

TrustSECO - Een Gedistribueerd Grootboek voor Betrouwbaarheidsinformatie in het Software Ecosysteem

UU Slinger Jansen, TrustSECO: Een Vertrouwensinfrastructuur voor een Veerkrachtig Software Ecosysteem

Dit voorstel valt onder de volgende NCSRA III pijlers: Design en Defense

TrustSECO, is een te ontwikkelen infrastructuur in een gedistribueerde ledger voor de versteviging van software package managers. Momenteel is het software ecosysteem vol van (onterecht) vertrouwen. Bij het downloaden van een softwarepakket uit een package manager (zoals npm, de pakketbeheerder voor de programmeertaal JavaScript) verwacht een gebruiker dat dit pakket is geschreven door betrouwbare ontwikkelaars, gecompileerd met een betrouwbare compiler, en geen kwetsbaarheden bevat. In het verleden is echter al te vaak gebleken dat dit vertrouwen onterecht is. In Stuxnet werd bijvoorbeeld een compiler geïnfecteerd die vervolgens elk gecompileerd programma infecteerde. In OpenSSL werd de heartbleed kwetsbaarheid pas maanden na identificatie publiek gemaakt. Met TrustSECO wordt een infrastructuur gebouwd die deze vertrouwensgegevens opslaat, garandeert, en via consensus bevestigt en goedkeurt.