Onderzoeksvoorstel

Detectie en Beheersing van Privilege Creep binnen RACF op IBM z/OS-mainframes.

Bachelorproef, 2025-2026

Brecht Huys

E-mail: brecht.huys@student.hogent.be
Co-promotor: Nog te bepalen – Synalco

Samenvatting

Toegangsbeheer vormt een belangrijke pijler binnen de beveiliging van IBM z/OS omgevingen, waar RACF wordt ingezet om gebruikersrechten te beheren en de vertrouwelijkheid, integriteit en beschikbaarheid van systemen te waarborgen. Binnen dit domein vormt privilege creep een hardnekkige uitdaging, waarbij gebruikers door functiewijzigingen, tijdelijke taken of het ontbreken van systematische herzieningen toegangsrechten houden die niet langer nodig zijn voor hun huidige rol, wat leidt tot verhoogde beveiligingsrisico's en non-compliance. Dit onderzoek vertrekt vanuit de hoofdonderzoeksvraag hoe privilege creep binnen RACF op IBM z/OS-mainframes kan worden geïdentificeerd, geanalyseerd en technisch beperkt zodat gebruikersrechten in overeenstemming blijven met het least privilegeprincipe. De voorgestelde methodologie combineert documentanalyse van het toegangsbeheerproces, technische analyse van RACF configuratiegegevens en logbronnen, en de ontwikkeling en evaluatie van een technische Proof of Concept met, door realistische testscenario's. Verwacht wordt dat dit onderzoek zal leiden tot een reproduceerbare detectiemethode die overmatige of ongebruikte rechten inzichtelijk maakt en inzetbaar is ter ondersteuning van periodieke access reviews en auditvoorbereiding. Indien deze resultaten worden bevestigd, kan worden geconcludeerd dat een technisch ondersteunde aanpak een effectieve bijdrage levert aan het beheersen van privilege creep en het versterken van security en compliance binnen RACF omgevingen.

Keuzerichting: Mainframe Expert
Sleutelwoorden: RACF, z/OS, Privilege Creep, Access Control, Mainframe Security

Inhoudsopgave

1. Inleiding

Toegangsbeheer is een essentieel onderdeel van informatiebeveiliging binnen organisaties die gebruikmaken van IBM z/OS mainframes. In dergelijke omgevingen wordt RACF (Resource Access Control Facility) ingezet om gebruikers, groepen en toegangsrechten tot systeembronnen te beheren. Door de hoge mate van centralisatie en de bedrijfskritische aard van mainframe systemen is correct en gecontroleerd rechtenbeheer van groot belang voor zowel operationele continuïteit als compliance met beveiligingsstandaarden.

De doelgroep van deze bachelorproef bestaat uit IT professionals die verantwoordelijk zijn voor identity and access management en security binnen z/OS mainframe omgevingen, zoals mainframe security administrators, systeem programmeurs en audit of compliance verantwoordelijken. Deze professionals worden in de praktijk geconfronteerd met complexe RACF configuraties en een groeiend aantal gebruikers en rechten.

Binnen deze context stelt zich het concrete probleem van *privilege creep*. Door functiewijzigingen, tijdelijke opdrachten en het ontbreken van systematische herzieningen behouden gebruikers vaak toegangsrechten die niet langer noodzakelijk zijn voor hun huidige rol. Dit probleem leidt tot verhoogde beveiligingsrisico's, verminderde auditbaarheid en potentiële non compliance. De centrale onderzoeksvraag van deze bachelorproef luidt dan ook: *hoe kan privilege creep binnen het RACF toegangsbeheerproces van IBM z/OS mainframes worden geïdentificeerd, geanalyseerd en technisch beperkt zodat gebruikersrechten in lijn blijven met het least privilegeprincipe?*

De onderzoeksdoelstelling van deze bachelorproef is het ontwikkelen van een technisch onderbouwde oplossing in de vorm van een Proof of Concept die privilege creep detecteerbaar maakt binnen RACF. Naast de geschreven scriptie wordt het onderzoek als succesvol beschouwd wanneer de Proof of Concept in staat is om overmatige of ongebruikte rechten inzichtelijk te maken en bruikbaar is ter ondersteuning van access reviews en security audits.

2. Literatuurstudie

Binnen het domein van identity and access management wordt het principe van least privilege algemeen erkend als een fundamentele beveiligingsmaatregel, waarbij gebruikers uitsluitend toegang krijgen tot de middelen die noodzakelijk zijn voor hun functie (Carter, 2022). In de praktijk blijkt het afdwingen van dit principe echter complex, zeker in omgevingen met langdurige gebruikersaccounts en frequente functiewijzigingen.

Privilege creep wordt in de literatuur beschreven als het geleidelijk opstapelen van toegangsrechten over tijd, vaak als gevolg van organisatorische veranderingen en gebrekkige intrekkingsprocessen (Jain, 2025). Verschillende studies tonen aan dat privilege creep een belangrijke oorzaak is van interne beveiligingsincidenten en auditbevindingen (Romero, 2025). Binnen mainframe omgevingen is dit probleem extra uitgesproken door de fijnmazige en historisch gegroeide toegangsstructuren.

RACF biedt uitgebreide mogelijkheden voor toegangscontrole via gebruikersprofielen, groepen, dataset en resourceprofielen, maar vereist een hoge mate van expertise om deze correct te beheren (Garitano, 2024). Bestaand onderzoek focust voornamelijk op algemene oplossingen of cloudomgevingen, terwijl er relatief weinig aandacht is voor technische detectiemethoden specifiek gericht op RACF configuraties.

Dit onderzoek onderscheidt zich door de focus op een technische analyse van privilege creep binnen RACF en door het ontwikkelen van een concrete detectiemethode in de vorm van een Proof of Concept, in plaats van louter beleidsmatige aanbevelingen.

3. Methodologie

Deze bachelorproef hanteert een toegepaste onderzoeksaanpak waarbij analytische en technische onderzoeksmethoden worden gecombineerd om de deelvragen binnen het probleemdomein en het oplossingsdomein te beantwoorden. In een eerste fase wordt inzicht verworven in privilege creep, het least privilegeprincipe en RACF toegangsmechanismen. Dit gebeurt door een combinatie van literatuurstudie, documentanalyse en data analyse. Hierbij wordt vakliteratuur over privilege creep, toegangsbeheer en beveiligingsprincipes bestudeerd, RACF documentatie en gebruikersprofielen geanalyseerd en configuratiegegevens en logbestanden onderzocht om patronen van overmatige rechten te identificeren. Deze fase beantwoordt de deelvragen: 'Wat is privilege creep binnen RACF?', 'Wat zijn de oorzaken van privilege creep?' en 'Wat is de impact van privilege creep op de organisatie en compliance?

In een tweede fase wordt de technische kant onderzocht door een Proof of Concept te ontwikkelen die privilege creep automatisch kan detecteren. Dit omvat een analyse van gebruikersrechten, groepslidmaatschappen en toegangsprofielen die relevant zijn voor overmatige rechten, gevolgd door het ontwerp en de implementatie van een tool of script dat afwijkende of ongebruikte rechten identificeert volgens vooraf gedefinieerde criteria. De Proof of Concept wordt vervolgens getest met representatieve scenario's en de resultaten worden geanalyseerd op bruikbaarheid, reproduceerbaarheid en bijdrage aan het least privilegeprincipe. Deze fase beantwoordt de deelvragen: 'Hoe kan privilege creep technisch worden opgespoord binnen RACF?', 'Welke methoden en criteria zijn effectief voor het detecteren van overmatige of ongebruikte rechten?' en 'Hoe kunnen deze inzichten gebruikt worden om gebruikersrechten te beperken en in lijn te brengen met het least privilegeprincipe?

In de laatste fase worden de resultaten van de voorgaande fasen geïntegreerd en geanalyseerd om concrete aanbevelingen te formuleren voor het beheersen van privilege creep. De synthese van bevindingen uit de literatuurstudie, documentanalyse en Proof of Concept wordt gebruikt om richtlijnen op te stellen voor periodieke access reviews, automatisering van detectieprocessen en beleidsaanpassingen. Daarbij wordt ook de praktische toepasbaarheid van deze aanbevelingen beoordeeld zodat ze direct inzetbaar zijn voor IT professionals die verantwoordelijk zijn voor toegangsbeheer en security. Het eindresultaat van het onderzoek bestaat uit een analyseverslag, een werkende Proof of Concept en een overzichtsrapport met synthese en aanbevelingen, waarmee zowel inzicht in privilege creep wordt geboden als concrete stappen voor de beheersing ervan.

4. Verwacht resultaat, conclusie

Dit onderzoek zal naar verwachting resulteren in een technische Proof of Concept die privilege creep binnen RACF-omgevingen systematisch kan detecteren. De Proof of Concept genereert duidelijke rapporten en indicatoren waarmee gebruikers en rechten geïdentificeerd worden die mogelijk niet langer functioneel noodzakelijk zijn.

Voor de beoogde doelgroep biedt dit resultaat concrete meerwaarde, doordat het ondersteuning biedt bij periodieke access reviews, auditvoorbereiding en het optimaliseren van het toegangsbeheerproces. Bovendien kan de oplossing dienen als basis voor verdere automatisering of integratie binnen bestaande securityprocessen.

Indien de verwachte resultaten worden beves-

tigd, kan worden geconcludeerd dat een technisch ondersteunde detectiemethode een effectieve bijdrage levert aan het beheersen van privilege creep binnen RACF. Dit versterkt de security posture en bevordert de naleving van het least privilege-principe in IBM z/OS mainframe omgevingen.

Referenties

Carter, M. K. (2022). Techniques To Approach Least Privilege.

Garitano, G. (2024). Getting Started with RACF: Essential Configuration Steps.

Jain, N. (2025). Privilege Creep: The Silent Risk Lurking In Your Workforce.

Romero, M. (2025). Privilege Creep: What It Is and How To Prevent It.