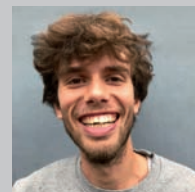


Daan Mulder

mulderdaan@live.nl



Het keerpunt van Marie Beth van Egmond

# Je moet ook een beetje jezelf ergens in verliezen

Het is misschien wel toepasselijk dat ik Marie Beth van Egmond, Junior Crypto Specialist bij de afdeling Cyber Security & Robustness van onderzoeksorganisatie TNO niet in levende lijve spreek, maar via Skype. Het is *lockdown*, tenslotte. “Ik las in je eerdere Keerpunten dat je graag thee drinkt,” zegt ze, terwijl ze zichzelf achter de computer een kop inschenkt. Zelf loop ik ook nog even naar de keuken om een kop thee te halen, voor we met interview beginnen.

*Hoe zag je werkdag eruit voordat de hele corona-toestand uitbrak?*

“Heel erg gevarieerd eigenlijk. Ik werk nu zo’n anderhalf jaar bij TNO. Daar doen we onderzoek in samenwerking met bijvoorbeeld banken of zorgverzekeraars. Wij kijken wat er allemaal mogelijk is met de technologie die zij over een jaar of vijf willen inzetten. Ik maak er dan een demonstratie van — een ‘demo’ — in Python. En ik maak en geef ook veel presentaties. Eigenlijk zit ik het meest van mijn tijd in Powerpoint te werken.

Een project gaat bijvoorbeeld over witwasdetectie. Dat gaat over hoe banken fraudeurs kunnen detecteren door op een privacy-vriendelijke manier data uit te wisselen. Daarvoor kun je een techniek gebruiken waar wij veel onderzoek naar doen, Secure Multi-Party Computation (MPC).

Bij zo’n project komen ook heel veel ingewikkelde juridisch dingen kijken, waar ik dan zelf geen verstand van heb. Maar ik kan daar dan wel uit technisch oogpunt over meedenken. Dus dan zit ik aan tafel met allemaal, tja, mannen die daarover praten: fraude-experts van de Rabobank, mensen van compliance, die weten heel veel van die wettelijke dingen.”

*Hoe is het om nu thuis te moeten zitten?*

“Eigenlijk gaat alles gewoon door. Ik merk alleen wel dat de dingen die ik heel

leuk vind, er nu veel minder zijn. Zoals met collega’s praten, en samen nadenken over dingen. Het is toch wel een bepaald soort energie die je samen hebt; soms zat ik gewoon een hele dag met mensen in een kamertje te werken.”

*Waar overleg je dan over, over hoe je het moet programmeren?*

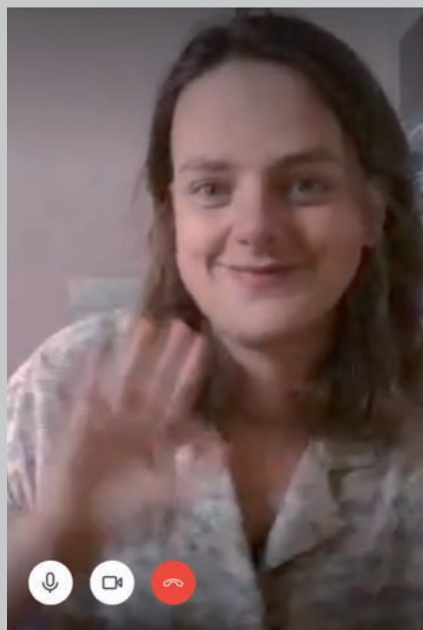
“Meer over concepten. Met MPC, bijvoorbeeld, zijn er allerlei cryptografische oplossingen mogelijk. Wiskundig gezien

kun je wel elke mogelijke berekening maken, in de praktijk is het anders omdat een heel ingewikkeld algoritme gewoon erg veel rekentijd kost. Welk protocol is dan het meest geschikt?

Het idee van MPC is dat je met meerdere partijen een berekening kunt uitvoeren, zonder dat je je eigen data deelt. Je kunt bijvoorbeeld zo getallen optellen: stel ik ben met A en B samen en we willen ons gemiddelde salaris berekenen, zonder dat we elkaar ons salaris vertellen. Dat kan via een algoritme: we kiezen elk drie getallen die opgeteld gelijk zijn aan ons eigen salaris. Eén van die getallen geef ik aan A, een ander getal geef ik aan B, de derde houd ik zelf. Zij doen hetzelfde met hun drie getallen. Dan tellen we elk de drie getallen die we hebben bij elkaar op en die uitkomsten delen we met elkaar. Daar berekenen we het gemiddelde van: zo weet niemand elkaars salaris, maar weten we wel het gemiddelde.

Maar als twee van die mensen hun salaris wél met elkaar delen, weten ze ook wat die derde verdient. Wiskundig gezien zijn er allerlei waarschuwingen: als je een protocol kiest, hoort er een getal bij dat iets zegt over of het nog veilig is als een bepaald aantal deelnemers onderling data deelt. En je moet altijd bedenken dat hoe meer berekeningen je samen doet, hoe meer je over de data van de anderen kan achterhalen.

Wat er met witwassen vaak gebeurt, is dat er geld naar verschillende banken wordt gestuurd. Die banken mogen hun transactienetwerken niet zomaar met elkaar delen. Wij proberen een algoritme te verzinnen dat die fraude kan detecteren,



Marie Beth van Egmond tijdens het Skype-interview

en te bedenken hoe je daar een veilig MPC-protocol van kunt maken.”

*Heb je het gevoel dat er goed met privacy om wordt gegaan?*

“Ja, op zich wel. Dat wij dit onderzoek doen, kun je op twee manieren benaderen. Je kan zeggen dat MPC iets slechts is: ‘Waarom moet die data überhaupt op één of andere manier bij elkaar komen?’ Tegenovergesteld kun je natuurlijk ook zeggen: ‘In plaats van dat die data echt bij elkaar wordt gezet, hebben we een techniek waardoor we er toch mee kunnen rekenen.’ Tot nu werkt men bijvoorbeeld in de zorg met een trusted third party, een partij die de berekeningen doet, maar belooft verder niks met die data te doen. MPC is een technische vervanging daarvoor, en privacytechnisch gezien een verbetering.”

*Was het wennen om in zo’n werkritme te komen?*

“Ja, best wel. Wat ik het moeilijkste vond, is dat het zo afgebakend is. Als je studeert, ben je met je vrienden op een universiteit, je gaat daarna misschien met ze eten, en daarna nog wat huiswerk maken, en zo rolt dat verder. Nu moet ik heen en weer reizen naar Den Haag, heb ik vaste werktijden. Dat vond ik heel lastig. Wel fijn dat je in het weekend niets te doen hebt, maar ik sliep niet zo goed doorde- weeks en ging dan in het weekend tot in de middag slapen. Maar dan moest ik de week erna weer vroeg op. Ik kon er de eerste maanden echt niet mee omgaan.”

*Is het erg een mannencultuur?*

“Het wordt wel wat minder; het aantal vrouwen is afgelopen jaar verdubbeld. Van 3 naar 6, van de 60; nouja, een deel van de afdeling werkt in Groningen, maar alle vrouwen zitten in Den Haag. Voor mij in het dagelijks leven eerder 6 op 30 dus. Ik merk er zelf eigenlijk niet zo heel veel van. Wel een keer dat ik mijn zorgen ergens over had uitgesproken, en dat een collega zei: ‘Ja, jullie vrouwen maken jullie ook overal zorgen over, je moet naar de mannen kijken.’ Moet ik me nu per se als man gaan gedragen? Maar de meeste zijn heel zachtaardige nerds, hoor.

Wat een collega zei, wat ik wel herkenbaar vond, is dat we als security-mensen

als beroepsdeformatie hebben dat mensen ook bij elkaar de zwakke plek gaan zoeken. Zoals je dat bij een algoritme ook doet. Als je samen koffie aan het drinken bent, wordt er het hardst gelachen als je een zwakte bij iemand hebt ontdekt, en daar een grapje over weet te maken.”

*Denk je dat je hier over tien jaar nog werkt?*

“Ik weet het niet zeker. Ik mis de echte wiskunde weleens: het gevoel dat je had als je een nieuw boek opensloeg en dat je dan dacht: ik snap hier HE-LE-MAAL niks van, en dat je na een paar maanden langzaam begon te begrijpen waar het over ging. Dat voelt wel heel krachtig. Ik vond wiskunde wel altijd heel erg leuk, maar ik had nooit het gevoel van: dit is nou iets waar ik heel goed in ben. Nu merk ik in mijn werk dat er dingen zijn waar ik wél goed in ben, zoals leiding geven of nadenken over concepten, en daar kritisch op zijn.”

*Waarom ben je eigenlijk wiskunde gaan studeren?*

“Ik heb eerst bèta-gamma gedaan, een brede studie waar je na een jaar je ‘major’ kiest. Toen deed ik daar een vak logica, dat vond ik heel erg leuk. Ik had denk ik nooit wiskunde gekozen toen ik direct van de middelbare school kwam. Ik wist wel dat je dat kon studeren, maar ik had geen tien voor wiskunde, ik had gewoon een acht.

Ik weet nog dat ik de eerste weken wel eens huilend boven mijn huiswerk zat. Het was denk ik de eerste keer in mijn leven dat ik dacht: dit gaat misschien wel helemaal niet lukken. Daarvoor was alles een beetje leren, en dan lukt het wel. Ik weet nog heel goed dat we bezig waren met de epsilon-delta-definitie, en dat ik het gewoon niet snapte. De werkcollegedocent had een aantekening gemaakt in mijn schrift over een van die sommen, waar ik een hele avond naar gekeken heb tot ik dacht: oh, oké, zo zit het! Toen dacht ik: ik kan dit dus wel begrijpen, maar ik moet hiervoor wel heel hard werken. Als ik een slechte werkcollegedocent had gehad dat eerste halfjaar, was ik misschien wel met de studie gestopt.”

*Kom je uit een wiskunde-gezin?*

“Nee, helemaal niet. Mijn ouders zijn psychiaters. Mijn twee broers en mijn zus doen wel allemaal iets technisch: oogarts en lucht- en ruimtevaarttechniek, en mijn zus doet theoretische natuurkunde. We houden wel allemaal van puzzelen, maar dat is vooral iets van de laatste jaren.

Mijn vader was cum laude afgestudeerd van zijn studie geneeskunde, maar hij zei daarover: cum laude afstuderen is het domste wat je kunt doen, dan heb je eigenlijk iets te makkelijk gekozen. Hij heeft ons wel altijd gepusht – nouja gepusht klinkt zo negatief – ‘gestimuleerd’ om dingen te doen die boven je macht liggen. Bij TNO gaat het er meer om je krachten te vinden en te versterken; waar je goed in bent, dat moet je uitbuiten. Dus dan moet ik aan mijn vader denken, als ik bezig bent met iets waar ik gewoon goed in ben: is dit niet een beetje saai?

Toen ik aan mijn scriptie begon, leefde mijn vader nog. In het begin dacht ik bij het schrijven: voor wie doe ik het nu eigenlijk? Met andere vakken heb je nog een docent, of andere mensen die het ook doen, maar die scriptie voelde echt alsof ik het helemaal uit mezelf moest halen. Toen dacht ik: de enige die het echt erg zou vinden als ik met mijn scriptie zou stoppen is mijn vader.

Wat ook wel betekent dat er iets wegviel toen hij overleed – dat klinkt een beetje gek – in een positieve zin, van een bepaalde druk om te presteren. Het was ook een heel klein beetje bevrijdend. Ik vind het moeilijk uit te leggen. Toen ik bijvoorbeeld een half jaar naar Portugal ging, op uitwisseling, vond hij dat wel prima, maar hij was wel heel bang dat ik mijn studie niet zou afmaken. Dat ik het allemaal net zo lang zou uitsmeren tot ik op een gegeven moment geen zin meer zou hebben.

Uiteindelijk denk ik wel dat mijn ouders allebei heel veel vertrouwen hadden in ons, dat we het zo ver zouden schoppen. Ik geloof er nog steeds niet in dat je altijd moet doen waar je goed in bent. Je moet ook een beetje jezelf ergens in verliezen, door een barrière van weerstand heen. Dan kom je toch steeds verder. ☘

Goede suggesties voor een Nederlandse wiskundige met een keerpunt in zijn of haar carrière zijn welkom via [keerpunt@nieuwarchief.nl](mailto:keerpunt@nieuwarchief.nl).