Integritetsverifikation inom Inbyggda System

Uppdragsbeskrivning inför Examensarbete

Axel Blomén & Douglas Fjällrud

2026-01-11

Innehållsförteckning

Bakgrund

Codiax AB är ett företag verksamma inom inbyggda system. De har en bred kompetensprofil och utvecklar driftsäkra system inom allt från medicintekniska lösningar till domänspecifik telemetri inom industriella processer.

Syfte

Vårt mål är att assistera Codiax Sweden AB i att möta kunders allt mer uppmärksammade säkerhetskrav. I moderna system är säkerhet ett kontinuerligt arbete snarare än en ursprunglig egenskap. För att säkerställa långsiktig kvalitet krävs därför rigorösa rutiner och metoder för att löpande verifiera, validera och testa produkter i bruk.

Problemformulering

I sammankopplade inbyggda system är det viktigt att genomföra uppdateringar i säkerhetssyfte. Dessa uppdateringar levereras rutinmässigt via mekanismer som inte kräver fysisk tillgång till målenheten. Dessa mekanismer implementeras ofta genom säkra kanaler, trots detta kräver vår hotbild säkerhet i flera lager.

När uppdateringen sedan landar är det önskvärt att genomföra vissa automatiserade kontroller gällande mjukvarupaketets authenticitet och integritet.

Det är även viktigt att målenheten i standardoperation kontrollerar vitala delar av filsystemet för att itendifiera eventuella intrång.

Det är avgörande att dessa säkerhetsegenskaper implementeras i linje med kundens säkerhetsmässiga krav, och förhåller sig till vederbörande kravspecifikation.

Mål

Det slutgiltiga systemet skall med hjälp av metoder som systematiskt verifierrar maskinvarans integritet samt autenticitet kunna hantera felsituationer på ett lämpligt sätt, beroende på applikationsdomän.

Systemet skall vara framtidssäkert och lätt att underhålla. Det ska förhålla sig till etablerade standarder inom såväl kryptografi som applikation, samt på ett effektivt och idiomatiskt sätt bemöta och behandla de säkerhetskrav som iscensatts av kundens hotbild.

Avgränsningar

Vår implementation är initialt plattformsspecifik då arkitekturer och processorarkitekturer tillhandahåller olika mekanismer för dessa typer av rutiner. Möjligheter att utöka vår implementation till andra tillverkare existerar, men initialt så fokuserar vi på den plattform som står i fokus.

Resurser

Eftersom vår implementation initialt kommer att vara plattformsspecifik kommer vi konsultera dokumentation från vår huvudsakliga chip vendor, NXP. Även Yocto har övergripande dokumentation rörande ämnet. Vår bootloader, u-boot, kommer att behöva undersökas för att göra implementationen mer generell. Vi kommer att använda oss av de specialister anställda vid Codiax Sweden AB i Stockholm.

Tidsplan

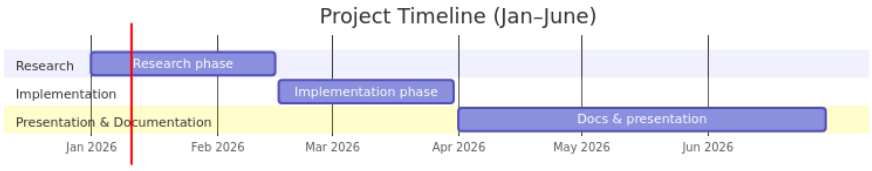

Figure 1: Ganttschema