Sharemind®: A Secure Multi-Party Computation (MPC) Platform Implementing Privacy by Design and Privacy by Default

Triin Siil
General Counsel
triin.siil@cyber.ee
Overview

- About Cybernetica
- About Sharemind
  - What is it?
  - How has it been applied in practice?
  - How does it interact with the data protection regulation?
Introduction to Cybernetica

- Estonian ICT R&D company, founded in 1997
- Key products:
  - Information security solutions
  - e-Government solutions
  - Communication solutions
  - Surveillance and border guard solutions
- About 125 people
- 10% with PhD degrees
Cybernetica’s Product Portfolio

- Cybernetica has brought security technologies from research to practice for 20 years.
- Unified Exchange Platform
  - E-governments in Azerbaijan, Estonia, Finland, Haiti, Namibia
- Verifiable Internet Voting Software Tivi.io
  - Marketed through Smartmatic
- Smart-ID Digital Signature Technology
  - Marketed through SK ID Solutions AS
Department of Privacy Technologies (DPT)

- DPT applies privacy technologies to allow companies and governments to process more data without privacy concerns.

Data owners

- Industry
- Public sector
- People

Barriers

- Privacy regulation
- Business secrets
- Distrust

Data users

- Researchers
- Decision makers
- General public
Sharemind® Privacy-Preserving Data Analytics

Confidential data

Analyze without ever seeing the data

Privacy controls for third parties

New knowledge

- Sharemind goes beyond data protection requirements.
- Data owners encrypt data on-site and upload to Sharemind®.
- Data analysts build and run queries without accessing the data.
- Sharemind® processes the queries without removing the protection.
- Authorised users receive query results in an encrypted format.
Achievements in Practical Applications (1)

- **2013 – 2015 PRIST project**: implementing Sharemind in privacy-preserving statistical analysis on linked databases
  - **New**: first-ever voluminous registry-based MPC application
- **Problem**: by 2012, nearly 43% of IT students enrolled in Estonia’s universities in the last five years had failed to graduate
- **Hypothesis**: Estonia’s booming IT industry is hiring too hungrily and causing students to fail at school
- **Question**: do IT students work more in parallel with studies?
- **Result**: no relation between working during studies and not graduating on time for IT-students

June 26, 2017
Estonia 2014: IT Student Graduation Rate was around 40%
Regulation Prevented a Data-Driven Answer

Tax records

Has the student worked?
In which period?
In an IT company?

Barriers
Data Protection
Tax Secrecy

How is working related to not graduating on time?

Education records

When did student enrol?
When did he/she graduate?
In an IT curriculum?
The data owner can maintain control of processing by co-hosting Sharemind.

Sharemind achieves compliance with privacy requirements and security policies by processing data in an encrypted form.

Only final results are published to the analyst.

Relations between working and school dropout.
Sharemind® Powered the Privacy-Preserving Study in the PRIST project

- Source data:
  - 10 million tax records,
  - 600,000 education records.
- Sharemind hosted by government agencies and Cybernetica.
- Data owners used the Sharemind encryption tools to upload data.
- Data never existed outside the source in an unencrypted state.
Sharemind® Powered the Privacy-Preserving Study in the PRIST project

- Data scientists used Sharemind tools to run the analysis.
- Sharemind prevented queries outside the study plan.
- Reports were given to industry, universities and the government.
- **Result**: no clear relation between working during studies and not graduating.
Achievements in Practical Applications (2)

- **2016 – 2017 SEN project**: implementing Sharemind to evaluate the efficiency of support measures for students with special educational needs (SEN)
  - Data owners were the same as in the PRIST project (Tax and Customs Board, Ministry of Education and Science)
  - **New**: Input data for an MPC application was partially stored on a cloud server for the first time
  - **Questions**: What is the employment rate of pupils with SEN after school? Does employment and salary depend on learning in special classes or inclusive education in regular schools?
  - **Result**: The employment rate is related to the special educational need. Students with SENs that need a lot of support are somewhat less likely to be employed.
Is Sharemind® Compliant with Data Protection Regulations? (1)

- Estonia’s Data Protection Authority (EDPA) declined to review our application for a permission to process personal data in the PRIST project.
  - EDPA: no need for EDPA’s permission because there is no processing of personal data taking place in the given circumstances (data is unidentifiable).
  - EDPA: the combination of technology and processes ensured that private data was not processed and the requirements of the Data Protection Act need not apply.
- Assumption: no identifiable records are published.
Is Sharemind® Compliant with Data Protection Regulations? (2)

- EDPA stated that if data controllers encrypt data and no personal data is not published from the study, further studies with Sharemind do not need to apply for the DPA permit.
  - SEN project involved sensitive data (students with special educational needs)
  - Essentially the same conclusion as for the PRIST project
EDPA Letter 29.08.2016 No 2.1.-5/16/1271 (translation)

“Having analysed your … application and taking into consideration the additional clarifications provided by you … our position is that it is not necessary to apply for a permission from the DPA for carrying our a research project using a method whereby data providers insert the personal data in the given sample to Sharemind. This principle applies, if the data providers do not exchange personal data before inserting them to Sharemind and the data does not reach the researcher in identifiable form in any of the phases of the research.”
What will Change for Sharemind® in the Context of the GDPR?

- Sharemind can be used:
  - by data owners (controllers): an appropriate technical measure designed to implement data-protection principles (GDPR article 25 (1))
  - by data owners (controllers): an appropriate technical measure to ensure that by default personal data are not made accessible to an indefinite number of natural persons without the individual's intervention (GDPR article 25 (2))
  - by data analysts (processors): a tool for analysing anonymous data (GDPR recital 26)
Does Sharemind® Process Personal Data?

Input parties → Computation nodes → Computation nodes → Result party
Additional Information (1)

- The secret sharing used in Sharemind is standardised in ISO/IEC 19592-2 and achieves up to information-theoretic security (as good as one time pad in cryptography).

- For further legal analysis on secret sharing, please see:
Additional Information (2)

- For further information and analysis on secret sharing, please see:
  - The full overview of the modules and ancillary elements of the Sharemind technology is available at https://sharemind.cyber.ee/secure-computing-platform/.

June 26, 2017
Recent Publications on Sharemind®

  - Available at: http://ieeexplore.ieee.org/document/7676176/
  - (Also: http://eprint.iacr.org/2015/1039)

  - Available at: http://dx.doi.org/10.1515/popets-2016-0019