

ONDERZOEKSVOORSTEL

Detectie van Privilege Creep in RACF via Analyse van Gebruikers-, Groeps- en Resourceprofielen op IBM z/OS.

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 privilege-principe. 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	1
2	Literatuurstudie	2
3	Methodologie	3
3.1	Analysefase – Probleemdomein	3
3.2	Ontwikkel- en testfase – Oplossingsdomein	3
3.3	Synthese- en evaluatiefase	3
4	Requirementanalyse	4
4.1	Doelstelling van de Proof of Concept	4
4.2	Stakeholders	4
4.3	Functionele requirements	4
4.4	Niet-functionele requirements	4
4.5	Randvoorwaarden en aannames	4
4.6	Afgrenzing	4
4.7	Gefaseerde planning	5
5	Verwacht resultaat, conclusie	5
	Referenties	5

1. Inleiding

Toegangsbeheer vormt een essentieel onderdeel van informatiebeveiliging binnen organisaties die gebruikmaken van IBM z/OS-mainframes. In deze omgevingen wordt RACF (Resource Access Control Facility) ingezet om gebruikers, groe-

pen en toegangsrechten tot systeembronnen te beheren. Door de hoge mate van centralisatie en de bedrijfskritische aard van mainframes is een correct en gecontroleerd rechtenbeheer van cruciaal belang voor zowel operationele continuïteit als naleving van beveiligings- en compliancevereisten.

De doelgroep van deze bachelorproef bestaat uit IT-professionals die verantwoordelijk zijn voor identity and access management en security binnen z/OS-mainframeomgevingen, zoals mainframe security administrators, systeemprogrammeurs en audit- of complianceverantwoordelijken. In de praktijk worden zij geconfronteerd met complexe en historisch gegroeide RACF-configuraties, een toenemend aantal gebruikers en frequente functiewijzigingen.

Binnen deze context stelt zich het probleem van *privilege creep*. Door functiewijzigingen, tijdelijke opdrachten en het ontbreken van systematische toegangsherzieningen behouden gebruikers vaak toegangsrechten die niet langer noodzakelijk zijn voor hun huidige rol. Dit leidt tot verhoogde beveiligingsrisico's, verminderde auditbaarheid en potentiële non-compliance met interne en externe regelgeving. De centrale on-

derzoeksvraag 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?*

Om deze hoofdonderzoeksvraag te beantwoorden, wordt het onderzoek opgesplitst in deelvragen binnen het probleemdomein en het oplossingsdomein. Binnen het probleemdomein wordt onderzocht: (1) welke vormen van privilege creep voorkomen binnen RACF-omgevingen, (2) welke RACF-mechanismen bijdragen aan het ontstaan ervan, (3) welke organisatorische en technische oorzaken een rol spelen en (4) welke risico's en compliance-implicaties hieruit voortvloeien.

Binnen het oplossingsdomein wordt gefocust op: (1) welke RACF-data-elementen geschikt zijn voor het technisch detecteren van privilege creep, (2) hoe overmatige of ongebruikte toegangsrechten objectief kunnen worden geïdentificeerd, (3) hoe deze detectie kan worden geautomatiseerd in een Proof of Concept en (4) in welke mate deze oplossing inzetbaar is ter ondersteuning van access reviews en security audits.

Aanvullend worden binnen het oplossingsdomein volgende technische deelvragen onderzocht: (1) welke RACF-commando's, extractbestanden of SMF-records nodig zijn om gebruikers-, groeps- en resource-autorisaties te verzamelen voor analyse, (2) op welke manier RACF-autorisaties technisch kunnen worden geanalyseerd om overmatige rechten te detecteren op basis van groeps-hiërarchie, rolafebakening en laatste gebruiksdata, en (3) hoe een technische Proof of Concept deze RACF-gegevens kan verwerken en omzetten in reproduceerbare rapporten die privilege creep objectief aantonen.

De onderzoeksdoelstelling van deze bachelorproef is het ontwikkelen van een technisch onderbouwde Proof of Concept die privilege creep binnen RACF detecteerbaar maakt. Het onderzoek wordt als succesvol beschouwd wanneer de Proof of Concept in staat is om RACF-gegevens te analyseren, overmatige of ongebruikte rechten inzichtelijk te maken en gestructureerde rapporten te genereren die bruikbaar zijn voor periodieke toegangscontroles en auditvoorbereiding.

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. Dit principe wordt breed toegepast in informatiebeveiligingsstandaarden en -frameworks om de impact van ongeautoriseerde toegang te minimaliseren en de risico's

van privilege escalerende exploitatie te beperken (Corporation, 2026b, 2026d).

Verschillende studies en technische richtlijnen tonen aan dat het afdwingen van het least privilegeprincipe in de praktijk complex is, vooral in omgevingen met langdurige gebruikersaccounts en frequente functiewijzigingen. Privilege creep het geleidelijk opstapelen van toegangsrechten over tijd ontstaat vaak als gevolg van organisatorische veranderingen, onvoldoende intrekingsprocessen en het ontbreken van systematische herzieningen (Jain, 2025; Romero, 2025). Deze problematiek geldt algemeen binnen identity management, maar is extra uitgesproken in mainframeomgevingen door de fijnmazige en historisch gegroeide toegangsstructuren en de centrale rol van systemen zoals RACF (Corporation, 2026c, 2026d).

Specifiek voor IBM z/OS-omgevingen biedt RACF uitgebreide mogelijkheden voor toegangscontrole via gebruikersprofielen, groepen, dataset- en resourceprofielen. RACF ondersteunt authenticatie, autorisatie, auditing en logging om de beveiliging van systeembronnen te waarborgen (Corporation, 2026c, 2026d). De technische documentatie van IBM beschrijft deze mechanismen en de noodzakelijke expertise voor correct beheer, waaronder het configureren van profielen, toegangsrechten en het gebruik van auditmogelijkheden om activiteiten te monitoren (Corporation, 2026d).

Bovendien worden in de mainframe-documentatie en compliance-richtlijnen ook best practices beschreven voor het beheer van toegangsrechten, onder andere door het periodiek controleren van privileges en het toepassen van least privilege binnen toegangsbeheerprocessen (Corporation, 2026a, 2026e). Standaarden zoals ISO/IEC 27001 benadrukken het belang van access control policies en regelmatige herziening van gebruikersrechten als onderdeel van een Information Security Management System (ISMS) (Corporation, 2026e). NIST SP 800-53 bevat eveneens security controls die nauw verwant zijn aan least privilege en privilege management binnen toegangsbeheer en complianceprocessen (Force, 2026).

Bestaand onderzoek rond privilege creep richt zich vaak op algemene IAM-problemen of oplossingen in moderne IT-omgevingen en cloudinfrastructuur, terwijl er relatief weinig aandacht is voor technische detectiemethoden specifiek gericht op RACF-configuraties binnen mainframe-omgevingen. Dit onderzoeksvoorstel 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 (Jain, 2025; Romero, 2025).

3. Methodologie

Deze bachelorproef hanteert een toegepaste onderzoeks aanpak waarbij analytische en technische onderzoeksmethoden worden gecombineerd om zowel het probleemdomein als het oplossingsdomein te onderzoeken. Het onderzoek wordt uitgevoerd in drie duidelijk afgebakende fasen: een analysefase, een ontwikkel- en testfase en een synthese- en evaluatiefase.

3.1. Analysefase – Probleemdomein

In de analysefase wordt inzicht verworven in het ontstaan en de impact van privilege creep binnen RACF-omgevingen. Hiervoor worden drie onderzoeksmethoden toegepast: literatuurstudie, documentanalyse en stakeholderinterviews.

De literatuurstudie richt zich op academische en technische bronnen rond privilege creep, least privilege en identity and access management. Daarnaast wordt een documentanalyse uitgevoerd op volgende RACF- en z/OS-gerelateerde documentatie:

- IBM RACF Security Administrator's Guide (Corporation, 2026d)
- Compliance- en auditrichtlijnen met betrekking tot toegangsbeheer en least privilege (voor Cybersecurity België, 2026)
- RACF Administration Guide (Corporation, 2026c)

Aanvullend wordt een technische analyse uitgevoerd op RACF-configuratiegegevens. Hierbij worden RACF-extracten en configuratiegegevens onderzocht om inzicht te krijgen in gebruikersstructuren, groepshiërarchieën en toegekende autorisaties. De analyse focust op het identificeren van patronen zoals:

- gebruikers met meerdere of overlappende groepslidmaatschappen;
- langdurig toegekende privileges zonder duidelijke functionele noodzaak;
- afwijkingen ten opzichte van het least privilegeprincipe.

Om de technische bevindingen te contextualiseren, worden semigestructureerde interviews afgenomen met stakeholders, waaronder mainframe security administrators en auditverantwoordelijken. Deze interviews focussen op:

- het huidige toegangsbeheerproces binnen RACF;
- bestaande procedures voor toekenning en intrekking van rechten;
- ervaren knelpunten bij access reviews en audits;
- verwachtingen ten aanzien van geautomatiseerde detectie van privilege creep.

3.2. Ontwikkel- en testfase – Oplossingsdomein

In de tweede fase wordt een technische Proof of Concept ontwikkeld die privilege creep binnen RACF detecteert aan de hand van analyse van specifieke RACF-data-elementen.

De Proof of Concept analyseert onder meer volgende RACF-data-elementen:

- Gebruikersprofielen (USERID, SPECIAL-, OPERATIONS en AUDITOR-attributen)
- Groepslidmaatschappen en groepshiërarchieën
- Dataset- en general resource profielen met bijhorende autorisaties;
- Beschikbare laatste-gebruik- of activiteitsinformatie.

De technische oplossing wordt geïmplementeerd als een script of tool dat RACF-exportgegevens verwerkt. De focus ligt op reproduceerbaarheid en transparantie, zodat de analyse herhaalbaar is en de resultaten begrijpelijk blijven voor RACF-beheerders. De output van de Proof of Concept bestaat uit gestructureerde rapporten waarin potentiële gevallen van privilege creep per gebruiker worden weergegeven.

De Proof of Concept wordt getest binnen een afgebakende z/OS-testomgeving of een gesimuleerde dataset die representatief is voor een productieomgeving. Hierbij worden fictieve gebruikers en autorisaties gebruikt om reële RACF-situaties na te bootsen zonder operationele systemen te beïnvloeden.

De testfase omvat minstens drie representatieve scenario's:

- Gebruikers met privileges afkomstig uit meerdere groepen die niet langer aansluiten bij hun huidige rol;
- Gebruikers met verhoogde rechten die gedurende een langere periode niet gebruikt zijn;
- Accounts met uitzonderlijke of historisch gegroeide autorisaties zonder duidelijke functionele noodzaak.

3.3. Synthese- en evaluatiefase

In de laatste fase worden de resultaten van de analyse- en ontwikkel fase samengebracht. De werking van de Proof of Concept wordt geëvalueerd op basis van correctheid, reproduceerbaarheid en praktische inzetbaarheid. Op basis van deze evaluatie worden concrete aanbevelingen geformuleerd voor het beheersen van privilege creep binnen RACF, met focus op periodieke access reviews en technische ondersteuning van auditprocessen.

4. Requirementanalyse

Dit hoofdstuk beschrijft de functionele en niet-functionele vereisten voor de ontwikkeling van de Proof of Concept (PoC) die privilege creep binnen RACF-omgevingen detecteert. De requirements zijn afgeleid uit de analyse van het probleemdoain, de literatuurstudie, technische documentatie en de verwachtingen van betrokken stakeholders zoals RACF-beheerders en auditverantwoordelijken.

4.1. Doelstelling van de Proof of Concept

Het doel van de Proof of Concept is het ondersteunen van RACF-beheerders en auditors bij het identificeren van potentiële gevallen van privilege creep. De PoC moet inzicht bieden in historisch gegroeide, overbodige of risicovolle autorisaties en zo periodieke access reviews en auditprocessen faciliteren.

4.2. Stakeholders

De belangrijkste stakeholders binnen dit onderzoek zijn:

- RACF security administrators, verantwoordelijk voor gebruikers- en autorisatiebeheer;
- Auditverantwoordelijken, betrokken bij interne en externe compliance-audits;
- Organisaties die z/OS- en RACF-omgevingen beheren en geconfronteerd worden met strenge compliance-eisen.

4.3. Functionele requirements

De Proof of Concept moet minimaal voldoen aan volgende functionele vereisten:

- FR1: Het systeem moet RACF-exportgegevens kunnen inlezen en verwerken zonder directe koppeling met een productieomgeving.
- FR2: Het systeem moet gebruikersprofielen analyseren, inclusief SPECIAL, OPERATIONS en AUDITOR-attributen.
- FR3: Het systeem moet groepslidmaatschappen en groepshiërarchieën in kaart brengen per gebruiker.
- FR4: Het systeem moet dataset- en general resource autorisaties per gebruiker kunnen correleren.
- FR5: Het systeem moet potentiële privilege creep detecteren op basis van vooraf gedefinieerde criteria, zoals:
 - overlappende of cumulatieve autorisaties;

- langdurig toegekende privileges zonder recente activiteit;
- uitzonderlijke of historisch gegroeide rechten.

- FR6: Het systeem moet per gebruiker een gestructureerd rapport genereren met gedetecteerde risico's en bijhorende toelichting.

4.4. Niet-functionele requirements

Naast functionele vereisten moet de Proof of Concept ook voldoen aan volgende niet-functionele eisen:

- NFR1: De oplossing moet reproduceerbaar zijn, zodat analyses op identieke datasets steeds hetzelfde resultaat opleveren.
- NFR2: De werking en output van de tool moeten transparant en interpreteerbaar zijn voor RACF-beheerders.
- NFR3: De Proof of Concept mag geen wijzigingen aanbrengen aan RACF-configuraties of productiegegevens.
- NFR4: De oplossing moet schaalbaar zijn voor RACF-omgevingen met een groot aantal gebruikers en autorisaties.
- NFR5: De verwerking van gegevens moet conform zijn met geldende security- en compliance-richtlijnen.

4.5. Randvoorwaarden en aannames

Bij de ontwikkeling van de Proof of Concept wordt uitgegaan van volgende randvoorwaarden en aannames:

- Er is toegang tot representatieve RACF-exportgegevens of gesimuleerde datasets;
- De focus ligt uitsluitend op detectie en rapportering, niet op automatische remediatie;
- De oplossing wordt ontwikkeld als een standalone script of tool zonder grafische gebruikersinterface;
- De Proof of Concept is gericht op technische haalbaarheid en conceptuele validatie, niet op productiegebruik.

4.6. Afgrenzing

Buiten de scope van deze bachelorproef vallen:

- real-time monitoring van RACF-activiteit;
- automatische intrekking of wijziging van autorisaties;
- integratie met externe Identity & Access Management-platformen.

4.7. Gefaseerde planning

Het onderzoek wordt uitgevoerd volgens onderstaande planning:

- **Fase 1 – Analyse (februari 2026):** literatuurstudie, analyse van RACF-documentatie, identificatie van relevante data-elementen en uitwerking van detectiecriteria.
- **Fase 2 – Ontwerp (maart 2026):** functioneel en technisch ontwerp van de Proof of Concept, inclusief datamodellen en rapportagestructuur.
- **Fase 3 – Implementatie (april 2026):** ontwikkeling van de Proof of Concept en verwerking van RACF-gegevens.
- **Fase 4 – Testen en evaluatie (mei 2026):** uitvoering van representatieve scenario's en evaluatie op basis van vooraf vastgelegde criteria.
- **Fase 5 – Synthese en rapportering (mei 2026):** analyse van resultaten, formuleren van aanbevelingen en finaliseren van de bachelorproef.

Corporation, I. B. M. (2026b, 21 januari). *Least privilege principle*. <https://www.ibm.com/docs/en/aix/7.2.0?topic=privileges-least-privilege-principle>

Corporation, I. B. M. (2026c, 21 januari). *RACF® Administration Guide*. <https://www.ibm.com/docs/en/szs/3.1.0?topic=manual-racf-administration-guide>

Corporation, I. B. M. (2026d). Security Server RACF Security Administrator's Guide.

Corporation, I. B. M. (2026e, 21 januari). *What is ISO 27001?* <https://www.ibm.com/products/cloud/compliance/iso-27001>

Force, J. T. (2026). Security and Privacy Controls for Information Systems and Organizations.

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.

voor Cybersecurity België, C. (2026). CYBER FUNDAMENTALSESSENTIEEL.

5. 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 bevestigd, 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

Corporation, I. B. M. (2026a, 21 januari). *IBM z/OS RACF Security Technical Implementation Guide*. https://stigviewer.cyberprotection.com/stigs/ibm_zos_racf