Guillaume Bour

guillaumebour guillaumebour guillaumebour.fr

Application domains: Health, Maritime, Aviation, Water infrastructures

CORE COMPETENCIES

- System architecture and software development
- Application security testing
- Hardware security testing
- Misc: UNIX administration, LaTeX, CAD, 3D Printing

LANGUAGES

French	:	Mother tongue
English	:	Fluent (TOEIC 955/990)
Norwegian	:	Basic notions
German	:	Basic notions (A2/B1)

WORK EXPERIENCE

RESEARCH SCIENTIST
SINTEF Digital
September 2019 - now
Trondheim • Norway

- Part of the Cyber Security Research Group

MASTER'S THESIS PROJECT
SINTEF Digital
January 2019 - June 2019
Trondheim • Norway

- Assessment of embedded medical devices security
- Hardware pentesting technics, Black Box testing methodology

CYBER SECURITY INTERN
Telindus Luxembourg
June and July 2018
Esch-Sur-Alzette • Luxembourg

- Developed an Ethical Hacking training to introduce people to the penetration testing methodology with a soft spot on infrastructure pentests
- Based on the OSSTMM (Open Source Security Testing Methodology Manual)
- Set up a hacking lab using VMware tools (vSphere, ESX and Horizon)

IT SECURITY INTERN
Excellium Services
July and August 2017
Contern • Luxembourg

- Developed a reporting tool for the penetration testing team
- Worked with common vulnerabilities databases (CVE, CPE, CWE) and scoring systems

EDUCATION

2018 - 2019
NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET (NTNU)
Trondheim • Norway
MSc in communication technology, with information security specialization

2016 - 2019
INSTITUT NATIONAL DES SCIENCES APPLIQUÉES DE TOULOUSE (INSA)
Toulouse • France
Diplôme d'ingenieur in computer science and network

2014 - 2016
LYCÉE FABERT
Metz • France
CPGE MPSI / MP* - mathematics, physics and computer science

2014
LYCÉE JEAN MOULIN
Forbach • France
Baccalaureat equivalent to high school diploma, in science, with honors

MAIN PROJECTS

RAGNAROK
Jan 2022 - now

Researcher & PL

The Ragnarok project aims to build competence on (I)IoT security and position SINTEF Digital as a champion on how to deal with the inevitable collapse of the automation pyramid.

- Lead the activity on (I)IoT device security (security testing and secure development)
- Contribute to applications related to IoT security

B-WATERSMART
Feb 2022 - now

Lead developer

B-WaterSmart accelerates the transformation to water-smart economies and societies in coastal Europe and beyond.

- Lead the development of a framework assessment tool for water

FRITIDSBÅTPLATTFORMEN
Spring 2021 - now

Researcher

The objective in this project is to build a digitally supported platform for cross-sectoral cooperation against recreational boating accidents.

- Involved in the privacy and security aspects of the platform
- Involved in the architecture and the development of the Proof of Concept

HERMCHAIN & PASS4CHAIN
Jan 2021 - now

Researcher

Digitisation using blockchain technology for secure documentation of catch, transport and processing of whitefish.

- Developing a new consensus algorithm based on DPoS, for Hyperledger Sawtooth
- Set up of an on-premise cloud (based on MAAS)

DIGITAL TORC
Sep 2020 - now

Lead developer

The Digital TORC tool is a digital adaptation of the serious game TORC, developed at SINTEF. The game focuses on training for operational resilience capabilities. From a technical perspective, it is a collaborative platform, where the players can interact with the game and be trained against unsolicited events. The platform was successfully used during a workshop of the European Commission on Hybrid Threats in June 2021 (60+ participants). In addition, the platform has been used as an asset in several applications submitted in 2021. It will also be used widely in TECHNOCRACI.

- Developed, deployed and operated the first version of the tool
- Supervised the creation of the training scenarios in the STOP-IT project
- Lead and managed the development of the second version of the platform
- Supervised Bachelor's students on the development of part of the management application

DIGITAL WATER CITY
April 2020 - now

Researcher

The project aims to help the modernisation of the overall water and sewage infrastructure in the European Union. In particular, the project develops and demonstrates 15 digital solutions, covering a whole range of innovative digital technologies, such as augmented reality, mobile technology, cloud computing, sensors, etc.

- Part of the security team, helping with the security assessment of the solutions
- Responsible for task 4.2, aiming at developing the DWC Risk Identification Database and Risk Reduction Measures Database
- Responsible for task 4.3, aiming at delivering a cyber-physical security assessment of the digital solutions in DWC

- Developed an open-source tool for risk events and risk reduction measures visualisation
- Performed a security assessment of one of the digital solutions which uses IoT sensors

CYSIMS-SE
March 2020 - March 2021

Researcher & Developer

CySiMS-SE is a project funded by the Research Council of Norway aiming to demonstrate and operationalise a secure communication solution for the maritime sector. The solution includes a PKI scheme and the necessary hardware and software for secure information exchange across systems on the bridge, off-bridge and on shore.

- Contributed to the PKI prototype specification
- Developed the prototype of the PKI used to secure communications and services in the maritime sector
- Studied the use of CRLite as a revocation mechanism for the maritime sector, compared to CRL

MAKERSPACE
Jan 2020 - now

Researcher

This project aims to build a Makerspace and community of makers in Strindvegen 4, thus stimulating creativity and strengthening collaboration between research groups.

- Set up the MakerSpace (acquiring 3D printers, tools, electronics, etc.)
- Arranged and gave courses to other colleagues in the department (Python programming)
- Built a hardware hacking lab, to be used for security assessment or by students
- Manage the Makerspace's server

5G SECURITY
Nov 2019 - Dec 2020

Researcher

The objective of the 5G Security internal project was to position SINTEF on the topic of 5G.

- Participated at the first ever 5G Hackaton in Oulu in Finland where we ended up at the first place
- Set up the SINTEF 5G Network now used in 5G RAKSHA (using Amarisoft products)

DIGITAL SERVICE FACTORY (SINTEF CONNECT)
Nov 2019 - Feb 2020

Researcher

The objective in this project was to reuse competencies cross-institutes. As such, my role was to help the development team at SINTEF Ocean with security matters.

- Helped with the integration of security in the CI/CD pipeline
- Assessed the security of web applications
- Gave an introduction to the OWASP Top 10 and to Web Application pentesting

SESAR
Nov 2019 - now

Researcher

The projects under the SESAR umbrella are a concentration of all EU research and development activities in developing the next generation Air Traffic Management.

- Member of the SESAR Cybersecurity team, helping solutions to deal with security issues
- Part of the security group in the solution developing the Future Satellite Communications Data Link
- Evaluated the practitioners' perceptions of the SecRAM in ATM projects

SICHAIN 2.0
Oct 2019 - Dec 2019

Researcher

The SiChain 2.0 was used to build Blockchain competencies within the department.

- Studied the concept of "channels" in Hyperledger Fabric and its limits
- Modelled a medication distribution problem
- Developed a Proof of Concept now used as starting point for the HealthDemocratization demo's Blockchain part

HEALTH DEMOCRATIZATION Sep 2019 - now
Researcher & Task Leader

The Health Democratization project, lead by NTNU, aims at reenforcing the HealthData Infrastructure and Mobility and Assurance through Data Democratization.

- Performed security assessments of medical devices, leading to an ICS Medical Advisory from CISA
- Supervised two master's students on their work on the pacemaker's ecosystem security (thesis delivered in 2021)
- Supervised a Master's student's work on Bluetooth Low Energy security
- Supervising a Master's student on his work on the HMU security (to be delivered in spring 2022)
- Design and specification of the data provenance layer of the developed platform
- Leading the development of the SINTEF Demo

PUBLICATIONS

PAPERS

2022

- G. Bour, R. Borgaonkar and M. E. G. Moe, "Experimental security analysis of connected pacemakers", in *Proceedings of the 15th International Joint Conference on Biomedical Engineering Systems and Technologies*, INSTICC, 2022, pp. 35–45
- K. Bernsmed, G. Bour, E. Bergström *et al.*, "An evaluation of practitioners perceptions of a security risk assessment methodology in air traffic management projects", *Journal of air transport management*, to appear.

2021

- *Security challenges in multi-modal communication*, Zenodo, Oct. 2021. DOI: 10.5281/zenodo.5603879. [Online]. Available: https://doi.org/10.5281/zenodo.5603879
- G. Bour, K. Bernsmed, R. Borgaonkar *et al.*, "On the certificate revocation problem in the maritime sector", in *Nordic Conference on Secure IT Systems*, Springer, 2020, pp. 142–157

2019

- G. N. Bour, "Security analysis of the pacemaker home monitoring unit: A blackbox approach", Master's thesis, NTNU, 2019

TALKS

2022

- Blockchain for fish supply chain traceability, YEAR Webinar on Blockchain

2021

- A glimpse into the future of aviation, Tekna Forskring for framtiden
- Hacking Medical Devices, ADA

2020

- On the Certificate Revocation Problem in the Maritime Sector, NordSec 2020
- Harming patients by hacking into their medical devices, fiction or reality?, KiD Cybesecurity
- Blockchain related projects at SINTEF, KiD Blockchain
- Results from 5 years of testing the Cyber security of pacemakers, FDA Cybersecurity Workgroup
- Hacking the Pacemaker Ecosystem, Catch IDI

STUDENTS SUPERVISION & MENTORING

2021/2022

- 1 Master's student from NTNU, working on pacemaker security (HMU firmware reverse engineering)

2020/2021

- 3 Bachelor's students from Université de Lorraine, France, working on the development of the management application for the Digital TORC platform

2019/2020

- 2 Master's students from NTNU, working on pacemaker security
- 1 Master's student from Université Bretagne Sud, France, working on Bluetooth Low Energy Security

MISCELLANEOUS

CVES

CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number. In 2019, I discovered and reported the following vulnerabilities:

- CVE-2019-18256
- CVE-2019-18254
- CVE-2019-18252
- CVE-2019-18248
- CVE-2019-18246