Bachelorproef toegepaste informatica (2024-2025)

Hoe kan trust management effectief worden geïmplementeerd voor het beveiligen van bedrijven met heterogene gesegmenteerde netwerken?

Thibo Haezaert
thibo.haezaert@student.hogent.be
Promotor: Gilles Blondeel
Co-promotor: Dirk Mussen (KBC)
Hogeschool Gent, Valentin Vaerwyckweg 1, 9000 Gent

Samenvatting

In moderne, heterogene bedrijfsnetwerken is het essentieel om zorgvuldig te bepalen welke systemen welke root- en intermediate-certificaten vertrouwen. Dit proces, bekend als trust management, houdt niet alleen het technisch beheren van truststores in, maar vooral het strategisch toewijzen van vertrouwen op basis van de rol, locatie of functie van een systeem binnen het netwerk.

Een foutieve toekenning van vertrouwen kan leiden tot verhoogde cyberrisico's of het falen van kritieke communicatie. Deze bachelorproef onderzoekt hoe trust management effectief kan worden geïmplementeerd binnen gesegmenteerde netwerken met zowel Windows- als Linux-systemen.

Na een literatuurstudie werd een proof-of-concept uitgewerkt waarin vier beheeroplossingen werden getest:

- *Windows: via Group Policy Objects (GPO) en System Center Configuration Manager (SCCM)*
- *Linux: via Ansible en Chef*

Deze tools maken het mogelijk om truststores centraal te beheren en contextspecifiek toe te wijzen, afgestemd op netwerksegmentatie.

Aanbevelingen richten zich op integratie met bestaande PKI-processen, uitbreidbaarheid naar grotere infrastructuren en verfijnde toewijzingscriteria.

Onderwerpen zoals security, MacOS en IoT vielen buiten scope en vormen mogelijkheden voor toekomstig onderzoek.

Keuzerichting: Systeem- en Netwerkbeheer

Sleutelwoorden: Root certificates, Truststores, Trust management, SCCM, Chef, Ansible, HashiCorp Vault

1. Introductie

Moderne bedrijfsnetwerken zijn vaak *heterogeen* en *gesegmenteerd*, wat het beheer van vertrouwensrelaties tussen systemen bemoeilijkt. Een cruciaal onderdeel hiervan is het bepalen welke root- en intermediate-certificaten elk systeem mag vertrouwen.

Trust management verwijst naar het centrale proces waarbij organisaties certificaatvertrouwen toewijzen aan systemen op basis van hun rol, locatie of functie binnen het netwerk. Onvoldoende of overmatig vertrouwen in certificaten verhoogt respectievelijk het risico op operationele fouten of beveiligingsincidenten.

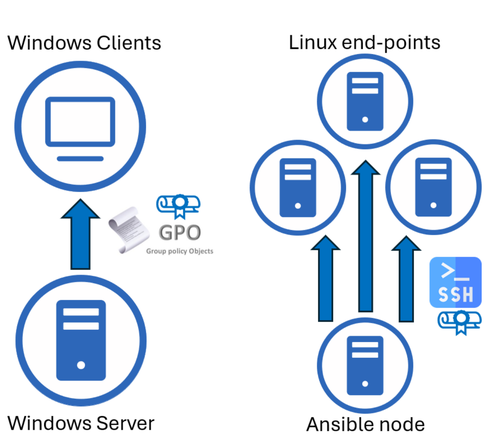
Deze bachelorproef onderzoekt hoe trust management effectief kan worden geïmplementeerd in zulke netwerken. De focus ligt op:

- Tools en technieken voor truststorebeheer en hun beperkingen.
- Centraal beheer van truststores over diverse endpoints.
- Differentiatie per netwerksegment.
- Implementatie in een proof-of-concept omgeving.
- Evaluatie van effectiviteit en schaalbaarheid.
- Praktische aanbevelingen voor bedrijven.

2. Proof-of-concept

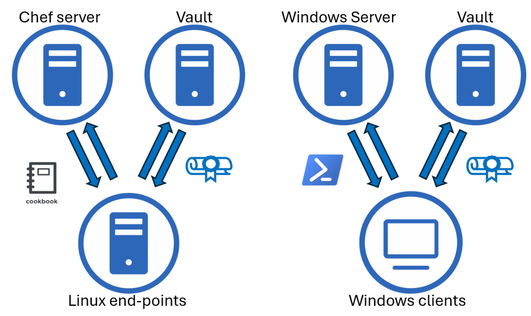
Een virtuele proof-of-concept omgeving werd opgezet met Windows- en Linux-endpoints, verdeeld over gesegmenteerde netwerken. Elk segment kreeg een eigen set root-certificaten toegewezen.

In de eerste oplossing werd gebruikgemaakt van **GPO's** (Windows) en **Ansible** (Linux) om certificaten toe te wijzen op basis van OU's of end-point groepering. Deze methode bleek echter beperkt in schaalbaarheid: PowerShell ondersteunt geen beheer van GPO-certificaten, en Ansible vereist SSH-connecties naar alle endpoints.



Figuur 1: Procesoverzicht oplossing 1

De tweede oplossing verbeterde de schaalbaarheid door gebruik te maken van **SCCM** met PowerShell-scripts (Windows) en **Chef** cookbooks (Linux). Beide platformen haalden certificaten op uit een centrale **HashiCorp Vault**, gestructureerd per netwerksegment. Endpoints selecteerden de juiste segmentdata via parameters of node-attributen.



Figuur 2: Procesoverzicht oplossing 2

3. Conclusies

Dit onderzoek toont aan dat trust management effectief geïmplementeerd kan worden via een gecentraliseerde architectuur waarin de inhoud van truststores per systeem verschilt op basis van netwerksegmentatie.

De combinatie van een centrale certificaatbron (zoals HashiCorp Vault) met tools zoals GPO's, SCCM (Windows) en Ansible of Chef (Linux) maakt het mogelijk om root- en intermediate-certificaten doelgericht te verdelen.

Elke oplossing heeft voor- en nadelen in termen van schaalbaarheid, snelheid en beheercomplexiteit. De proof-of-concept bevestigt dat organisaties trust kunnen toewijzen op basis van een andere gewenste context (bv. segment, rol, locatie), zolang de onderliggende tooling hierop wordt afgestemd.

4. Toekomstig onderzoeken

Hoewel de voorgestelde oplossing succesvol werd gevalideerd in een gecontroleerde proof-of-concept omgeving, blijven er verschillende pistes voor verder onderzoek. Enkele belangrijke aandachtspunten zijn:

- **Schaalbaarheid**: Onderzoeken hoe de architectuur presteert in grootschalige productienetwerken met honderden tot duizenden endpoints.
- **Integratie met PKI**: Analyseren hoe truststore-updates kunnen worden afgestemd op certificaatlevenscycli via bestaande Public Key Infrastructure (PKI)-diensten.
- **Ondersteuning van andere platformen**:
  - *macOS*: Verkennen van beheermogelijkheden voor Apple-systemen.
  - *IoT-apparaten*: Aangepaste methoden ontwikkelen voor devices die niet ondersteund worden door klassieke tools.
- **Beveiligingsanalyse**:
  - Beveiligen van de centrale certificaatbron (bijv. HashiCorp Vault).
  - Garanderen van integriteit en authenticiteit van communicatie tussen beheertools en endpoints.

HO
GENT