

EXAMENSARBETE Exploring the extension of Software Bill of Materials Usage**STUDENTER** Andreas Bergqvist, Karl-Philip Ble Cato**HANDLEDARE** Lars Bendix (LTH), Jonas Stigeberg (ABB), Christer Wibom (ABB)**EXAMINATOR** Emelie Engström (LTH)

Utökande av SBoMs roll och användning

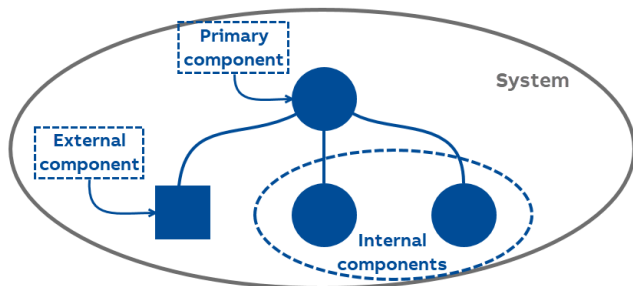
POPULÄRVETENSKAPLIG SAMMANFATTNING **Andreas Bergqvist, Karl-Philip Ble Cato**

Vi har i detta projekt identifierat nyckeldata punkter 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.

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.

Under de senaste åren har antalet attacker på digitala komponenter ökat markant. År 2024 upptäcktes över 700,000 infekterade filer.

Bilden nedan visar ett system med fyra komponenter, där den översta bygger på funktioner från de tre nedre. En SBoM för detta system skulle då innehålla information om alla inkluderade komponenter.



Vi har i vårt arbete identifierat vilken information som är viktig för mjukvaruingenjörer på

ABB för deras programmeringsrelaterade arbetssuppgifter. Därefter har vi definierat vad en SBoM ska innehålla för data punkter 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 skapa en SBoM. Den information som ligger utanför standarden kallar vi utökade data punkter, och när dessa inkluderas i en SBoM kallar vi den för en extended SBoM, eller eSBoM. Dessa utökade data punkter som genom att inkluderas i ingredienslistan kan underlätta vid mjukvaruutveckling. Från våra data punkter har vi sammanställt en lista med användningsområden för denna utökade ingredienslista. Vi har även i projektet testat att skapa och använda en eSBoM.

Under arbetets gång har vi funnit nya användningsområden för den SBoM som kommer behöva genereras. Med anledning av detta har vi argumenterat för att skapandet ska ske tidigt, istället för sent i projektet, så att SBoM:en kan vara tillgänglig hela vägen. 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 såväl internt som externt.