan få ”specifik assurans” att en produkt eller tjänst är tillräckligt säker för att kunna släppas till konsumentmarknaden.

Forskningsfrågan har adresserats genom att utveckla en metod för säkerhetsbevisning (”cybersecurity assurance cases”). Focus är fordonsindustrin och tar stor inspiration from ”safety cases” som används i stor utsträckning för att argumentera för ”skälig försiktighet” där standarden ISO 26262 vanligen tillämpas inom fordonsindustrin.

Detta projekt har adresserat följande frågeställningar:

- Vilka bevis behöver samlas in under utvecklingsprocessen (till exempel: metrik för kod och design, testresultat, spårbarhet)
- Hur byggs argumentation från de tillgängliga bevisen.

Metoden har varit från att först kartlägga de behov som finns i industrin och de metoder som finns beskrivna i litteraturen för att uppfylla behoven. Detta har lett fram till en utveckling av generell metod för argumentation för tjänster och produkters säkerhet. Den generell metoden består av återanvändbara augment och argumentens logiska uppbyggnad, hur insamling av bevis för argument går till samt hur man uppfyller standarder.
Validering av den generella metoden har gjorts genom fallstudie i vagnsprojekt.

5 Mål

Det övergripande målet för projektet är att tillhandahålla metoder och verktyg för bedömning av släppta produkters uppfyllnad av cybersäkerhetsmål till fordonsindustrin. Den centrala frågeställningen är: Hur kan en projektledare få specifikt bekräftat att en färdigutvecklad produkt är tillräckligt säker och kan släppas till produktion? I praktiken fokuserar vi på två aspekter: (1) vilka bevis behöver samlas ihop under mjukvarans utvecklingsprocess och (2) hur bygger man upp argumentation för försäkran om tillräcklig cybersäkerhet utifrån de tillgängliga bevisen.

Kvantitativt så var målet att gå höja den tekniska mognadsgraden från ”demonstrera genomförbarhet” till ”applikation i riktig miljö”.

Mognadsgrad är fritt översatt av ”technology readyness level” (TRL) och att öka mognadsgraden från TRL 3 till TRL 5, för specifika definitioner av begreppen se vidare https://www.nasa.gov/directorates/heo/scan/engineering/technology/technology_readiness_level

6 Resultat och måluppfyllelse

Det främsta bidraget till industrin är en metod för uppbyggandet av så kallade säkerhetsbevisning (”cybersecurity assurance cases”) som är en metod för försäkran om tillräcklig cybersäkerhet hos ett system. Metod ska hjälpa till med formuleringen av argumentation och dess struktur, som innebär exempelvis hur man bäst bryter ned säkerhetsteser till under-teser på ett sätt som är välgrundat och komplett. För att uppnå detta har ett bibliotek av typiska mönster för nedbrytning av teser tagits fram. Dessutom ska nödvändiga bevis för att bestyrka teserna samlas in från ett antal olika artefakter.

Målet har varit att öka mognadsgraden från att visa att det är genförbart att göra en säkerhetsbevisning (”cybersecurity assurance case”) till att kunna tillämpning i den tilltänkta miljön, dvs för riktiga fordonsprojekt och har därmed uppnått den tilltänkta mognadsgraden (TRL5). Detta har delvis uppnåtts då AB Volvo har gjort en första implementation av en säkerhetsbevisning (”cybersecurity assurance case”) baserat på resultaten från CASUS och med hjälp av verktyget NorSTA. Strukturen har ändrats under arbetet med att implementera strukturen så ett iterativt arbetssätt har använts. Utmaningen har bestått i vilka ”bevis” som behövs för att stödja argumentationen för typgodkännande mot de nya legala kraven i R155 som saknar en vedertagen tolkning. Det ursprungliga målet att skriva en rapport baserad på verktyget har inte kunnat uppnås då det iterativa arbetssättet inte stabiliserats tillräckligt för att motivera tiden för en rapport som skulle behövas ändras inom några veckor.

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	Dissemination genom publikationer samt regionalt nätverk
Föras vidare till andra avancerade tekniska utvecklingsprojekt	X	Fortsatt akademisk forskning
Föras vidare till produktutvecklingsprojekt	X	Produktionsprojekt redan i processen att certifieras.
Introduceras på marknaden	X	Se ovan
Användas i utredningar/regelverk/ tillståndsärenden/ politiska beslut		Syftet med projektet är att svara på regelverk, inte påverka dem

7.2 Publikationer

Projektrapporter:

- D1.1 Industrial survey
- D1.2 Systematic literature review
- D2.1 Methodology to construct a security case
- D2.2 Definition of KPIs and evidence collection methods
- D2.3 Standards compliancy analysis*
- D3.1 & D3.2 Prototype tool & Validation experience report

De två sista rapporterna var planerade som separata levarabler, men har slagits samman på grund av att förutsättningar har ändrats sedan planen gjordes och nya verktyg har dykt upp. Organisationer har rört sig mot inköp av verktyg istället för egenutveckling. Rapporten har lagts på is och resurserna har lagts på att använda verktyget NorSTA. Orsaken har berörts i avsnittet resultat och måluppfyllelse och är i korthet att förutsättningarna inte anses stabila.

* omfattningen reducerades till endast en standard (ISO/SAE-21434) jämfört med flera i ursprungsplanen .

Vetenskapliga artiklar som en direkt följd av projektet:

- Mazen Mohamad, Jan-Philipp Steghöfer, Riccardo Scandariato, Security Assurance Cases State of the Art of an Emerging Approach, Empirical Software Engineering, To appear
- Mazen Mohamad, Örjan Askerdal, Rodi Jolak, Jan-Philipp Steghöfer, Riccardo Scandariato, Asset driven Security Assurance Cases with Built-in Quality Assurance, International Workshop on Engineering and Cybersecurity of Critical Systems (ENCYCRIS), 2021
- Mazen Mohamad, Alexander Åström, Örjan Askerdal, Jörgen Borg, Riccardo Scandariato, Security Assurance Cases for Road Vehicles: an Industry Perspective, International Conference on Availability, Reliability and Security (ARES), 2020 2)
- Mazen Mohamad has successfully achieved his Lic: Mazen Mohamad, Towards Understanding and Applying Security Assurance, May 2021 3) The following paper is

currently under review: Mazen Mohamad, Rodi Jolak, Örjan Askerdal, Jan-Philipp Steghöfer, Riccardo Scandariato, CASCADE: An Asset-driven Approach to Build Security Assurance Cases for Automotive Systems, Transactions on Cyber-Physical Systems, 2021

8 Slutsatser och fortsatt forskning

Det återstår flera frågor med akademisk höjd där fortsatt forskning pågår i värden och av projektdeltagare. En slutsats är att mycket av projektresultaten är redo för industriell tillämpning, men att en sådan tillämning inte är enkel då behovet av formell redovisning redan är ett faktum för flera intressenter. Vedertagen tolkning av myndighetskrav har varit en utmaning i detta projekt.

9 Deltagande parter och kontaktpersoner

AB Volvo, Askerdal Örjan
Göteborgs Universitet, Mazen Mohamad
Volvo Cars, Henrik Broberg