

EXAMENSARBETE Exploring the extended software bill of materials**STUDENTER** Andreas Bergqvist, Karl-Philip Ble Cato**HANDLEDARE** Lars Bendix (LTH), Jonas Stigeberg (ABB), Christer Wibom (ABB)**EXAMINATOR** Emelie Engström (LTH)

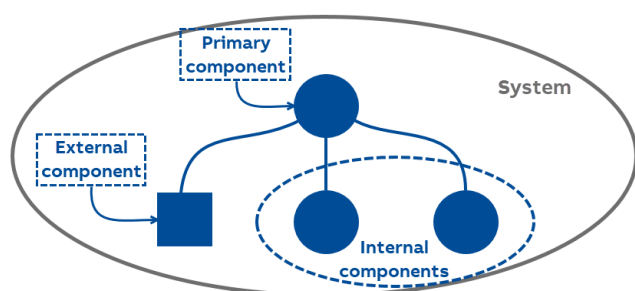
eSBoM: En skräddarsydd mjukvarulista

POPULÄRVETENSKAPLIG SAMMANFATTNING Andreas Bergqvist, Karl-Philip Ble Cato

Vi har i detta projekt identifierat nyckeldatapunkter och potentiella användningsområden för en Software Bill of Materials, SBoM, samt tagit fram ett förslag om en skräddarsydd SBoM, anpassad för användarens behov och omständigheter.

Under de senaste åren har antalet attacker på digitala komponenter genom mjukvarukedjan ökat markant, år 2024 upptäcktes över 700,000 skadliga paket.

SBoM:en i ett vardagsscenario: Tänk dig att du står vid ett buffébord, där ligger flera olika maträtter och du ska sammanställa en tallrik. Vid varje maträtt ligger en ingredienslista som hjälper dig ta hänsyn till eventuella allergier när du plockar ihop din mat. Modern mjukvaruutveckling fungerar på ett liknande sätt, tallriken med mat är den färdiga produkten, maträtterna är mjukvarukomponenter, allergierna är sårbarheter, SBoM är ingredienslistan.



Vi har i vårt arbete identifierat vilka datapunkter som är relevanta för anställda på ABB för att de ska kunna genomföra sina programmeringsrelaterade arbetsuppgifter. Därefter har vi definierat vad en SBoM ska innehålla för datapunkter för att uppfylla juridiska krav ställda av

USA och EU, vår definition kan ses som en standard och användas som utgångspunkt för alla som är intresserade av att implementera en SBoM. De datapunkter som ligger utanför standarden kallar vi utökade datapunkter, och när dessa inkluderas i en SBoM kallar vi den för en extended SBoM, eller eSBoM. Dessa utökade datapunkter som genom att inkluderas i ingredienslistan kan underlätta vid mjukvaruutveckling. Från våra datapunkter har vi sammanställt en lista med användningsområden för denna utökade ingredienslista. Vi har även i projektet bevisat att en eSBoM är mer än bara ett koncept genom att skapa en proof of concept som kan användas på ett av våra utökade användningsområden.

Under arbetets gång har vi funnit användningsområden inom utvecklingsprocessen för den SBoM som kommer behöva genereras. Med anledning av detta har vi argumenterat för att skapandet ska ske tidigt, istället för sent i projekttidslinjen, så att SBoM:en kan följa med komponenten. Vår förhoppning är att vårt arbete leder till att fler företag implementerar en SBoM tidigt i sina projekt, och därigenom ökar sin spårbarhet och transparens internt och förstärker informationsutbytet mellan olika professioner på olika avdelningar. Vi vill att en SBoM ska få ta sin roll som en självklar datastruktur i varje projekt, och därigenom bli ett verktyg som används internt, såväl som externt.