



Evaluation of Mathematics, ICT and Technology (EVALMIT) 2023-2024

Self-assessment for research groups

Date of dispatch: 19 September 2023

Deadline for submission: 31 January 2024

Institution (name and short name): University of Oslo (UiO)

Administrative unit (name and short name): Department of Informatics (IFI)

Research group (name and short name): Digital Security (SEC)

Date: 25.01.2024

Contact person: Nils Gruschka

Contact details (email): nilsgrus@ifi.uio.no

Content

1. Organisation and strategy	3
1.1 Research group's organisation.....	3
1.2 Research group's strategy.....	4
1.3 Relevance to the institutions	6
1.4 Research group's resources	6
1.5 Research group's infrastructures.....	7
1.6 Research group's cooperations	8
2. Research quality	9
2.1 Research group's scientific quality.....	9
2.2 Research group's societal contribution	15
3. Challenges and opportunities	17

1. Organisation and strategy

1.1 Research group's organisation

Describe the establishment and the development of the research group, including its leadership (e.g. centralised or distributed etc.), researcher roles (e.g. technical staff, PhD, post docs, junior positions, senior positions or other researcher positions), the group's role in researcher training, mobility and how research is organised (e.g. core funding organisation versus project based organisation etc.).

With a staff of more than 400, The UiO Department of Informatics (IFI) is a “powerhouse” for informatics training and research in Northern Europe. It is the largest such unit in Norway and the one with the strongest international rankings. Around a comprehensive core in computer science, IFI interprets informatics in substantial breadth: from microelectronics and signal processing to participatory design or digital innovation. In 2023, IFI hosts five BSc and eight MSc study programs, with close to 2500 students. The department is organized in four thematic sections, each of which comprising 2–5 research groups.

In 2012 it was decided by IFI that engagement in the areas of information security must be strengthened. This was highlighted in the strategy documents 2014 and 2019. This led to the foundation of the research group on “Digital Security” (SEC) in 2019 as part of the section “Digital infrastructure and security”. The group started with 2 permanent positions (professor/associate professor) and gained another one in 2022. Finally, in 2023 we were able to fill a fourth permanent position. In addition, the group has several post docs and PhD candidate, many of them are working in one of the many projects that group was able for acquire. Finally, the group has many adjunct positions; researchers and teachers that have their main position in industry, academia, or governmental organizations. They are bringing their expertise to the education offered by the group and strengthen the research collaboration with external partners.

The group has a group manager for administrating the groups resources and representing the group in the department's committee. The group holds bi-weekly meetings for the whole research group but also “executive meetings” including the permanent staff. Overall, the professional and social collaboration inside the group is excellent.

Table 1. List of number of personnel by categories

Instructions: Please provide number of your personnel by categories.

For institutions in the higher education sector, please use the categories used in DBH, <https://dbh.hkdir.no/datainnhold/kodeverk/stillingskoder>.

Please add new lines or delete lines which are not in use.

	Position by category	No. of researcher per category	Share of women per category (%)	No. of researchers who are part of multiple (other) research groups at the admin unit	No. of temporary positions
No. of Personnel by position	Professor (1013)	1	0	0	0
	Associate Professor (1011)	2	0	0	0
	Postdoctoral Fellow (1352)	1	0	0	1
	Doctoral Research Fellow (1017)	6	17	0	6
	Adjunct Associate Professor (1011)	3	33	0	3
	Adjunct Lecturer (1009)	2	0	0	2

1.2 Research group's strategy

a) Describe the research group's main goals, objectives and strategies to obtain these (e.g. funding, plans for recruitment, internationalisation etc. within the period 2012-2022).

The group is researching in different areas of information/cyber security. The main directions are identity management and privacy, cyber defense and threat intelligence, and pen testing. The group is still very new (2019) and small and we are planning further recruitments in the next years.

Cyber security is a crucial topic for national security in Norway as well as in the strategies of the European Union. The SEC group is actively involved to national and EU research projects. In addition, we contribute to security education, not only at the University, but also to the public, high school teachers and students, and, finally, in continuing education in our professional studies.

b) Please describe the benchmark of the research group. The benchmark for the research group should be written by the administrative unit in collaboration with the research group. The benchmark can be a reference to an academic level of performance (national or international) or to the group's contributions to other institutional or sectoral purposes.

Benchmark External Funding:

The SEC was and is involved in many different research projects and very successful in gathering external funding. As an example: in 2022 we had nearly 7 MNOK income from external projects.

Benchmark Collaboration with External Partners:

The group has strong national and international collaborations with partners from academia, industry, governmental agencies and standardization organizations (details see below).

Benchmark Group Size:

The group started in 2019 with 8 employees (2 permanent) and had 2022 15 employees (3 permanent). (And this has further increased in 2023 to 18 employees (4 permanent)).

c) Describe the research group contribution to education (master's degree and/or PhD).

The master study program "Information Security" is mainly operated by the SEC group. The group offers many courses in cyber security:

- IN2120 – Informasjonssikkerhet
- IN3210/IN4210 – Network and Communication Security
- IN4180 – Cyber Operations
- IN5290 – Ethical Hacking
- IN5540 – Privacy by Design
- IN5080 – Security and Risk Management

In addition, the group is contributing to professional studies courses (*etter- og videreutdanning*, EVU)

We also supervise most master thesis projects in the study program "Information Security". Between 2019 and 2022 in total 78 master students (i.e. on average 19.5 per year) have successfully finished their studies under the supervision of a group member.

Finally, the group is very active in PhD education. Between 2019 and 2022 in total 3 PhD candidates have successfully defended their thesis (and additional 3 in 2023). Given that SEC only had 2 staff in this period, it reflects that the group is very active in PhD education.

d) Describe the support the host institution provides to the research group (i.e., research infrastructure, access to databases, administrative support etc.).

The group has a lab (SecurityLab) for different kind of research tasks.

For establishing EU project, the department and the faculty offer very good administrative and financial support.

1.3 Relevance to the institutions

Describe the role of the research group within the organisation. Consider the group's contribution towards the institutional strategies and objectives and relate the group's benchmark to these.

Security was for the last 10 years (and still is) a strategic goal of the department. The group is researching in different areas of information security. The main directions are identity management and privacy, cyber defense and threat intelligence, and pen testing.

1.4 Research group's resources

Describe the funding portfolio of the research group the last five years (2018-2022).

In addition to the base funding (permanent positions, PhD positions from KD (ministry for science and education)) the group is very successful in acquiring projects, mainly from RCN and from the EU. Here is a list of some larger projects (details in Table 4):

- OsloAnalytics (RCN)
- CyberHunt (RCN)
- JACOB (EU)
- ABRI (US Army)
- ACT (RCN)
- P4C (RCN)

Table 2. Describe the sources of R&D funding for the research group in the period 2018-2022.

	2018 (kNOK)	2019 (kNOK)	2020 (kNOK)	2021 (kNOK)	2022 (kNOK)
Basic funding	1475	2828	3900	3341	3267
Funding from industry and other private sector sources	0	0	0	0	0
Commissioned research for public sector	0	0	0	0	0
Research Council of Norway	6325	3077	1195	4314	5984
Grant funding from other national sources	0	0	0	0	0
International funding e.g. NIH, NSF, EU framework programmes	1390	1070	0	590	1416
Other	0	0	0	0	0

1.5 Research group's infrastructures

Research infrastructures are facilities that provide resources and services for the research communities to conduct research and foster innovation in their fields. [These](#) include major equipment or sets of instruments, knowledge-related facilities such as collections, archives or scientific data infrastructures, computing systems communication networks. Include both internal and external infrastructures.

a) Describe which national infrastructures the research group manages or co-manages.

None

b) Describe the most important research infrastructures used by the group.

Many research tasks require computation resources. In many projects, the group makes use of the Norwegian Research and Education Cloud (NREC).

In addition, the group manages the "UiO HackingArena". The purpose of the arena is to offer an exclusive and innovative learning platform for ethical hacking and is used by students from UiO but also from other Norwegian universities. The arena presents a wide range of hacking challenges, covering various skill levels from beginners to experts. Each challenge includes a solution that is readily available in both step-by-step online format and through concise video demonstrations.

1.6 Research group's cooperations

Table 3. Reflect on the current interactions of the research group with other disciplines, non-academic stakeholders and the potential importance of these for the research (e.g. informing research questions, access to competence, data and infrastructure, broadening the perspectives, short/long-term relations).

Interdisciplinary (within and beyond the group)	Cyber security depends highly on the application area and, therefore, (interdisciplinary) collaboration is vital. The group has good cooperation with many partners. Examples are: • Norwegian Computing Center (NR) on AI/ML and NLP • Norwegian Institute for International Affairs (NUPI) on national security issues.
Collaboration with other research sectors e.g. higher education, research institutes, health trusts and industry.	The group has good cooperation with other researcher in different sectors (industry, academia, governmental). Examples are: • Mnemonics • Oslo Metropolitan University (OsloMet) • Norwegian Defence Research Establishment (FFI) • The European Union Agency for Cybersecurity (ENISA) • Norwegian National Security Authority (NSM) • Norwegian Water Resources and Energy Directorate (NVE)
<u>Transdisciplinary</u> (including non-academic stakeholders) <i>Transdisciplinary research involves the integration of knowledge from different science disciplines and (non-academic) stakeholder communities with the aim to help address complex societal challenges.</i>	The group is strongly involved in standardization of security solutions. This includes engagement in different working groups under the OASIS Open organisation. One member of the SEC group was recently voted into the board of directors of OASIS Open.

2. Research quality

2.1 Research group's scientific quality

Describe the research profile of the group and the activities that contribute to the research group's scientific quality. Consider how the group's work contributes to the wider research within the group's field nationally and internationally.

The group is researching in different areas of information security. The main directions are identity management and privacy, cyber defense and threat intelligence, and pen testing. The results have been published in high-ranking conferences, journals, and books (details see under the link to the research group's web site below).

Please add a link to the research group's publication list at the research group's website:

<https://www.mn.uio.no/ifi/english/about/strategy/evalmit/sec.html>

Table 4. List of projects

Instructions: Please select 5-10 projects you consider to be representative/the best of the work in the period 1 January 2012 – 31 December 2022. The list may include projects lead by other institutions nationally or internationally. Please delete tables that are not used.

Project 1: CyberHunt (2020 – 2025)	Project owner(s) (project leaders organisation)	UiO
	Total budget and share allocated to research group	13.4 MNOK / 11.6 MNOK
	Objectives and outcomes (planned or actual) and link to website	CyberHunt aims at investigating and developing automated cyber-threat hunting technology based on AI and semantic modelling for predicting and detecting sophisticated adversarial attacks taking into consideration all phases of the cyber kill chain in a holistic fashion. https://www.mn.uio.no/ifi/english/research/projects/cyberhunt/
Project 2: Oslo Analytics (2016 – 2021)	Project owner(s) (project leaders organisation)	UiO
	Total budget and share allocated to research group	16.2 MNOK / 11.9 MNOK
	Objectives and outcomes (planned or actual) and link to website	The focus of the Oslo Analytics project at UiO is to develop models and practical solutions for cyber-threat intelligence. https://www.mn.uio.no/ifi/english/research/projects/oslo-analytics/index.html
Project 3: Raksha (2021 – 2025)	Project owner(s) (project leaders organisation)	SINTEF

	Total budget and share allocated to research group	3 MNOK / 3 MNOK
	Objectives and outcomes (planned or actual) and link to website	The project delivers a 5G cyber-range platform empowered with tools for risk assessment, attack simulation, evaluation, and demonstration of defensive solutions for NGCC. https://www.sintef.no/en/projects/2021/raksha-5g-security-for-critical-communications/
Project 4: JCOP (2021 – 2024)	Project owner(s) (project leaders organisation)	UiO
	Total budget and share allocated to research group	1.7 MEUR / 0.36 MEUR
	Objectives and outcomes (planned or actual) and link to website	JCOP is a prototypical implementation of Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, and a model that can be applied to all EU Member States. https://www.mn.uio.no/ifi/english/research/projects/jcop/
Project 5: P4C: Partnership for Cybersecurity (2018 – 2022)	Project owner(s) (project leaders organisation)	UiO
	Total budget and share allocated to research group	6.7 MNOK / 5.3 MNOK
	Objectives and outcomes (planned or actual) and link to website	P4C is a network for competence, research, and innovation in cyber security. https://www.mn.uio.no/ifi/english/research/networks/p4c/

Table 5. Research group's contribution to publications

Instructions: Please select 5-15 publications from the last 5 years (2018-2022) with emphasis on recent publications where group members have a significant role. **If the publication is not openly available, it should be submitted as a pdf file attached to the self-assessment.** We invite you to refer to the Contributor Roles Taxonomy in your description: <https://credit.niso.org/>.

Cf. Table 1. List of personnel by categories: Research groups up to 15 group members: 5 publications. Research groups up to 30 group members: 10 publications. Research groups above 30 group members: 15 publications.

Please delete tables that are not used.

Publication 1: A framework for analyzing authentication risks in account networks. <i>Computers & Security, Volume 135. December 2023. DOI: 10.1016/j.cose.2023.103515</i>	Authors (Please highlight group members)	Daniela Pöhn, <u>Nils Gruschka</u> , Leonhard Ziegler and <u>Andre Büttner</u>
	Short description	This article presents the Authentication Analysis Framework (AAF). AAF evaluates account types and primary and fallback authentication methods for each account, before analyzing the overall account network. By detecting transitive risks, weak links can be discovered and subsequently strengthened.
	Research group's contribution	• Developed the idea (together with 1. author). • Wrote ½ article. • Created the reference implementation.
Publication 2: Simulating SQL injection vulnerability exploitation using Q-learning reinforcement learning agents	Authors (Please highlight group members)	<u>László Erdődi</u> , <u>Ávald Áslaugson Sommervoll</u> , <u>Fabio Massimo Zennaro</u>
	Short description	In this paper, we propose a formalization of the process of exploitation of SQL injection vulnerabilities. Our work fits in the wider research on the development of intelligent agents for autonomous penetration testing and white-hat hacking, and our results aim to contribute to understanding the potential and the limits of reinforcement learning in a security environment.

https://www.sciencedirect.com/science/article/pii/S2214212621001290	Research group's contribution	100 % SEC group
Publication 3: The Agent Web Model: modeling web hacking for reinforcement learning. <i>Int. J. Inf. Secur. 21, 293–309 (2022).</i> DOI: 10.1007/s10207-021-00554-7	Authors (Please highlight group members)	<u>László Erdődi, Fabio Massimo Zennaro</u>
	Short description	We present in this paper a model that formalizes web hacking tasks for reinforcement learning agents. Our model, named Agent Web Model, considers web hacking as a capture-the-flag style challenge, and it defines reinforcement learning problems at seven different levels of abstraction.
	Research group's contribution	100 % SEC group
Publication 4: The Impact of Quantum Computing on Present Cryptography <i>International Journal of Advanced Computer Science and Applications(IJACSA), Volume 9 Issue 3, 2018.</i> DOI: 10.14569/IJACSA.2018.090354	Authors (Please highlight group members)	<u>Vasileios Mavroeidis, Kamer Vishj, Mateusz D. Zych, Audun Jøsang</u>
	Short description	The aim of this paper is to elucidate the implications of quantum computing in present cryptography and to introduce the reader to basic post-quantum algorithms.
	Research group's contribution	100 % SEC group
Publication 5: Cyber Threat Intelligence Model: An Evaluation of Taxonomies,	Authors (Please highlight group members)	<u>Vasileios Mavroeidis, Siri Bromander</u>

Sharing Standards, and Ontologies within Cyber Threat Intelligence <i>2017 European Intelligence and Security Informatics Conference (EISIC)</i> DOI: 10.1109/EISIC.2017.20	Short description	This paper introduces the Cyber Threat Intelligence (CTI) model, which enables cyber defenders to explore their threat intelligence capabilities and understand their position against the ever-changing cyber threat landscape.
	Research group's contribution	100 % SEC group

Table 6. Please add a list with the research groups monographs/scientific books. Max 10 listed: title, first three authors et al and link to webpage (if any). Please delete lines which are not used.

1	<u>Audun Jøsang</u> . Informasjonssikkerhet: Teori og praksis. Universitetsforlaget, 2021. 312 sider. ISBN: 9788215055893.
2	<u>Audun Jøsang</u> . Subjective Logic: A Formalism for Reasoning Under Uncertainty, ISBN 978-3-319-42337-1, Springer Verlag, 2016.
3	Christoph Sorge, Luigi Lo Iacono, and <u>Nils Gruschka</u> , "Sicherheit in Kommunikationsnetzen." ISBN 978-3486720167, Walter de Gruyter, 2013

2.2 Research group's societal contribution

Describe the societal impact of the group's research. Consider contribution to education, economic, societal and cultural development in Norway and internationally.

The group contributes to Norwegian (and international) society through different initiatives:

- We are partner/co-organizer of the "Sikkerhetsfestival", the largest arena in Norway for experience exchange in cyber security.
- We contribute to the national security through strong collaboration with Norwegian authorities and military research facilities.
- We are hosting public seminars on cyber security.
- We are offering course information security for professional/continuous education and therefore contributing to life-long learning.
- We are present in different public media (TV, newspapers)

Table 7. The research group's societal contribution, including user-oriented publications, products (including patents, software or process innovations

Instructions: Please select 5–10 of your most important user-oriented publications or other products from the last 5–10 years with emphasis on recent publications/products. For each item, please use the following formatting: Please delete lines which are not used.

No.	Name of publication/product	Date of publication/product	Link to the document
1	“Kunstig intelligens kan brukes til å bedre medisinske analyser – men hva med personvernet?”	November 2023	https://www.titan.uio.no/teknologi/2023/kunstig-intelligens-kan-brukes-til-a-bedre-medisin.html
2	“Justisministeren hadde TikTok på telefonen – hvor farlig er egentlig slike apper?”	February 2023	https://www.titan.uio.no/teknologi/2023/justisministeren-hadde-tiktok-pa-telefonen-hvor-farlig-er-egentlig-slike-apper.html
3	“Utdanning, forskning og innovasjon i cybersikkerhet”,	March 2022	https://www.altomsamfunnssikkerhet.no/samfunnssikkerhet-og-beredskap/utdanning-forskning-og-innovasjon-i-cybersikkerhet/
4	“Ekspertene mener mediene blåste opp pro-russisk hackerangrep”	September 2022	https://nrkbeta.no/2022/09/06/eksperter-mener-mediene-blaste-opp-pro-russisk-hackerangrep/
5	“Podcast: En reise i informasjonssikkerhet med Professor Audun Jøsang”	October 2020	https://www.dataforeningen.no/ny-podcast-en-informasjonssikkerhetsreise-med-professor-audun-josang/

3. Challenges and opportunities

Information about the strengths and weaknesses of the research group is obtained through the questions above. In this chapter, please reflect on what might be the challenges and opportunities for developing and strengthening the research and the position of the group.

The area of information security is an attractive and dynamic research field that will continue to grow. Security has many interdisciplinary applications with increasing collaboration potential with academia, public sector, and industry (incl. SMEs). Recurring Cyber-attacks on enterprises and critical infrastructures show the high demand for cyber security knowledge in our modern world.

On the other hand, these properties make security also a very competitive field. This makes it hard to find and recruit staff with the right expertise, but also to compete for funding and students.

The job situation for students with security education is extremely good. Virtually all our students have found a new position before finishing their masters. However, the high demand and good payments in industry makes it very hard to find students that start a PhD and follow a career in academia.

A particular challenge for the SEC group is the staffing situation. We are a rather new and small group and covering many areas of cyber security research and offering security education is very challenging with an imminent threat of overworked staff.