Z-CERT Position paper ‘MPC in de Zorg’

De Z-CERT-missie "Nederlandse Zorg Digitaal Veilig" betreft de beschikbaarheid, integriteit en vertrouwelijkheid van data en IT-systemen van de Nederlandse zorg. Vanuit het ministerie van VWS wordt -mede met het oog op Europese regelgeving (EHDS)- ingezet op betere integratie en uitwisseling van zorgdata. Dat is belangrijk zowel voor behandelingen en verzorging ('primair gebruik') als voor wetenschappelijk onderzoek ('secundair gebruik'). 'Multi-Party Computation-technologie' (MPC) is voor beide gebruiksvormen elk op eigen wijze geschikt.

MPC is een cryptografische techniek die meerdere partijen in staat stelt gezamenlijk berekeningen uit te voeren op versleutelde data, zonder elkaars gegevens te onthullen. Het maakt analyses mogelijk op gevoelige informatie, terwijl de privacy gewaarborgd blijft en alleen het eindresultaat wordt gedeeld. Onze partner Nationaal Cyber Security Centrum (NCSC) heeft ervaring opgedaan met de op MPC-technologie gebaseerde oplossing 'SecureNed'. De techniek is daar voldoende snel, betrouwbaar, bruikbaar en anoniem gebleken en de benodigde onderzoeksvragen konden beantwoord worden (meer informatie op de volgende pagina).

Voor secundair gebruik past MPC goed bij de gestandaardiseerde werkwijze die het 'Transitieplan Landelijk Dekkend Netwerk' beoogt te realiseren. MPC is ook onderdeel van Health-RI's 'AI-dataplaformen’ (AIDA). In de zorg gaat secundair gebruik vaak -anders dan bij het NCSC- over het selecteren van cohorten, m.b.v. inclusiecriteria, en daarna statistische methoden toepassen (beschrijvende statistiek of machine learning). Moderne MPC-oplossingen zijn geschikt om zowel secundair gebruik te faciliteren als de privacy van patiënten te beschermen. Aandachtspunt is hoe MPC past bij toekomstige EHDS-standaarden. MPC-complexiteit abstraheren voor aanbieders van zorg (en zorgsystemen) zal sowieso cruciaal zijn voor succes. Op dit moment zijn ons geen andere methodes bekend die qua functionaliteit én qua privacy voor secundair gebruik net zo geschikt lijken als MPC. Zo is 'federated learning' vooral gericht op trainen van machine learning-modellen op grote datasets (met minder sterke privacy garanties) en bij aanleg van volledige datasets ontstaan snel herleidbaarheidsrisico's. MPC-inzet in primair gebruik is denkbaar voor scenario's waarin men analyses doet op de grote populatie, om vervolgens alleen resultaten over de relevante doelgroep te onthullen.

Tot slot: Centrale voorzieningen, zoals het Landelijk Dekkend Netwerk uiteindelijk beoogt te bieden, zijn een aantrekkelijk doelwit voor kwaadwillenden. Vanuit Z-CERT pleiten we daarom voor een solide beveiliging, die vanaf de beginfase wordt meegenomen in alle ontwerpen tot in de uitvoering, inclusief centrale securitymonitoring. Wij denken daarbij graag mee.

Z-CERT Position paper ‘MPC in de Zorg’

Toelichting NCSC-ervaring met MPC-technologie in SecureNed

Het NCSC heeft reeds enkele jaren ervaring opgedaan met de op MPC-technologie gebaseerde oplossing 'SecureNed' (van Roseman Labs). Daarbij heeft het NCSC intensief met de leverancier samengewerkt aan de ontwikkeling van de oplossing. Het NCSC zette SecureNed initieel in voor het uitsturen van enquêtes onder security-partners, waarbij de invuller volkomen anoniem blijft. Dit bleek de bereidheid om vertrouwelijke informatie te delen te vergroten. Vervolgens is SecureNed uitgebouwd naar zogenaamde 'dataverzoeken', wat het meest lijkt op het 'secundaire gebruiksdoel' uit dit document. Deze dataverzoeken zijn bij het NCSC ingezet om partijen zonder datatoegang toch inzicht te geven of er data is die overeenkomt met een gestelde vraag, waarbij partijen ook met elkaar in contact konden komen buiten het NCSC om. Een andere casus van het NCSC was een schaalbaarheidstest door vergelijking van grote hoeveelheden (fictieve) data in samenwerking met de politie. Hierbij liet SecureNed zien dat de prestaties overeind blijven bij grotere datavolumes.

Belangrijke inzichten zijn verder:

- De inzet van MPC-technologie vereiste bij NCSC ontwikkeling en implementatie binnen een specifieke bij het doel passende oplossing. Inmiddels is ook SaaS mogelijk.
- De deelname van alle betrokken partijen is bij de implementatie de doorslaggevende factor voor de implementatiesnelheid gebleken; de techniek is hierin niet belemmerend geweest nadat de oplossing voldoende ontwikkeld was.
- Deelnemers moeten expliciet toestemming geven voor de onderzoeksvraag bij gebruik van de MPC-oplossing, waarbij het voor aangesloten deelnemers mogelijk is om alleen resultaten te onthullen als er een minimaal aantal resultaten is. De onderzoeksvraag kan desgewenst goedkeuring van één of meer personen vereisen.
- MPC is ook inzetbaar wanneer bevraagde data niet exact dezelfde structuur heeft, wat bij zorgdata vaak het geval is.
- Bij MPC-toepassing in oplossingen met gesloten broncode zijn deze nog steeds te integreren met andere systemen via open gestandaardiseerde koppelvlakken (API's). Dergelijk API-gebruik faciliteert ook interoperabiliteit met verschillende oplossingen.
- Certificering, zoals het BSPA-schema van de AIVD, vergroot het vertrouwen in gebruikte software.
- De ontwikkeling en implementatie van elke IT-oplossing, dus ook met MPC-technologie, vereisen de nodige aandacht om te passen bij de beoogde inzet.