Contribution ID: **40** Type: **Presentation**

Technischer Datenschutz von personenbezogenen Daten

Wednesday, October 11, 2017 12:15 PM (30 minutes)

Etablierte Anonymitätsbegriffe wie k-Anonymität und Differential Privacy versprechen, dass die öffentliche Sicht auf personenbezogene Daten hinreichend verschleiert ist, um die Anonymität der betroffenen Personen zu gewährleisten. Doch für die korrekte Anonymisierung selbst müssen alle personenbezogenen Daten vollständig und zentralisiert vorliegen; die Betroffenen selbst haben keine unmittelbare Kontrolle mehr diese Daten. Während des Anonymisierungsvorgangs selbst sind die Daten also einer gewissen Gefahr ausgesetzt.

Dieser Gefahr kann man auf verschiedene Arten begegnen: Einerseits bietet die moderne Kryptographie Möglichkeiten verschlüsselte Daten zu verarbeiten ohne diese dabei Entschlüsseln zu müssen. Diese Verfahren sind jedoch sehr aufwändig und noch nicht praktikabel. Andererseits bieten moderne Intel-Prozessoren mit der SGX-Erweiterung eine Möglichkeit, Programmcode in einer geschützten Umgebung (einer sogenannten Enklave) auszuführen. Berechnungen innerhalb dieser Enklaven sind zwar effizient durchführbar; das Sicherheitsmodell basiert aber auf der grundlegenden Annahme, dass Intel als vertrauenswürdige dritte Partei agiert.

In diesem Vortrag wird aktuelle Forschung dazu vorgestellt, wie sich diese beiden Ansätze miteinander kombinieren lassen, sodass die Schwächen der beiden Ansätze abgemildert werden.

Track

BDAHM

Author: Mr HARTUNG, Gunnar (ITI)

Presenter: Mr GABEL, Matthias (KIT)