Hotanalys för positionsangivelsekedjan

Martin Boldt, Blekinge Tekniska högskola
Bengt Carlsson, Blekinge Tekniska Högskola

arena

ARENA REPORT 2008:7 2008-02-29

The ARENA project

ARENA is a national project that aims to build competence for a future introduction of a road user charging system for Heavy Goods Vehicles (HGVs) in Sweden. The project has been developed in accordance with EU Directives and the Swedish public authority plans to introduce a kilometre tax for HGVs. ARENA started in 2006 and is financed by the Swedish Road Administration and the Swedish Governmental Agency for Innovation Systems. NetPort.Karlshamn is the project coordinator.

The approach of ARENA is to take a wide view and not only focus on technology. Innovation potential, consequences and possibilities related to an implementation of road user charging is also important as well as respecting that different stakeholders have different needs and requirements. This requires interaction between relevant stakeholders at an early stage. The role of the ARENA project includes the following elements:

- acting as broker both between groups of stakeholders who normally do not meet and between competitors within the same group
- develop and support knowledge both within the project but also as a coordinator between other projects

A concept for a kilometre tax system in Sweden is developed with a functional approach, which does not prescribe any technical solutions. The concept is generic rather than specific, in the sense that it should be possible to implement the result in several ways. Hence, we are trying to define the system independently from its final technical design. The motivation for this is that the time horizon for realisation is far ahead, maybe 3-6 years, and we can expect considerably changes in technical preconditions over this period. The concept includes a number of characteristics that differs from existing systems, which will reduce cost, promote innovative solutions and enable European interoperability.

The work of ARENA will continue in ARENA 2.0, where the concept will be further developed in close cooperation with the industry and relevant authorities and administrations. A full-scale demonstration will be developed for the ITS World Congress in Stockholm 2009.

Swedish Road Administration

The Swedish Road Administration (SRA) is the national authority assigned the overall responsibility for the entire road transport system in Sweden. SRAs task is to co-operate with others to develop an efficient road transport network in the direction stipulated by the Swedish Government and Parliament. SRA has been commissioned to create a safe, environmentally sound and gender-equal road transport system that contributed to regional development and offers individuals and the business community easy accessibility and high transport quality.

VINNOVA

VINNOVA (Swedish Governmental Agency for Innovation Systems) is a State authority that aims to promote growth and prosperity throughout Sweden. VINNOVAs particular area of responsibility comprises innovations linked to research and development. The tasks are to fund the needs-driven research required by a competitive business and industrial sector, and to strengthen the networks that are such a necessary part of this work.

Innehåll

Inledning

ARENA projektet syftar (i korthet) till att utveckla en möjlig lösning för ett svenskt system för kilometerskatt. Utvecklingen sker i flera steg, där det första steget innebär att utveckla ett koncept till en lösning. En viktig del under utvecklingen av detta koncept är hur tillförlitligheten i den tekniska lösningen skall kunna garanteras. För att analysera detta så har en hotanalys genomförts med uppgift att identifiera vilka *hot* som finns mot den tekniska lösningen. Dessa hot har sedan transformerats till *risker* för att kunna motivera motmedel mot de risker som värderas som tillräckligt allvarliga för att adresseras.

Detta dokument beskriver denna hotanalys med en avgränsning till de delar som har med positionsangivelsekedjan att göra, d.v.s. allt från OBU (on-board unit), kommunikationskanal, till vissa delar av de centrala resurserna. Då hotanalyser baseras i stor utsträckning på uppskattningar varför ingen sådan dokumentation blir komplett. Med detta i åtanke ska alltså detta dokument ses som ett levande dokument som kontinuerligt uppdateras baserat på t.ex. nyuppkomna hot eller ändrade egenskaper för de redan existerande.

Som underlag till hotanalysen så har följande dokument använts:

- ”A New Approach to Control in the ARENA Concept for HGV Kilometre Tax in Sweden” (version 0.9)
- ”Proposal for System Design” (version 0.93)
- Thomas Peltiers, ”Information Security Risk Analysis”
- Predrag Mitrovic ”Handbok i IT-säkerhet, 4:e upplagan

Definitioner

DoS-attack	”Denial of Service”-attack, samma som överbelastningsattack
Hot	En beskrivning av en obehaglig/oönskad händelse[1].
Komm-länk	Kommunikationslänk som används för att kommunicera mellan OBU och central server (GPRS/GSM)
OBU	On-board unit eller ombordenhet, d.v.s. den elektronik som finns på en lastbil och som förmedlar fordonets position till vägskattesystemet.
Risk	Sannolikheten att ett hot inträffar[1].
Checksumma	Ett kontrolltal eller kontrollsumma som kan användas för att säkerställa att en datamängd är korrekt alternativt att den ej har modifierats sedan senaste gången checksumman beräknades.
Disassembler	Ett program som används för att transformera de instruktioner som en datorprocessor tolkar till assembly-instruktioner som är enklare för människor att tolka. Disassemblers används ofta för att analysera datorprogram med syfta att t.ex. knacka ev. kopieringsskydd.
Decompiler	Motsatsen till en kompilator som kan kompilera källkod skriven i ett visst programmeringsspråk till ett körbart program. En decompiler kan alltså återskapa källkoden från ett körbart program. Fungerar dock inte på alla programmeringsspråk.
Obfuskeringsteknik	Teknik som används för att försvåra analys av mjukvara (t.ex. m.h.a. en disassembler eller decompiler).

[1] Thomas R. Peltier, ”Information Security Risk Analysis”, CRC Press LLC, Boca Raton, USA, 2001.

Bakgrund

När positionsavgivelsekedjan ska göras säker (både driftmässigt och mot intrång) samt skyddas mot läckage av känsliga uppgifter måste tre grundförutsättningar uppfyllas. Systemet måste vara konfidentiellt, uppfylla integritetskrav och vara tillgängligt.

Att ett system är konfidentiellt betyder att informationen bara ska vara tillgänglig för behöriga användare, dvs det behövs någon form av verifiering av de användare som brukar systemet. Integritet innebär att information enbart får förändras på ett godkänt sätt, användaren måste vara säker på att de uppgifter som matas in också är de uppgifter som når fram till mottagaren. Slutligen måste systemet vara tillgängligt, dvs. tjänsten får inte vara oåtkomlig för behöriga användare. Dålig tillgänglighet kan bero både på driftsstörningar och på sabotage.

All information har värde, några tjänar på att system attackeras. Det är därför viktigt att vara någorlunda förberedd på vad som kan inträffa. I positionsavgivelsekedjan kan syftet vara att undvika debitering av kilometerskatt eller att komma över information som kan säljas till en konkurrent. Förutom de direkta ekonomiska konsekvenserna (staten förlorar inkomster) kan detta vara förödande för de enskilda åkerierna genom att konkurrenterna kan erbjuda billigare kontrakt eller kartlägga åkeriets körningar.

Ett sätt är att skåda framåt i tiden är genom att göra en säkerhetsanalys vilket i sin tur förhoppningsvis leder till säkra betalningsflöden och ökad acceptans för systemet. Vilken acceptans ett nytt system får beror på hur omgivningen ser ut, är det så att andra aktörer fuskar eller spionerar minskar tilltron. Dessutom kan det uppstå interna hot när ny teknik läggs till den redan befintliga. Brukarna måste uppleva systemet som rättvist, annars blir det svårt att få acceptans för genomförande av kilometerskatt. Systemet måste gå att lita på, därför är det viktigt att information skyddas från otillbörligt utnyttjande.

Andra viktiga säkerhetsparametrar att ta hänsyn till är flexibilitet och modifierbarhet. Det är förmodligen naivt att anta att ett system är färdigutvecklat vid driftstart. Till skillnad mot driftsmiljön, där man i förväg kan bestämma vad som ska ingå, går det inte att förutse vad en illvillig aktör kan hitta på. Det finns åtskilliga exempel att lära av (se tex. Shapiro och Varian 1999[2] om hur dekoderkort till satellitmottagare manipuleras resp. skyddas). Ett nytt system kommer att utsättas för angrepp som kräver modifiering av tekniken, därför måste en flexibilitet byggas in i förväg. Om då dessutom systemen konstrueras så enkelt som möjligt går det bättre att överblicka säkerheten.

[2] C. Shapiro, and H. R. Varian, Information Rules: A Strategic Guide to the Network Economy, Harvard Business School Press 1999.

Arbetsmetod

Vi har använt oss av en mycket vanlig metod, som bl.a. beskrivs i Peltiers bok Information Security Risk Analysis, för att identifiera vilka hot som finns mot postionsavgivelsekedjan. Metoden består av fem sekventiella steg som med fördel kan itereras för att erhålla en uppdaterat överblick över vilka hot som finns mot systemet.

Första steget innebär att *tillgångarna* i systemet identifieras. Alltså *vad* som behöver skyddas i systemet. Sådana tillgångar kan vara både fysiska entiteter så som OBU:ns säkra kärna till mer imaginära entiteter så som radiosignaler i etern. I det andra steget så kartläggs vilka hot som finns mot det tidigare identifierade tillgångarna genom en typ av *brainstorming*. I det tredje steget så skattas *sannolikhets-* och *konsekvensvärden* för respektive hot. I det fjärde steget så beräknas ett *riskvärde* för varje hot genom att multiplicera hotens konsekvens och sannolikhet. Baserat på detta riskvärde så prioriteras sedan hoten efter dess riskvärden. Detta får till följd att hot med låga riskvärde filtreras bort som antingen allt för osannolika alternativt som försumbara. I det sista steget så mappas motåtgärder mot de återstående hoten. Dessutom görs en skattning samt prioritering baserat på kostnaden hos dessa motåtgärder.

Arbetsgången ser alltså ut som följer:

1. Identifiera tillgångarna (det som ska skyddas)
2. Kartlägg hoten mot dessa tillgångar
3. Skatta sannolikhet samt konsekvens för varje hot
4. Beräkna riskvärde samt prioritera efter dessa
5. Identifiera lämpliga motåtgärder samt prioritera efter dess kostnad

I de nästkommande sektionerna i detta dokument så kommer våra resultat från vart och ett av ovanstående steg att förklaras närmare.

Identifiera tillgångar i systemet

Då vi studerat vilka komponenter som används då en position tas emot av ombordenheten samt då denna kommunicerar med centrala servrar så har vi hittat fyra stycken huvudgrupper av *tillgångar*. Dessa grupper baseras på var de hör hemma i systemet. De fyra grupperna består av *ombordenhet*, *kommunikationslänk*, *data* samt *centrala servrar*. Det är alltså endast systemdelar som är inblandade i positionsavgivelsekedjan som behandlas i denna hotanalys. Exakt vilka tillgångar som respektive grupp innehåller förklaras nedan.

OBU:n består av följande delar som har anammats då hotanalysen genomförts:

- Hårdvara, komponenter och kretskort som tillsammans utgör OBU:n
- Mjukvara, de datorprogram som körs på hårdvaran för att OBU: ska lösa sin uppgift
- Kommunikationsantenn, antennen som an änds för att kommunicera med servrarna
- GPS-antenn, den antenn som används för att ta emot GPS-signalerna
- Strömförsörjning, den elektronik som förser OBU:n med strömförsörjning
- Kablage, eventuella kablar som förbinder OBU:n med t.ex. GPS-antenn

Kommunikationslänken består av möjligheten att skicka data i etern samt tillgång till någon typ av mobilt kommunikationssystem så som GPRS eller GSM.

Den data som vi funnit vara tillgångar består av:

- Identifikationsdata, någon typ av identifierare för antingen en viss förare eller ett visst fordon
- Positionsdata, data som beskriver positionen för en viss OBU
- Tidsstämplar, som kopplar samman en händelse för ett visst fordon till en tidpunkt
- Kryptonycklar, de nycklar som används för att kunna kommunicera med servern över en krypterad linje

Följande tillgångar kopplade till den centrala servern har identifierats:

- Systemintegritet, att systemets integritet är överensstämmer med ett accepterat tillstånd som garanterar beräkningskorrekthet
- Databas, databasen innehållandes känslig data så som positionsavgivelser och identifikationsdata

Kartläggning av hoten

När tillgångarna väl identifierats i positionsavgivelsekedjan så kartlades vilka *hot* som fanns mot dessa tillgångar. Hoten delades upp i tre olika subgrupper baserat på ifall de var *fysiska*, *logiska* eller *mänskliga*[3]. De fysiska hoten består av sådant som fysiskt påverkar systemet eller dess komponenter, t.ex. stöld eller hårdvarufel. De logiska hoten är sådana som inte fokuserar på fysiska komponenter utan istället logiska rutiner eller mjukvara, t.ex. överbelastningsattacker eller buggar i mjukvaran. Den tredje gruppen hanterar hot som fokuserar på problem relaterat till människor. Härnäst kommer hoten i de tre olika grupperna att beskrivas.

Fysiska hot

F1) Stöld av OBU

Detta hot inkluderar alla former av stöld av OBU eller dess kringutrustning. Detta kan förekomma överallt från den plats de tillverkas på, där de installeras i fordonen men framför allt när OBU:n väl sitter i ett fordon genom inbrott. En hypotes är att just inbrott i fordonen kan bli vanligare ifall OBU:n innehåller kommersiellt tillgängliga standardkomponenter, t.ex. GPS-mottagare eftersom dessa kan anses vara stöldbegärliga.

F2) Förare saboterar OBU

Detta hot inkluderar alla typer av sabotage som föraren själv kan åsamka OBU:n eller dess kringutrustning för att denna ska sluta fungera. Dessa sabotage kan göras så att de ska efterlikna hot F6 för att slippa undan vägskatt.

F3) Extern aktör saboterar OBU

Alla typer av sabotage som åsamkas OBU:n av en extern aktör (alltså inte fordonsförare eller anställd på speditionsfirman). Ett exempel skulle t.ex. kunna vara att en extern antenn saboteras så att OBU:n inte kan kommunicera.

F4) Förare gör OBU strömlös

Detta hot inriktar sig på att föraren i fordonet gör så att OBU:n blir strömlös genom att bryta kontakten till strömförsörjningen. På så vis slutar OBU:n fungera och registrerar därmed inte färdvägen. Ifall föraren stoppas i en kontroll så kan denne hävda att det hela är ett fabrikationsfel/installationsfel.

F5) Extern aktör gör OBU strömlös

Dettta hot är samma som F4 men med undantaget att det är en extern aktör kopplar ur strömförsörjningen till OBU:n istället för föraren.

F6) OBU går sönder

Detta hot innefattar alla scenarios där OBU:n slutar fungera p.g.a. någon form av fabrikationsfel. Ingen har alltså aktivt försökt få OBU:n att haverera (se t.ex. F2). Här står alltså fordonsägaren utan ansvar men denne måste på något sätt ändå notifieras om att ett fel uppstått och att servicetekniker måste tillkallas.

[3] [3] Predrag Mitrovi´c, ”Handbok i IT-säkerhet, 4:e upplagan”, Pagina Förlag, Sundbyberg, 2005.

F7) Felaktig GSM/GPS-antenn
Sannolikheten att fabrikationsfel ska inträffa på några av antennerna kan anses vara ganska hög. Detta hot innebär att föraren inte gjort något för att OBU:n ska sluta fungera (p.g.a. kommunikationsproblem) och därför måste meddelas om att kommunikationen är ur funktion.

F8) Sabotage av enskild GPS/GSM-antenn
Detta hot kan liknas vid F7 men med det undantag att någon medvetet har saboterat antennen så att denna slutar fungera.

F9) Sabotage av flera GPS/GSM-antenner
Samma som F8 men i detta fall har sabotagen av GPS-antennerna spritt sig så att det inte drabbar bara enskilda antenner utan istället en större mängd sett ur ett systemperspektiv.

F10) Hårdvarufel i OBU
Detta hot innebär att OBU:n hårdvara sporadiskt eller helt slutar fungera korrekt p.g.a. av dess hårdvara innehåller fel. Det ligger alltså inte någon manipulering eller sabotage bakom.

F11) Kommunikationssystemet ur funktion
Detta hot innebär att kommunikationssystemet (t.ex. GSM-systemet för telefoni) går ner exempelvis på grund av ett stort och långvarigt strömavbrott. Kommunikationsutrustningen i fordonet fungerar alltså som den ska men eftersom den inte har något kommunikationsmedium till förfogande så kan den inte kommunicera med de centrala enheterna.

F12) Intern manipulering av data mellan komponenter på enskild OBU
Detta hot innebär att den data som skickas mellan komponenter internt på en enskild OBU manipuleras, t.ex. mellen GSM/GPRS-modulen och säkra kärnan. För att göra en sådan sak krävs avancerade tekniska kunskaper.

F13) Intern manipulering av data mellan komponenter på flera OBU:er
Även om det krävs så pass avancerade kunskaper att endast ett ytterst begränsat antal personer kan anses något sådant. men kan å andra sidan ofta automatiseras och replikeras så snart en enda person lyckas med manipuleringen. Detta betyder att det räcker att ett fåtal tekniskt kunniga personer hittar en väg runt skyddet för att en ”produkt” ska kunna distribueras till samtliga användare av systemet.

F14) Störning av data mellan OBU och GSM/GPRS-modul
Detta hot innebär att datan mellan OBU och GPS/GPRS-modulen störs ut i kablen som förbinder dessa komponenter. Resultatet blir att komm-länken bryts varvid OBU:n ej kan kommunicera med de centrala servrarna.

F15) Naturkatastrofer
Naturkatastrofer så som jordbävningar, översvämmningar, stormar och dyligt.

Logiska hot

L1) Felaktig mjukvara i OBU

Eftersom OBU:erna kommer att innehålla mjukvara så innebär felaktig mjukvara ett hot. P.g.a komplexiteten i den mjukvara som styr OBU:ernas funktionalitet så kan inte risken för fel/buggar i denna ej uteslutas.

L2) Sårbar mjukvara i OBU

På samma sätt som resonemanget för felaktig mjukvara i OBU:n förs (se L1) så kan man även anta att sådana mjukvarubuggar kan vara en säkerhetsrisk som gör OBU:n sårbar som attacker.

L3) Illasinnad programvara i OBU

Baserat på risken för sårbarheter i OBU:ns mjukvara (L2) så kan inte risken för att illasinnad programvara ska ta sig in i OBU:n uteslutas. Sådan illasinnad mjukvara skulle t.ex. kunna innebära exekvering av godtycklig mjukvara som i sin tur spionerar på fordonets position eller genomför överbelastningsattacker som OBU:ns hårdvara.

L4) Ingen tillgänglig komm-länk

Att fordonet befinner sig i ett område där det ej finns täckning för kommunikation är något som garanterat kommer att inträffa då rutter i glesbefolkade områden körs. Konsekvensen blir att OBU:n inte kan kommunicera med de centrala servrarna.

L5 Störning av komm-länk

Då OBU:n är beroende att att vid jämna mellanrum kunna kommunicera med de centrala servrarna så får alla typer av sörning av denna kommunikation allvarliga konsekvenser. Detta hot innebär att någon stör ut kommunikationen t.ex. genom att använda en störsändare som stör signalerna i etern.

L6) Avlyssning av komm-länk

Eftersom all kommunikation till och från OBU:n sker trådlöst så är kommunikationen tillgänglig för avlyssning i etern. Incitament för sådan avlyssning kan vara att få kännedom om positions och identifikationsdata för fordon i närområdet.

L7) Modifiering av data över komm-länk,som drabbar flera åkare

Då all kommunikation till/från OBU:n sker trådlöst så innebär detta även att trafik kan fabriceras och skickas så att den ser ut att komma från någon annan. Detta innebär att en attackerare kan utge sig för att vara någon annan i sin kommunikation.

L8) Fabricering av data över komm-länk som drabbar flera åkare

Samma resonemang som används i L7 innebär också att trafik kan fabriceras över komm-länken så att den ser ut att komma från någon annan. Detta innebär att en attackerare kan utge sig för att vara någon annan i sin kommunikation. Ett exempel skulle vara att en etern aktör utger sig för att vara den centrala servern i jakt på positions-/identifikationsdata.

L9) DoS-attack mot komm-länk drabbar flera åkare

Ifall trafik kan fabriseras (se L8) så innebär detta även att DoS-attacker kan utföras, t.ex. mot de centrala servrarna. Ett scenario är då en attackerare simulerar flera olika OBU:er för att

genomföra en stor mängd uppkopplingar mot servrarna så att dess resursersanvändning skjuter i höjden så att legitim användning ej längre är möjlig.

L10) Central server onåbar
Konsekvensen blir samma som för L9 men i det här fallet finns det inget illasinnat uppsåt bakom förlusten av serverns funktionalitet. Ett exempel skulle t.ex. vara att servern ”går ner” på grund av någon typ av hårdvaru- eller mjukvarufel.

L11) Obehörigt tillträde till central server och data
Detta hot innebär att personer som ej borde ha tillträde till vissa funktioner eller viss data på de centrala servrarna ändå får det. Orsaken skulle kunna vara felkonfigurerade säkerhetsmekanismer eller fel/buggar i dessa.

L12) Fallbacklösning onåbar p.g.a. driftsfel
Detta hot innebär att fallbacklösningen, som ska vara tillgänglig då det normala systemets funktionalitet störs, även den slutar fungera p.g.a. driftsfel. Om denna fallbacklösning är telefonbaserad (exempelvis ett call-center) så skulle ett sådant driftsfel kunna vara ett illa tajmat fel eller överbelastning i televäxeln.

L13) Fallbacklösning onåbar p.g.a. sabotage
Konsekvensen av detta hot liknar till viss del L12 men en stor skillnad är att det i detta fall finns en eller flera aktörer som aktivt jobbar för att sabotera fallbacklösningen. Denna skillnad innebär att man inte alltid kan vidta några motåtgärder för att få systemen funktionsdugliga igen, t.ex. då en storskalig DoS-attack drabbar de centrala servrarna.

Mänskliga hot

M1) Felaktig funktionalitet av OBU p.g.a. handhavandefel
Detta hot innebär att OBU:n används på ett felaktigt sätt p.g.a. handhavandefel från fordonsföraren. Detta skulle t.ex. kunna innebära felaktig inmatning av data till OBU:n för hur många hjulaxlar fordonet för tillfället har.

M2) OBU slutar fungera p.g.a. handhavandefel
Detta hot innebär att funktionaliteten hos OBU:n helt upphör p.g.a. handhavandefel från fordonsägaren. Exempelvis genom att denne ej ansluter strömförsörjningen på ett tillfredställande sätt så att kontakten senare bryts och OBU:n blir utan strömförsörjning.

M3) Läckage av data från central server
Hotet att obehöriga kommer över data från de centrala servrarna kan även klassas som mänskliga. Ett exempel är ifall de som administrerar eller jobbar med dessa servrar luras m.h.a. ”social engineering” att lämna ut känslig information. Detta hot skulle även kunna innefatta olika scenarios där anställda mutas för att lämna ut känslig information.

M4) Felaktig behörighet på central server
Detta hot innebär att anställda som jobbar med information i de centrala servrarna har högre rättigheter än de egentligen behöver. Detta betyder att de kan komma åt delar i systemen som de egentligen inte behöver för att sköta sina arbetsuppgifter. Dessa allt för höga rättigheter kan användas för att t.ex. komma åt känslig information som egentligen inte skulle kunna nås.

Sannolikhet och konsekvens för hoten

När hoten mot tillgångarna kartlagts så togs värden fram för *sannolikhet* och *konsekvens* kopplat till respektive hot. Detta gjordes under en workshop där både BTH, Sweco och Netport var representerade. Sannolikheten för att ett visst hot realiseras uppskattades då till ett värde på en femgradig skala där 1 är lägst och 5 är högst sannolikhet för att någon del av systemet någon gång ska drabbas. Vi använde oss av följande femgradiga sannolikhetsstege för dessa sannolikhetsvärden:

1) Ytterst osannolikt, t.ex. naturkatastrof så som större jordbävning
2) Kan inte helt uteslutas, t.ex. stort strömavbrott
3) Kommer sannolikt att inträffa
4) Kommer med stor sannolikhet att inträffa
5) Kommer säkert att inträffa, t.ex. att OBU slutar fungera p.g.a. fel

Vidare beskriver konsekvensvärdena hur stor negativ påverkan ett hot får ifall det verkligen realiseras. Även konsekvensen uppskattas på en femgradig skala där 1 ska tolkas som en försumbar konsekvens och 5 som en katastrofal konsekvens. Vi använde oss av följande motiveringar då vi satte konsekvensvärdena:

1) Driftsfel som drabbar enskild åkare
2) Handhavandefel eller sabotage som drabbar enskild åkare
3) Driftsfel som drabbar flera åkare
4) Handhavandefel eller sabotage som drabbar flera åkare
5) Storskaligt driftsstörning eller sabotage

Baserat på de uppskattade värdena för sannolikhet och konsekvens så beräknades därefter ett *riskvärde* för varje hot genom att multiplicera sannolikheten och konsekvensen. I nästa arbetsmoment så prioriteras de olika hoten efter just dessa riskvärden.

Fysiska hot

Id	Hot	Sanno-likhet	Konse-kvens	Risk-värde
F1	Stöld av OBU	4	2	8
F2	Förare saboterar OBU	3	2	6
F3	Extern aktör saboterar OBU	2	2	4
F4	Förare gör OBU strömlös	5	2	10
F5	Extern aktör gör OBU strömlös	2	2	4
F6	OBU går sönder	5	1	5
F7	Felaktig GPS-antenn	5	1	5
F8	Sabotage av enskild GPS-antenn	3	2	6
F9	Sabotage av flera GPS-antenner	2	4	8
F10	Hårdvarufel i OBU	2	1	2
F11	Kommunikationssystemet ur funktion	2	3	6
F12	Intern manipulering av data mellan komponenter på enskild OBU	4	2	8
F13	Intern manipulering av data mellan komponenter på flera OBU:er	3	4	12
F14	Störning av data mellan OBU och GSM/GPRS-modul	4	2	8

F15	Naturkatastrofer	1	5	5

Logiska hot

Id	Hot	Sanno-likhet	Konse-kvens	Risk-värde
L1	Felaktig mjukvara i OBU	4	3	12
L2	Sårbar mjukvara i OBU	2	4	8
L3	Illasinnad programvara i OBU	2	5	10
L4	Ingen tillgänglig komm-länk	4	3	12
L5	Störning av komm-länk	2	4	8
L6	Avlyssning av komm-länk	3	4	12
L7	Modifiering av data över komm-länk, drabbar flera åkare	2	4	8
L8	Fabricering av data över komm-länk, drabbar flera åkare	2	4	8
L9	DoS-attack mot komm-länk, drabbar flera åkare	2	5	10
L10	Central server onåbar	3	5	15
L11	Obehörigt tillträde till central server och data	2	4	8
L12	Fallbacklösning onåbar p.g.a. driftsfel	3	3	9
L13	Fallbacklösning onåbar p.g.a. sabotage	2	5	10

Mänskliga hot

Id	Hot	Sanno-likhet	Konse-kvens	Risk-värde
M1	Felaktig funktionalitet av OBU p.g.a. handhavandefel	5	2	10
M2	OBU slutar fungera p.g.a. handhavandefel	4	2	8
M3	Läckage av data från central server	2	5	10
M4	Felaktig behörighet på central server	2	4	8
M5	Användaren ”glömmer” OBUn	5	2	10
M6	”Chinese wall” problematik	4	2	8
M7	Avg. mottagaren lämnar oriktiga uppgifter	2	5	10

Riskprioritering baserat på riskvärdena

Baserat på riskvärdena så kan de minst sannolika och minst kritiska hoten filtreras bort så att de verkligt allvarliga kan tillägnas mer resurser. Vi har valt att applicera ett filter som skalar bort alla hot som har ett riskvärde lägre än 8. Detta betyder att alla hot som har ett riskvärde på 8 eller högre adresseras genom motåtgärder, medan övriga hot accepteras och därför inte kräver någon motåtgärd.

Att en gräns vid just 8 appliceras beror på att vi ville filtrera bort samtliga hot som hade antingen ett sannolikhetsvärde *eller* konsekvensvärde satt till 1. Däremot ville vi inkludera alla riskvärde som är resultatet av ett sannolikhetsvärde samt konsekvensvärde satt till medel (dvs 3 på den femgradiga skalan) eller högre. Dessutom ville vi garantera att alla hot med ett sannolikhetsvärde eller ett konsekvensvärde satt till ett värde över medel (dvs 4 eller 5) inkluderas i den vidare analysen. Givet dessa förutsättningar så var den enda kandidaten just 8.

För att förstå den gjorda prioritetsordningen bör man se problematiken ur både åkarens och myndighetens synvinkel. För åkaren gäller att om andra fuskar så försämras dennes konkurrensvillkor och om spionage förekommer blir affärsutvecklingen sämre. Dessutom kan inte åkaren bortse ifrån att den egna personalen medvetet eller omedvetet påverkar systemet för att dra egna fördelar. Ur myndighetens synvinkel måste tre hot undanröjas:

- Storskaligt fusk - riskerar finansieringen
- Riktat fusk – riskerar tilltron till systemet
- Sabotage - riskerar tillförlitligheten

Sammanfattningsvis kan vi konstatera att alla hot som har minst ett av sannolikhetsvärdet eller konsekvensvärdet satt till 1 filtreras bort. Detta gäller även ifall ett av dessa båda värden är mindre än medel såvida det andra då inte är satt till 4 eller 5. Resultatet av en sådan filtrering blir att enskilt fusk, som inte sker systematiskt, ses ett mindre problem. Så länge varken tillförlitligheten, finansieringen eller tilltron till systemet försämras kan man mer eller mindre bortse från denna typ av fusk. Nedan presenteras en sorterad lista över de filtrerade listan av hoten.

Fysiska hot

Id	Hot	Risk-värde
F13	Intern manipulering av data mellan komponenter på flera OBU:er	12
F4	Förare gör avsiktligt OBUn strömlös	10
F1	Stöld av OBU	8
F9	Sabotage av flera GPS-antenner	8
F12	Intern manipulering av data mellan komponenter på enskild OBU	8
F14	Störning av data mellan OBU och GSM/GPRS-modul	8

Logiska hot

Id	Hot	Risk-värde
L10	Central server onåbar	15
L4	Ingen tillgänglig komm-länk	12
L1	Felaktig mjukvara i OBU	12
L6	Avlyssning av komm-länk	12
L3	Illasinnad programvara i OBU	10
L13	Fallbacklösning onåbar p.g.a. sabotage	10
L9	DoS-attack mot komm-länk, drabbar flera åkare	10
L12	Fallbacklösning onåbar p.g.a. driftsfel	9
L2	Sårbar mjukvara i OBU	8
L5	Störning av komm-länk	8
L7	Modifiering av data över komm-länk, drabbar flera åkare	8
L8	Fabricering av data över komm-länk, drabbar flera åkare	8
L11	Obehörigt tillträde till central server och data	8

Mänskliga hot

Id	Hot	Risk-värde
M1	Felaktig funktionalitet av OBU p.g.a. handhavandefel	10
M3	Läckage av data från central server	10
M5	Användaren ”glömmer” OBUn	10
M4	Felaktig behörighet på central server	8
M2	OBU slutar fungera p.g.a. handhavandefel	8

Identifiering av motåtgärder och angelägenhetsgrad

I det sista steget analyseras vilka lämpliga motåtgärder som existerar för de hot som inte kan accepteras baserat på dess relativt höga riskvärden. För varje hot presenteras en motåtgärd tillsammans med en *kostnadsuppskattning* på en femgradig skala som ser ut som följer:

1) Försumbar kostnad
2) Låg kostnad, t.ex.teknik för att uppmärksamma förare på låg strömnivå i OBU
3) Medelkostnad, t.ex. användning av manipuleringsskyddad teknik i OBU
4) Hög kostnad, t.ex. upprätthållande av väl fungerande fallback lösning
5) Ohanterbart hög kostnad, t.ex. skydd mot störning av komm.-länk

Baserat på kostnaden och riskvärdet så beräknas en *prioritet* (angelägenhetsgrad), dvs hur pass angeläget det är att implementera motåtgärden. Detta värde beräknas på en glidande skala genom att dividera kostnaden med riskvärdet. Vilket ger ett värde inom gränserna 0,2 (lägst riskvärde / högst kostnad) och 25 (högst riskvärde / lägst kostnad). Då vi filtrerar bort alla hot med ett riskvärde mindre än 8 så kommer detta prioritetsvärde alltid vara större eller lika med 1,6 samt mindre eller lika med 25.

Högst angelägenhetsgrad har alltså motåtgärder högst riskvärde (t.ex. sannolikhet 5 och konsekvens 5) och där genomförande kostnaden för motåtgärden är låg (t.ex. 1). Det omvända gäller givetvis också. Nedan listas alla hot samt dess tillhörande motåtgärder sorterat efter dess angelägenhetsgrad.

Motåtgärder

Id	Motåtgärd	Risk-värde	Kost-nad	Prio-ritet
L4	Lokal buffring av data tills möjlighet för kommunikation ges då denna data kan skickas.	12	2	6
L6	Kryptering av kommunikation vilket då implicerar att OBU:n först måste knäckas för att nycklarna ska läcka.	12	2	6
F4	OBUn notifierar förare vid låg strömnivå.	10	2	5
L10	Reservsystem för hårdvara, kommunikationsutrustning och strömförsörjning.	15	3	5
L3	Endast exekvering av godkänd och signerad mjukvara	10	2	5
L12	Ha rutiner i beredskap för att hantera sådana situationer, t.ex. genom kontrakt som preciserar vad som gäller	9	2	4,5
F13	Använd manipulerings-/avlyssningssäkrad hårdvara och kryptera all kommunikation mellan komponenter i OBU:n	12	3	4
F1	Stöldrisken minskar ifall OBU:n inte innehåller komponenter med högt andra handsvärde, t.ex. kommersiellt tillgängliga GPS-moduler	8	2	4
L1	Verklighetstrogna och grundliga test av all mjukvara	12	3	4
L7	Kryptering av kommunikation vilket då implicerar att OBU:n först måste knäckas för att nycklarna ska läcka	8	2	4
L8	Kryptering av kommunikation vilket då implicerar att OBU:n först måste knäckas för att nycklarna ska läcka	8	2	4
L11	Korrekt åtkomstskydd och autentisering av användarna	8	2	4
M4	Kontinuerlig verifiering av behörighetsåtkomsten	8	2	4
L13	Rutiner som säkrar bevisinsamling och kontakt med polis	10	3	3,3

F12	Använd manipulerings-/avlyssningssäkrad hårdvara och kryptera all kommunikation mellan komponenter i OBU:n	8	3	2,7
F14	Använd manipulerings-/avlyssningssäkrad hårdvara i OBU:n	8	3	2,7
M6	Införa Chinese Wall modell	8	3	2,7
M1	Tydlig visualisering av OBU-konfigurationen samt böter då en OBU används som ej stämmer med fordon.	10	4	2,5
M3	Kontinuerlig kontroll samt utbildning av anställda	10	4	2,5
M5	Utbyggt externt kontrollsystem	10	4	2,5
M7	Stickprovskontroll, korrekthet i drift	10	4	2,5
L9	Endast begränsat implicit skydd genom juridiska åtgärder	10	5	2
L2	Penetrationstestning av all mjukvara	8	4	2
M2	Tydlig visualisering av OBU:ns konfiguation och status	8	4	2
F9	Verifiera GPS-signal (stöd för detta måste implementeras i GPS-systemet)	8	5	1,6
L5	Endast begränsat implicit skydd genom juridiska åtgärder	8	5	1,6

Motåtgärdsbeskrivning

Då prioriteterna av motmedlen sammanställs i en lista som ovan kan dessa grupperas i fyra olika grupper som *topp-prioriterade, högprioriterade, medelprioriterade, lågprioriterade*. De topprioriterade motmedlen omfattas av dem som har en prioritet på 5 eller 6 och dessa är samtliga kostnadseffektiva att implementera. Därefter kommer de högprioriterade motmedlen som har ett prioritetsvärde på 4 vilket innebär att dessa är intressanta att studera vidare eftersom de ger ett bra skyddsratio relativt dess kostnad. Vidare följer de medelprioriterade motåtgärderna och för dessa gäller det att noga överväga vilka som bör implemeteras. Sist kommer de lågprioriterade motåtgärderna som samtliga är dyra att implementera och som endast adresserar hot med låga riskvärden. Nedan beskrivs de olika motåtgärderna i mer detalj efter deras grupptillhörighet.

Topprioriterade motåtgärder

Den ena av de två högst prioriterade motåtgärderna innebär att all trafik mellan OBU och de centrala servrarna krypteras. Kostanden för sådana motmedel är låg eftersom tekniken finns tillgänglig som standardkomponenter idag. Trots detta skyddar kryptering mot allehanda hot mot både integritet och konfidentialitet av kommunikationen mellan OBU och de centrala servrarna (se L6, L7 och L8).

Den andra högst prioriterade motåtgärden adresserar hot L4 som innebär att fordonet befinner sig där det inte fick möjlighet till kommunikation, t.ex. utanför täckningsområdet för GSM-nätet. Motåtgärden blir då att lokalt buffra upp all data som skulle skickas så att denna kan skickas vid senare tillfälle, då kommunikationsmöjligheter ges istället.

En annan högt prioriterad motåtgärd som motverkar att användaren avsiktligt bryter strömförsörjningen till OBU:n (se F4). En sådan motåtgärd bygger på att en enkel visuell eller ljudbaserad notifierare används för att meddela föraren i fordonet då OBU:n kräver dennes uppmärksamhet, t.ex. då OBU:n har låg strömnivå, dvs föraren kan inte i efterhand påstå att han var ovetandes om problemet. Denna enkla motåtgärd minskar risken för

handhavandefel från föraren då data ska matas in i OBU:n om exempelvis antal hjulaxlar på fordonet.

Användning av reservsystem på de centrala servrarna får även en hög prioritering. Detta innebär att flera identiska servrar körs parallellt så att backupsystem finns tillgängliga ifall en server havererar p.g.a. t.ex. hårdvarufel. Detta gäller likaväl nätverksutrustning som nätverksanslutning (se L10).

Motmedel mot illasinnad programvara i form av att endast exekvering av signerad programvarat tillåts hamnar även högt i prioriteringen eftersom en sådan motåtgärd kan användas utan någon större kostnad. En sådan motåtgärd skulle säkerställa så att endast mjukvara från tillförlitliga parter tillåts exekvera (se L3).

Att kunna hantera en situation där hela vägskattesystemet slutar fungera samtidigt som även fallbacklösningen ”går ner” p.g.a. driftsfel är ytterst viktigt (se L12). Genom att noggrant precisera vad som gäller för sådana situationer i de kontrakt som ingås med t.ex. kunderna så kan ett på förhand känt worst-case scenario garanteras. Vissa driftsfel kan även avstyras ifall redundanta system används som en slags ”fallbacklösning” på fallbacklösningen.

Högprioriterade motåtgärder

Motmedel mot intern manipulering av data mellan OBU-komponenter (se F13) prioriteras högt bl.a. baserat på deras relativt låga kostnad. Sådana motmedel behövs eftersom både mjukvara och hårdvara går att analysera med hjälp av olika verktyg (t.ex. disassemblers). Exempel på sådana motmedel är obfuskringstekniker som används för att försvåra analysen av mjukvaran. Dessutom kan checksummor användas för att kontrollera så att mjukvarans integritet är oförändrad under körning. Teknik som tillhandahåller manipulerings och avlyssningssäkrad hårdvara erbjuds idag som COTS. Ett exempel är smartcards.

För att motverka stöld av OBU:er (se F1) så bör dessa inte inkludera vissa typer av standardkomponenter som kan öka stöldbegärligheten. Istället bör custom-tillverkade komponenter användas för att minska andrahandsvärdet och därav förhoppningsvis även stöderna. Om exempelvis en kommersiellt erkänd GPS-mottagare eller GSM-modul inkluderas p.g.a. av dess låga pris så kan stöldbegärligheten antas vara hög och stölderna av OBU:er skjuta i höjden.

För att motverka de problem som kan uppstå ifall felaktig mjukvara körs i OBU:n (se L1) så bör all mjukvara testas noggrant innan den tas i bruk. Förutom löpande testning under själva utvecklingsstadiet så skall all mjukvara testas ute på fältet under en väl tilltagen tidsperiod. Dessa tester ska givetvis ske i så realistisk miljö som möjligt för att på så vis få en verklighetstrogen testperiod.

Detaljerad beskrivning av motmedel mot modifiering samt fabricering av data som skickas över komm-länken finns under motmedel mot L6.

Risken att vissa personer har alltför höga rättigheter i systemet (L11 ooch M4) kan minskas genom att säkerställa att väl fungerande autentiseringsmekanismer används samtidigt som de gällande rättigheterna kontinuerligt verifieras och valideras. Införandet av pentrationstester

som har som mål att identifiera sårbarheter i system kan också användas för att ytterligare minska denna risk.

Medelprioriterade motåtgärder

Vissa av hoten som syftar till att attackera fallbacklösningen (se L13) kan man inte skydda sig mot på något säkert sätt. Ett sådant exempel är överbelastningsattacker där t.ex. telefonväxlen till ett call-center överbelastas så att legitima kunder inte kommer åt tjänsterna. Visst implicit skydd kan erhållas genom att rutiner på förhand tas fram för hur hantering av sådana här situationer ska haneras, t.ex. hur bevisinsamlingen ska se ut samt när och på vilket sätt polisen ska kopplas in.

Mer information om motmedel mot F12 och F14 finns beskrivet under motmedel mot F13.

För att motverka felaktig funktionalitet hos OBU:n p.g.a. att föraren felaktigt konfigurerat den (se M1) så bör någon typ av notifierare användas för att informera föraren om hur OBU:n är konfigurerad samt dess status (se motmedel mot F4). Vidare bör det även vara olagligt att använda en OBU som inte stämmer överens med fordonets nuvarande funktion, t.ex. antal hjulaxlar. Om en förare ertappas i en kontroll med att ha en felaktigt konfigurerad OBU så ska detta vara belagt med böter vilket ger ett förebyggande skydd.

Lågprioriterade motåtgärder

Något direkt skydd mot att en DoS-attack inträffar mot komm-länken (se L9) finns egentligen inte (detta har vi representerat m.h.a. kostnadsvärdet satts till 5). Visst förebyggande skydd kan erhållas genom juridiska åtgärder som gör sådana attacker olagliga vilket i viss mån kan avskräcka vissa attackerare.

Som skydd mot sårbar mjukvara i OBU:n kan penetrationstestning av de färdiga programmen nämnas (se L2). Genom att använda färdiga produkter för att söka efter olika typer av sårbarheter så kan dessa upptäckas innan mjukvaran början användas skarpt.

Ett motmedel mot OBU-handhavandefel från användaren är någon typ av notifierare av OBU:ns konfiguration samt status (se motmedel mot F4).

Teknik för att skydda sig mot att en attackerare lurar GPS-systemet genom att skicka in falska signaler till denna (se F9) finns inte idag och därför får detta motmedel ett så pass högt kostnadsvärde. Eventuellt skulle det kunna gå att skydda sig mot denna typ av attack genom att signera de signaler som satelliterna skickar ut. Något som antagligen kostar mycket pengar att genomföra.

Att skydda sig mot att någon stör ut kommunikationslänken med hjälp av en störsändare (se L5) går inte vilket vi har låtit visualisera med hjälp av det högsta kostnadsvärdet på denna motåtgärd. Detta höga värde ger till följd att motåtgärden får en bottenplacering på prioriteringslistan. Visst implicit skydd kan fås genom att störsändare är förbjudna att använda enligt lag vilket därför kan ha en avskräckande effekt.

Analys av säkerheten

I föregående avsnitt beskrevs de olika motmedel som kopplats till de identifierade hoten. För att få fram prioritetsordningen på dessa motmedel så beräknades kvoten av riskvärdet och kostnaden för att åtgärda hotet. Riskvärdet i sin tur är produkten av sannolikheten att hotet realiseras samt dess konsekvens. Tillsammans ger dessa parametrar en uppskattning av hur säkerhetsåtgärder kan/bör prioriteras. Dessa bedömningar behöver inte vara de samma som när driftsfel rättas till vilket nedanstående exempel visar:

- De fysiska hoten om intern manipulering av data mellan komponenter på enskild OBU (F12) respektive flera OBUer (F13) ger olika riskvärden (8 respektive 12). Det högre riskvärdet för F13 beror på att konsekvenserna blir större eftersom flera åkare är inblandade trots att sannolikheten för att detta ska inträffa bedöms som mindre sannolikt. Kostnaden för att rätta till felen är de samma eftersom felet åtgärdas på den enskilda OBUn, dvs om en lösning implementeras (manipulerings/avlyssningssäkrad hårdvara plus krypterad kommunikation mellan komponenter i OBUn) under designfasen så åtgärdas båda felen. Säkerhetsanalysen ger F13 en relativt hög prioritering och på köpet får man att F12 också åtgärdas (som har en lägre prioritering).

- Fallbacklösning kan vara onåbar pga driftsfel (L12) eller sabotage (L13). Konsekvenserna av detta blir betydligt större vid sabotage (eftersom manipulation av data inte kan uteslutas) samtidigt som det är mera sannolikt att ett driftsfel uppstår. Sammantaget blir ändå riskvärdena ungefär desamma, dvs 10 för driftsfel och 9 för sabotage. Kostnaden för att åtgärda sabotaget är högre (felanmälan och loggning ger kostnad 3) än för driftsfel (rutiner som ger kostnad 2) vilket sammantaget ger topprioritet för driftsfel och medelprioritet för sabotage. I det här fallet är åtgärden förebyggande, dvs att rätta till ett driftsfel förebygger och delvis löser de motåtgärder som behövs för att komma tillrätta med sabotage.

Den högsta prioritering vi hittade hade värdet 6 och den lägsta 1,6. Vi fann tre olika prioriteringsgrupper:

- 6 - 5 hade högt riskvärde (medelvärde 11,4) och låg kostnad (medelvärde 2,2). Till en låg kostnad blir skyddet avsevärt förbättrat för totalt 5 identifierade hot.

- 4 – 2,7 hade lågt riskvärde (medelvärde 8,9) men fortfarande en låg kostnad (medelvärde 2,5). Till en låg kostnad kan kompletterande skydd ges för ytterligare 10 identifierade hot.

- 2,5 – 1,6 hade lågt riskvärde (medelvärde 9,0) men en hög kostnad (medelvärde 4,4). För dessa mera marginella hot (7 stycken) krävs en stor ekonomisk insats för att få till ett skydd.

Säkerhetsanalysen prioriterar både syfte (handhavandefel respektive sabotage) och storskalighet där en driftsanalys istället koncentrerar sig på de driftsmässiga konsekvenserna av en störning. Delvis överlappar dessa synsätt varandra (storskalighet ger oftast större konsekvenser), men delvis är de oförenliga (ett intrång som inte påverkar driften negligeras i driftsanalysen). För att belysa detta ges två exempel:

- En DoS- attack (denial of service) mot kommunikationslänken drabbar flera åkare (L9). Konsekvens och sannolikhet är de samma både i en drifts- och säkerhetsanalys, dvs mycket stora konsekvenser men begränsad sannolikhet. I säkerhetsanalysen gör vi bedömningen att kostnaden för skyddet är mycket hög helt enkelt därför att det är svårt att förutse och helt ut skydda sig mot en DoS-attack. En driftsanalys kompletterar istället systemet med back-up lösningar vilket också ger en mycket hög kostnad. Detta hot hamnade i lägsta prioriteringsgruppen därför att det säkerhetsmässigt inte går att göra så mycket. Däremot måste indirekta driftsmässiga åtgärder sättas in för att snabbt få upp systemet igen.

- Om illasinnad programvara installeras i OBUn (L3) behöver detta inte innebära någonting för driftsmässigheten, allt fungerar normalt aktiviteten sker i bakgrunden. I säkerhetsscenariet kan konsekvenserna vara katastrofala där sannolikheten för att detta inträffar inte går att bortse ifrån (med normalt basskydd om OBUn är mottaglig för yttre kommunikation). Eftersom åtgärdskostnaderna för denna typ av hot bygger på beprövad teknik blir dessa kostnader relativt små, dvs totalt blir detta en högt prioriterad åtgärd. Indirekt kan detta också stoppa andra intrång som den illasinnade programvaran öppnar upp för (systemet är inte längre betrott).

Vi har valt att koncentrera hotanalysen på OBU delen men ett par av attackerna (M3 och M4) innebär hot mot den centrala servern. Hantering av data (inbetald kilometerskatt) innebär att information om åkeriföretaget lagras på central server. som innehåller hot av olika svårighetsgrader. Det lätta problemet är olika debiteringsfunktioner. Här krävs att tillgång till register enbart ges till ett begränsat antal behörig personal. Ett svårare problem är trafikrapportering. Myndigheten ska kunna redovisa statistik samtidigt som integriteten för enskilda åkare inte hotas. Det svåraste problemet är hantering av metadata. Hur undviks att känslig information läcker ut (betalningsuppgifter, årssammanställningar) som egentligen inte har med den centrala servern att göra.

Diskussion

De olika presenterade värdena för prioritet och indirekt för sannolikhet, konsekvens och kostnad kopplade till hoten kan ifrågasättas därför att det inte finns något system i drift att utgå ifrån. Vi har valt att inte precisera exakt hur OBUn ser ut även om vi tänkt oss någon smartcard-baserad lösning där OBUn på ett enkelt sätt kan uppgraderas. Som ytterligheter finns tunga klienter (Tyska systemet) eller ingen klient alls (harmoniserad dieselskatt). Vi tänker oss alltså inte någon tung klient där stora delar av datauppgifterna bearbetas lokalt. Ur säkerhetssynpunkt är detta en fördel, resurserna kan läggas på att säkerställa de centrala enheterna istället för att sprida åtgärdena på varje OBU (däremot behöver detta inte nödvändigtvis vara bättre ur driftssynpunkt, en central server som lägger av stoppar all verksamhet).

Vi förutsätter alltså att fordonet har en stationär/mobil ombordenhet som kommunicerar med central server och att programkoden finns på smartcard. Skyddet av programvara innebär därför att smartcard och den information som finns lagrat på detta måste skyddas mot olika typer av analys och manipulering. Med hjälp av t.ex. disassemblers och decompilers så kan duktiga tekniker analysera och manipulera mjukvaras funktionalitet utan att ha tillgång till dess källkoden. För att skydda mot detta kan man använda sig av följande tre tekniker:

- Obfuskering, dvs. dölja programvarukoden, för att försvåra analys av smartcard
- Integritetskontroll, säkerställ att programkoden är oförändrad vid körning
- Säker kommunikation via kryptering så att oförvanskad data överförs

Obfuskeringstekniker används alltså för att försvåra analys av mjukvara. Fördelen med sådana tekniker är att de höjer ribban som en attackerare måste ta sig över för att knäcka systemet. Dock ger det ingen garanti mot att en rillräckligt duktig attackerare kan ta sig runt obfuskeringen och därmed hitta de instruktioner som finns där. Just att kunna analysera mjukvara är en förutsättning för att en attackerare ska kunna modifiera dess funktionalitet efter sina egna önskemål. En nackdel med obfuskeringstekniker är att de resulterar i mer komplex hantering av mjukvaran under utvecklingen, vilket potentiellt kan ge fler fel som resultat. För att komma runt detta så krävs i sin tur utökad testning för att säkerställa att mjukvaran fungerar korrekt innan den tas i bruk.

Förutom att försvåra analysen av mjukvara så kan man också vidta åtgärder för att säkerställa att integriteten är oförändrad under exekvering. Detta löses genom att beräkna kontrollsummor för de delar av programmet som man tror attackerare kommer att manipulera, dvs. en manipulation kommer att upptäckas. Under körning av programmet så beräknas nämligen kontrollsummorna på nytt och jämförs med de som sparats. Om manipulation upptäcks så vidtas åtgärder, t.ex. försätts enheten i ett säkert läge. Det är fullt möjligt att använda flera olika checksummor på en gång. Dessa kan även interagera för att "kontrollera" varandra och därmed komplicera knäckningen för attackeraren. Ett par problem med kontrollsummor är att de visar vilka delar av programmet som man försöker skydda och var man eventuellt lagrar sina "säkra" kontrollsummor.

Genom att kryptera programmet så länge som det ligger på smartcardet så försvåras analysen av det. Så snart programmet startar så avkrypteras det till minnet där det körs. När det är

färdigt så återgår det till sitt krypterade tillstånd på smartcardet, dvs. om man försöker läsa informationen på kortet så är den oläslig. Det går även att skydda programmet i minnet genom att kryptera det även här för att endast avkryptera de instruktioner som körs för tillfället. På så vis kan en eventuell attackerare aldrig finna programmet avkrypterat ens i minnet utan denne kommer istället endast finna en eller ett par avkrypterade instruktioner åt gången. Nackdelen med en sådan lösning är främst att prestandan påverkas negativt eftersom krypteringsfunktionen ständigt krypterar eller avkrypterar mjukvaran under körning.

Smartcard ger ett visst hårdvaruskydd i sig som dessutom kan förstärkas genom olika skyddshöljen (för exempel se Anderson 2001[4]). Å andra sidan har fordonsägaren tillgång till kortet och kan därmed manipulera det om denne förstår hur det fungerar. Alltså, gäller det att vidta åtgärder för att försvåra analys av kortet. Dessa åtgärder höjer nivån så att endast personer med avancerade kunskaper om *både* hårdvaru- och mjukvaru-"knäckning" kan lyckas. Dessutom ger smartcard ett flexibelt skydd eftersom nya smartcards kan distribueras ifall befintlig säkerhetslösning inte håller längre.

En normal systemutveckling börjar med kravspecificering som följs av att designen fastställs, systemet implementeras och olika tester på tillförlitligheten utförs (bas, funktions och systemtest finns med vid mjukvaruutveckling) innan systemet når användaren. Ur kostnadssynpunkt är undvikna fel mycket bättre än upptäckta, det kan ibland röra sig om en faktor 100 i utvecklingskostnader. Går det att i kravspecifikationen och i designfasen undvika att fel uppstår eller blir mera hanterbara ska detta göras. Detta gäller både driftsstörningar och i synnerhet säkerhetsbrister, därför att de senare är svåra att upptäcka under testfasen. Genom att göra en hotanalys av positionsavgivelsekedjan har detta arbete påbörjats. I nästa steg ska OBUn, kommunikationslänken och de centrala resurserna preciseras för att mera i detalj kunna analysera tänkbara säkerhetsbrister. Detta är en iterativ process som sker både före, under och efter systemimplementering.

[4] R. Anderson Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley 2001

Sammanfattning

I säkerhetsanalysen har hot baserade på sannolikhet, konsekvens och kostnad resulterat i en prioritetsordning för fysiska, logiska och mänskliga hot. En hotanalys blir aldrig helt färdig, de systemförbättringar som införs genererar nya säkerhetsproblem. Två slutsatser kan dras av detta.

För det första ska säkerhetsanalysen vara en integrerad del av systemutvecklingen under alla dess faser både före och efter att systemet satts i drift. Genom att kombinera säkerhets- och driftsaspekterna kan underhållet effektiviseras liksom att kostnaderna kan hållas nere.

För det andra om det går att välja mellan en enkel och en mera komplicerad design (tänk lätta och tunga klienter), så välj den enklare. Det går lättare att förutse framtida säkerhetsbrister om designen är enklare och det går lättare att byta ut ingående komponenter som inte svarar upp mot säkerhetskraven (typexempel byt smartcard om detta blivit utnyttjat av inkräktare).

Till skillnad mot driftsproblem är säkerhetsproblemen av typen allt eller inget. Säkerhetsbrister märks inte i dagliga verksamheten utan bygger på att kunna förutse hot och på att kunna reagera snabbt. En form av kapprustning uppstår, ett system blir aldrig säkert utan både angrepp och försvar utvecklas efterhand. Därför tror vi att en säkerhetslösning baserat på dynamiska säkerhetsmekanismer (tänk smartcards där nya kan distribueras ifall de befintliga kringgåtts) är att föredra framför statiska då dessa förlorar allt skydd så snart nuvarande mekanismer kringgåtts.

List of ARENA reports

ARENA REPORT 2008:1. “Road User Charging of Heavy Goods Vehicles in Sweden”. Final report ARENA 1., NetPort.Karlshamn

ARENA REPORT 2008:2. Sundberg, J., Janusson, U., and Sjöström., “A kilometre tax for heavy goods vehicles in Sweden – A conceptual systems design. Part 1: Requirements and preconditions”., SWECO VBB

ARENA REPORT 2008:3. Sundberg, J., Janusson, U., and Sjöström., “A kilometre tax for heavy goods vehicles in Sweden – A conceptual systems design. Part 2: Proposals for systems design”., SWECO VBB

ARENA REPORT 2008:4. Sundberg, J., “A New Approach to Control in the ARENA concept for HGV kilometre tax in Sweden”., SWECO VBB

ARENA REPORT 2008:5. Hamilton, C J. “A market based approach to achieve EFC interoperability in Europe”., Policy Technology

ARENA REPORT 2008:6. Eliasson, C and Fiedler, M., “Dimensioning study for road user charging”. Blekinge Institute of Technology.

ARENA REPORT 2008:7. Boldt, M and Carlsson, B,. “Hotanalys för positionsangivelsekedjan”. Blekinge Institute of Technology.

ARENA REPORT 2008:8. Davidsson, P and Persson, J., “A Criteria-Based Approach to Evaluating Road User Charging Systems”.,Blekinge Institute of Technology

ARENA REPORT 2008:9. Sundberg, J., “PM kring legala frågeställningar”., SWECO VBB

ARENA REPORT 2008:10. Janusson, U., Berg, P and Udin, C., “ARENA DEMO”., SWECO VBB

ARENA REPORT 2008:11. Sundberg, J., PM kring kostnadsberäkning”., SWECO VBB

ARENA REPORT 2008:12. Forss, M., Gustafsson, I., and Källström, L., “ARENA RUC Seminar 1 & 2 – Summary of the seminars”., NetPort.Karlshamn

ARENA REPORT 2008:13
Published papers produced within the project

ARENA
NetPort.Karlshamn
Biblioteksgatan 4 • 37435 Karlshamn • Sweden

Project partners:
Swedish Road Administration • SWECO • BMT Transport Solutions • Blekinge Institute of Technology • NetPort.Karlshamn

www.arena-ruc.se