

De Onderzoeksgroep
Software Languages Lab

nodigt U graag uit op de openbare verdediging van het proefschrift van

Laurent Christophe

ter behaling van de graad van Doctor in de wetenschappen

Titel van het proefschrift:

Herkomstbewuste Dynamische Analyse van JavaScript

Promotor:

Prof. dr. Coen De Roover (VUB)

Co-promotor:

Prof. dr. Wolfgang De Meuter (VUB)

dinsdag 27 januari 2026 om 17u

**VUB Etterbeek campus, Pleinlaan 2, Elsene,
Promotiezaal D.2.01**

Live stream:

<https://lachrist.github.io/defence>

Samenstelling van de jury:

Prof. dr. Ann Nowé (VUB, chair)

Prof. dr. Jens Nicolay (VUB)

Prof. dr. Elisa Gonzalez Boix (VUB)

Prof. dr. Michael Pradel (Uni-Stuttgart, DE)

Prof. dr. Tom Van Cutsem (KULeuven)

Curriculum vitae

Ik ben een enthousiaste programmeur en een actieve bijdrager aan open-sourceprojecten. Mijn expertise omvat de implementatie van programmeertalen, functioneel programmeren, reflectief programmeren, gedistribueerde systemen en, meer recentelijk, generatieve AI.

Persoonlijke homepage:

<https://lachrist.github.io>

LinkedIn:

<https://linkedin.com/in/lachrist>

Abstract van het doctoraatsonderzoek

Dynamische programma-analyse, die het gedrag van een programma tijdens uitvoering onderzoekt, is essentieel in domeinen zoals beveiliging en softwareonderhoud. Dit proefschrift richt zich op herkomstbewuste analyse, zoals dynamische taint-analyse, waarbij het noodzakelijk is om te volgen hoe gegevens zich tijdens uitvoering verspreiden. Om analyses onafhankelijk van de uitvoeringsomgeving uit te voeren, is een gangbare aanpak het instrumenteren van de broncode van het doelprogramma. Het ontwikkelen van robuuste instrumentatiegebaseerde analysetools wordt echter belemmerd door drie belangrijke uitdagingen in de meeste beheerde talen: de syntactische complexiteit van de taal bemoeilijkt instrumentatie; optimalisaties in de representatie van onveranderlijke waarden maken het volgen van herkomst moeilijk; en de gedistribueerde aard van moderne toepassingen vereist coördinatie van de analyse.

Dit proefschrift presenteert een nieuw modulair kader om deze uitdagingen te overwinnen voor JavaScript. Om instrumentatie te vereenvoudigen, transpileren we programma's naar een kernvariant. In vergelijking met JavaScript gebruikt deze kernvariant eenvoudigere constructies, vermindert het aantal syntactische knooppunttypes met 57% en slaagt nog steeds voor 99,8% van de officiële JavaScript-conformiteitstest. Om onveranderlijke waarden te volgen, introduceren we een waardegerichte aanpak die primitieve waarden promoot tot transparante referentiewaarden, waarvoor een toegangscontrolesysteem gebaseerd op reflectie nodig is. Vanwege de reflection-API van JavaScript levert deze methode hoge precisie en transparantie op, zij het met een prestatie-overhead. Ten slotte, om de analyse van gedistribueerde toepassingen te coördineren, centraliseren we de analyselogica in een toegewezen proces. Deze architectuur biedt hoge expressiviteit en gemak voor de analyseontwikkelaar, maar brengt extra communicatie-overhead met zich mee.

Dit onderzoek bevordert de stand van de techniek door een modulair kader te bieden voor het bouwen van robuuste instrumentatiegebaseerde tools voor herkomstbewuste analyses in JavaScript.