INF3510 Hjemme-eksamen

Oppgave:
Autonomous Vehicles Security, T149

Kandidatnr:
15570
15602

May 15, 2017

Autonomous Vehicles Security

De siste årene har vi stadig fått mer og mer av selvkjørende kjøretøy. Fly i dag flyr nesten bare på autopilot,[1] og selvkjørende biler begynner å komme. I Tesla sine nye biler begynner autopiloten å bli så bra at man kan nesten si at den er selvkjørende. Med denne utviklingen kommer det potensielt også mange nye faremomenter, f.eks. feil i software, hacking av bilene etc. Er dette reelle farer som kan føre til alvorlige konsekvenser? Dette er noe man må ta hensyn til når man begynner å utforske denne nye teknologien. I denne oppgaven skal vi se nærmere på sikkerheten rundt autonome biler. Hvilke potensielle trusler finnes, hva er de og hvordan kan vi beskytte oss mot de. Blir veiene egentlig tryggere med autonome biler, enn det de er i dag?

Hvordan fungerer det

Biler er ikke det de pleide å være lengre. Hvis man bare går noen år tilbake var bilen ikke mer enn et verktøy som fikk en person fra a til b. Etter en stund når teknologien utviklet seg, utviklet bilene seg også. Det kom stadig nye funksjoner som skulle gjøre alt mye lettere og mer behagelig for brukeren. Radio, navigasjon, cruise-control og mange flere funksjoner. Det kom software som du kunne installere på telefonen for å kontrollere komponenter på bilen, f.eks. åpne dører, starte motoren og skru lyktene av og på.[2] Alt dette for at eieren skulle få en bedre opplevelse. Det nyeste nå er det vi kaller selvkjørende biler. Dette er biler som benytter seg av sensorer, og meget avansert software med algoritmer som gjør utregninger, og på denne måten klarer å styre bilen selv. Dette er revolusjonerende innen bilindustrien. Se for deg at du skal på hytten din i helgen og er sliten etter jobb og vil egentlig ikke kjøre ut dit. Alt du da trenger å gjøre er å taste inn lokasjonen du skal til og sette deg tilbake i setet, så gjør bilen resten for deg. Dette høres jo helt fantastisk ut, men det er ikke nødvendigvis like flott som det høres ut. Med denne nye teknologien følger det også ekstremt mange nye trusler, som kan potensielt være livstruende. Du har nå kommet halvveis frem til hytten din og slapper av i setet. Plutselig har noen andre hacket seg inn i bilen din og tar kontroll over gass, brems og styring. Dette er en reell trussel med disse nye bilene og kan ha fatale konsekvenser. Se for deg en annen situasjon hvor du skal på hytten din, men denne gangen er veien dekket av snø, siden det er

[1] Wikipedia, 2017
[2] Uconnect, 2017

vinterferie. Snøen gjør slik at det blir vanskelig for bilen å se skilt og markeringer på veien. Dette fører så til at bilen kjører rett frem i en sving, pga all snøen. Dette er også en skummel og realistisk situasjon som kan oppstå, uten nok sikkerhet.

Safety vs security

I den daglige talen bruker vi ofte ordet sikkerhet(security) i situasjoner hvor vi egentlig burde bruke ordet trygghet(safety). Når vi snakker om informasjonssikkerhet betyr de to ordene noe helt forskjellig. Bilutviklere i dag har veldig mye erfaring når det kommer til trygghet, men kanskje ikke like mye når det gjelder sikkerhet. Når vi snakker om tryggheten til disse nye selvkjørende bilene ser vi bort i fra angrep fra utsiden. Software feil eller svikt på den andre siden er direkte relatert til tryggheten. Mange andre ting påvirker tryggheten også naturligvis.

I bunn og grunn viser statistikken at de aller nyeste autonome bilene er ganske trygge.[3] I disse nye selvkjørende bilene må man stole enormt mye på programvaren i bilen. Bare en liten feil kan ha fatale konsekvenser.[4] Bilene har sensorer overalt rundt seg, som samler inn data. Denne dataen blir brukt til å gjøre utregninger, og til syvende og sist; kjøre bilen. I Tesla sine nyeste biler finnes det en autopilot hvor bilen er nesten helt selvkjørende. De sier dog at sjåføren alltid må ha to hender på rattet, og holde øye med veien og trafikken, i tilfellet noe skulle gå galt.[5] For å få til dette på en trygg måte, kreves det ekstremt mye software og hardware. Tesla har i de nyeste bilene sine 8 kameraer, 12 ultrasoniske sensorer, og en radar som vender fremover. I tillegg til dette, en kraftig maskin som gjør beregninger på data som samles inn.[6] Elon Musk, som er CEO av blant annet Tesla sier selv at disse bilene er tryggere enn vanlige biler som styres av mennesker, som statistikken også er enig i. Den første dødelige krasjen som skjedde med en Tesla hvor autopiloten ble brukt skjedde først etter ca. 130 millioner miles. Hvis man ser på alle biler USA skjer det i gjennomsnitt et dødelig krasj etter 94 millioner miles.[3] Nå er riktignok denne dataen basert på ett enkelt krasj hos tesla, så det kan være at antall miles går ned med tiden.

For Google sine selvkjørende biler har det i skrivende stund vært 14 til-

[3](Zachary Shahan, 2016)
[4](Neal E. Boudette JAN. 19, 2017)
[5](The Tesla Motors Team 2015)
[6](Vegard Møller Johnsen 2016)

feller med kollisjon, hvor i kun ett av tilfellene var skylden feil i software til bilen. De 13 andre tilfellene var det en annen sjåfør sin skyld. [7] Ifølge ulykkesrapporten som ble levert til DMV (Department of Motor Vehicles) så støtte Google bilen på et uforventet problem, det lå sandsekker rundt et kumlokk i dens fil.[8] Denne obstruksjonen gjorde at Google bilen var nødt til å benytte seg av filen ved siden av i samme kjøreretning. Etter den hadde latt et par biler passere, forberedte bilen seg på å utføre manøveren. En buss nærmet seg bakfra og kunne tydelig sees i venstre speil, skrives det i rapporten fra DMV; "The Google car test driver saw the bus approaching in the left side mirror but believed the bus would stop or slow to allow the Google car to continue." Dette skjedde da ikke, og bussen kolliderte med Google bilen. Dette var da et utfall av feilende software. [9]

I bunn og grunn virker det som om produsentene har kommet langt når det kommer til tryggheten. Hvis vi som sagt bare ser på statistikken antyder den at det egentlig er tryggere å sitte på som passasjer i en selvkjørende bil, enn å faktisk kjøre den selv.[3] Et annet spørsmål er hvor bra sikkerheten er i disse bilen. Hvor lett er det egentlig for en hacker å ta kontroll over bilen din, og hvordan kan dette potensielt skje? Videre skal vi ta for oss disse spørsmålene.

CAN-buss

Allerede i juli 2015 demonstrerte Charlie Miller og Chris Valasek hvordan de klarte å hacke og ta kontroll over en Jeep fra en laptop helt trådløst.[10] De kom inn i systemet gjennom "the entertainment unit" og klarte å ta kontroll over gass, brems, styring osv. I denne Jeepen var det installert Uconnect som er et system som lar eieren av bilen starte bilen, låse opp etc via en app. Det var dette systemet som også gjorde at Charlie og Chris klarte å få fjernstyrt tilgang til hele bilen. Uconnect systemet var da installert i flere hundre tusen biler. Systemet ble oppdatert ikke så alt for lenge etter, hvor dette problemet ble tatt hånd om.

Et populært mål for hackerne er bilens CAN-buss, men hva er egentlig en CAN-buss? CAN-bussen transporterer forskjellig type informasjon, til

[7](McFarland, 2016)
[8]DMV rapport fra krasjet vedlagt i kildelisten
[9](Vishal, Matur, 2017) og (Davies, 2016)
[3](Zachary Shahan, 2016)
[10](Samuel Gibbs 2015)

forskjellige styreenheter. Uten CAN-bussen ville det vært behov for én ledning for hver enkelt type informasjon. Motivasjonen bak dette var altså kraftig reduksjon av antall ledninger. Dataoverføringen med en CAN-buss fungerer omtrent som en telefonkonferanse. En deltaker (styreenhet) "snakker" informasjonen (dataen) sin inn i et ledningsnett, mens de andre deltakerne kan høre denne informasjonen. Noen deltakere synes informasjonen er interessant og bruker dem, andre ignorerer det.[11]

For å klare å styre gass, brems, styring og alle de andre essensielle funksjonene ved en bil må man ha tilgang til CAN-bussen. Via CAN-bussen sendes det kommandoer som utføres, hvis de blir godkjent.[11] Selv om en hacker får tilgang til CAN-bussen betyr det ikke nødvendigvis at han/hun har kontroll over hele kjøretøyet. Bilen sender fortsatt sine egne meldinger og meldinger fra hackere kommer i konflikt med disse, eller gjenkjennes som en melding som kan føre til error i bilen av noe slag.[11] Jeep-hackerene løste dette problemet ved å tvinge bilen inn i det som kalles "diagnostic mode". Dette lar de få mye mer kontroll, med færre begrensninger. Dette ble senere fikset ved at bilene ikke kan bli satt i denne modusen med mindre bilen kjører i 5mph eller lavere.

Et forebyggende tiltak er å verifisere meldingene som sendes til CAN-bussen. På denne måten kan man finne ut om det faktisk er en melding som kommer fra bilen, eller fra en ukjent kilde. Verifiseringen kan skje på ulike måter. I Jeepen som ble hacket i 2015 hadde hver kommando i CAN-bussen et identifikasjonsnummer som inkrementeres med 1 for kommando.[10] Dette var forøvrig en dårlig måte å verifisere, da hackerne klarte å lure systemet nokså lett. De fant ut av denne verifiseringsmetoden ganske fort, og sendte da meldinger med ID nummer som økte med 1. Dette førte til at systemet faktisk stengte meldingene som kom fra bilen ute. Dette på grunn av at systemet så på meldingene fra hackerne som de ekte meldingene, og de som kom fra sjåføren som de falske. Resultatet av dette var at de som hacket bilen hadde full kontroll over hva som skjedde, mens sjåføren satt på som en blindpassasjer.[10]

Må man da bruke mer avanserte måter for å verifisere meldingene til CAN-bussen? Et problem med dette er at det tar tid å verifisere. I en bil er det kritisk at bilen bremser med en gang når for eksempel bremsen blir trykket inn. Derfor kan det være en bedre løsning å forhindre at angripere

[11](Steve Corrigan, 2008) og (Wikipedia, 2017)
[10](Samuel Gibbs, 2015)

får tilgang til CAN-bussen i utgangspunktet. På denne måten slipper man å bruke unødvendig mye tid på verifisering av meldinger, og bilen bremser når den skal. I tilfellet hvor de hacket jeep'en fikk de tilgang til CAN-bussen gjennom Uconnect, som er et software som skulle gjøre alt enklere for bileiere.[10] Slike nye systemer og funksjoner er ofte det som åpner dørene for angripere. Det er da veldig viktig å vurdere risikoene rundt det også, og kanskje prioritere sikkerheten.

Hvordan øke sikkerheten

Det er ikke alltid så ekstremt mye som skal til for å øke sikkerheten. Det er ofte lett å være litt naiv, og ikke tenke nok på det. Under kan vi se noen punkter med tiltak, som potensielt kan øke sikkerheten ganske mye. Flere av disse punktene bør kanskje være åpenbare, men blir fortsatt ikke alltid tatt hensyn til.

Ikke prioriter nye egenskaper over sikkerhet

Det er stor etterspørsel blant forbrukere etter biler med nye og effektive funksjoner, mens bekymringen for at disse funksjonene muligens kan bli hacket er svært lav. White hat hackere har allerede demonstrert en del av sårbarhetene disse funksjonene har medført. [12] Når cybersikkerhet ekspertene Charlie Miller and Chris Valasek hacket en 2014 Jeep Cherokee var dette fordi at de oppdaget en metode slik at de kunne hoppe fra bilens underholdnings buss direkte til CAN-bussen. Dette er en typisk strategi, angripe den mest sårbare overflaten, slik at man kan angripe mer verdifulle ting etter å ha kommet inn via denne overflaten. [12]

Ikke vær slapp med tillatelse

Tradisjonelt har bilprodusenter gitt personene som tilkobler seg til bilen et adgangsnivå på likhet med root-adgang i en PC. Om du logger inn på en bils data-buss, har du tradisjonelt sett hatt en slags "alltid-på" adgang.[13] Bilen sier egentlig at hvis du kan kalle på meg, så er du OK. Du har et underholdningssystem med en grad av tillatelser, og så er det kommando- og kontrollsystem som kan gjøre ting som å aktivere bremsen. Bilindustrien begynner å lage en separasjon av kommandoer for brukere som i hovedsak sier: 'Du kan gjøre disse 10 tingene, men du kan ikke gjøre disse andre 10

[12](Hern, 2016)
[13](Buntz , 2016)

tingene.

Varsom på en tredjeparts etter-produksjons modifikasjoner
En av de største risikoene for biler er nå modifikasjoner som skjer etter de er blitt ferdig produsert, gjerne modifikasjoner som har trådløs funksjonalitet.[13] Vi er kjent med at bilen automatisk kobler opp telefonen din, hvis den er kjent, der nivået av kontroll er begrenset til en Bluetooth tilkobling. Slike tredjeparts programvare er en stor utfordring for bilprodusenter, fordi dette er noe de ikke har kontroll over. En løsning til dette vil være en modell som er tillatelses basert. Et skybasert sikkerhetssystem kan brukes til å bekrefte forespørsler fra tredjepartsprogrammer og gi adgang til de den verifiserer. En app kan programmeres til å gi fra seg en liste med ting den ønsker å gjøre. Sikkerhetssystemet kan da overvåke den og deretter velge å gi tillatelse til å utføre ønsket handling eller ikke. En bilprodusent kan også velge å svarteliste visse tredjepartsprodukter som er uønsket. I en sak som dette, vil plattformen ikke la den gjøre noe som helst i mistanke om at det er malware. [13]

Sett sikkerhet over kostnader
Hos en bilprodusent er det ofte to 'rivaliserende leirer'. Den ene har som hovedfokus å gjøre hva de kan for å optimalisere ytelsen og forbedre sikkerheten til produsentens biler. Den andre andre leiren har som hovedfokus å gjøre hva de kan for å kutte kostnader og maksimere lønnsomheten. Sikkerhet kan bli nedprioritert grunnet kuttingen av den andre leiren.[13]

Det er ingen tvil om at det er konkurrerende firmaer som ønsker å være først ute med en kommersiell selvkjørende bil.[14] Gitt et marked som er klar for dette kan den økonomiske gevinsten være enorm. Dette kan da være en årsak til at sikkerhet blir nedprioritert til en viss grad over tid.

Hvem gjør angrep?

Vi har snakket mye om disse hackerne som prøver å bryte seg inn i systemene våre, men hvorfor gjør de egentlig dette? Hva er motivasjonen til disse angrepene? For ikke alt for mange år siden bestod hacker miljøet mye av én type folk. Dette var folk som drev med hacking rett og slett fordi de kunne.

[13](Buntz , 2016)
[14](Vince Bond Jr, 2012)

Med andre ord hadde de ingen reelle motiver.[17] I dag er det dog veldig annerledes. Det finnes flere ulike type hackere, med helt forskjellige motiver. Vi kan dele de inn i noen få grupper.

1. "White hat hackers"
   De som hacket Jeep'en er av denne kategorien. Dette er folk som bryter seg inn i systemer, for å finne feil, eller svakheter i de. Etter at feil eller svakheter har blitt funnet rapporteres det inn til produsenten slik at de kan utbedre feilen. Deres motivasjon er kanskje å få en utfordring å bryne seg på hvor de eventuelt kan bidra til å gjøre systemet mer sikkert.

2. Kriminelle hackere/ "black hat hackers"
   Dette er folk som bruker sine hacke ferdigheter til ulovlige formål, alt fra for å tjene penger til utpressing av andre slag. Disse utgjør en stor gruppe av hackere. Det er denne type hackere den vanlige mannen i gaten bekymrer seg for, og dette av en god grunn.

3. "Activist hackers"
   Folk som er politisk eller religiøst motivert, som f.eks. gruppen Anonymous eller terrororganisasjoner som ISIS. Dette er strengt talt en subkategori under 'kriminelle hackere' hvor de i stedet for økonomisk motivasjon har heller en religiøs/politisk motivasjon.

4. "Intelligence agencies"
   Dette er folk fra et statlig lovgivende organ, som kan for eksempel hacke seg inn på en mistenkts telefon for å lytte inn på hva som blir snakket om etc. Dette er en gruppe som har vært mye i media i det siste, særlig anklagelsen mot Russland for å ha blandet seg inn i det amerikanske valget.[15] Skandalen med CIA og Samsung som kom ut i Wikileaks er en sak som er verdt å nevne seg.[16]

5. Hacker fordi de kan
   Denne gruppen består av folk som hacker rett og slett fordi de kan, og ikke har noen reelle motiver. Hvis vi går noen år tilbake utgjorde

[17](Jemima Kiss, 2016)
[15](Harding, 2016)
[16](Price, 2017)

denne gruppen en mye større andel. Dette er hverken black eller white hat hackers, deres motivasjon er trolig kun å få testet sine ferdigheter og se om de klarer å hacke systemer. Rapporterer de sine funn til produsenten faller de under white hat hackers, bruker de funnene sine til noe kriminelt faller de under black hat hackers.

Det er de kriminelle hackerne som utgjør den største trusselen. Det at de er motivert av penger gjør de veldig farlige.[17] Et naturlig spørsmål er da hvordan de skal få penger ut av å hacke en bil. Det som er kjent som "ransomware" er en ekte fare. Dette går ut på å hacke seg inn i et system og holde offeret sin data som "gissel", og evt. true med å lekke dataen eller lignende hvis ikke en såkalt "ransom" betales.[18] Med kjøretøy, eller mer spesifikt biler kan angriperen f.eks. holde bilen som gissel frem til han/hun får betalt av eieren. Et annet motiv hos de kriminelle hackerne kan rett og slett være at de ønsker å påføre fysisk skade hos en person. Hvis man klarer å få kontroll over et kjøretøy med en person inni, er det ingen tvil om at dette ganske lett kan gjøres. Dette så vi et godt eksempel på da Charlie Miller og Chris Valasek, klarte å ta full kontroll over gass, brems og styring i Jeep'en, som vi har snakket om tidligere. I mange systemer i dag brukes det ulike autoriseringsmetoder, for å verifisere en bruker eller enhet. F.eks. i nettbanken hvor man må skrive inn personnummer, engangskode og eget passord. Dette er nettopp for å bekrefte at det er en legitim bruker som prøver å få tilgang til visse ressurser. Er dette noe som kan anvendes i vårt tilfellet?

Access control og autorisering

Dette er begreper som brukes litt om hverandre hele tiden. Egentlig går de ut på ganske forskjellige ting. Det er ikke slik at Access control er det samme som authorization.

Hva er autentisering?
Autentisering er prosessen som blir brukt for å forsikre om at en person, bruker eller et system. Når en person har blitt autentisert får han/hun en autorisering.

Hva er autorisasjon?
Nivået av autorisasjon en skal gi til en bruker er fast bestemt ved å undersøke flere egenskaper (metadata) tilknyttet brukeren. For eksempel så

[17](Jemima Kiss, 2016)
[18](Wikipedia, 2017)

kan data tilknyttet en bruker indikere om de er medlem av en gitt gruppe som 'kunde' eller 'administrator', eller det kan indikere at de har et betalt medlemskap for en gitt tjeneste, eller det kan indikere at de fortsatt er i en 90 dagers prøveperiode, listen er lang. Autorisasjon inkluderer også 'authorization management', dette er et system som gir funksjonaliteten til å lage autorisasjonsregler. For eksempel så kan det gi en administrator lov til lage en regel som tillater andre brukere å redigere og publisere innhold til en nettside. 'Authorization management' bruker ofte grupper, roller, privilegier og tillatelser for å definere disse reglene.

Hva er access control?
Access control er prosessen av å håndheve den nødvendige sikkerheten for en bestemt kilde. Med en gang vi vet hvem brukeren er og hvilket autorisasjonsnivå brukeren har og det er bestemt hva vi skal/ikke skal gi brukeren tilgang til, så må vi fysisk sette disse sperrene slik at brukeren ikke får tilgang til noe han egentlig ikke skal. Mangel på tilstrekkelig access control er oftere grunnen til sikkerhets sårbarheter i applikasjoner enn defekt autentisering- og autorisasjon mekanismer. Dette simpelt fordi access control er mer komplekst å implementere og blir mer komplekst med applikasjonen som også blir mer komplekst fordi den blir sikret.

I vår situasjon hvor det er snakk om kjøretøy, er det ikke noen form for "user authentication". Hvis man har nøklene til den bil og setter seg inn i den trenger du ikke å taste inn ett passord før du begynner å kjøre. Dette er i og for seg greit nok. Det som dog burde passes på er at kommandoene som kommer til CAN-bussen faktisk kommer fra bilen, og ikke en hacker som sitter hjemme i leiligheten med en laptop. Et ID nummer som øket med 1 for hver kommando er kanskje ikke sikkert nok.

Hacking av et fly

Vi har vist mye til biler og eksemplifisert mye med biler, men hva med andre kjøretøy? Som nevnt tidligere er fly blitt utrolig automatisert, men har denne automatiseringen samt tilføring av underholdnings systemer gjort flyene sårbare for hacking?

En mann ved navnet Chris Roberts, hevder å ha klart å hacke seg inn til flyets 'Thrust Management Computer' via flyets underholdningssystem. [19] Da han var inne, utførte han en "climb command" som førte til at en

[19](Kim Zetter, 2015)

av flyets motorer begynte å "klatre" som førte til at det bevegde seg mot siden. Peter Lemme, en mann som var en av hoved ingeniørene for Boeings 'thrust management system' fram til 1989, sier at det er kun mulig å gjøre dette på begge motorene samtidig, ikke splittet. Han legger også til at den eneste måten man kunne ha hacket seg inn til TMS ville vært ved å få tilgang til boksen som har systemet for så å omprogrammere det, hvor det allerede er massevis av sperrer for å sørge for at systemet ikke kan endre seg under en flight. Han avkrefter også Roberts påstand om å ha kommet seg inn til TMS'en gjennom flyets underholdningsportal.[19] Det stemmer at underholdningsportalen er knyttet til flyets system, hvor den får data om flyets høyde og posisjon sendt til seg og vist på skjermen til passasjeren. Den eneste haken til påstanden til Roberts er at data bussen er 'output only', som vil si at underholdningsportalen kun kan motta data, ikke sende noe til flyets system.[19]

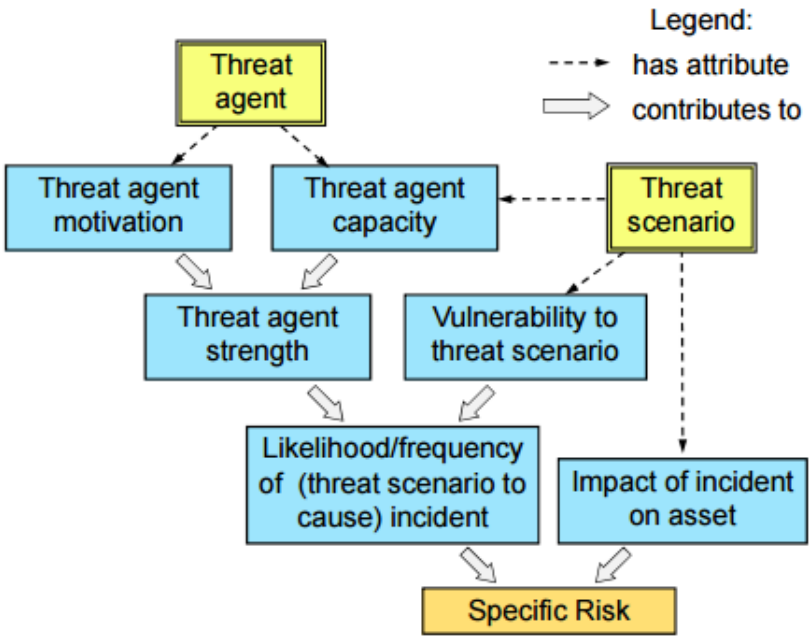
Roberts har også hevdet å finne sårbarheter i flyenes satellittkommunikasjon systemer.[19] Sårbarhetene muliggjorde han å hoppe fra SATCOM (satellittkommunikasjon systemet) til underholdningsportalen også videre til kontrollene i kabinen. Kommandoene han mente han kunne utføre etter dette var å utløse oksygenmaskene. Lemme avkrefter dette også.[19] SATCOM er vanligvis plassert i taket bakerst i flyet og tilkoblet via kabler til avionikken som er lokalisert under cockpiten. All kommunikasjon mellom avionikken, SATCOM og underholdningsportalen skjer gjennom separerte radiokanaler. Noen radiokanaler er for passasjerene, andre for pilotene. Disse er 'air-gapped' og krysser hverandre overhodet ikke, sier Lemme. Derfor mener han at denne teorien ikke er troverdig.[19]

Ingen i skrivende stund har klart å hacke et fly. Alle påstandene til Roberts har blitt avkreftet av legitime kilder.[19] Det er ikke vanskelig å forstå hvorfor sikkerheten til flyets systemer er så sikre, hvis en hacker skulle fått kontroll over flyet kan det ha katastrofale konsekvenser.

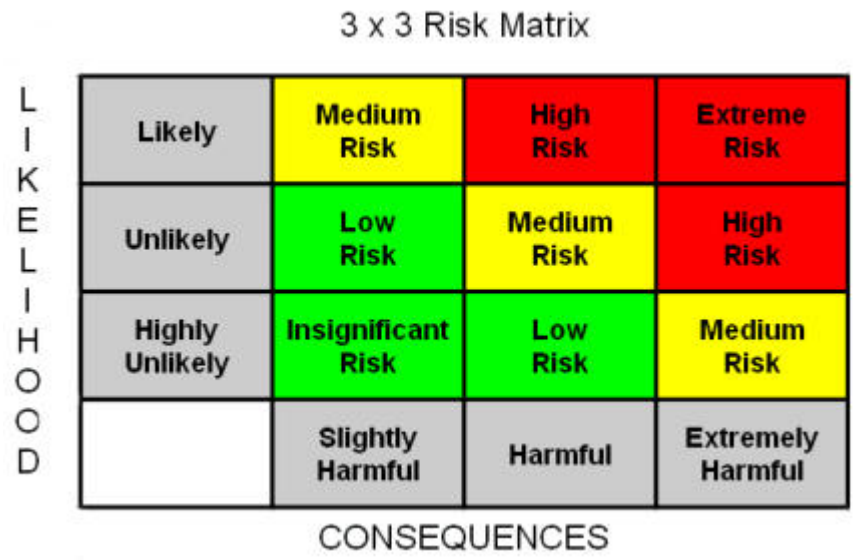
Risikovurdering

Det er helt klart at vi må tenke på sikkerheten rundt denne nye teknologien, men hva er egentlig sannsynligheten for at et slik angrep skjer, og hvor skadelig kan det potensielt være? Vi kan ta en titt på en spesifikk risiko modell, som vi ser under.

[19](Kim Zetter, 2015)



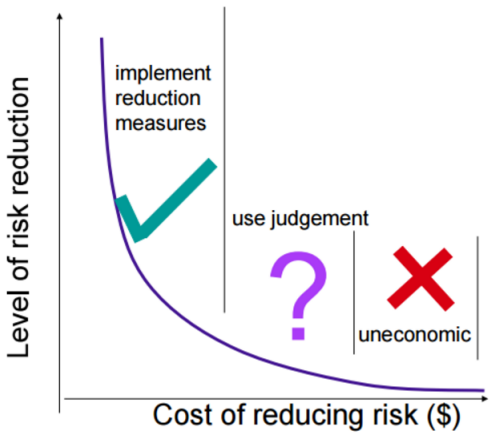
Vi kan begynne nederst i modellen. Den spesifikke risikoen avhenger av sannsynligheten for et angrep og hvor stor skade det vil potensielt gjøre. Sannsynligheten avhenger igjen av hvor fragilt systemet er, og styrken til angriperen. Angriperen sin styrke avhenger igjen av dens motivasjon og kapasitet. Vi kan forenkle hele modellen, og si at størrelsen på en risiko består av to komponenter, sannsynligheten og konsekvenser (probability and impact). Ut ifra disse to faktorene kan vi generere denne kjente risiko evaluerings matrisen. Her kan vi se et nokså simpelt diagram som beskriver denne risikoen.



Som vi ser er den totale risikoen en kombinasjon av de to faktorene. I vårt tilfellet handler det om den potensielle risikoen når en angriper angriper systemet hos et kjøretøy. Vi kan ta et generelt eksempel og se på et tilfelle hvor en hacker prøver å få kontroll over et kjøretøy slik som med jeep'en vi har snakket om tidligere. I dag faller vi kanskje i boksen "Highly Unlikely" når det kommer til sannsynligheten for at dette skjer. Mens når vi ser på konsekvensene av dette kan vi fort ende i boksen "Extremely Harmful". Hvis noe slikt skjer kan det fort få fatale konsekvenser. Hvis vi da tar hensyn til disse to faktorene ender vi kanskje med en middels høy risiko. Dette er som sagt et veldig generelt og vagt scenario som vi vurderer risikoen til. Når man driver med risikovurdering jobber vi ofte med mye mer konkrete risikoer.

Det vi kan se fra diagrammet under er at hvis kostnadene blir for høye og risikoen reduseres for lite, er det rett og slett ikke økonomisk gunstig å gjøre tiltak. Hvis man dog har en ekstremt høy risiko som også koster mye å utbedre blir det kanskje vanskelig å ta avgjørelser.

Det er veldig fristende å kanskje da se den andre veien, og ikke gjøre noe med dette. I ettertid når man har blitt utsatt for et angrep virker kanskje dette ikke like smart. I vårt tilfelle hvor det er snakk om sikkerheten rundt autonome biler finnes det mange risikoer som ville havnet i "very high" boksen under "consequences" i risikomatrisen vår. Det er da viktig å ta hensyn til dette, selv om det kanskje vil påføre litt ekstra uønskede kostnader.



Hvem har ansvaret?

Hvis det skulle skje en ulykke av noe slag, er det ikke alltid like lett å si hvem som har ansvaret. Det er veldig lett for pårørende å gi bilprodusenten skylden, men dette er kanskje ikke alltid tilfellet. På nettsiden til Tesla skriver de helt tydelig at det er sjåføren som bruker autopilot som er ansvarlig.

> "Tesla Autopilot functions like the systems that airplane pilots use when conditions are clear. The driver is still responsible for, and ultimately in control of, the car." [20]

Selv om det ikke forventes at autopiloten skal feile, er det ingen dum ide av Tesla og skriver dette. Antageligvis er akkurat dette også en del av "Terms and conditions" når du kjøper bilen, men disse klarte vi ikke å få tilgang til. På denne måten klarer de i hvertfall å frasi seg noe ansvar. Et annet spørsmål er hvem som har ansvaret hvis bilen din blir hacket, og styrt ut i grøften ved siden av veien. Det er til nå et ganske utenkelig scenario, og om dette er tatt hensyn til i "Terms and conditions" hos bilprodusenter

[20] (The Tesla Motors Team 2015)

er ganske tvilsomt. Det bilprodusentene kanskje er mer tvilsomme til er såkalte tredjeparts etter-produksjons modifikasjoner. I disse tilfellene har de lite kontroll over hva som skjer, og vil derfor ikke sitte igjen med ansvaret heller.

MISRA (The Motor Industry Software Reliability Association) har visse standarder og retningslinjer som skal følges av produsentene. Art Dahnert (managing consultant at application security firm Cigital) sier; "There are some standards like MISRA and a couple of other guidelines that some manufacturers require of suppliers, but that needs to happen a lot more universally and at a much stricter level." [21]

Som denne industrien vokser, er det ingen tvil om det bør stilles strenge og konkrete krav til sikkerheten også. Hvem som dog har ansvaret hvis en ulykke inntreffer, er vanskelig å svare på i dag. Dette kommer veldig an på situasjon til situasjon. Hvis rett og slett det er en svakhet i software til en produsent, som lar en angriper bryte seg inn, er det naturlig å tenke seg at produsenten også er ansvarlig. Hvis man på den andre siden har benyttet seg av f.eks. tredjeparts etter-produksjons modifikasjoner som åpner døren for en hacker og ikke er godkjent av produsenten, er det ikke like lett å si hvem som er ansvarlig.

Konklusjon

Det har ikke vært et tilfelle hvor et kjøretøy (annet enn Jeep eksempelet) har blitt hacket og tatt styring over. Dette skyldes en blanding av godt fokus på sikkerhet blant produsentene, nøye testing av tryggheten til softwaret og at det å hacke kjøretøy for ransomware ikke er lukrativt nok til å trumfe de mest populære målene når det gjelder hacking. Slik ting er nå er risikonivået for ulykker størst når det gjelder feil i bilens software kontra hacking. Når det gjelder tryggheten til softwaret til de selvkjørende kjøretøyene er det vanskelig å komme med et standpunkt. Her vil nok hva som blir definert som trygt variere fra person til person. Noen vil kanskje mene at hvis antall ulykker forårsaket av feil i software til selvkjørende biler er lavere enn antall ulykker forårsaket av sjåfører så kan det anses trygt nok, andre vil kanskje mene at så lenge ulykker grunnet software feil inntreffer i det hele tatt så er det ikke trygt nok.

[21] (Hillary Tuttle 2017)

Automatiserte biler er en stadig utviklende prosess, det meste er tatt høyde for, men noen ganger vil hendelser som er vanskelig (kanskje umulig) å forutse inntreffe (som kumlokk hendelsen til Google bilen). Sannsynligheten for at slike hendelser inntreffer er riktignok minimal.[22] Men etter slike hendelser blir softwaret utbedret og produsentene tar læring fra det.[22]

En god regel for å minimere skadeomfanget samt risiko for en ulykke av uforutsette hendelser er å be sjåføren alltid være klar til å ta over, så hvis en situasjon skulle oppstå hvor autopiloten i bilen ikke 'forstår', kan sjåføren håndtere den. Dette er riktignok noe blant annet Tesla ber sjåførene om å gjøre.

Litt av skeptisismen rundt det å la en datamaskin ha fullstendig kontroll over styringen til en bil skyldes kanskje at folk overvurderer sine egne evner til å kjøre bil, at det at man selv har kontroll gir en slags illusjon av falsk trygghet. Her ligger trolig en av de større utfordringene rundt automatiserte kjøretøy, overbevise folket om at sikkerheten og tryggheten er i henhold. Hvordan vil folk reagere på et fly uten piloter? Eller en bil uten ratt og pedaler? Dette er problemstillinger firmaer som vil gjøre selvkjørende kjøretøy kommersielt ta stilling til.

Veien videre

Til syvende og sist, hvis vi kun ser på statistikken taler den i favør til autonome biler når det kommer til trygghet. Elon Musk(CEO for Tesla) sier selv at det er opptil 38%(basert på antall miles før dødlig krasj)[3] tryggere å kjøre med Tesla sin autopilot enn å kjøre bilen selv. Det er ingen tvil om at tryggheten til disse bilene begynner å komme på plass, men hvordan er sikkerheten?

De siste årene har bilindustrien utviklet seg enormt, og det forventes ikke at det stopper. Når bilene utvikles med alle sine nye funksjonaliteter, er det som sagt også ekstremt viktig å tenke på risikoaspektene rundt det. Om kanskje ikke alt for mange år består veiene av et flertall autonome biler, som kommuniserer med hverandre og er koblet opp mot nettet. Hvis sikkerheten ikke er tilstrekkelig på plass i et slikt scenario kan dette ha ekstremt uheldige konsekvenser. Sikkerheten rundt biler har ikke vært et stort tema tidligere,

[22](McFarland, 2016)

og dette av god grunn. Hvis vi ser på biler for 10 år siden var det noen helt andre maskiner. Slik industrien utvikler seg i dag, er det på tide å begynne ta sikkerheten på alvor også.

Til nå har det ikke vært noen kjente tilfeller av kjøretøy som har blitt hacket av noen med onde intensjoner. Det eneste tilfellet vi har sett til nå white hat hackerne som hacket jeep'en. Det de riktignok har bevist er at det ikke er umulig. Hvis de klarer det, er det ikke tvil om at noen med andre intensjoner også klarer det.

Kilder:

[1] https://en.wikipedia.org/wiki/Autopilot
Autopilot (Wikipedia, 26 April 2017)

[2] http://www.driveuconnect.com/features/uconnect_access/ *Uconnect webpage, 2017*

[3] https://cleantechnica.com/2016/06/30/1st-tesla-autopilot-fatality-130-million-miles/
1st Tesla Autopilot Fatality ... After 130 Million Miles (Zachary Shahan, June 30th, 2016)

[4] https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html
Tesla's Self-Driving System Cleared in Deadly Crash (Neal E. Boudette JAN. 19, 2017)

[5] https://www.tesla.com/blog/your-autopilot-has-arrived
Your Autopilot has arrived (The Tesla Motors Team, October 14, 2015)

[6] http://www.tv2.no/a/8671663/
Nyhet fra Tesla: Alle bilene skal være selvkjørende (Vegard Møller Johnsen, 20.10.2016)

[7] https://www.washingtonpost.com/news/innovations/wp/2016/02/29/for-the-first-time-googles-self-driving-car-takes-some-blame-for-a-crash/?utm_term=.f369a1e5a6b2
For the first time, Google's self-driving car takes some blame for a crash (Matt McFarland, February 29, 2016)

[8] https://www.dmv.ca.gov/portal/wcm/connect/3946fbb8-e04e-4d52-8f80-b33948df34b2/Google+Auto+LLC+02.14.16.pdf?MOD=AJPERES
Report of traffic accident involving an autonomous vehicle

[9] http://www.govtech.com/transportation/Google-Autonomous-Car-Experiences-Another-Crash.html
Google Autonomous Car Experiences Another Crash (Vishal Mathur, juli 17, 2015)

https://www.wired.com/2016/02/googles-self-driving-car-may-caused-first-crash/
Google's Self-Driving Car Caused Its First Crash (Alex Davies, 29.02.2016)

[10] https://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control
Jeep owners urged to update their cars after hackers take remote control (Samuel Gibbs, 21 July, 2015)

[11] http://www.ti.com/lit/an/sloa101a/sloa101a.pdf
Introduction to the Controller Area Network (CAN) (Steve Corrigan, August 2002–Revised July 2008)

https://en.wikipedia.org/wiki/CAN_bus
CAN bus (Wikipedia, 20 April 2017)

[12] https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security
Car hacking is the future – and sooner or later you'll be hit (Alex Hern, 28 August 2016)

[13] http://www.ioti.com/security/short-guide-preventing-cars-being-hacked
A Short Guide to Preventing Cars from Being Hacked (Brian Buntz 01 Jun, 2016)

[14] http://www.autonews.com/article/20120930/OEM01/120929845/automakers-grapple-with-rising-tide-of-industrial-espionage
Automakers grapple with rising tide of industrial espionage (Vince Bond Jr. September 30, 2012)

[15] https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election
What we know about Russia's interference in the US election (Luke Harding 16 December 2016)

[16] http://nordic.businessinsider.com/wikileaks-claims-cia-mi5-hacked-samsung-smar=UK&IR=T
Wikileaks claims the CIA hacked into Samsung smart TVs and used them as secret microphones (Rob Price 07 Mar 2017)

[17] https://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw
Your next car will be hacked. Will autonomous vehicles be worth it? (Jemima Kiss 13 March 2016)

[18] https://en.wikipedia.org/wiki/Ransomware
Ransomware (Wikipedia 19 April 2017)

[19] https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/
Is It Possible for Passengers to Hack Commercial Aircraft? (Kim Zetter, 05.26.15)

[20] https://www.tesla.com/blog/your-autopilot-has-arrived
Your Autopilot has arrived (The Tesla Motors Team, October 14, 2015)

[21] http://www.rmmagazine.com/2017/02/01/hacking-cars/
Hacking Cars (Hilary Tuttle, February 1, 2017)