From research to production: the cases of internet voting and confidential data analysis

Oliver Väärtnoo, CEO
25.07.2017
Our Story from the Beginning…

kubevnićs (kybernetēs)
"steersman, governor, pilot, or rudder"

1948 Norbert Weiner, "the scientific study of control and communication in the animal and the machine."

1956 Louis Couffignal, "the art of ensuring the efficacy of action."

1960 Institute of Cybernetics, Estonian Academy of Sciences.
About Cybernetica

- **Estonian ICT company**, founded in 1997
- We develop and sell **mission-critical** e-government, information security, radio communications and surveillance software products and systems
- We inspire **new areas of advancement through** interactions between **research and development**
- As of 2016 **we are 120 people** and **10 MEUR in revenues**
  - 50% from exports (Main markets: Indonesia, USA, EU).
Internet Voting
Internet Voting in Estonia, a brief history

- 2001 - first research on the topic in Cybernetica
- 2003 - participation in National Elections Council’s Working group
  - Design and security analysis of the system
- 2004 - procurement for the system design, realization and support
- 2005 - first internet voting enabled elections
- 2009 - voting application renewal (tech upgrade and new threats)
- 2013 - introduction of a mobile device based verification application
- 2014 - joint venture between Smartmatic and Cybernetica
- 2017 - full system upgrade in Estonia (end-to-end verification)
Internet Voting in a Nutshell

- Encrypted vote
- Signed vote
- Public/private key pair

[Diagram of internet voting process involving encryption and signing]
Internet Voting in Estonia

% of citizens
% of voters

0%  5%  10%  15%  20%  25%  30%  35%
Sharemind®, the Concept

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

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 confidential data.
- Sharemind® processes the queries without removing the protection.
- Authorized users receive query results in an encrypted format.
Value Added Tax Avoidance is a 100M€+ Problem
Solving the Problem with Sharemind

- Confidentiality of honest taxpayers is guaranteed from both internal leaks and external attacks.
- There is no single party who can decrypt data and, thus, break privacy. Control is distributed among parties.

Sharemind-based risk analysis system matches encrypted declarations without decrypting them and finds companies with a risk of VAT fraud.
Estonia 2014: IT Student Graduation rate is around 40%
Regulation Prevented a Data-Driven Answer

Tax records

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

Data Protection
Tax Secrecy

How is working related to not graduating on time?

Barriers

Education records

When did student enrol?
When did he/she graduate?
In an IT curriculum?
Notable Points about the Study

- The Estonian Data Protection Agency stated that 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.
- The Internal Oversight of the Tax and Customs Board agreed to provide unmodified tax records after a code and process review.
International Evaluation on Scientific Excellence, 2017: “Cybernetica provides an outstanding example of a commercial R&D unit.”