Binärt reproducerbara mjukvarubyggen

Av Henrik Lenger

Motivation:
För att upprätthålla hög assurans i våra produkter, behöver vi på ett övertygande sätt kunna påvisa att en viss kompilerad binärkod verkligen härrör från viss underliggande källkod.

Problemställning:
Ett intuitivt sätt att verifiera en viss binär, vore att helt enkelt kompilera koden igen, och jämföra resultaten. Dock introducerar de flesta förekommande kompilatorer för byggtillfället specifik information i de resulterande binärerna (typiskt tidsstämplar, eller annan miljöspecifik information.) Två binärer, som kompilerats från samma källkod, men vid olika tillfällen, kommer därför med hög sannolikhet innehålla skillnader. Att i detalj undersöka varje skillnad, för att manuellt bedöma vilken påverkan den eventuellt kan ha, upplevs inte som realistiskt. Vi vill istället undersöka möjligheten att genom att manipulera, eller konfigurera, kompileringsprocessen göra den helt binärt deterministisk. Så att den idealt kan repeteras åratal senare, och nå ett identiskt resultat med den ursprungliga kompileringen.

Språk och miljö:
Typiskt skrivs källkod i, i branschen normalt förekommande högnivåspråk, och korskompileras på PC, mot olika inbyggda mål-miljöer.