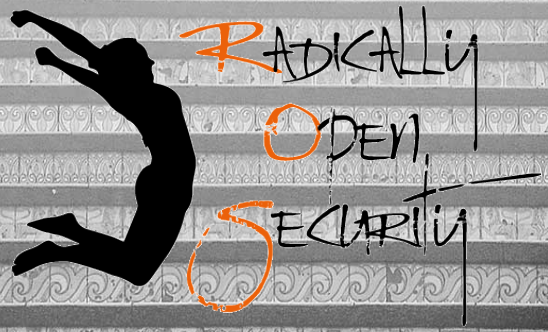
Eisen aan AI

Dr. Melanie Rieback



Oct 5, 2021

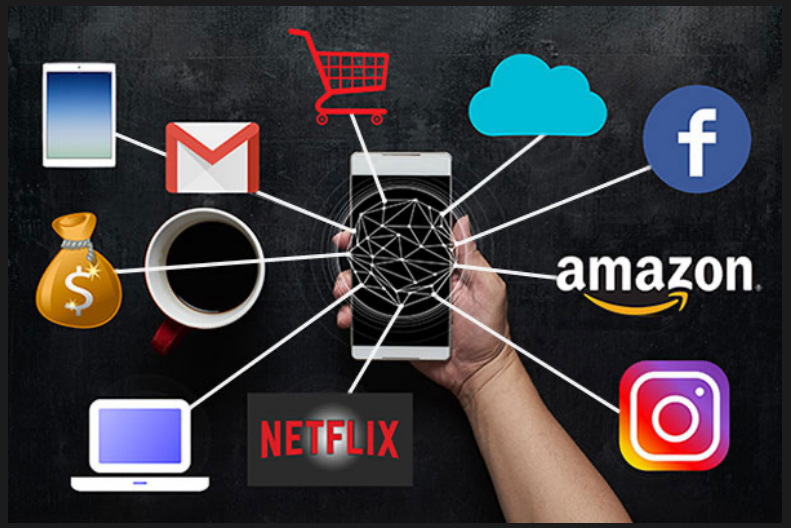
melanie@radicallyopensecurity.com

Wie ben ik?

- CEO/Co-founder van Radically Open Security
- Voormalig Asst. Professor Computer Science @ VU
- Faculteit: Singularity University
- “Meest innovatieve IT Leider van Nederland” (CIO Magazine)

Ons leven is steeds meer digitaal

- Werk / Communicatie / Onderzoek / Vrije tijd / Winkelen / Dating / enz…
- Internet of Things
- Trend in stroomversnelling geraakt door COVID-19



Ook de overheid gaat “digitaal”

- Overheidsgebruik van AI:
  - Verkeersboetes
  - Fraude-opsporing
  - Risicobeoordeling bij recidive
  - Immigratiecontrole
  - Militaire wapens (incl. drones)
  - Voorspellend politiewerk
  - Enz...

Dreiging: Gebrek aan transparantie

- AI is soms “unsupervised”
- Machine Learning algoritmen zijn een “zwarte doos”
- Hierdoor is het onmogelijk na te gaan hoe de beslissingen tot stand zijn gekomen
- (Zelfs voor de makers van de systemen)

Dreiging: Gegevensverzameling

- Gegevensverzameling is gevaarlijk
- Er is geen privacy zonder beveiliging
- Spanningsveld AVG/GDPR
  - Bewaring van gegevens
  - Inspectie/verificatie is moeilijk
  - Volledige naleving is onmogelijk
- Er bestaan oplossingen
  - Dataminimalisatie
  - Pseudoanonimisering
  - (In de praktijk zelden toegepast)

Dreiging: Vooroordelen

- Software ontwikkelaars maken systemen die passen in hun wereldbeeld
- Vooroordelen zijn te vinden in:
  - Code
  - Algoritmen
  - Training data sets
- Vooroordelen uiten zich:
  - Raciaal / economisch / geografisch / enz..
- Dit is moeilijk te voorkomen

Dreiging: Bedrijfsbestuur

- AI-ethiek is GEEN trolleyprobleem
- Bedrijfsmodellen vormen een grotere bedreiging
- Bedrijven zijn niet-transparant en niet-democratisch
- Zelfs aandeelhouders kunnen bestuurders niet altijd ter verantwoording roepen
- Dit is ook een probleem voor overheden

Casestudy

vs.

Oplossingen

- Open-source
- Verbeterd ondernemingsbestuur
- Sociaal aankoopbeleid
- Technologie

Technologie vs. Zakelijke Problemen

- Ik heb de laatste 20 jaar van mijn carrière privacyverbeteringstechnologieën (PET's) gebouwd
- Ik ben het beu geworden om technologische ‘pleisters’ te ontwikkelen om ons te redden van Google, Apple, Facebook, enz.
- Problemen t.a.v. bedrijfsmodellen vereisen oplossingen t.a.v. bedrijfsmodellen
- Dit wordt onder het tapijt geveegd, omdat het ontwikkelen van nieuwe technologieën "sexier" en gemakkelijker is
- Technologie op zichzelf gaat onze "AI problemen" NIET oplossen

Vragen?

RADICALLY OPEN SECURITY

melanie@radicallyopensecurity.com