Oslo Activities related to the Secure Connected Trustable Things

Christian Johansen

University of Oslo

cristi@ifi.uio.no

@

19th SWITS Seminar within the
Framework of the Swedish IT Security Network for PhD students
3-4 June 2019, Karlstad

I will present:

- 3 projects: SCOTT, IoTSec, MeasurEGrid
- 7 research topics

Main people involved, from Oslo (others mentioned further):


Olaf Owe


Josef Noll


Manish Shrestha


Farzane Karami


Toktam Ramezani


Elahe Fazeldehkordi


Shukun Tokas


Tore Pedersen


Namrah Azam


Hamed Arshad


Maunya Moghadam

SCOTT: Joint Undertaking

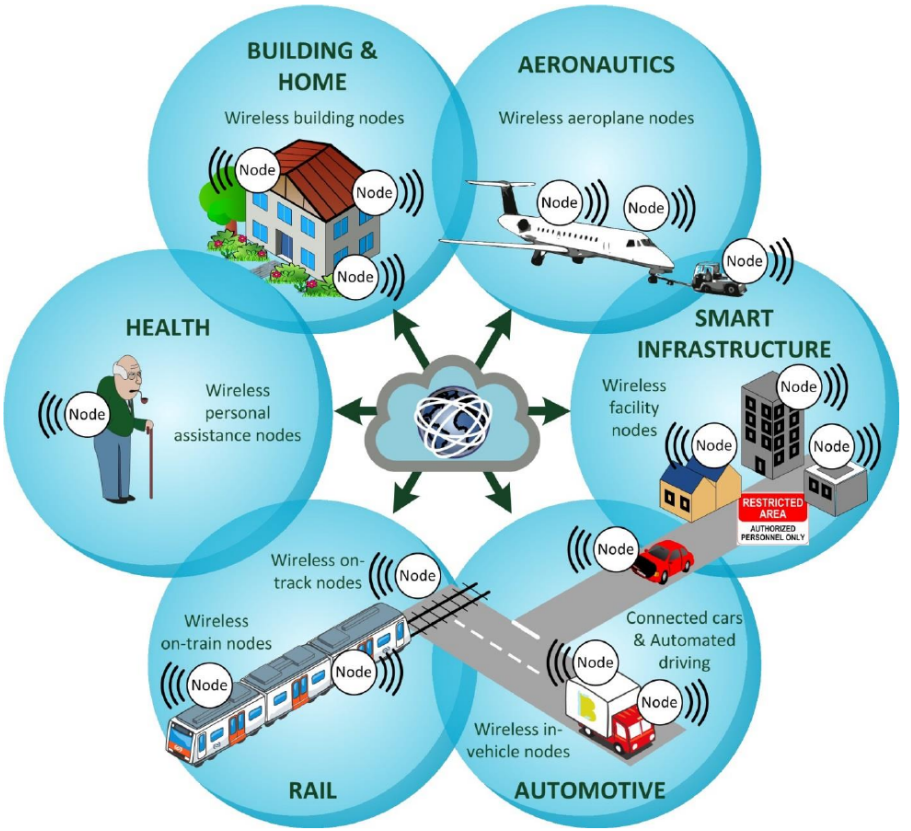
- 3 years project, financed in part by JU ECSEL and National governments research council
- 57 partners from 12 countries (EU + Brazil)
- total budget ca.39 M€, EU support 10.5 M€, national 12.5 M€

SCOTT: Joint Undertaking

- 3 years project, financed in part by JU ECSEL and National governments research council
- 57 partners from 12 countries (EU + Brazil)
- total budget ca.39 M€, EU support 10.5 M€, national 12.5 M€
- Coordinated by Virtual Vehicle Institute in Austria;
  - Technology Coordinator: University of Oslo (UiO)
- NO partners: UiO; OsloMet;
  Eye Networks; TellU; Telenor;
  Smart Innovation Norway; Wolffia

SCOTT: Joint Undertaking

- 3 years project, financed in part by JU ECSEL and National governments research council
- 57 partners from 12 countries (EU + Brazil)
- total budget ca.39 M€, EU support 10.5 M€, national 12.5 M€
- Coordinated by Virtual Vehicle Institute in Austria;
  - Technology Coordinator: University of Oslo (UiO)
- NO partners: UiO; OsloMet;
  Eye Networks; TellU; Telenor;
  Smart Innovation Norway; Wolffia
- 15 Industrial Use Cases / Pilots
- 4 Technology Lines with
  - ca. 50 Tech. Building Blocks
- Norway: Managin 5 BBs:
  - BB24.A Managed Wireless
  - BB24.I Semantic ABAC (UiO)
  - BB24.L Network slicing
  - BB26.F Measurable Security (UiO)
  - BB26.G Privacy labels (UiO)



SCOTT: Joint Undertaking

UiO works on:

- Managed Wireless
  - Together with Eye Networks to detect faults in wireless infrastructure and to redress them remotely. Applied to home and office environments.
- Network slicing
  - Together with OsloMet and Telenor
    to provide wireless security based on SDN-style of network separations, applied to 5G technology and for IoT to have basic connectivity.
- WP30 - Open Innovation Arena
  - Managing the innovation activities of SCOTT (not technical)
    Josef has very good experience with such technology transfer
- Semantic ABAC and Measurable security are mentioned later.
- Links: http://scott-project.eu NO site: https://its-wiki.no/wiki/SCOTT:Home


Josef Noll


Maunya Doroudi Moghadam


Hamed Arshad


Toktam Ramezani


Christian Johansen

IoTSec – Security in IoT for Smart Grids

- 5 years project, financed in part by Norwegian Research Council
- total budget ca.32 MNOK until 2020
- Coordinated by University of Oslo
- 6 founding partners (+ ca. 10 associated):
  UiO; Norwegian Computing Centre;
  Simula research labs; NTNU@Gjøvik;
  eSmart Systems; Smart Innovation Norway;

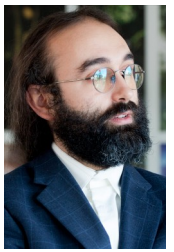
- Link: https://its-wiki.no/wiki/IoTSec:Home


Josef Noll


Olaf Owe

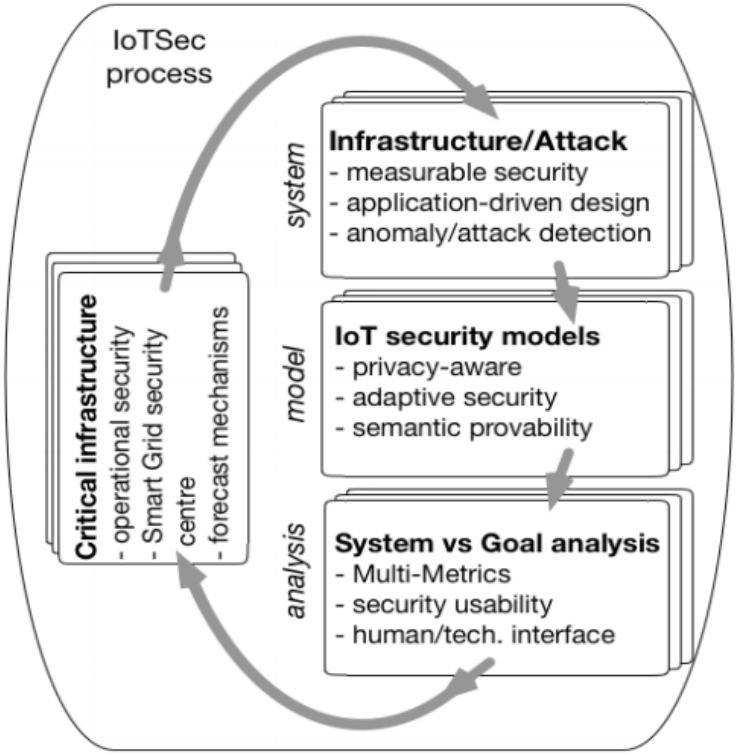

Elahe Fazeldehkordi


Namrah Azam


Christian Johansen

IoTSec – Security in IoT for Smart Grids

- 5 years project, financed in part by Norwegian Research Council
- total budget ca.32 MNOK until 2020
- Coordinated by University of Oslo
- 6 founding partners (+ ca. 10 associated):
  UiO; Norwegian Computing Centre;
  Simula research labs; NTNU@Gjøvik;
  eSmart Systems; Smart Innovation Norway;
- Working on:
  - Smart Grid distribution net security;
  - SmartMeter communication security with Norwegian Energy Directorate (NVE)
  - Adaptive security;
  - Formal modelling and verification
  - Human aspects in security
- Link: https://its-wiki.no/wiki/IoTSec:Home




Josef Noll


Olaf Owe


Elahe Fazeldehkordi


Namrah Azam


Christian Johansen

MeasurEGrid – Measurable security and privacy for services on the Smart Electricity Grid

- 4 years project, financed in part by Norwegian Research Council and eSmart Systems (in Halden)
- 1 PhD student hired: Manish Shrestha (finishing 2020)

- links

www.mn.uio.no/its/english/research/projects/measuregrid/

Manish Shrestha

Josef Noll

Davide Roverso

Christian Johansen

MeasurEGrid – Measurable security and privacy for services on the Smart Electricity Grid

- 4 years project, financed in part by Norwegian Research Council and eSmart Systems (in Halden)
- 1 PhD student hired: Manish Shrestha (finishing 2020)

- Working on:
  - Smart Grid Security Classification;
  - Applied to Smart Home Energy Management Systems;
  - Using the Multi-metrics approach to Measurable Security (see Josef)
  - Using the tool NOR-STA (from Gdansk University)
  - Extending ANSSI methodology with details about Connectivity and Protection mechanisms

- links

www.mn.uio.no/its/english/research/projects/measuregrid/

Table 6: Smart Grid Security Classes.

Catastrophic	Class A	Class D	Class E	Class F	Class F
Major	Class A	Class B	Class D	Class E	Class F
Moderate	Class A	Class B	Class C	Class E	Class E
Minor	Class A	Class B	Class B	Class C	Class D
Insignificant	Class A	Class A	Class A	Class B	Class C
Impact / Exposure	E1	E2	E3	E4	E5

Table 5: Exposure evaluation: Connectivity (Sec. 3.1) vs. Protection Level.

PL1	E4	E4	E5	E5	E5
PL2	E3	E3	E4	E4	E4
PL3	E2	E2	E3	E3	E3
PL4	E1	E1	E2	E2	E2
PL5	E1	E1	E1	E1	E1
Protection / Connectivity	C1	C2	C3	C4	C5

Manish Shrestha

Josef Noll

Davide Roverso

Christian Johansen

Measurable security, privacy, and dependability

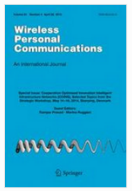
- Josef has promoted during several projects (pSHIELD; nSHIELD; IoTSec)
- Multi-metrics for compositional measuring of SPD of complex syst.

Josef Noll

Measurable security, privacy, and dependability

- Josef has promoted during several projects (pSHIELD; nSHIELD; IoTSec)
- Multi-metrics for compositional measuring of SPD of complex syst.
- Some Outcomes:
  - A book
    Info: ISBN 9781138042759 from CRC Press
  - PhD defended + seeral MSc theses
  - Adopted in the SCOTT project

Josef Noll



Wireless Personal Communications

April 2015, Volume 81, Issue 4, pp 1359–1376 | Cite as

Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems

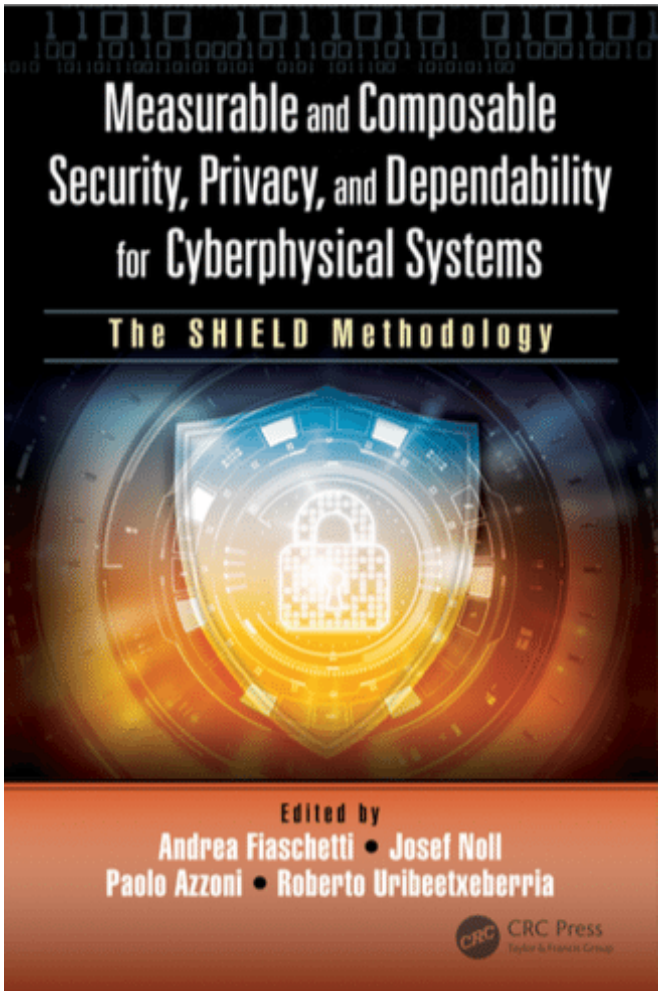
Authors | Authors and affiliations

Iñaki Garitano, Seraj Fayyad, Josef Noll

Article

First Online: 13 March 2015

536 Downloads | 13 Citations



Semantic Attribute Based Access Control

- **Hamed Arshad**
  - Is PhD student in the Reliable Systems group at UiO
  - Working with SCOTT on the Semantic ABAC tech.block

Hamed Arshad

Josef Noll

Christian Johansen

Semantic Attribute Based Access Control

- **Hamed Arshad**
  - Is PhD student in the Reliable Systems group at UiO
  - Working with SCOTT on the Semantic ABAC tech.block
- Combining Semantic technologies with Attribute Based Access Control
  - Attributes for: *subjects, resources, context, action*, have values
  - Are mutable, e.g., nrFilmViews++
  - Are used to define a Role (dynamically): Position=Doctor AND Speciality=Cardeology


Hamed Arshad


Josef Noll


Christian Johansen

Semantic Attribute Based Access Control

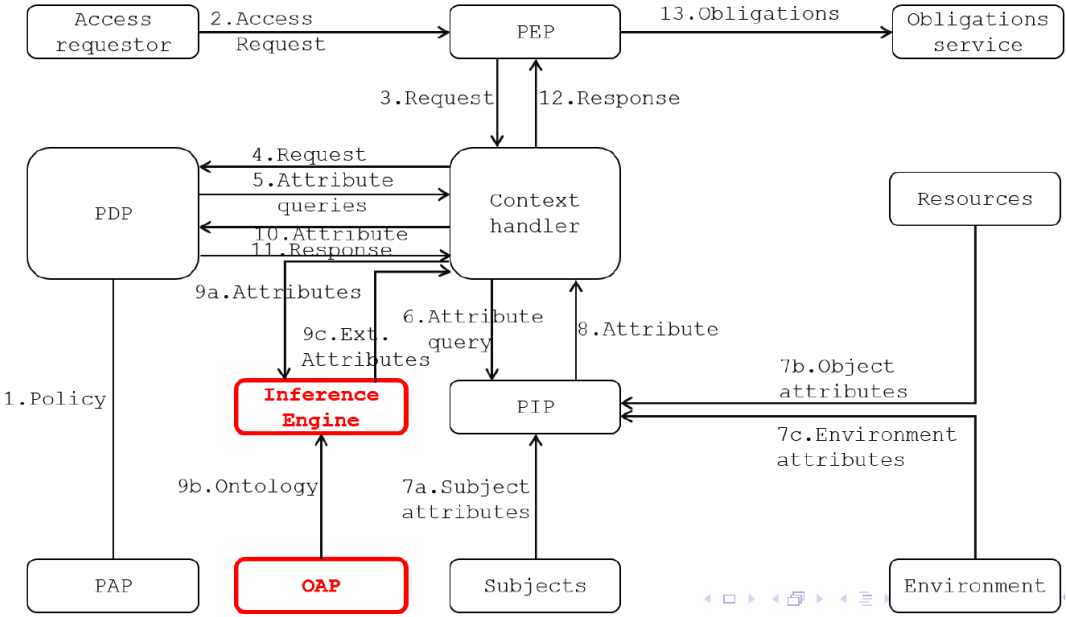
- **Hamed Arshad**
  - Is PhD student in the Reliable Systems group at UiO
  - Working with SCOTT on the Semantic ABAC tech.block
- Combining Semantic technologies with Attribute Based Access Control
  - Attributes for: *subjects, resources, context, action*, have values
  - Are mutable, e.g., nrFilmViews++
  - Are used to define a Role (dynamically): Position=Doctor AND Speciality=Cardeology
- Ontology reasoning to:
  - Combine equivalent terminology Doctor == Lege
  - Infere complex policies „Adult“ can be inferred from „DriverLicence“ or „Age > 18“

Hamed Arshad

Josef Noll

Christian Johansen

- ***Extending the XACML architecture***
  - Adding a component to the architecture



Attribute Based Encryption with Enforcible Obligations using Intel SGX

- Hamed did internship at Chalmers and started work with Gerardo and Pablo on
  - OB-ABE: Adding enforcible obligations over arbitrary ABE schemes
  - Adding Ontology reasoning to ABE

Hamed Arshad

Pablo Picazo-Sanchez
(Chalmers/Gothenburg)

Gerardo Schneider
(Chalmers/Gothenburg U.)

Christian Johansen

Attribute Based Encryption with Enforcible Obligations using Intel SGX

- Hamed did internship at Chalmers and started work with Gerardo and Pablo on
  - OB-ABE: Adding enforcible obligations over arbitrary ABE schemes
  - Adding Ontology reasoning to ABE
- More on OB-ABE:
  - Uses hardware security guarantees from Intel SGX to enforce before decryption the execution of Obligations like: sendEmail; notifyBySMS; log;
  - All clients much have CPUs with Intel SGX enabled
  - Properties :
    A) Enforcible Obligations (proven using ProVerif)
    B) Backward Compatibility
    C) Conservative Extenssion (wrt. ABE Sec.Props.)

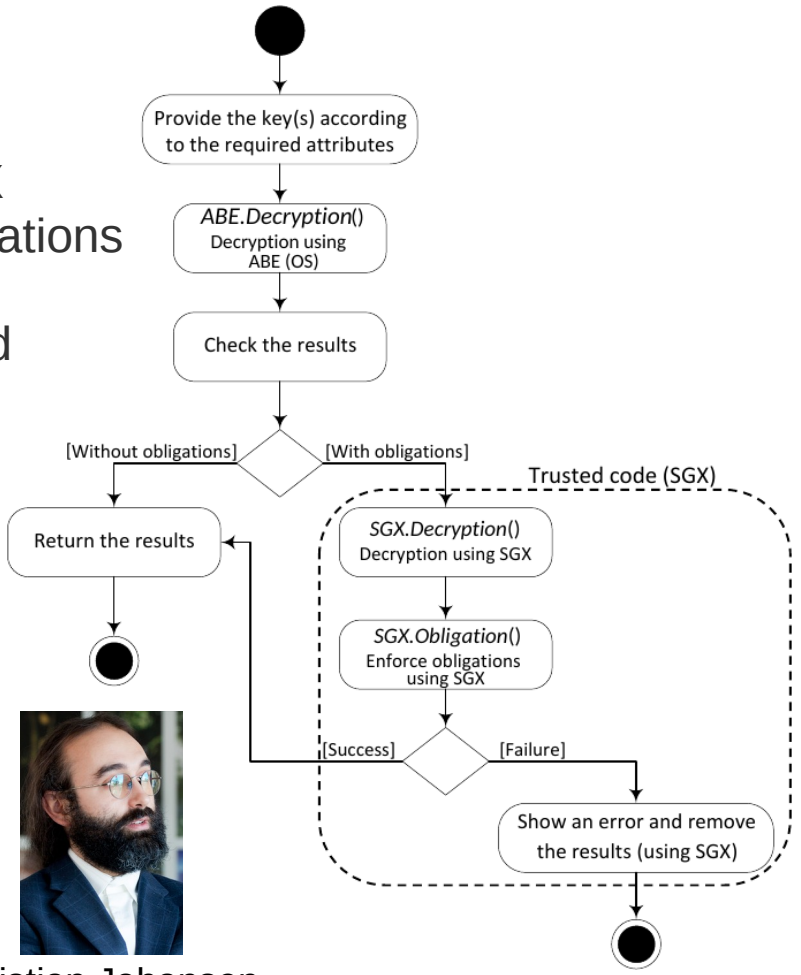


Fig. 4: Decryption process of the OB-ABE scheme.

Hamed Arshad

Pablo Picazo-Sanchez
(Chalmers/Gothenburg)

Gerardo Schneider
(Chalmers/Gothenburg U.)

Christian Johansen

Wrappers for Secure Concurrent Objects

- **Farzane Karami**
  - Is PhD student in the Reliable Systems group at UiO
  - With main supervisor Olaf Owe
- Internship at Chalmers and started working with Gerardo as well

Farzane Karami

Olaf Owe

Gerardo Schneider
(Chalmers/Gothenburg U.)

Christian Johansen

Wrappers for Secure Concurrent Objects

- **Farzane Karami**
  - Is PhD student in the Reliable Systems group at UiO
  - With main supervisor Olaf Owe
- Internship at Chalmers and started working with Gerardo as well
- Information Flow security
  - for Concurrent Object-Oriented languages with Futures
  - based on the Actor model of concurrency (e.g., Scala, Creol)
  - uses wrappers arround both objects and futures to manage the information flow at run-time
  - This is a trade-off between
    - Static-analysis, which is restrictive, and
    - Run-time analysis, which is slow

Basic constructs

$X := E$
$X := \texttt{new}\ C(\overline{E})$
$X := \texttt{new}_{Lev}\ C(\overline{E})$
`return` E
`if` C `th` S [`el` S'] `fi`
`while` C `do` S `od`

Call constructs

$!M(\overline{E})$
$Q!M(\overline{E})$
$Q!O.M(\overline{E})$

Access constructs

$Q?(\overline{X})$
[`await` $Q?$]; $Q?(\overline{X})$

Figure 2: Unified Synta

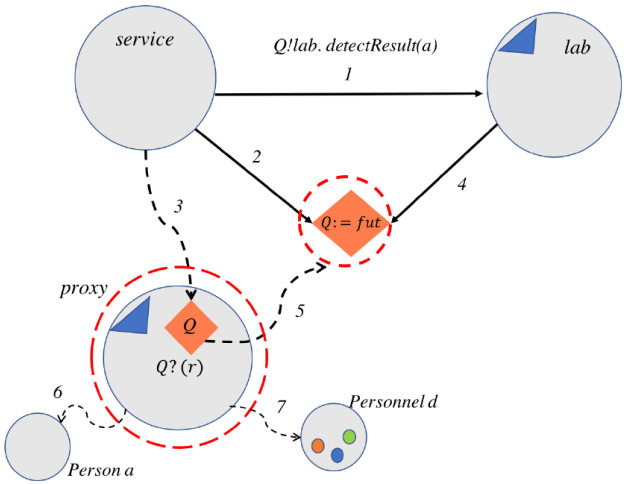


Figure 8: Information flow security regarding wrappers.


Farzane Karami


Olaf Owe


Gerardo Schneider
(Chalmers/Gothenburg U.)


Christian Johansen

Object-Oriented and Privacy-by-Design

- **Shukun Tokas**
  - Is PhD student in the ConSeRNS interdisciplinary group at UiO
  - With main supervisor Olaf Owe
- Develop Object-Oriented programming languages
  - Extended with privacy specification concepts
    - Principals ; Purposes ; Access rights
  - And Proof techniques to guarantee privacy policy compliance
- Goal: „To help bridge the gap between GDPR and programmers“

Shukun Tokas

Olaf Owe

Object-Oriented and Privacy-by-Design

- **Shukun Tokas**
  - Is PhD student in the ConSeRNS interdisciplinary group at UiO
  - With main supervisor Olaf Owe
- Develop Object-Oriented programming languages
  - Extended with privacy specification concepts
    - Principals ; Purposes ; Access rights
  - And Proof techniques to guarantee privacy policy compliance
- Goal: „To help bridge the gap between GDPR and programmers“
- Details:
  - Object Interfaces are the Principals;
  - Latice of Purposes and Access rights are used to Annotate Methods
  - Type-and-effect system is used to prove compliance by static analysis

```
interface Doctor extends Nurse{
  Void doctorTask(Patient p) :: P_Doc
}
```

Shukun Tokas

Olaf Owe

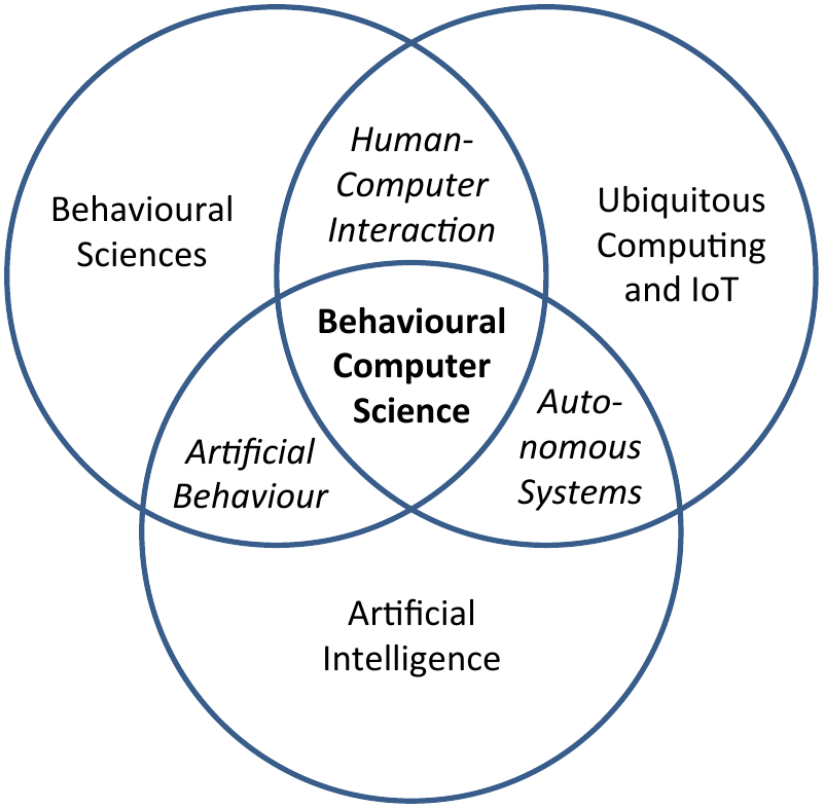
$$
\begin{array}{lcll}
A & ::= & read \mid incr \mid rincr \mid write \mid self & \text{basic access rights} \\
 & & \mid A \sqcap A \mid A \sqcup A & \text{combined access rights} \\
\mathcal{P} & ::= & (I, R, A) & \text{policy} \\
\mathcal{P}s & ::= & \{\mathcal{P}^*\} \mid \mathcal{P}s \sqcap \mathcal{P}s \mid \mathcal{P}s \sqcup \mathcal{P}s & \text{policy set} \\
\mathcal{RD} & ::= & \textbf{purpose}\ R^+ & \\
 & & [\textbf{where}\ Rel\ [\textbf{and}\ Rel]^*] & \text{purpose declaration} \\
Rel & ::= & R^+ < R^+ & \text{sub-purpose declaration}
\end{array}
$$

Security Ceremonies

- Concept coined in 2007 by Carl Ellison
- Two main aspects/challenges
  - Incorporating the Human as nodes
    - in such a way to make analysis and security proofs possible.
  - Composition of Protocols
    - in parallel, sequential, vertical, etc.
- Tore Pedersen
  from the Norwegian Defence Intelligence School
  does research in Behavioural Sciences
  - We focus on human models (e.g., persona)
  - How can these be used by formal methods?


Tore Pedersen


Christian Johansen



Thank you for your Attention!

Christian Johansen

University of Oslo

cristi@ifi.uio.no

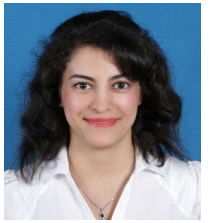

Olaf Owe

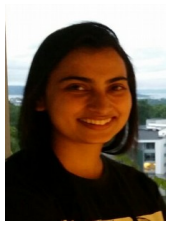

Josef Noll


Manish Shrestha


Farzane Karami


Toktam Ramezani


Elahe Fazeldehkordi


Shukun Tokas


Tore Pedersen


Namrah Azam


Hamed Arshad


Maunya Moghadam