ESSENTIAL

Evolving Security ScienE through Networked Technologies, Information policy And Law

INTRODUCING MY PhD RESEARCH

Merve **Baş Seyyar**

university of groningen

NTNU
Norwegian University of Science and Technology

Netherlands Forensic Institute
Ministry of Justice and Security

COINS Winter School, Finse, Norway, 07 May 2019

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Agenda

- Introducing myself
- Introducing Essential Project
- Introducing my research
  - Research problem
  - Planned contributions
  - Research questions
  - Choice of methods
  - Current work
    - Introducing Hansken
    - Introducing PIA

PIA: Privacy Impact Assessment

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Who am I?

- ✓ B.Sc. in Mathematics,
- ✓ M.Sc. in Cyber Security Engineering,

- ✓ 2.5 years working experience as a researcher at Cyber Security Institute in TUBITAK,

- ✓ Since January 2018, PhD Researcher at UG and NTNU,
- ✓ Currently at NFI.

TUBITAK: Scientific and Technological Research Council of Turkey
NFI: Netherlands Forensic Institute
UG: The University of Groningen

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

ESSENTIAL Project

Evolving Security SciencE through Networked Technologies, Information Policy And Law (https://www.essentialresearch.eu/)

- Funded under EU's Horizon 2020 (H2020) Marie Sklodowska-Curie Innovative Training Networks,
- 13 Early-Stage Researchers (ESRs), 6 Academic Beneficiaries, 7 Industrial partners,
- Interdisciplinary, double or joint PhD degree,
- ESSENTIAL's 2 main goals:
  1. to train inter-disciplinary security experts and professionals, to tackle security threats in a systematic manner.
  2. to increase societal resilience and security by addressing in an interdisciplinary manner 15 research topics.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Problem Description

The increasing volume in data collection and processing necessitates reconsideration of existing digital forensics (DF) process from a different angle, this of privacy preservation. In order to prevent privacy abuses more efficiently, a shift towards proactive solutions like Privacy by Design (PbD) and privacy by default is expected. This new point of view has not been addressed yet in DF.

Privacy by Design in Large Scale Digital Forensics

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Research Questions

1. How to detect and limit privacy exposures during DF process?
2. What strategies are used to enforce PbD out of the forensics scope?
3. What are the data and process oriented aspects of DF related to PbD?
4. What are the effects of big data to PbD?
5. How to implement PbD without reducing the effectiveness and speed of digital investigations?

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Planned Contributions

- Finding better and effective ways of limiting privacy exposures during a digital investigation.
- Providing a basis for better understanding of the current state of the art concerning PbD.
- Introducing a framework adding end to end life cycle protection for personal data.
- Providing compliance with Directive (EU) 2016/680 and accountability, transparency.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Choice of Methods

- Literature Review
- Case Study
  - Privacy Impact Assessment (PIA) on Hansken
- Semi-structured Interview (@NFI & @Økokrim)
- Experimentation
  - Differential Privacy >>> Privacy Enhancing Technology
  - Fuzzy Logic >>> Privacy Preserving Data Mining
- Implementation and evaluation of proof of concept

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Current Work

Research Questions:

1) How to conduct PIA in big data forensics?
2) What are privacy risks in DF when processing large amount of data?

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

What is Hansken?

A service-based approach for processing and investigating multiple terabytes of seized digital material:

Digital Forensics as a Service (DFaaS).

Hansken
Netherlands Forensic Institute

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Key Ideas

HANSKEN

- Minimization of the case lead time,
- Maximization of the trace coverage and
- Specialization of people involved.

XIRAF
(Hansken's predecessor)

- Automated pre-processing,
- Uniform data representation,
- A set-based query model,
- Web-based access.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Hansken's Design & Implementation Principles:

1. Security (Confidentiality, Integrity, Availability)
2. Privacy
3. Transparency
4. Multi tenancy
5. Future proof
6. Data retention
7. Reliability
8. High availability

Sociological Needs

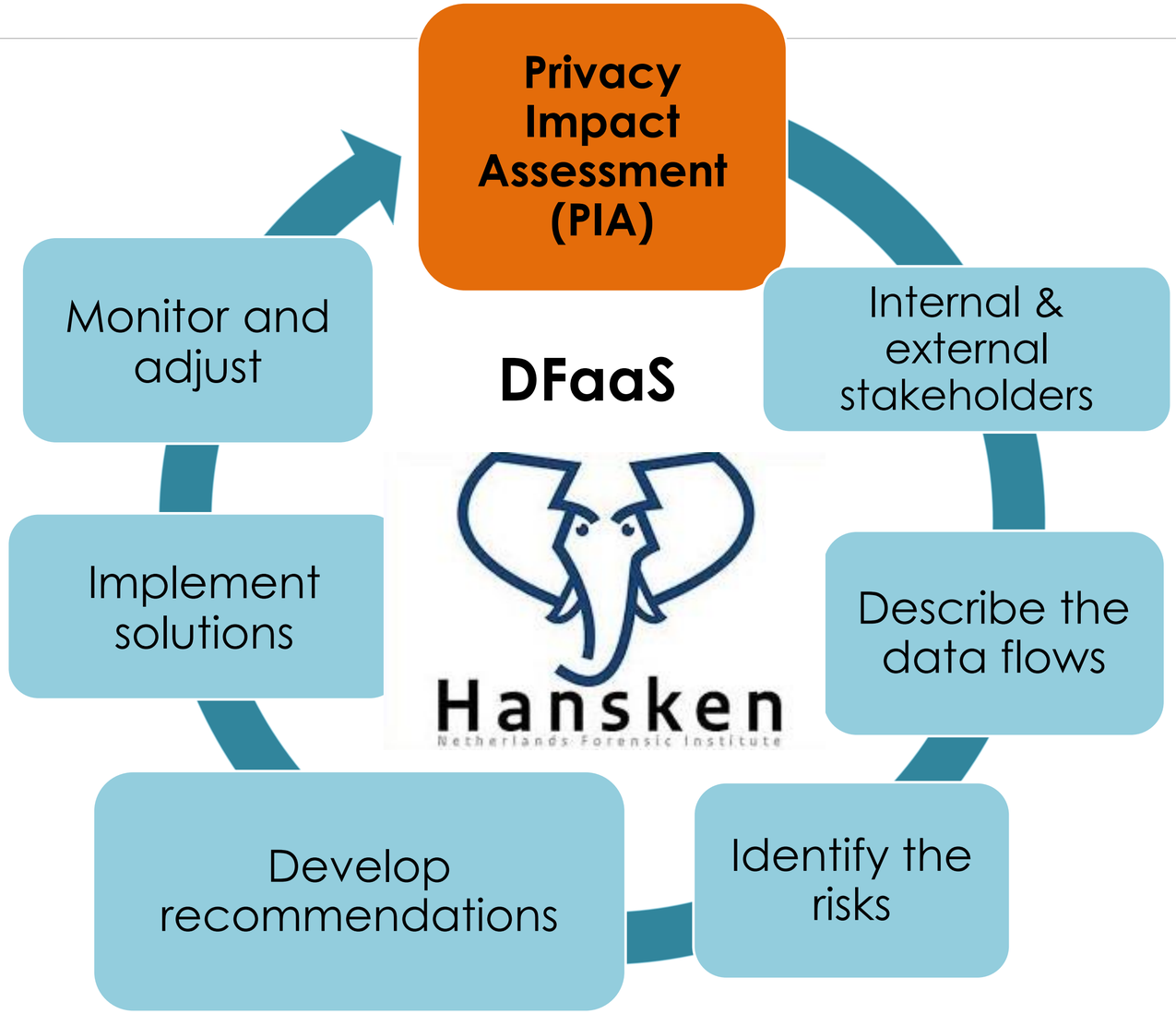
Business Needs

Distributed Implementation

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

PIAs

PIAs are tools to evaluate
the origin, nature, particularity and severity of risks
to the rights and freedoms of natural persons
to determine the appropriate measures.



This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.

Thank you for your attention

m.bas.seyyar@essentialresearch.eu
merve.seyyar@ntnu.no

References

- W. Alink, R. A. F. Bhoedjang, P. A. Boncz, and A. P. de Vries. XIRAF – XML-based indexing and querying for digital forensics. Digital Investigation, 3:50–58, Sept. 2006.
- European Union. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 and repealing Council Framework Decision 2008/977/JHA, May 2016.
- T. Marquenie. The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework. Computer Law & Security Review, 33(3):324–340, June 2017.
- Ministerie van Justitie en Veiligheid. Hansken - Products and services - Netherlands Forensic Institute, https://www.forensicinstitute.nl/research-and-innovation/latest-forensic-innovations/hansken
- H. M. A. van Beek, E. J. van Eijk, R. B. van Baar, M. Ugen, J. N. C. Bodde, and A. J. Siemelink. Digital forensics as a service: Game on. Digital Investigation, 15:20–38, Dec. 2015.
- K. Wadhwa and R. Rodrigues. Evaluating privacy impact assessments. Innovation: The European Journal of Social Science Research, 26(1-2):161–180, Mar. 2013.

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant Agreement No. 722482.