Hans WINDERIX – Abstract van de thesis

Computers zijn niet meer weg te denken uit onze gedigitaliseerde samenleving. Zo zijn we onder meer afhankelijk geworden van computersystemen die instaan voor het beheer van onze vitale infrastructuur en vertrouwen we een toenemend aantal toepassingen privacygevoelige informatie toe. We zouden dan ook mogen verwachten dat ze zich op een juiste en veilige manier gedragen. Jammer genoeg schetst de realiteit een eerder somber beeld als het over de veiligheid van onze hedendaagse computersystemen gaat.

De oorzaak van deze kwetsbaarheden is vaak te wijten aan aannames die ontwikkelaars maken bij het ontwerp en de implementatie van software die niet gelden op het moment dat het programma wordt uitgevoerd door een computer.

Abstractie is een belangrijke techniek om de complexiteit van computersystemen te beheersen. Computerprogramma's worden meestal geschreven in hogere programmeertalen. Deze talen bieden een aantal concepten aan die het ontwikkelaars eenvoudiger moeten maken om de functionaliteit van computerprogramma's uit te drukken en om te redeneren over de eigenschappen van de programma's die ze ontwerpen. Een compiler is een computerprogramma dat de taak heeft om deze concepten (of abstracties) te verlagen naar een voorstelling die geschikt is om uitgevoerd te worden door een machine die helemaal geen notie heeft van de voor mensen gemaakte abstracties.

Deze aanpak heeft echter een aantal nadelen. Bij de vertaalslag tussen die twee werelden verdwijnen een aantal - vaak impliciete - veiligheidsgerelateerde eigenschappen die gelden op het hogere abstractieniveau waarvan de programmeur gebruikt maakt wanneer hij redeneert over de veiligheid van zijn programma. Hierdoor wordt de machinecode kwetsbaar voor aanvallers die interageren met het systeem op het lagere abstractieniveau.

Met veilige compilatie beoogt men om de eigenschappen omtrent veiligheid, die uitgedrukt zijn door concepten in een hogere programmeertaal, te behouden nadat de programma's zijn omgezet naar uitvoerbare machinecode. Deze techniek laat ontwikkelaars toe om na te denken over de veiligheid van computertoepassingen op een comfortabel abstractieniveau.

De masterscriptie van Hans Winderix onderzoekt de haalbaarheid van een open platform voor veilige compilatie waar de veiligheidseigenschappen expliciet en op een generieke manier op de verschillende abstractieniveaus kunnen worden voorgesteld en verwerkt. Een platform waar gemeenschappelijke modellen en algoritmes tal van programmeertalen en computerarchitecturen ondersteunen.

De belangrijkste bijdrage van zijn thesis is een voorstel voor zo een eengemaakt platform. Hij ontwikkelde een prototype dat de eigenschap van isolatie, uitgedrukt in de C en Rust programmeertalen, bewaart na compilatie naar Sancus en Intel SGX, twee veiligheidsarchitecturen die hardware primitieven aanbieden om de abstractie van isolatie op een efficiënte te kunnen behouden na compilatie.