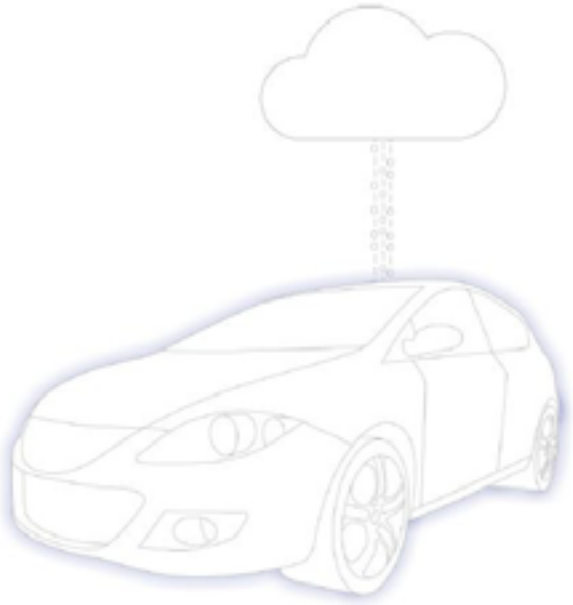
Case story: Detekterar och förebygger intrång

Fokus: Informationssäkerhet i bilar

2015 startade Bosch sin verksamhet i Lund, då var de bara 10 personer men växte snabbt till 100 killar och tjejer. Numera har de 8 affärsenheter i Lund.

Richard Baumbach, Program Manager och mjukvaruarkitekten Johan Simonsson jobbar på avdelningen Escrypt, för security inom Automotive. De tar fram mjukvarulösningar som kan användas för att höja informationssäkerheten i bilar så att hackare inte kan komma åt mjukvaran och ta över, fjärrstyra eller riskera säkerheten. Försöker någon göra intrång i mjukvaran varnas biltillverkaren via molnet.

"Utvecklarna uppskattar att de inte har en manuell testorganisation som sitter och trycker på knappar."



"Första utmaningen var att ta fram en produkt och ha den färdig och testad inom ett år. Vi arbetade agilt för att ta fram en prototyp, men redan efter ett halvår fick vi ett uppdrag från en kund och övergick därför snabbt till att göra en kundrelease istället. Resultatet blev mycket uppskattat och vi demade för olika biltillverkare som blev mycket intresserade och på den vägen är det", berättar Richard, en av de första som startade upp kontoret i Lund.

Escrypt arbetar agilt och det kan ibland krocka med bilindustrins arbetssätt. För att tillmötesgå biltillverkarnas arbetssätt dokumenterar man allt för att kunna visa att man uppfyller alla nivåer genom att dokumentera allt, även vad som blivit testat. Escrypt har tagit hjälp av en expert från bilindustrin som hjälper dem att gå igenom processens alla delar och sätta dem en efter en.

Bosch styrenheter hittar du i många olika bilmodeller

ECU (Electronic Control Unit), styrenheter, berättar vad som ska göras i bilen. Det kan finns mellan 40-80 ECU från olika leverantörer i en bil, beroende på bilmodell och Boschs styrenheter finns i många olika bilmodeller.

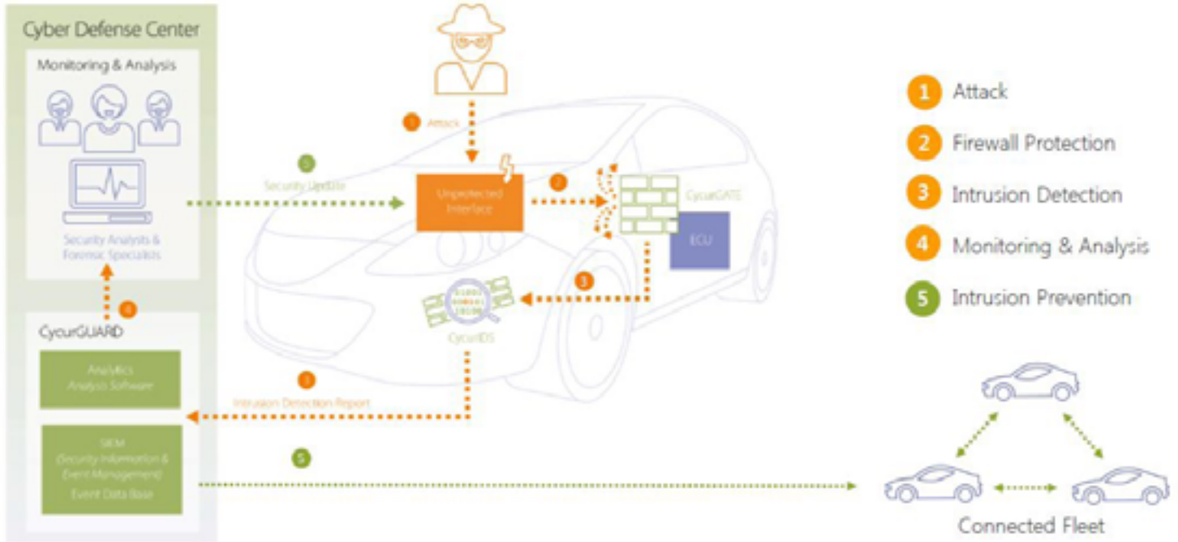
Stoppar cyberattacker

"Hackarna utvecklar ständigt nya cyber-attacker för att ta kontroll över nätverket i en bil, det gäller för tillverkarna att hålla jämna steg. Tack och lov är det inte helt enkelt att hacka en bil, man måste verkligen vet vad man gör", berättar Johan.

Traditionella it-miljöer har brandväggar, men i 4:e generationens brandväggar finns det något som heter IDPS (Intrusion Detection and Prevention Systems). IDPS lyssnar på en lina och kontrollerar om allt verkar normalt eller inte. Den visar vilken sannolikhet det är för intrång och om det finns risk för en attack skickas en rapport till experter som avgör om det är ett riktigt hot och vilken åtgärd som behöver vidtas. Allt går via en server i molnet, vilket gör att man kan se om attacken gäller fler än en bilmodell och då förebygga intrång på flera bilar samtidigt. Se figuren på nästa sida.

Värde 1: Automatisera arbetet forts.

Richard Baumbach och Johan Simonsson



Escrypt jobbar enligt Continuous Integration, vilket innebär automatisering av utvecklingsarbetet, som i slutänden sparar massor med tid och pengar.

För att uppnå en så hög automationsgrad som möjligt i de första stegen, är hela utvecklingsnivån baserad på en intern Linux distribution som Bosch har i huset, Open Source desktop. Den är baserad på Ubuntu 16.04 LTS och är anpassad efter Boschs nätverk. Detta är en är en av de grundläggande komponenterna till att de lyckas uppnå önskad automationsgrad och ett väldigt flexibelt system så fort.

”Det kan vara rätt så komplicerat att automatisera, men med Johans erfarenhet från tidigare jobb på ett Telecom företag, har det gått mycket bra och det har verkligen varit värt det”, berättar Richard. *”Utvecklarna uppskattar att de inte har en manuell testorganisation som sitter och trycker på knappar”,* säger Johan.

Värde 2: Enhetstest och Statisk kodkontroll

Bilindustrin har extremt höga krav för testtäckning. För att uppnå kraven kör Escrypt bland annat enhetstester och statisk kodkontroll med verktyg från tex. PRQA. De uppnår därmed 100% testtäckning.

”Vi har sammanfört dessa två ***värde****, extremt höga automationskrav samtidigt som vi har väldigt höga krav på att allt verkligen blir testat. En testdriven utvecklingsmetodik där man pushar unit test och sin kod samtidigt”,* berättar Johan.

Verktygskedjan

Första steget är att börja med källkoden enligt Test Driven Development, där de tar fram unit test och källkod tillsammans och bygger upp den på C-funktions nivå. Denna kod är uppdelad i ett antal små logiska moduler som de kompilerar och kör på PC:n eller korskompilerar för alla target de har stöd för.

Varje modul i sin tur testar de med lite kod i början för att få den att snurra på target. Tillsammans med en JTAG kan man flasha ner och få tillbaka resultat om testkoden fungerade på den specifika arkitekturen. Här kommer de använda ett Phyton script som via ett färdigt API kommer styra Lauterbach.

”Vi valde Lauterbach som har bra PC-stöd för både Linux och Windows men även bra nivå av hårdvarustöd”, säger Johan.

Andra steget är Integrationstest och test av komponenten i sin helhet. Komponenten är extremt flexibel, där Escrypt har sitt konfigurationsverktyg vid sidan som genererar all dynamisk minneshantering till själva biblioteket. Med Escrypts konfigurationsverktyg kan kunden själv konfigurerara hur IDS-modulerna ska bete sig mot den specifika målgruppen. De tillsammans kompilerar man på PC och korskompilerar för alla targets och varje binär i sin tur flashas på hårdvaran.

Tredje steget är Systemtest och Processor In the Loop (PIL), när man verkligen testar på en targetenhet på kundens ECU. Escrypt använder flashningsmöjligheten men läser även ut testrapporterna från de interna strukturerna inne på ECUn. ECUn matas med kopiösa mängder data, både bra och dålig. Därefter detekteras de villkor som bestämts skall detekteras. Till detta planerar Escrypt att ta hjälp av Lauterbach.

”Dessa tre steg, startar från Jenkins i olika sammanhang utan att de individuella teammedlemmarna behöver göra någonting. När de har pushat in kod i systemet, kommer systemet att triggas och köra igång automatiskt”, berättar Johan.

Continuous Delivery

”Eftersom vi har 100% testtäckning av koden, har vi tagit steget fullt ut och gått vidare från Continuous integration till Continuous Delivery. Så när vi har gått igenom de automatiserade testerna, vet vi att dokumenten är skapade och att kvalitetsnivåerna är uppfyllda och redo att skickas till en Integratör som i sin tur startar nästa steg. Detta innebär att man kör i målsystemet tillsammans med de andra byggklossarna i ett specifikt system”, berättar Johan.

Av: Maria Gustavsson

www.nohau.se