My Experience doing a PhD

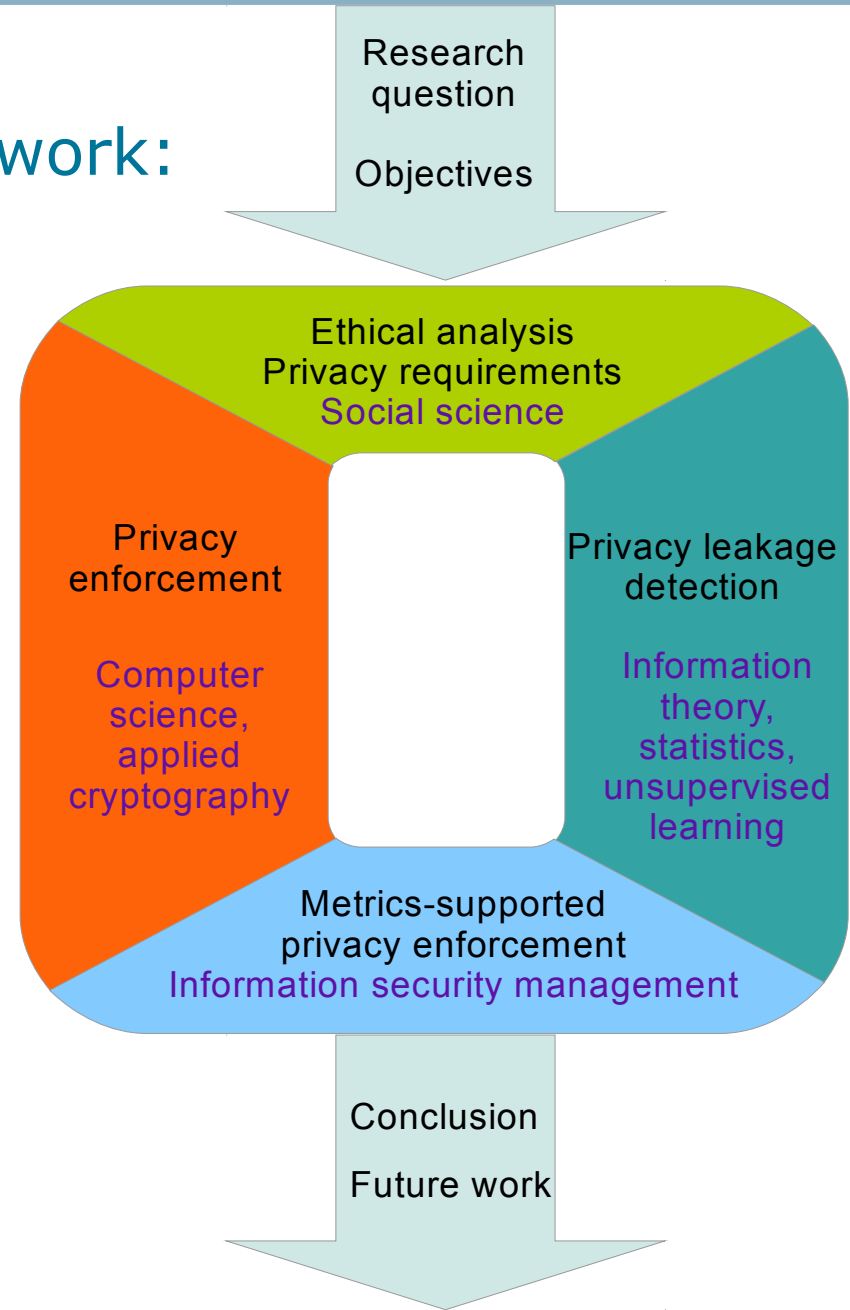Nils Ulltveit-Moe <nils.ulltveit-moe@uia.no>

2014 COINS Ph.D. student seminar, Tromsø, 13-15. October

UNIVERSITY OF AGDER

telenor

Prevention, protection and REaction to CYber attackS to critical infrastructurEs
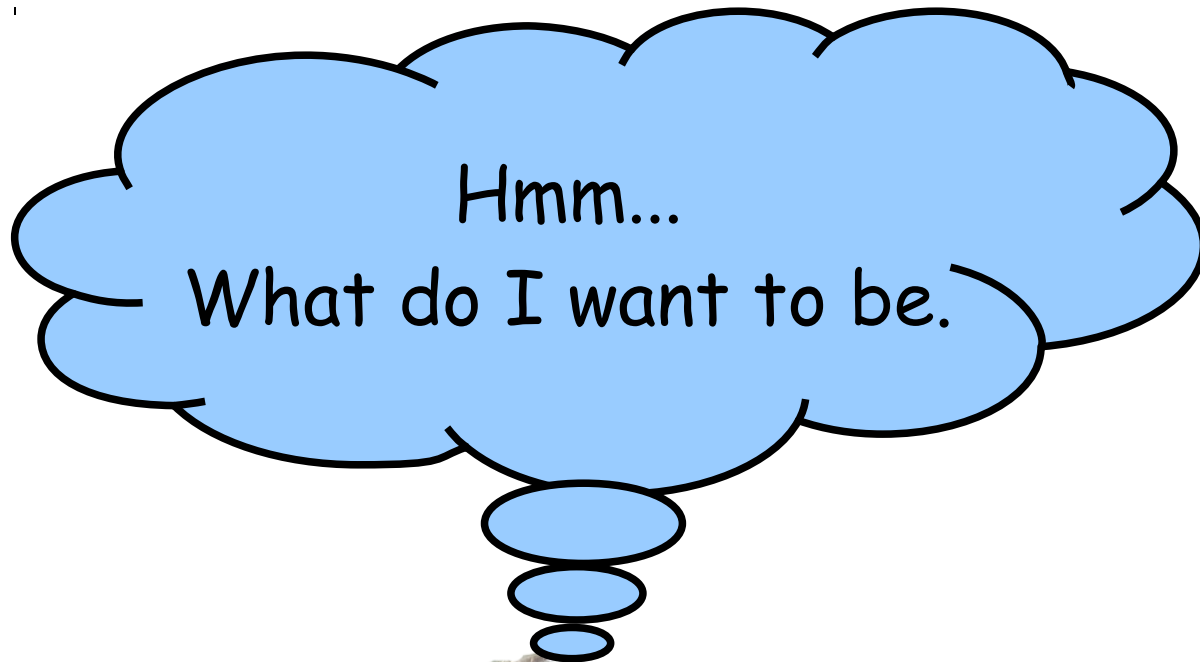PRECYSE

SEVENTH FRAMEWORK PROGRAMME
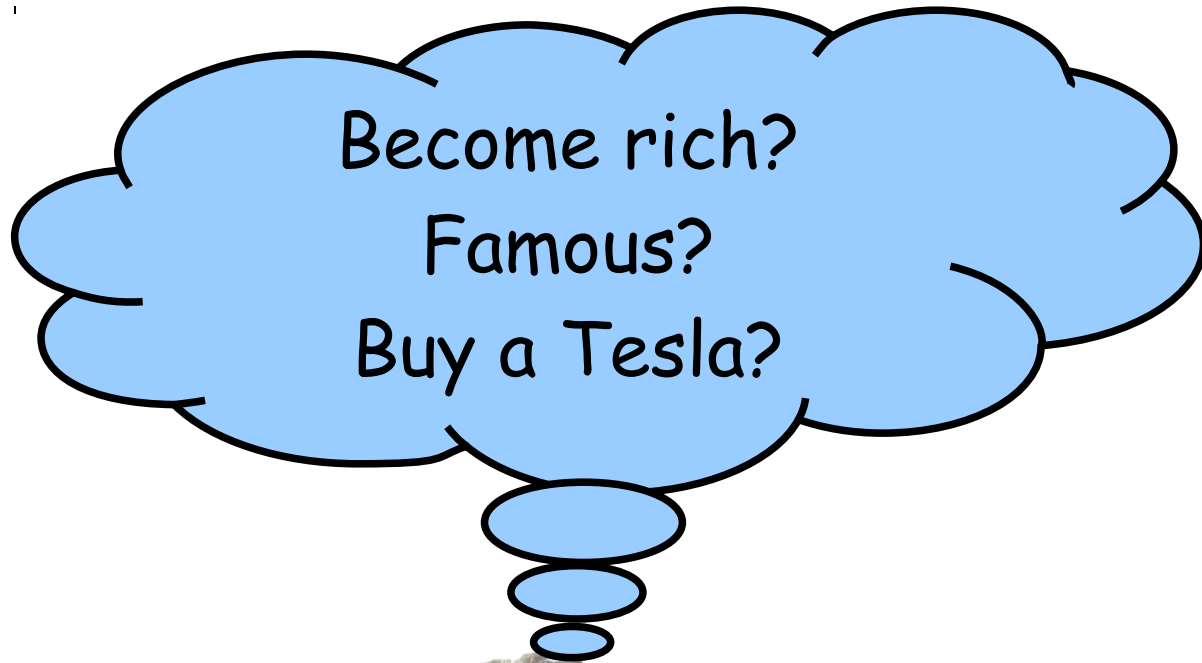
A polished view of my PhD work:

- Research Objective:
  Reduce leakage of private or confidential information in Intrusion Detection System (IDS) alarms
- Two main research topics:
  - Privacy leakage metrics
  - Enforcement of privacy policies

Research question

Objectives

Ethical analysis
Privacy requirements
Social science

Privacy enforcement

Computer science, applied cryptography

Privacy leakage detection

Information theory, statistics, unsupervised learning

Metrics-supported privacy enforcement
Information security management

Conclusion

Future work

Reality - me having a 40 years crisis.

Reality - me having a 40 years crisis.

Become rich?
Famous?
Buy a Tesla?

Reality - me having a 40 years crisis.

Well - it did not really start like this, but almost:

- I already worked with a FP6 project: **EIAO**
- Project came to conclusion.
- What shall I do now?
  - Work in industry, earn money?
  - Go back to full-time teaching?
  - Or continue with research?
- The thought of doing a PhD grew on me...
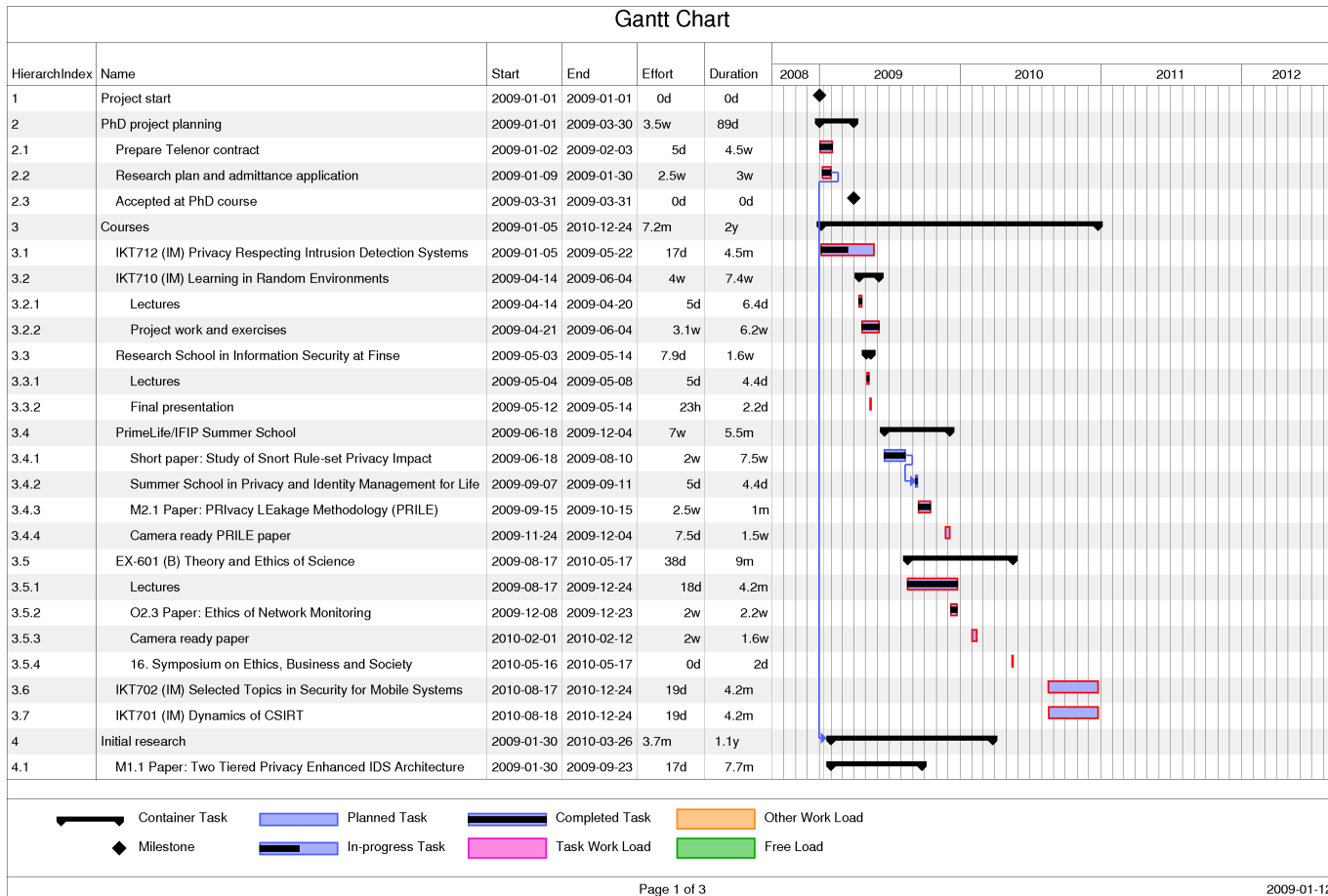
Take a PhD!

The decision:

- My fantastic supervisor, professor Vladimir Oleshchuk, convinced me - *Take a PhD in information security!*

- But:
  - Can I afford it?
  - Am I good enough?
  - Will I get the position?

Take a PhD!

Personal objectives

- I wanted my PhD work to be interesting and relevant for future research
- I wanted to update my knowledge to be more industry-relevant, to increase my market value
  - This is useful, for example when doing salary negotiations...
- I wanted to make the world a little better place to live in
  - Do research that makes a difference
- I wanted to lay the foundations for future research projects
- No overtime (yeah, right...)
- Ultimately, I planned for an academic career.

Planning the PhD

HierarchIndex	Name	Start	End	Effort	Duration
1	Project start	2009-01-01	2009-01-01	0d	0d
2	PhD project planning	2009-01-01	2009-03-30	3.5w	89d
2.1	Prepare Telenor contract	2009-01-02	2009-02-03	5d	4.5w
2.2	Research plan and admittance application	2009-01-09	2009-01-30	2.5w	3w
2.3	Accepted at PhD course	2009-03-31	2009-03-31	0d	0d
3	Courses	2009-01-05	2010-12-24	7.2m	2y
3.1	IKT712 (IM) Privacy Respecting Intrusion Detection Systems	2009-01-05	2009-05-22	17d	4.5m
3.2	IKT710 (IM) Learning in Random Environments	2009-04-14	2009-06-04	4w	7.4w
3.2.1	Lectures	2009-04-14	2009-04-20	5d	6.4d
3.2.2	Project work and exercises	2009-04-21	2009-06-04	3.1w	6.2w
3.3	Research School in Information Security at Finse	2009-05-03	2009-05-14	7.9d	1.6w
3.3.1	Lectures	2009-05-04	2009-05-08	5d	4.4d
3.3.2	Final presentation	2009-05-12	2009-05-14	23h	2.2d
3.4	PrimeLife/IFIP Summer School	2009-06-18	2009-12-04	7w	5.5m
3.4.1	Short paper: Study of Snort Rule-set Privacy Impact	2009-06-18	2009-08-10	2w	7.5w
3.4.2	Summer School in Privacy and Identity Management for Life	2009-09-07	2009-09-11	5d	4.4d
3.4.3	M2.1 Paper: PRIvacy LEakage Methodology (PRILE)	2009-09-15	2009-10-15	2.5w	1m
3.4.4	Camera ready PRILE paper	2009-11-24	2009-12-04	7.5d	1.5w
3.5	EX-601 (B) Theory and Ethics of Science	2009-08-17	2010-05-17	38d	9m
3.5.1	Lectures	2009-08-17	2009-12-24	18d	4.2m
3.5.2	O2.3 Paper: Ethics of Network Monitoring	2009-12-08	2009-12-23	2w	2.2w
3.5.3	Camera ready paper	2010-02-01	2010-02-12	2w	1.6w
3.5.4	16. Symposium on Ethics, Business and Society	2010-05-16	2010-05-17	0d	2d
3.6	IKT702 (IM) Selected Topics in Security for Mobile Systems	2010-08-17	2010-12-24	19d	4.2m
3.7	IKT701 (IM) Dynamics of CSIRT	2010-08-18	2010-12-24	19d	4.2m
4	Initial research	2009-01-30	2010-03-26	3.7m	1.1y
4.1	M1.1 Paper: Two Tiered Privacy Enhanced IDS Architecture	2009-01-30	2009-09-23	17d	7.7m

Legend: Container Task, Milestone, Planned Task, In-progress Task, Completed Task, Task Work Load, Other Work Load, Free Load

Page 1 of 3 — 2009-01-12

Planning the PhD

- To ensure relevance for future research projects:
  - I *read the open FP7 security calls*
  - Privacy-enhancing technologies was a hot area
  - I had former experience from developing an IDS appliance
- Decided to do research on *privacy-enhanced network monitoring services*
- Also wanted to participate in writing FP7 project proposals
  - Create my own job as a researcher
  - Integrate and further develop PhD work in future research projects
  - Basically, ensure that the research has *future impact*

About work effort

- Taking a PhD is similar to being a top-level athlete.

- A lot of dedicated effort, training and practice is needed.

- Forget normal working hours and holidays...

- But also keep physically fit

- *Make sure you finish on time!*

  - I did not, as you can see...

  - Juggling project and PhD is not fun.

  - Finishing PhD without funding is even less fun...

Hours 2009
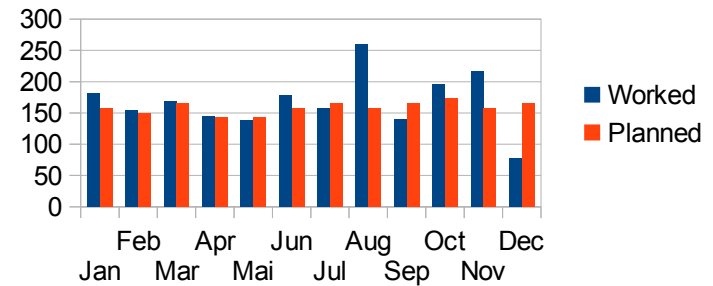
Hours 2011
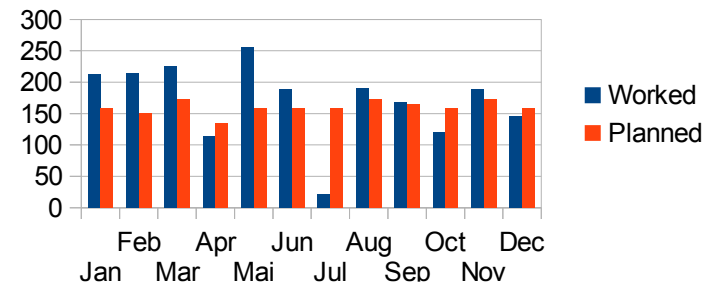
Hours 2012
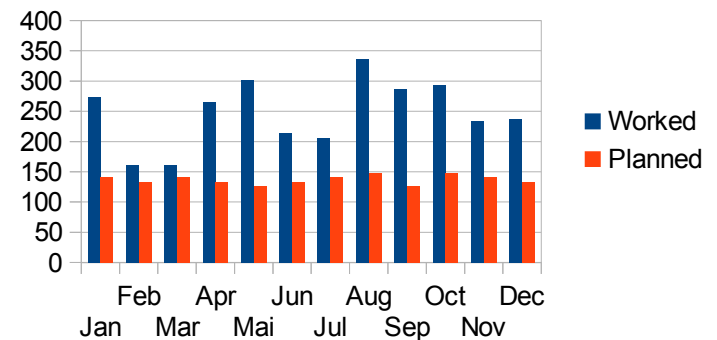
Know your strengths - choose courses with care

Course	Title	Effort (h)	ECTS	Effort/ETCS	Comments	Risks
IKT711	Principles of pattern recognition	16	5	**3,2**	Good programming skills, knew some of the curriculum in advance.	
IKT623	Principles of AI	67,9	5	**13,58**	Good programming skills, knew some of the curriculum in advance.	
IKT710	Learning in Random Environments	111,4	5	22,28	Good programming skills.	
EX601	Theory of Science	123,6	5	24,72	Report ended up in conference presentation and journal publication.	Difficult to publish across disciplines.
External	Winter School, Finse	53,8	2	26,9		Getting course from other institution approved.
IKT712	Special curriculum	155,5	5	31,1	Self study on privacy-enhanced IDS.	Unclear curriculum scope.
External	PrimeLife summer school, Nice	116,1	3	38,7	Conference presentation +journal paper.	Getting course from other institution approved.
IKT715	eHealth and mobile security summer scool	200,1	5	40,02	Report ended up in conference + journal paper.	Publishing results may cause lack of research focus.

If you want to finish your PhD on time:

- Make a plan and *stick to it.*
  - *Focus - going off at tangents is not recommended[wife]...*
  - *Focus* means having one research target, not two or many...
- Do not:
  - Start writing EU project proposals
  - Work on an EU project while finishing your PhD
  - Get sidetracked into other interesting research areas
  - Take on responsibility as a union representative
  - Try to write a social science paper, just to see if you can do it
  - Do in-depth research of all layers of the protocol stack - limit scope as necessary
  - Try to get access to IDS data from commercial MSS providers
  - Define your own self-study course items
  - Take non-standard courses that may be hard to get recognised by your university
  - Get stuck on futile research paths
    - Husk fjellvettreglene: "Vend i tide - det er ingen skam å snu"

UNIVERSITY OF AGDER
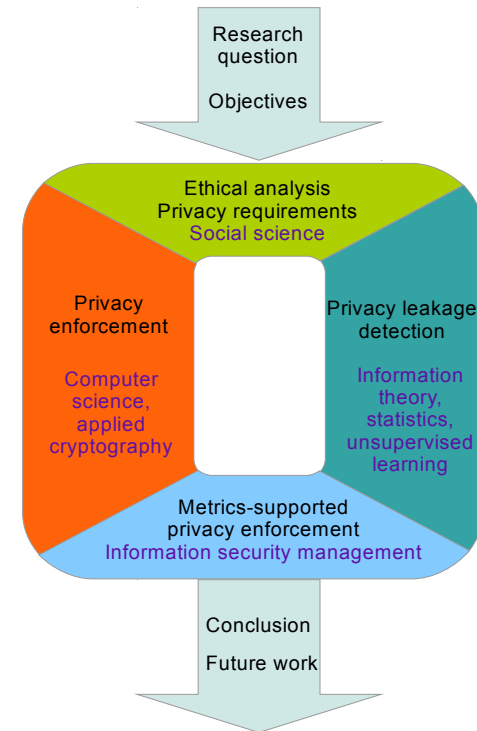
Summary of Experience doing a PhD

- Taking a PhD is a great opportunity.
- Interesting and giving work.
- I have learnt a lot, now technically an expert according to Gladwell criteria.
- Have got me up to speed as a researcher.
- Good research outcome, poor pay.
- I hope others can learn from my experience, to avoid:
  - problems with timeliness;
  - poor work/free time balance;
  - and some common pitfalls.
- Dissertation:
  http://brage.bibsys.no/xmlui/handle/11250/194485

|	
Timeliness	5,33 years, 2,44 years (81%) longer than planned.
Effort used = 10265h	Key to success: practicing a field for more than 10000 hours (Gladwell, The Story of Success). Poor work to leisure ratio. Is it worth it?
Focus	Dissertation contains 7 out of 12 papers
Course performance	Research work slowed down course progress. Problems getting external courses accepted.
Research outcome	5 conference papers, 7 journal articles, 3 conference presentations, 2 submitted papers, 29 other dissemination.
Exploitation, dissemination, Impact	PhD work integrated in 2 EU projects, 2 ongoing master projects, 3 open source projects.

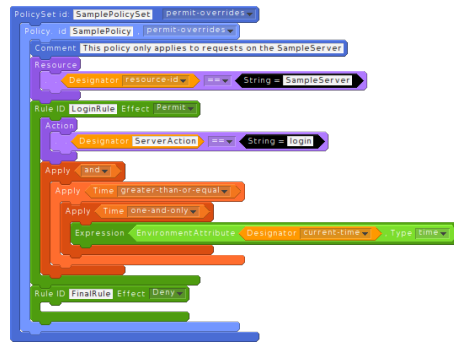UNIVERSITY OF AGDER

Main Exploitable Results and Impact of PhD work

Reversible Anonymiser for XML services
http://launchpad.net/reversible

SnakeSpeed Beta
Compete with snakes on eating the frog.
http://sf.net/projects/snakespeed
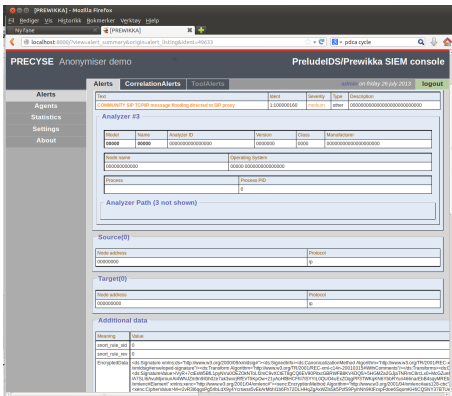
Demonstrate privacy-enhanced operation of Prelude-IDS

Scratch-based XACML Policy Editor (student project)
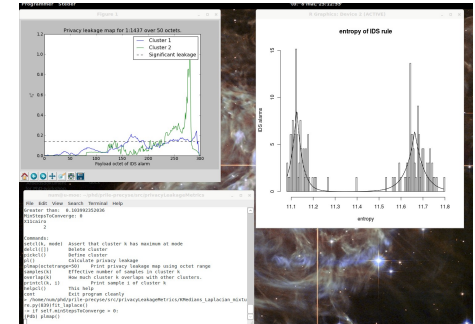
Privacy Leakage Calculator

PRECYSE

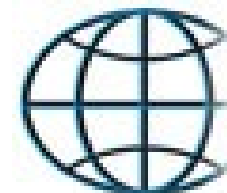Me: Førsteamanuensis (Associate professor) at UIA

SEMIAH

Ulltveit-Moe, Privacy-enhancing Network Monitoring

8. April 2014

Thank you!
Questions?