New Foundations for Separation Logic

Hiep, H.A.

Samenvatting

Titel:

Nieuwe fundamenten voor separatielogica

Het onderzoek dat in dit proefschrift wordt gepresenteerd betreft één van de meest belangrijke vragen in programmatuurkunde op dit moment: hoe zorgen we ervoor dat software geen geheugenbeveiligingsgaten bevat? Geheugenbeveiligingsgaten zijn de grootste veroorzaker van veelvoorkomende kwetsbaarheden en lekken, en zijn een ernstige bedreiging voor de stabiliteit en veiligheid van onze digitale wereld. Deze vraag is dermate belangrijk dat het is geëscaleerd tot het hoogste niveau. In een recent persbericht van het Witte Huis (26 februari 2024) vraagt de National Cyber Director van de Verenigde Staten de academische gemeenschap om hulp om dit hardnekkige probleem op te lossen:[1]"het aanpakken van [deze uitdaging] is noodzakelijk om te zorgen voor de lange-termijn beveiliging van ons digitale ecosysteem en om onze nationale veiligheid te beschermen." Het bijbehorende rapport adviseert over het gebruik van programmeertalen die geheugenveilig zijn, en geeft nadrukkelijk aan dat gebruik van *formele methoden* leidt naar de zeer gewenste vrijheid van bugs, waaronder de vrijheid van geheugenbeveiligingsgaten.

In dit proefschrift bestuderen we formele methoden voor het analyseren van software op correctheid, waarbij correctheid betekent dat software voldoet aan diens specificatie en incorrectheid betekent dat er een bug schuilgaat. De focus ligt op separatielogica, een formele methode ontworpen als een schaalbare techniek voor het garanderen van vrijheid van geheugenveiligheidsgaten. Vandaag de dag is separatielogica een bewezen wetenschapsgebied: de afgelopen twintig jaar is het uitgebreid bestudeerd binnen de academie, en zijn er tal van succesvolle toepassingen in de industrie waarbij geheugenbeveiligingsgaten worden bestreden. Zo wordt separatielogica als techniek toegepast om met wiskundige zekerheid te bewijzen dat geheugenveiligetalen (zoals Rust en Go) daadwerkelijk de belofte nakomen om "volledige categorieën bugs, niet alleen te mitigeren, maar te vermijden."

In twee delen presenteert dit proefschrift belangrijke wetenschappelijke bijdra-

[1] `https://www.whitehouse.gov/oncd/briefing-room/2024/02/26/press-release-technical-report/`

gen die een kloof in de academische literatuur dicht. Het eerste deel bevat de ontbrekende **volledigheidsstelling voor separatielogica**, dat gelijk staat aan het fundamentele resultaat van Gödel voor de predicatenlogica. Volledigheid is belangrijk voor elke formele methode omdat het laat zien dat de formele methode adequaat gebruikt kan worden, om alles wat valide is te demonstreren. Eindelijk introduceert het tweede deel **dynamische separatielogica**, dat een alternatieve manier geeft voor het analyseren van geheugenbeveiligingsproblemen zodat het nu mogelijk is om basale specificaties te bewijzen zonder extra logische technieken. Dit is belangrijk omdat het 'achterwaartse compatibiliteit' geeft met technieken voor geautomatiseerd redeneren die optimaal werken voor predicatenlogica.