SFU

OFFICE OF THE VICE-PRESIDENT, ACADEMIC AND PROVOST

8888 University Drive, Burnaby, BC
Strand Hall | 3100
Canada V5A 1S6

TEL: 778.782.5731
FAX: 778.782.5876

vpacad@sfu.ca
www.sfu.ca/vpacademic

MEMORANDUM

ATTENTION	Senate	**DATE**	November 18, 2021
FROM	Wade Parkhouse, Associate Vice-President, Academic and Vice-Provost and Chair, SCUP	**PAGES**	1 of 1
RE:	Full Program Proposal for a Master of Science in Professional Cybersecurity (SCUP 21-39)		

At its November 17th, 2021 meeting, SCUP reviewed and approved the Full Program Proposal for a Master of Science in Professional Cybersecurity in the School of Computing Science within the Faculty of Applied Sciences.

Motion:
That Senate approve and recommend to the Board of Governors the Full Program Proposal for a Master of Science in Professional Cybersecurity in the School of Computing Science within the Faculty of Applied Sciences, effective Spring 2023 or later.

For Information:
Included with the full program proposal and approved by SGSC subject to approval by Senate:

1) New calendar entry: Master of Science in Professional Cybersecurity

C: U. Glässer, J. Wang

SFU GRADUATE AND POSTDOCTORAL STUDIES

Simon Fraser University
Maggie Benston Centre 1100
8888 University Drive
Burnaby, BC V5A 1S6

TEL 778.782.3042
FAX 778.782.3080

gradstudies@sfu.ca
www.sfu.ca/grad

MEMORANDUM

ATTENTION Senate Committee on University Priorities (SCUP)

DATE November 3, 2021

FROM Jeff Derksen,
Chair of Senate Graduate Studies Committee (SGSC)

RE: Full program proposal: Master of Science in Professional Cybersecurity

For approval:
At its meeting on October 4, 2021, SGSC approved the full program proposal for a Master of Science in Professional Cybersecurity from the Faculty of Applied Sciences. SGSC is recommending it to SCUP for approval, effective **Spring 2023.**

Motion:
That SCUP approve and recommend to Senate the full program proposal for a Master of Science in Professional Cybersecurity from the Faculty of Applied Sciences, effective **Spring 2023**.

For Information:
Included with the full program proposal and approved by SGSC subject to approval by Senate:

1) New calendar entry: Master of Science in Professional Cybersecurity

SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

Professional Cybersecurity

Full Program Proposal

November 22, 2021

School of Computing Science

Faculty of Applied Sciences

SUMMARY

Simon Fraser University (SFU) is defined by its dynamic integration of innovative education, cutting-edge research and far-reaching community engagement. SFU was founded in 1965 with a mission to bring an interdisciplinary approach to learning, embrace bold initiatives, and engage with communities near and far. Today SFU is consistently ranked amongst Canada's top comprehensive universities and is one of the world's leading teaching and research institutions.

The School of Computing Science proposes the creation of a new graduate degree program, Professional Cybersecurity (the "Program"), which will align with and reinforce SFU's strategic and academic plans as well as the Province of British Columbia's (BC's) commitment to stimulate industry-focused programs that support high demand occupations in the province's technology sector. This will be achieved through the delivery of a professional master's program in cybersecurity conceived in close collaboration with leading industry partners and government organizations. Students will acquire the technical background knowledge and practical skills needed to meet BC's growing demand for cybersecurity professionals; they will graduate with the capacity to become national and international leaders in developing cybersecurity solutions for secure technologies, products and services across Canada's growing IT sector and beyond.

Cyberattacks are increasingly frequent, severe and sophisticated. Responding to the globally evolving threat landscape, security technology is advancing, but not fast enough to keep pace with the threat. Information security breaches routinely compromise protection of sensitive data and information, exposing personal identities, intellectual property and financial assets. The result is mounting damages in the hundreds of billions of dollars, the erosion of trust in conducting business and collaboration in cyberspace, and the risk of catastrophic events that cause crippling damage to companies and even countries[1]. Critical infrastructure like electric power grids, oil and gas pipelines, communication networks and smart transportation systems provide vitally important services; disruptions can have severe consequences for public safety and national security[2]. Advanced threats targeting such infrastructure, often in the form of *zero-day exploits*[3], may not only cause temporary service disruptions but can cripple major system components physically, causing lasting damage that can threaten human safety beyond comprehension.

[1] Engineering Trustworthy Systems: A Principled Approach to Cybersecurity. *CACM*, ACM, June 2019.
[2] Canadian Centre for Cyber Security. National Cyber Threat Assessment 2020, CSE, 2020.
[3] Zero-day exploits target security hardware-software system flaws not known prior to an attack, making those attacks virtually invisible to and unstoppable by conventional cybersecurity protection.

1) Proposed credential to be awarded

Master of Science

2) Location of program

The Program will be offered at the Burnaby Mountain Campus.

3) Academic unit(s) offering proposed program

School of Computing Science (CS) in the Faculty of Applied Sciences (FAS)

4) Anticipated program start date

January 1, 2023

5) Anticipated completion time

The Program will normally be completed in four to five terms, depending on whether students complete one (mandatory) or two (one mandatory and one voluntary) four-month industrial internship or co-op terms.

6) Contact information

Dr. Jiannan Wang, Professor and Program Director, School of Computing Science, 778-782-4288, jnwang@sfu.ca

Dr. Uwe Glässer, Professor, School of Computing Science, 778-782-6775, glaesser@sfu.ca

PROGRAM DETAILS

7) Aims, goals and/or objectives of the proposed program

The primary objective of the graduate degree Program is to help BC and Canada build resilience against cyber threats by boosting the development and future growth of a thriving cybersecurity ecosystem driven by innovation in education, science and technology. This initiative responds to a dramatic shortage of cybersecurity professionals projected by the Information Security Branch, Province of British Columbia; the Canadian Centre for Cyber Security, Communications Security Establishment (CSE); ISED Canada[4]; Cisco; Fortinet; Palo Alto Networks; Gartner; Deloitte; KPMG; ISACA; (ISC)2[5] and other trusted sources.

"While cybersecurity is an **interdisciplinary course of study** including aspects of law, policy, human factors, ethics, and risk management, it is fundamentally a computing-based discipline." (Joint Task Force on Cybersecurity Education[6]). The broader view of cybersecurity involves technology, people, information and processes to enable assured operations in the context of adversaries. Hence, the Program curriculum extends beyond the scope of core computing science subject matters and explores and presents a range of key topics from several other disciplines. Specifically, this relates to applied cryptography (mathematics), cybercrime and cyber forensics (criminology), risk assessment and management (business), statistical learning and data analytics (statistics), and ethics and privacy (humanities).

This leading-edge graduate degree program will aim to engage students in experiential learning through unique hands-on training in cybersecurity core technologies and supporting tools. The well-rounded curriculum teaches cybersecurity skills such as penetration testing, intrusion detection, malware analysis, cryptoanalysis, cyber risk assessment, cloud and mobile security, and secure software design. Two intensive lab courses focus on practical skills using industrial-strength cybersecurity tool environments and training materials from global industry leaders including Cisco, Fortinet, Palo Alto Networks and Trend Micro.

Technical training provided in classrooms and laboratories will also be paired with practical experience through an industrial internship or co-op program of at least four months, working with external partner organizations in industry, finance and government. This way, the Program prepares graduates for working in a wide range of IT sectors in need of cybersecurity knowledge

[4] Cyber Security Innovation Network Program. Innovation, Science and Economic Development (ISED) Canada, 2021.
[5] The International Information System Security Certification Consortium. (ISC)[2] Cybersecurity Workforce Study, 2019.
[6] Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Joint Task Force on Cybersecurity Education, Version 1.0, December 2017.

and skills, and expedites their absorption into the job market. Graduates from this program can expect to easily find well-paying jobs right now and even more so in the future.

Considering the increasing security needs of citizens, businesses and government organizations, the economic growth in cybersecurity, the resulting demand for skilled labour as well as the existing experience with professional computer science training, one can expect strong demand for the Program. This would mean a steady revenue stream for CS, FAS and SFU.

8) How does the proposed program fit within the mandate of the institution?

The proposed program builds upon the Faculty of Applied Sciences' strong commitment to technology-based innovation and furthers SFU's interest in supporting the development of vibrant and technologically innovative communities. Through partnerships with global industry leaders (Cisco, Fortinet, Palo Alto Networks and Trend Micro), financial services (Mastercard, and Royal Bank of Canada), government (Canadian Centre for Cyber Security) and professional organizations (ISACA) and by offering a cutting-edge curriculum, this program is positioned to advance Faculty and University level goals in several key areas. Expanding collaborations with industry, and growing the talent pool needed for technology transfer and launching new start-ups are front and centre. This specifically involves developing cybersecurity solutions for secure digital technologies, products and services across BC and Canada's IT sector.

9) How does the proposed program support the current academic and strategic plan of the institution?

The Program aligns with SFU's strategic interest in exploring and capitalizing on opportunities to advance innovative degree credentials and exciting academic programming, especially in creative technologies with special focus on professional degrees at the master's level. SFU also seeks to "create more opportunities for experiential learning, work- and community-integrated learning and not-for-credit and international experiences. These initiatives will help students, faculty and staff become even more engaged with communities, ranging from local to global, in the continued quest to ensure a healthy planet and to improve the lives of the world's citizens."[7]

The Program is a direct outcome of the Faculty of Applied Sciences Academic Plan 2019-2023,[8] in which FAS outlines the expansion and diversification of professional graduate programs to provide "an increased range of opportunities for our students upon graduation, and for our professors for research." SFU's Applied Sciences mission is to address problems in society that are becoming increasingly complex and interdisciplinary. Considering the increasing threats, a secure cyberspace is a key element of our digital society. The Program's strong applied orientation responds to the urgency for producing well trained professionals needed more than ever for building stronger resilience against widespread and damaging attacks. This also calls for a mandatory term (or optionally two terms) of working with an organization in industry, finance

[7] Five-Year Academic Plan 2019-2024, Simon Fraser University, November 2018.
[8] Academic Plan 2018-2023, Faculty of Applied Sciences, June 2018.

or government on problems related to cybersecurity. This arrangement helps employers to assess a student's qualification and offers a seamless pathway to employment.

Cybersecurity is an opportunity for SFU and FAS to engage in an interdisciplinary field that is rapidly growing and undeniably in considerable demand.

10) Target Audience

The Program target audience is students who have completed a bachelor's degree in computer science or a related field and who wish to advance their education with a cybersecurity-focused graduate degree. For some, the motivation might be a career change; for those who are already working in information security, it may be the prospect of a promotion or consideration for management positions down the road. The Program appeals to this audience for several reasons. First, the significant need for highly qualified personnel in a sector driven by high-tech innovation and the integration of transformative technologies such as computer, network, cloud and mobile security, big data analytics, machine and deep learning (artificial intelligence) and their fusion in a broad range of interdisciplinary application fields means attractive employment opportunities. Second, cybersecurity offers plenty of opportunities for further specialization and alternative career trajectories. Third, the attractive earning potential for cybersecurity professionals, even when compared to other professions in the information and communications technology sector, will undoubtedly factor into the target audience's decision-making.

A comparable professional graduate degree program in Big Data, launched by SFU/CS in 2015, has seen steady growth ramping up to 1,000+ applications annually. Given this encouraging experience and the increasingly vital role of cybersecurity—fueled by frequent news media reports on vicious attacks locally, regionally and globally—, one can expect steady growth of the Program for the foreseeable future. Considerable interest in this field of study can also be gauged by the results of a web survey exploring student interest in a professional cybersecurity graduate degree in our School of Computing Science. Over a period of approximately two months, 39,858 users visited the website outlining such a program. This constitutes approximately 70% of all website visitors for the professional master's program during that time period.

11) Related programs in the institution or other British Columbia post-secondary institutions and outside of British Columbia

Simon Fraser University does not have any graduate or undergraduate program directly or indirectly related to the proposed program. Below is a list of cybersecurity programs offered in Canada that are similar to our proposed program offering. CIP 11.1003 can be used for all these programs.

Program Name	Program Type	Duration/Tuition	Admission Requirements
University of Guelph			
Master of Cybersecurity and Threat Intelligence	Course-based with capstone project	12 months DOM: $22,500. INTL: $42,000	4-year honours degree in computer science or computer engineering or another discipline with CS/CEng minor; 75% in the last four terms.
	Comment: Very similar to our program in delivery type, content and target demographic. Has the same goal of training cybersecurity professionals for the workforce. However, it doesn't have an industrial internship/co-op component, is shorter than our program and is offered face-to-face in ON.		
University of New Brunswick			
Master of Applied Cybersecurity	Course-based with capstone project	12 months DOM: $17,000; INTL: $22,622	Bachelor's degree in computer science or related field; min. average of B
	Comment: Offered face-to-face in Fredericton, NB. Is shorter than our program and does not include an industrial internship/co-op.		
Concordia University			
Master of Engineering in Information Systems Security	Course-based with co-op or project option	24 months DOM: $12,279; INTL: $28,575	Bachelor's degree or equivalent in computer engineering, electrical engineering, software engineering, or computer science.
	Comment: This is a course-based engineering program based in Montreal. The co-op and project options are not built-in but may be available to students upon application. The program is also longer than our proposed program.		

Program Name	Program Type	Duration/Tuition	Admission Requirements
Northeastern University			
	- Course-based with	24-36 months	

Master of Science in Cybersecurity	capstone project; - co-op optional; - On-campus, online, or hybrid model	DOM: $34,510; INTL: $44,863	Bachelor's degree; Academic or professional understanding of discrete mathematics, programming, systems administration and computer networks; GPA 3.00/4.00
	Comment: This program is similar to our proposed program but is quite a bit longer in duration (by 8-16 months), offers additional delivery modes (online and hybrid), and includes an optional co-op rather than a mandatory one. Though it is very similar to our proposed program, the on-campus experience is offered in Toronto and at campuses in the U.S., so it does not compete geographically with our proposed in-person offering in B.C.		
University of Ontario Institute of Technology			
Master of Information Technology Security	Full-time or part-time, course-based with capstone project or internship	24 months DOM: $12,575; INTL: $34,517	4-year honours degree in information technology or related field, minimum B average. One course each in advanced programming, advanced math, and operating systems.
	Comment: While this program is very similar to our proposed program, it is based in Ontario, so it would not compete geographically with our program offering.		
New York Institute of Technology			
Master of Science in Cybersecurity	Course-based with final project	24 months or less $39,518	4-year bachelor's degree in computer science or related field; min. GPA 2.85/4.00
	Comment: NYIT is an American private university with a campus in Vancouver. It has lower admission requirements than we are proposing for the cybersecurity masters. The NYIT program does not offer an industrial internship/co-op and is longer in duration than our proposed program. Further, the NYIT campus does not offer the typical university experience that our target audience desires.		
Queen's University			
NSERC Cybersecurity CREATE Program (M.Sc.)	Project-based	12 months DOM: $5,773; INTL: $12,928	Bachelor's degree in computer science with a high upper-class standing.
	Comment: This program differs from our proposed program as it is essentially course-based but with a substantial terms-long final project subject to a formal examination by a supervisory committee. The program is also relatively short in duration and does not include a mandatory industrial internship/co-op.		

12) What differentiates the proposed program from all other related programs in the province?

There is only one other master's degree program in cybersecurity offered in the Province of British Columbia: Master of Science in Cybersecurity at the New York Institute of Technology (NYIT). The NYIT program does not offer an industrial internship or co-op and appears to be longer in duration than the proposed program. All other related programs in the province are certificate or diploma programs and tend to focus on network security.

13) An overview of the level of support and recognition from other post-secondary institutions, and relevant regulatory or professional bodies

The Program was conceived in consultation with and with input from the following organizations and groups: City of Surrey, FAS External Advisory Council, Canadian Centre for Cyber Security, Communications Security Establishment (Government of Canada), Information Security Branch of the Province of British Columbia, ISACA Vancouver, Cisco, Fortinet, MDA, Palo Alto Networks, Shield4UC, Trend Micro, University of British Columbia, University of Victoria, Queen's University, and others. The opinions expressed in the support letters (see Appendix 3) strongly confirm that cybersecurity professional degree programs are in high demand in BC and Canada. The letters leave no doubt that decisive action for growing the cybersecurity talent pool is critical for future growth of a thriving cybersecurity ecosystem and that the School of Computing Science is well recognized as a competent academic leader to offer such a program. "Students graduating from the master's program will emerge as subject matter experts on a wide range of cybersecurity technologies and will be well suited to take on a variety of critical roles ranging from cyber research and architecture design to policy creation and the highly respected Chief Information Security Office (CISO) role."[9]

The proposed initiative resulted in several new collaborations with external partners like the Canadian Centre for Cyber Security, Cisco, Fortinet, Palo Alto Networks and Trend Micro. Industry partners are supplying highly valuable resources at no cost such as industrial-strength tool environments (firewalls, VMs, etc.) and training materials for building and running our industry-strength cybersecurity laboratory. Other partners are committing their time by offering guest lectures on cybersecurity topics to our students and by participating in program review meetings to provide feedback on evolving demands for cybersecurity education and training.

14) What added value will the proposed program offer graduates in terms of employment opportunities?

SFU does not currently offer a program in cybersecurity but offers a Bachelor of Science in Computing Science preparing students to start their career in the IT industry. With the continually

[9] Rob Rashotte, Vice President, Global Training & Technical Field Enablement, Fortinet (see letter).

evolving nature of computer science, not only do students need to learn the fundamentals of cybersecurity but they also need to familiarize themselves with a broad range of new and rapidly advancing topics in this field. The full gamut of a computer science (or closely related) undergraduate education is an essential prerequisite for the Program because of the quantitative nature and technical depth of cybersecurity. Students in the Program exclusively benefit from the highly focused curriculum and structure of a program designed to study in-depth advanced topics of computer and information security and to practice learned skills through intensive hands-on training and experiential learning. Two high-intensive six-unit mandatory lab courses exclusively available to students in the Program cover fundamentals and cutting-edge topics in a practical manner. Furthermore, dedicated industrial internship or co-op placements of either four or eight months with leading cybersecurity organizations are available to these students only.

Companies and organizations active in sectors such as health, finance, education, retail and advanced manufacturing in BC and Canada are in urgent need of cybersecurity expertise; this is going to be one of the foremost trends in the IT industry over the next decade. Program graduates will be readily equipped with skills to master penetration testing and fundamental knowledge in network security, application security, cloud security and threat intelligence, making them highly competitive in the job market. Strong relationships between CS and cybersecurity industry leaders like Fortinet, Cisco, Palo Alto Networks and Trend Micro will keep the Program abreast with evolving technological trends and industry practices to prepare our students for industry needs and expedite the absorption of graduates into the job market.

15) Do potential employers require a degree for graduates to gain employment in the field?

A comprehensive market study [5] on cybersecurity job opportunities shows that employment opportunities increase with education level, where 93% of job postings called for candidates with at least a bachelor’s degree. Many undergraduate programs offer a limited number of courses related to cybersecurity, in many cases only as an elective. Even this limited offering is a very recent development initiated by computer science programs in the last few years. This translates into many computer science graduates not being well trained for cybersecurity jobs, which is one of the main reasons for the lack of qualified personnel in this field. A professional master's degree in cybersecurity means superior technical skills and abilities compared to a general undergraduate computing science degree. From an employer’s perspective someone with a graduate degree is better qualified for working in IT security to protect sensitive digital assets and is a natural choice for positions such as Chief Information Security Officer (CISO), specifically for legal liability reasons, an increasingly critical factor for organizations with a web presence.

16) Potential areas/sectors of employment for graduates and/or opportunities for further study in the field

Upon completing the Program, graduates will be able to pursue additional education and training through graduate studies (e.g., MBA, PhD) across a wide variety of high-tech fields of study including, but not limited to, information and communications technology, Internet of Things (IoT) technology, advanced manufacturing, cyber threat intelligence, cybersecurity forensics, cyber risk management, applied data science and artificial intelligence, Smart Cities and smart transportation networks.

17) Does the proposal lead to a specific occupation?

Graduating students will be able to compete for a range of jobs in the cybersecurity and IT security job market including but not limited to the following jobs:[10]

- **Penetration and Vulnerability Testers** are responsible for performing application, web, network, and infrastructure penetration tests in an organization to probe for vulnerabilities. In addition, they review the physical security of the organization and conduct regular social engineering tests.
- **Cyber Threat Intelligence Analysts** study information relating to real and potential cyberthreats to help organizations to prioritize their risk and inform all aspects of their security programs.
- **Incident Responders** are responsible for responding to a threat and neutralizing it before more damage to organization assets occurs.
- **Network security engineers** are responsible for the design and delivery of network security which needs a deep understanding of topics such as computer network attacks, network architecture and protocols, deep packet inspection and intrusion detection and prevention systems.
- **Risk Analysts** assess the current security strategy, business continuity and disaster recovery plans, threats to the systems, and then calculate the impact of potential cyberattacks on the organization.
- **Cyber Crime Investigators** are primarily concerned with gathering evidence from digital systems that can be used in the prosecution of internet-based criminal activity. In today's world, many crimes include the use of the World Wide Web.
- **Cybersecurity Consultants** work in a variety of roles within the cybersecurity field. They often mimic both the attacker and the defender in computer systems, networks and software programs to find existing weaknesses and figure out how to strengthen systems to prevent hackers from exploiting vulnerabilities.

[10] For a comprehensive overview see also CyberSeek: Cybersecurity Career Pathways. National Initiative for Cybersecurity Education. U.S. Department of Commerce. https://www.cyberseek.org/pathway.html.

18) What labour market needs would the proposed program meet for the province? (Please include no more than 5 applicable National Occupational Classification (NOC) codes.)

Job market analysis

Cybersecurity as an identifiable degree field is still in its infancy, yet it has gained striking momentum in recent years [8]. Driven by significant workforce needs, the demand for post-secondary education in cybersecurity is steadily growing, with commercial and government sectors facing a widening gap between their growing needs to hire in this field and the number of skilled workforce available. Data and facts from leading analysts such as Deloitte and Gartner, professional organizations like ISACA and $(ISC)^2$, government departments like ISED Canada, and other recognized sources confirm that the skills shortage continues to be a reality, and research indicates that the skills shortage continues to worsen:

- The $(ISC)^2$ Cybersecurity Workforce Study, released in 2019, concluded that 4.07 million workers would be needed to fully close the gap.[11] This is in addition to the 2.8 million cybersecurity workers currently in the field globally. In their 2020 Cybersecurity Workforce Study they estimate the cybersecurity workforce gap for Canada is 16,562 for a total Canadian cybersecurity workforce of 101,963.[12] Overall, 64% of the responding organizations reported a shortage of cybersecurity staff and that security risks spring directly from those shortages.

- Cybersecurity is an important issue to educate students on. ICTC estimates that by 2023, Canada will see a demand for 40,000-53,000 cybersecurity practitioners (such as certified information systems security professionals, security architects, security engineers, security specialists, etc.) and in total there will be over 100,000 cybersecurity related jobs created (including occupations like ethical hacker, virus technician, vulnerability assessor, etc.) across a variety of industries.[13]

- "We're as close as possible to our unemployment rate being zero," says Sam Olyaei, senior research analyst at Gartner Security & Risk Assessment Summit in National Harbor, MD. "If you're a cybersecurity professional with any kind of skill set, you already have a job and multiple offers on the table. …" [9].

BC is turning into a global hub for services and products offered by cybersecurity industry leaders including Deloitte, Fortinet, Mastercard and other firms, as detailed under Question 31.

[11] $(ISC)^2$ Cybersecurity Workforce Study, 2019. Strategies for Building and Growing Strong Cybersecurity Teams, 2019.
[12] $(ISC)^2$ Cybersecurity Workforce Study, 2020. Cybersecurity Professionals Stand Up to a Pandemic.

[13]Information and Communication Technology Council (ICTC). Forecasting Demand for Cybersecurity Workers in Canada: 2017-2023. Ottawa, 2019.

The proposed cybersecurity program responds to the notorious talent shortage by graduating cybersecurity professionals who are ready to join the workforce.

The currently available National Occupational Classification (NOC) codes do not capture recent cybersecurity and information security specific job qualifications relevant to the IT industry (cf. Question 17) and, as such, do not show the real picture of the cybersecurity labour market needs. For the codes listed below, the job openings to job seekers ratio (projection of Cumulative Job Openings and Job Seekers over the Period of 2019-2028) does not reflect the actual job market situation for the cybersecurity field, neither nationally nor regionally. Recent surveys of the U.S. cybersecurity job market present an alarmingly different picture.

2171 Information systems analysts and consultants

Projected Job Openings: 111,000

Projected Job Seekers: 98,700

http://occupations.esdc.gc.ca/sppc-cops/occupationsummarydetail.jsp?&tid=80

2173 Software engineers and designers

Projected Job Openings: 27,500

Projected Job Seekers: 24,000

http://occupations.esdc.gc.ca/sppc-cops/occupationsummarydetail.jsp?&tid=82

Table 1. B.C. Labour Market Outlook 2019 (this is the latest addition)

NOC	Employment 2019	Job Openings 2019-2020	Wage Rate Low	Wage Rate Medium	Wage Rate High
2171	18,210	7,600	$26.15	$38.97	$54.95
2173	11,060	4,480	$24.36	$38.46	$60.00

https://www.workbc.ca/Labour-Market-Industry/Labour-Market-Outlook.aspx

19) Plans for admissions and transfer within the British Columbia post-secondary education system

Students within the BC post-secondary education system will be admissible to the Program provided they meet the admission requirements. Transfer into the Program will be more challenging due to the Program's cohort nature and the two mandatory core lab courses, specializing on hands-on training across a range of fundamental cybersecurity skills. Transfer requests will thus have to be reviewed on a case-by-case basis in consultation with the Program Director and relevant faculty members. In all cases, students will need to apply for admission to the Program during the open admission period. Students who have previous graduate-level course credits not counted toward a prior credential and sufficiently similar to courses in the Program may receive specific transfer credit counting toward the Program.

Program graduates may be accepted for graduate or professional school programs at other institutions, but the cybersecurity master's degree is not intended as preparation for a doctoral degree or a research career. For most graduates, it will be the final degree leading to distinctively advanced professional opportunities.

There are no regulatory professional bodies relevant to the Program.

20) Enrolment Plan

The anticipated student enrollment for the Program focuses on full-time students only as it will not offer a part-time option during this time period. For the first intake, we project to enroll about 35 students. Based on past trends in similar master's programs in the Faculty of Applied Sciences, we anticipate increased interest, but we plan on keeping the admission numbers steady at 35-40 students per intake since it matches our delivery capacity. Our enrolment plan aligns with SFU's Equity, Diversity and Inclusion (EDI) initiative. We will strictly follow and comply with EDI policies and procedures.

21) Delivery methods

The Program will normally be delivered in a traditional in-person classroom-based setting integrated with hands-on lab courses. Students will complete at least 30 units of graduate work divided into three sections: 12 units of specialized hands-on lab courses, which comprise two courses with 6 units each; 12 units of required core courses; 3 units of electives; and 3 units for an industrial internship placement, typically working for at least four months with an industry partner in the cybersecurity sector anywhere in Canada. The Program does not have a capstone. It will be delivered using a cohort model; this is required to manage the logistics around the highly specialized lab courses, which heavily rely on cutting-edge industrial-strength cybersecurity hardware-software test and tool environments. Furthermore, it will streamline organizational efforts for placing student interns at industry partners, normally during summer terms, and for the fall terms for students who take an 8-month industrial internship.

22) Eligibility for scholarships, awards, and financial aid

Students admitted to the Program will not be eligible for awards associated with the University's operating budget but will be eligible to apply for private awards, and CS will be approaching external entities for funding for such awards. Additionally, we will also seek industry sponsored scholarships from our industry partners. This portion of student funding is expected to increase by building a strong reputation of the Program over the first three years and beyond. Note that active students will still be eligible to utilize the University's financial aid program.

23) Does the proposed program offer an alternative exit, if appropriate?

The Program does not offer an alternative exit to students who do not complete the program requirements. However, for a short-duration, course-based, industry-focused degree like this one an alternative exit is not necessary, as individual courses carry considerable weight in industry. Students who successfully complete some, but not all, courses can use the knowledge gained in those courses for professional advancement in the cybersecurity field in the same way that one might use stand-alone, domain-specific, technical certificates. Regardless, to avoid hardships, we consider offering a Diploma in Cybersecurity based on completing a minimum number of course units as an option in the rare case that a student does not complete the program.

24) Resources required and/or available to implement the program

The proposed lab courses, Cybersecurity Lab 1 and Lab 2, focus on applied education and hands-on training in system, network, web and cloud security. These labs will be run by limited term faculty members, professors of professional practice and/or University Research Associates (see table Q26) knowledgeable in the lab content. The lab courses will be run in a dedicated laboratory space at the SFU Burnaby campus, equipped with industrial-strength computer hardware and software tools and test environments. This space will also include breakout discussion areas where the instructor or TAs can conduct impromptu discussions with groups of students. The room will have built-in projectors and other amenities. This new lab may be shared between professional master's programs (see Appendix 6).

Building on lessons learned from previous offerings of the Big Data Professional Computer Science program, we limit enrollment in each lab section to 35-40 seats and have instructors and teaching assistants all spend adequate time in the lab with the students. This will ensure that we can offer a truly premium lab experience by ensuring we have a high-quality lab for the students admitted into this program. Both lab courses include weekly empirical assignments to encourage a 'learning-by doing' approach, and multiple mini projects and term projects that familiarise students with the latest security threats and challenge them to mitigate such weaknesses. In preparing the lab course materials we will take advantage of training materials offered by top cybersecurity solution providers such as Fortinet, Palo Alto Networks, Cisco and Trend Micro. We will integrate various tools and products from these companies such as attack and defence tools, capture the flag platforms, and virtual machine frameworks in the two lab courses to acquaint students with advanced industry-specific knowledge and skills.

Professional computer science programs will be supported by dedicated administrative staff and the Program Director. Cost for administration will be shared equally between all programs.

Cybersecurity is also supported by 2 University research Associates (URA) and 1 continuing faculty member. They take charge of and teach each of the two lab courses and lecture courses. Each of the 6-unit lab courses will require 12 hours per week for students (using the typical 0.5 units per weekly lab hour). A limited term faculty member will be assigned to each 6-unit lab course, where each section will have a maximum capacity of 35-40 students. There will also be substantial teaching assistant support in the labs to assist students with their assignments.

To support the mandatory co-op or industrial internship component of the Program, the School of Computing Science will be working with the FAS graduate co-op office. The co-op administration of all 3 programs will be supported by 2 Co-op Coordinators, and 1 program Assistant. These co-op staff members will help the students prepare their applications, assist with the interview process, monitor the placements, deal with program marketing and opportunity development (in order to successfully place 30 students, the identification of over 100 possible positions is required). In the event that a student is unable to secure a co-op during the summer term, they will be required to go on academic break since no courses will be offered. The student will be able to apply for a co-op in the subsequent term or, if unsuccessful, will be required to undertake additional course work.

25) Program evaluation and academic/administrative oversight

Academic and administrative oversight will be provided by the Program Steering Committee. For now, the steering committee consists of the Program Director (Dr. Jiannan Wang), the Computing Science Graduate Program Director (Dr. Jiangchuan Liu), the Director of the School of Computing Science (Dr. Mohamed Hefeeda), one cybersecurity professor in the Program (Dr. Uwe Glässer), one university research associate in the Program (Dr. Mohammad Tayebi), and one Lecturer (Dr. Ouldooz Baghban Karimi). Additionally, we will invite a faculty member in SFU's School of Criminology to join the Steering Committee. Computing Science is strongly committed to gender balance and actively seeking to hire female faculty in cybersecurity related fields. The EDI commitment will be reflected in the future composition of the steering committee.

The Program will be reviewed internally using the same mechanisms that are used to review the other CS graduate programs. Any program changes will be administered through the existing Computing Science Graduate Program Committee.

The School has already considered the creation of an external program advisory board. Advisory members serve a 3-year term. Each member can serve, at most, two terms on the advisory board.

Advisory board members meet twice per year (usually early December & early April) to discuss strategic program priorities such as the expectations of the cybersecurity industry, related professional organizations and societal trends. Board members' feedback and guidance will allow the Program to be responsive to changes in its external environment due to technological advances and industry needs, government priorities, community and professional expectations,

and a challenging fiscal climate. Industrial internship employers and students will be invited to participate in surveys on a regular basis with respect to program content and structure.

26) Faculty member's teaching/supervision

Teaching and supervision of the Program will be provided by the CS faculty members listed in the table below, also showing their research expertise. Two University Research Associates (URAs) are fully dedicated to this program and funded by revenues from the program. The program delivery will not affect regular faculty members' involvement in other programs. For faculty recruitment and retention, we expect the Program to also have a strong positive impact on attracting new tenure-track faculty members to open faculty positions in Computing Science at SFU.

Computing Science faculty involved in delivering the Program

Course	Name	Research Area	Percentage
CMPT 727: Machine Learning	Mo Chen	Robotics and Autonomous Systems	13%
	Greg Mori	Computer Vision, Machine Learning	13%
	Oliver Schulte	Machine Learning, Computational Logic, Computational Decision Theory	13%
CMPT 780 Computer Security and Ethics	Uwe Glässer	Cybersecurity, Cyber Security Analytics	13%
CMPT 782 – Cybersecurity Lab 1	Mohammad Tayebi (URA)	Cybersecurity, Machine Learning	100%
CMPT 783 - Cybersecurity Lab 2	Khaled Diab (URA)	Cybersecurity, Distributed Systems	100%
CMPT 784 – Cyber Risk Assessment and Management	Uwe Glässer	Cybersecurity, Software Technology	13%
CMPT 785 – Secure Software Design	William Sumner	Software Development, Cybersecurity	13%
CMPT 786 - Cloud and Network Security	Ouldooz Baghban Karimi	Data and Network	13%
CMPT 787 – Ethical Hacking	Mohammad Tayebi (URA)	Lecture	13%
CMPT 788 – Information Privacy	Igor Shinkar	Computational complexity	13%

CMPT 789 – Applied Cryptography	Andrei Bulatov	Constraint Satisfaction, Complexity of Computation	13%

27) Is the program focus primarily on meeting social benefit(s) or economic benefit(s)?

Many forms of criminal activity have moved into cyberspace. Criminals are gaining benefits from operating in the cyber arena at national and transnational levels, affecting individuals, businesses, health care facilities and municipalities on a daily basis. Typical examples include stealing personally identifiable information, accessing confidential intellectual property, ransom attacks and attacks on critical infrastructure. This situation has a catastrophic impact across the world economy, resulting in massive economic losses. The growing cybercrime incidents now cost the world economy more than $1 trillion (USD), or just more than one per cent of the global GDP, which is up more than 50 per cent from a 2018 report that put global losses at close to $600 billion [13]. Half of all Canadian small and medium-size businesses have been the victim of a cyberattack [14]. Cybercrime complaints in Canada increased by 45% from 2014 to 2017 [15].

Students trained in the Program will be able to bolster technological systems to resist these styles of attacks. Still, the degree's primary focus will be on meeting economic benefits (see also Q. 30).

28) How would the proposed program advance social goods or government priorities?

Canada is one of the most connected countries in the world. We live our lives online and need to be able to trust our cyber systems. Digital technologies and the internet are increasingly important to innovation and economic growth. A safe and secure cyberspace is critical for Canada's competitiveness, economic stability and long-term prosperity [3]. The use of the internet by foreign intelligence agencies to conduct espionage increased dramatically in the last decade as a low-cost and low-risk approach to access classified documents. Based on CSIS reports there are daily attempts to penetrate the networks of the Government of Canada [16]. Attacks to critical infrastructure "which if disrupted, damaged, manipulated or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada." [17] Maintaining effective and reliable defences against cyberattacks is a priority for Canada to protect its national security, critical infrastructure, citizens' intellectual property and personal data.

Given the cyber threat situation that will only get worse, decisive action is needed now to boost development and future growth of a thriving cybersecurity ecosystem by innovation in education, science and technology. The staggering talent gap in cybersecurity is one of the main barriers to accomplishing this goal. Graduates of the Program will be well educated and trained to engage in the daunting task of reinforcing the cyber defence critical for BC and Canada to meet their priorities in protecting our citizens, businesses, economy and sovereignty.

29) What social, cultural, regional, community, environmental, institutional and/or intellectual benefit would the proposed program provide?

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching **$10.5 trillion** (USD) annually by 2025, up from $3 trillion (USD) in 2015. [14] This dire prospect is triggering enormous investments in information and computer security. The expected economic opportunities for the Canadian market arising from cybersecurity seem to easily justify and finance decisive federal investment into programs that protect Canadians and our economy. Our security and prosperity depend vitally on a safe and secure cyberspace, especially when facing a cyber-threat landscape that will only get worse. The Program will train students with the latest technology to fill the talent gap in this space with the mission of raising the standards of cybersecurity.

30) How would the proposed program support economic growth and/or government economic priorities?

The Province of British Columbia will directly benefit from the launch of the Program, which strongly aligns with BC's primary goal of investing in technology and innovation. The demand for post-secondary cybersecurity education is steadily growing, with commercial and government sectors facing a widening gap between their growing needs to hire in this field and the number of skilled workforce available.

By training the next generation of cybersecurity professionals, the Program supports the BC Government's current strategic plan to make BC a global hub for innovation and connectivity. Part of this plan is the development of future tech talent, supporting research and innovation, and putting BC companies in a better position to compete globally. Graduates from the proposed program would join the tech workforce in capacities allowing them to contribute in leading roles—ranging from cyber research and architecture design to policy creation and the highly respected Chief Information Security Office (CISO) role to the development and implementation of innovative technologies, products and services for a safe and secure cyberspace.

[14] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

31) What direct and/or indirect economic, industrial or labour market benefits would the program offer the student, community, region or province?

With $34.9 billion in annual revenue in 2019, the Province of British Columbia has one of the fastest-growing high technology sectors in Canada.[15] More than 130,000 people were employed in this sector in BC in 2019. The Program is proposed in response to the notorious talent shortage by graduating cybersecurity professionals who are ready to join the workforce; the program would offer enormous economic, industrial, and labour market benefits to the Province by providing much needed talent to BC's tech sector.

In 2020, Mastercard announced that Vancouver is home to its new Global Intelligence and Cyber Centre, one of six global technology centres; the other five are in New York and St. Louis (USA), Pune-Vadodara (India), Dublin (Ireland) and Sydney (Australia). Mastercard's Vancouver centre is a $510 million investment, which will accelerate innovation in digital and cybersecurity, artificial intelligence, and the Internet of Things and will develop new cyber solutions for the payments ecosystem worldwide.[16] The centre houses members from Mastercard's Research & Development, Operations & Technology, and Cyber and Intelligence divisions, and will grow to 380 FTEs and offer 100 co-op positions, in partnership with Canadian universities [19].

In 2016, Deloitte opened its fourth Canadian Cyber Intelligence Centre in Vancouver, expanding its Canadian operation (with three other centres based in Montreal, Toronto and Calgary). These centres bring together leading experts in cyber risk with state-of-the-art technology to offer a full suite of managed security services including customized, integrated services like incident response and threat intelligence around the clock.[17]

Fortinet, a global leader in cybersecurity technology and services, has partnered with Simon Fraser University to provide hardware and software as critical components for this program. Fortinet's largest R&D facilities are in Burnaby, BC as is the FortiGuard Labs team, providing threat intelligence for their world-wide operations. The Program appeals to Fortinet as a local source for producing much needed experts for years to come.

Graduates from the proposed Program would help BC businesses, organizations and consumers safeguard their operations and mitigate cyber risks by building resilience against cyber threats. This may result in huge savings by reducing direct and indirect damages such as caused by ransomware and distributed-denial-of-service (DDoS) attacks. The economic and labour market benefits the Program offers to students are high employability, above average compensation and strong job security.

---

[15] Profile of the British Columbia Technology Sector: 2020 Edition - Prepared for the Ministry of Jobs, Economic Recovery and Innovation by BS Stats, March 2021.
[16] Mastercard opens global cybersecurity centre in Vancouver. IT World Canada, January 23rd, 2020 [19].
[17] Canadian-based Cyber Intelligence Centres at Forefront of Global Cybersecurity. Deloitte, 2020 [20].

References

[1] O. Sami Saydjari. Engineering Trustworthy Systems: A Principled Approach to Cybersecurity. *Communications of the ACM*, Vol. 62, No.6, June 2019, 63-69.

[2] Canadian Centre for Cyber Security. National Cyber Threat Assessment 2020. Communications Security Establishment (CSE), Government of Canada, 2020. https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

[3] National Cyber Threat Assessment 2018. Canadian Centre for Cyber Security. Communications Security Establishment (CSE), Government of Canada, 2018. https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018

[4] N. Perlroth, and S. Shane. In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc. The New York Times, 2019. https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

[5] K. Slyter. Is a Cyber Security Degree Worth It? The Facts You Can't Ignore, 2019. https://www.rasmussen.edu/degrees/technology/blog/cyber-security-degree-worth-it/

[6] S. Morgan. Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally By 2021. https://cybersecurityventures.com/jobs/

[7] U.S. Bureau of Labor Statistics, Employment Projections program, Information Security Analyst Job Outlook, 2020. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

[8] Cybersecurity Curricula. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. A Report in the Computing Curricula Series Joint Task Force on Cybersecurity Education, ACM, IEEE, AIS SIGSEC, and IFIP, Version 1.0., 2017. https://cybered.hosting.acm.org/wp/

[9] K. Panetta. Confront the Cybersecurity Talent Shortage. Adjust your current hiring strategy to attract the best cybersecurity talent in a competitive job market. Gartner, 2017. https://gartner.com/smarterwithgartner/solve-the-cybersecurity-talent-shortage/

[10] Deloitte. The changing faces of cybersecurity: Closing the cyber risk gap. Toronto Financial Services Alliance (TFSA), 2018. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-rep ort-pov-aoda-en.PDF

[11] CyberSeek™ Data Confirms the Ever-Present Need to Expand Cybersecurity Talent Pipeline. NIST, July 16, 2020. https://www.nist.gov/news-events/news/2020/07/cyberseektm-data-confirms-ever-present-need-expand-cybersecurity-talent

[12] Noor Subeh. British Columbia Tech Sector a Leader in Canada. Trade and Invest B.C. December, 2018. https://www.britishcolumbia.ca/global/trade-and-investment-british-columbia-blog/december-2018/british-columbia-tech-sector-a-leader-in-canada/

[13] McAffee, The Hidden Costs of Cybercrime, December 2020. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

[14] Canadian Chamber of Commerce, Cyber Security in Canada: Practical Solutions to a Growing Problem, April 2017. https://www.cambridgechamber.com/userContent/documents/Advocacy/170403_Cyber_Security_in_Canada.pdf

[15] Howard Solomon. Canadian Police Frustration Over Cyber Crime Shows at Conference, IT World Canada, November 7, 2017. https://www.cambridgechamber.com/userContent/documents/Advocacy/170403_Cyber_Security_in_Canada.pdf

[16] Canadian Security Intelligence Service. CSIS Public Report 2019, 2019. https://www.canada.ca/content/dam/csis-scrs/documents/publications/PubRep-2019-E.pdf

[17] Public Safety Canada, Threats to Canada's Critical Infrastructure. https://www.publicsafety.gc.ca/lbrr/archives/cn000034012674-eng.pdf

[18] Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019. https://www.isc2.org/Research/-/media/6573BE9062B64FC7B4B91F20ECC56299.ashx

[19] Lynn Greiner. Mastercard Opens Global Cybersecurity Centre in Vancouver. *IT World Canada*, January 23rd, 2020. https://www.itworldcanada.com/article/mastercard-opens-global-cybersecurity-centre-in-vancouver/426381

[20] Canadian-based Cyber Intelligence Centres at Forefront of Global Cybersecurity. Deloitte, 2020. https://www2.deloitte.com/ca/en/pages/risk/articles/canadian-based-cyber-intelligence-centres-at-forefront-of-global-cybersecurity.html

APPENDICES

Appendix 1 Calendar entry

School of Computing Science | Professional Cybersecurity

Master of Science

Description of Program

The Master of Science in Professional Cybersecurity program engages students in developing specialized knowledge and practical skills in the area of cybersecurity. The program trains students to build and maintain safe systems and infrastructure that can withstand digital attacks. Foundational topics such as penetration testing, malware analysis and configuration of firewalls are covered as part of the curriculum complemented by advanced teaching in cryptography, secure software design and ethical hacking, among others. Students take instructional and lab courses, in a cohort, and complete work placement through SFU's co-op program, allowing them to tackle real-world scientific, engineering, and social-economic problems and gain valuable project management experiences while expanding their network of industrial contacts. This full-time master's program is suitable for students with a strong aptitude in computer science, or other quantitative fields, such as engineering and mathematics.

Admission Requirements

Applicants must satisfy the University admission requirements as stated in Graduate General Regulation 1.3 in the SFU Calendar. Applicants should normally have a bachelor degree, or equivalent in computer science or a related field. Students who do not meet the minimum university requirements may be recommended as conditional or qualifying students as per Graduate General Regulation (GGR) 1.3.8 or 1.3.9.

For further information on conditional or qualifying admission requirements, please contact the Program Coordinator.

Program Requirements

This program consists of course work, and co-op or graduate project for a minimum of 30 graduate units.

Students must maintain a minimum 3.0 CGPA throughout their graduate career.

Students complete all of:

CMPT 756 - Distributed and Cloud Systems (3)
CMPT 782 - Cybersecurity Lab I (6)
CMPT 783 - Cybersecurity Lab II (6)
CMPT 789 - Applied Cryptography (3)

and an additional nine units of graduate courses in Computing Science

and one of

CMPT 626 - Graduate Co-op I (3)

or

CMPT 629 - Graduate Project (3)

Program Length

Students are expected to complete the program requirements in four terms.

Other Information

Co-op

A co-op is an integral part of this program. However, it is offered on a competitive basis.

All students are required to apply for a co-op. With assistance from the co-op coordinator for this program, students will be expected to find a suitable industry partner. Students may complete one or two terms of co-op. The latter option is in place to satisfy requests from our industrial partners for continuity and to carry out a large-scale project. Students are required to enroll in at least one of the program courses in the term following their co-op.

In the event that a student is unable to secure a co-op during the summer term, they will be required to go on academic break since no courses will be offered. The student will be able to apply for a co-op in the subsequent term or, if unsuccessful, will be required to undertake additional course work. In consultation with the program director, the student may complete a graduate project in their final term to fulfill program requirements.

Academic Requirements within the Graduate General Regulations

All graduate students must satisfy the academic requirements that are specified in the graduate general regulations, as well as the specific requirements for the program in which they are enrolled.

Appendix 2 Letters of support

Following are copies of seven letters of support from the following organizations:

- Canadian Centre for Cyber Security
- Fortinet Corp.
- MDA Systems Ltd.
- ISACA Vancouver Chapter
- Coast Capital Savings
- CyberSC
- University of British Columbia

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

UNCLASSIFIED
TLP:WHITE

October 5, 2020

Uwe Glässer
Professor, Computing Science
Simon Fraser University - SFU
Burnaby, BC Canada V5A 1S6

Dear Uwe,

Canada is one of the most connected countries in the world. We live our lives online, and we need to be able to trust our cyber systems. Digital technologies and the internet are increasingly important to innovation and economic growth. A safe and secure cyberspace is important for the security, stability and prosperity of Canada, and good cyber security is critical to Canada's competitiveness, economic stability, and long-term prosperity.

Efforts by academia and the private sector to raise awareness of cyber security, to better train users and decision makers, and to enhance Canada's cyber security workforce are vital to Canada's cyber security goals. We at the Canadian Centre for Cyber Security (Cyber Centre) would recommend that educational authorities give strong consideration to any well-structured program in cyber security. While we have not reviewed in detail the SFU's program, the description provided sounds like a comprehensive, yet practical hands-on approach that will undoubtedly introduce a well-prepared cadre of cyber security professionals into the Canadian workforce.

Canada is currently facing a shortage of qualified cyber security workers. Initiatives such as SFU's new academic program, *Professional Master of Cyber Security,* and efforts to protect critical infrastructure in Canada can help provide real world skills development and cross-disciplinary training for students, graduates and external collaborators involved with these programs. These people can serve as the foundation for the cyber security work ahead for Canada.

For your reference, the Cyber Centre is Canada's national government authority on cyber security. The Cyber Centre leads the federal government's response to cyber security events and works to protect and defend the country's valuable cyber assets. The mandate of the Cyber Centre is four-fold: to inform Canada and Canadians about cyber security matters; to protect Canadians' cyber security interests through targeted advice, specific guidance, direct hands-on assistance and strong collaborative partnerships; to defend cyber systems, including government systems, by deploying sophisticated cyber defence solutions; and to develop both specialized cyber defence technologies for sharing across Canada and the innovative cyber security workforce that will underpin our future prosperity. As such, there is clearly a growing demand for qualified cyber security professionals in the marketplace, and given the fast pace at which the cyber threat landscape is evolving in Canada, and the complexities involved in staying abreast of the risk mitigation strategies necessary to respond, it is critical that this field begin to be seen as a profession unto itself, rather than simply an adjunct to other computer science domains.

Thank you for involving the CCCS in the inaugural offering of this important new program, and we applaud your efforts to promote a more cyber secure future for Canada.

Sincerely yours,

Christine Beauchamp

Director, Client Engagement and Incident Detection

September 18, 2020

To Whom It May Concern,

The cybersecurity skills shortage continues to be a reality, and research indicates the skills shortage continues to worsen. The $(ISC)^2$ Cybersecurity Workforce Study, released in 2019, concluded that 4.07 million workers would be needed to fully close the gap. This is in addition to the 2.8 million cybersecurity workers currently in the field globally.

Simon Fraser University, in working with Fortinet and other leading organizations, has established the Professional Master's Program specialization in Cybersecurity to help close the skills gap. Fortinet continues to be a part of this program as a member on Simon Fraser's Industry Steering Committee to help guide curriculum.

Students graduating from the master's program will emerge as subject matter experts on a wide range of cybersecurity technologies and will be well suited to take on a variety of critical roles ranging from cyber research and architecture design to policy creation and the highly respected Chief Information Security Office (CISO) role.

While Fortinet has partnered with Simon Fraser University to provide hardware and software as critical components of this program, we are also very excited about the source of highly skilled cybersecurity graduates. Fortinet's largest R&D facilities are located in Burnaby BC as is our FortiGuard Labs team. As such the Simon Fraser University Master's Program in Cybersecurity is sure to provide Fortinet with much needed experts for years to come.

Fortinet values Master's degree graduates from Simon Fraser University. In recent years 50% of our new graduates hired received Master's degrees and 20% of all new graduates that we hired obtained their degrees from Simon Fraser University. Fortinet has supported Simon Fraser University's internship programs for many years, hosting students as part of research collaborations.

I encourage you to consider a Master's degree in Cybersecurity from Simon Fraser University. It is my opinion that the most relevant programs today are those that have been developed as collaborations between industry and academia and this is exactly what Simon Fraser University has created with this and other programs. Organizations are in need of individuals with advanced security knowledge and the right training and education from the right academic institutions.

Sincerely,

Rob Rashotte
Vice President, Global Training & Technical Field Enablement
Fortinet

899 Kifer Road
Sunnyvale, CA 94086

Tel: +1-408-235-7700
Fax: +1-408-235-7737

www.fortinet.com

September 18, 2020

Dr. Mohamed Hefeeda
Director, School of Computing Science
Simon Fraser University
Burnaby

RE: Letter of Support for Cyber Security Masters Program

Dear Dr. Hefeeda,

As you may know, MDA is Canada's leading Space Company and a major employer of highly qualified personal in Canada. We are hiring large numbers of graduates from Universities from both inside and outside of Canada. A high percentage of those hired have Masters or PhD degrees.

We are recognizing that Cyber Security is an emerging key technology that affects many aspects of our business. The immediate need is to keep MDA's IT infrastructure safe, which is a huge challenge giving the distributed nature of the company, the large workforce, and the diverse cyber security needs which include the management of classified and commercially sensitive information.

An emerging need is in our systems business where customers are starting to ask about the cyber security measures that would keep their new system and data secure and free of tampering. MDA is therefore recognizing the challenge to enhance its system, data, and service offerings with cyber and data security features.

To achieve all these objectives, we anticipate that we would need University graduates who have hands-on training in cyber security and can help with these tasks without lengthy initial in-house training. Moreover, we would expect these new hires from University to bring the latest advances and state-of-the-art in cyber security knowledge to MDA.

Thus, for all these reasons, MDA strongly supports the SFU initiative to create a fully independent professional master's program in Cyber Security.

Best regards,

Hans Wehn
Director, Research & Development
Earth Observation Systems
Hans.Wehn@mdacorporation.com
604-231-2412

ISACA
Vancouver Chapter

September 23, 2020

Dr. Mohamed Hefeeda
Director, School of Computing Science
Simon Fraser University

Dear Dr. Hefeeda:

On behalf of ISACA Vancouver and the 600+ IT Risk, Audit and Cybersecurity professionals we represent from the Province of BC, we are delighted to express our support for the Simon Fraser University School of Computing Science proposal for the creation of a Cybersecurity Master of Science in Professional Computer Science Program. As the risks associated with cybercrime continue to grow, it is more critical now than ever for government to invest in programs like this to assure our society has the skills necessary to thwart cyberattacks.

We are particularly supportive of SFU's focus on a strong applied orientation including hands-on training, paired with real-world experience from an industrial internship program of at least four months. Preparing graduates for a smooth transition into the IT security sector is critical to allow government and businesses to deliver the security outcomes we so desperately need.

Digital transformation must be a priority for Canadian businesses seeking to compete in an increasingly digital world. But digital transformation must be preceded by security transformation to mitigate the organizational risks associated with transformational change. It is programs like SFU's Cybersecurity Master of Science that will ensure the requisite cybersecurity skills required to support digital transformation are available to employers in the years to come.

The ISACA Vancouver team will continue to support SFU with its efforts in establishing and fine tuning this program. If there is anything we can do to assist the Ministry of Advanced Education, Skills & Training while SFU's application is being reviewed, please do not hesitate to ask either of us. We would be pleased to assist in any way we can.

Yours sincerely,

ISACA Vancouver Chapter

Katarzyna Szetelnicka

Katie Szetelnicka
President

Justin Malczewski
Past President's Advisory Council

Coast Capital Savings Federal Credit Union
Help Headquarters
800-9900 King George Blvd, 6th Floor
Surrey, BC V3T 0K7
T 604.517.7400 F 604.517.7587
www.coastcapitalsavings.com

SUPPORT LETTER

September 28, 2020

Dr. Mohamed Hefeeda
Director, School of Computing Science
Simon Fraser University
8888 University Drive
Burnaby, BC V5A 1S6

Dear Dr. Hefeeda,

Canada is one of the most connected countries in the world. Our security and prosperity depend vitally on a safe and secure cyberspace. With cyberattacks increasing in frequency, severity and sophistication, the demand for cyber security talent is steadily growing across North America and other parts of the world. This trend is expected to continue for the foreseeable future. The Cybersecurity Master of Science in Professional Computer Science program proposed by the School of Computing Science at Simon Fraser University is a great opportunity for increasing the number of graduate students in this critical high-tech sector.

With over 20+ years of experience in IT and Information Security and my current roles as manager of IT Security at Coast Capital Savings and Cyber Officer with the Canadian Armed Forces, I am writing to express my support for the proposed program. Given its focus on applied education and hands-on training, the program responds to the increasing demand for hiring IT security experts across a wide range of government and industry sectors in British Columbia and Canada.

The demand for post-secondary education in cybersecurity is steadily growing, with commercial and government sectors facing a widening gap between their growing needs to hire in this field and the number of skilled workforce available. Building on five years of experience with the professional master's program in Big Data, the School of Computing Science at SFU is the right institution to offer a program in cybersecurity. Offering such a program in the Province of British Columbia aligns with the B.C. Government's decision to invest in growing technology and innovation in the province.

Please feel free to reach out to me if you have any questions or concerns.

Sincerely,

Hardeep Mehrotara

Hardeep Mehrotara
CISM, CISSP, CISA, CICP

CYBER SC RISK SERVICES

SECURING BUSINESS GROWTH

Letter of Support:
Cybersecurity Master of Science Program

As a proud graduate of Simon Fraser University (BSc Computing Science, 2008) I am incredibly humbled to write this letter of support for the Cybersecurity Master of Science in Professional Computer Science Program. Over the course of my career I have seen the cybersecurity field evolve from being a hidden cost centre to being a source of competitive differentiation. When I started my career cyber security was the realm only for the big banks, healthcare, and government sectors.

Today, there is an overflowing demand for trained cyber security professionals – across all sectors spanning small business to enterprise. The rise of the digital economy and virtual workforce makes cybersecurity that much more important. Countless cyber security postings go unfilled or take 6+ months to fill here in British Columbia. There simply are not enough qualified professionals to take on this surplus demand of cyber security work. The lack of professionals with applied educations and hands-on training in cybersecurity is staggering. These unfilled jobs costs organizations financially and without having the right resources exposes them to heightened cyber risk. This potentially causes the economy millions of dollars in loss annually.

The proposed Cybersecurity Master of Science program provides a talent pipeline to help meet the ever growing needs that are continually arising for industry, government, and businesses. The economic benefit to the local economy and positive job growth is huge as organizations that are currently waiting months (or are unable) to fill their cybersecurity job vacancies will now be able to find excellent candidates to lead the cyber security programs. Cybersecurity will be one of the most in-demand job fields for at least the decade if not the foreseeable future.

Quite simply I am thrilled to finally see a Cybersecurity Master of Science program developed by some of the finest educational minds from a world-class educational institution being offered right here in British Columbia. The sheer influence that this program will have on the local job market cannot be underestimated. The graduates of this program will be able to have an immediate positive impact on the cybersecurity of local organizations in our province. I applaud the University for developing this program and taking the lead in offering elite cybersecurity education and for securing the digital economy for years to come.

Regards,

Dominic Vogel
Founder & Chief Strategist CyberSC

THE UNIVERSITY OF BRITISH COLUMBIA

Faculty of Science, Office of the Dean
2178 - 2207 Main Mall
Vancouver, BC Canada V6T 1Z4

Phone 604 822 3336
Fax 604 822 5558

September 24, 2020

Dr. Eugene Fiume
Dean, Faculty of Applied Sciences
Simon Fraser University
8888 University Drive
Burnaby, BC V5A 1S6

Dear Eugene,

I am delighted to express my strong support for your proposal for a Cybersecurity Master of Science in Professional Computer Science Program. This proposal comes at a particularly opportune time. As the world is increasingly relying on electronic communication and highly-connected society through powerful and sophisticated computer networks, the need to effectively tackle cyber threats is essential, and we need to do everything we can to increase awareness, education, and expertise on the topic.

In British Columbia, this opportunity is particularly appealing. The Cascadia Innovation Corridor and the Digital Supercluster are two examples for the unique position of our province in terms of cross-fertilization of industrial initiatives and applied research in academia. This calls for pushing forward with a bold and innovative professional education agenda. Developing interdisciplinary high-tech programs with an increased focus on applied education and hands-on training is critical to the IT security sector and the future of the Province of British Columbia. We have a significant gap to close here with Ontario and Quebec.

SFU's Faculty of Applied Sciences has a terrific track record that spans research, academic education, and industry collaborations. The Faculty is a visionary leader in big data education initiatives, with the highlight being a strong professional master's program in Big Data, which is going on for five years and is extremely successful. Given this, the School of Computing Science is well positioned to offer the proposed program in cybersecurity.

The province of British Columbia will greatly benefit from the launch of such a program, which would strongly align with its primary goal of investing in technology and innovation. Based on the above-mentioned growing importance of cybersecurity, the demand for post-secondary education in the field is steadily growing, with commercial and government sectors facing a widening gap between their growing needs to hire in this field and the number of skilled workforce available.

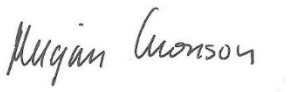
Altogether, I am pleased to see the progress that both of our universities are making in

computational domains in the context of professional education. At UBC, we have a very successful professional master's program in data science with a high level of demand. I believe we are just seeing the tip of the iceberg in terms of demand for professional programs in the province. Market research and the unprecedented number of applicants to existing professional programs strongly demonstrate this and paint an optimistic future.

Future growth of a thriving cybersecurity ecosystem needs to be driven by innovation in education, science and technology, successful start-ups, and collaborations with global leaders. The proposed program is a valuable contribution to this strategic initiative.

My best wishes of success of this exciting program!

Sincerely,



Meigan Aronson
Dean, Faculty of Science

Appendix 3 Memo from the library

SFU SIMON FRASER UNIVERSITY

MEMO

SFU Library

8888 University Drive
Burnaby, BC V5A 1S6
Canada

ATTENTION Christina Margraf

FROM Patty Gallilee

RE Cybersecurity Master of Science in Professional Computer Science

DATE 27 October 2021

Dear Christina,

The library fully supports the creation of the newly proposed Professional Cybersecurity Program.

As there are no new courses proposed for this program, we are confident we are equipped to support students in this program with existing resources.

The primary support person in the Library for this program is Holly Hendrigan, Liaison Librarian for Computing Sciences. Holly provides research and teaching support, and expertly stewards our ever-adapting collection of Computing Science resources.

Graduate students are also well supported by the SFU Library Research Commons, and other Library resources and services such as Research Data Management.

The SFU Library welcomes the creation of this program this program, and looks forward to partnering with it as it develops.

Best,
Patty Gallilee
Associate Dean of Libraries, Collections and Scholarly Communication

Patty Gallilee

SIMON FRASER UNIVERSITY ENGAGING THE WORLD

Appendix 4 Details of program steering committee (if applicable)

Include names and titles of people on the steering committee.

- Jiannan Wang (Director, Professional Computer Science Program)
- Jiangchuan Liu (Director, Graduate Program in Computing Science)
- Mohamed Hefeeda (Director, School of Computing Science)
- Uwe Glässer (Professor, School of Computing Science)
- Mohammad Tayyebi (University Research Associate)
- Ouldooz Baghban Karimi (Lecturer, School of Computing Science)

We consider adding another faculty member from the School of Criminology.

Appendix 5 Abbreviated curriculum vitae for faculty

Mo Chen

Assistant Professor
School of Computing Science, Simon Fraser University
ASB 9971-8888 University Drive
Burnaby, BC, Canada V5A 1S6
Distal Fellow, NSERC Canadian Robotics Network
mochen@cs.sfu.ca

Education

Stanford University, Stanford, CA, USA

Postdoctoral Researcher, Aeronautics and Astronautics, 2017/08 – 2018/07

- Advisor: Marco Pavone

University of California, Berkeley, Berkeley, CA, USA

Ph. D., Electrical Engineering and Computer Science, 2011/08 – 2017/07

- Advisor: Claire Tomlin

University of British Columbia, Vancouver, BC, Canada

B. A. Sc., Engineering Physics (EE option), Mathematics Minor, 2006/09 – 2011/06

Research Interests

- **Theory**: formal verification, reachability analysis, system decomposition, parallel computing, verification and machine learning, game theory
- **Applications**: multi-agent robotic systems, safety-critical systems, human-robot interactions, human intent inference, assistive technology, UAS traffic management, internet of things

Teaching and Advising

Teaching

- CMPT 419/726: Machine Learning – Spring 2020
- CMPT 125: Introduction to Computing Science and Programming II – Spring 2020
- CMPT 894: Directed Reading in Deep Reinforcement Learning – Spring 2020
- CMPT 419/983: Robotic Autonomy: Algorithms and Computation – Fall 2019
- CMPT 125: Introduction to Computing Science and Programming II – Spring 2019
- CMPT 882: Special Topics in Artificial Intelligence: Robotic Decision Making – Spring 2019

Advising

- I direct the SFU Multi-Agent Robotic Systems (MARS) lab, whose research focuses combining traditional analytical methods in robotics and modern data-driven techniques.
- The SFU MARS Lab is home to 9 PhD, 5 MSc, and 4 undergraduate students

Recent Grants

- NSERC Discovery ($140,000 over 5 years) and Discovery Launch Supplement ($12,500 over 1 year)
- Huawei-SFU Visual Computing Joint Lab ($200,000 over 2 years)
- Canada's Digital Technology Supercluster with Terramera Inc. ($182,000 over 2 years), in collaboration with Martin Ester and Ghassan Hamarneh
- CFI John R. Evans Leaders Fund ($750,000), in collaboration with Manolis Savva

Recent Invited Talks

- Mo Chen, "Optimal Control and Machine Learning in Robotics," Workshop on High Dimensional Hamilton-Jacob Method in Control and Differential Games, Institute for Pure & Applied Mathematics, University of California, Los Angeles, Los Angeles, California, March 30 - April 3, 2020
- Mo Chen, "Optimal Control and Machine Learning in Robotics," *NSERC Canadian Robotics Network Distal Fellow seminar*, by video conference from Vancouver, BC, Jan. 9, 2020.
- Mo Chen, "Robotic Safety and Reinforcement Learning," *University of Melbourne Electrical and Electronics Engineering invited seminar*, Melbourne, VIC, Australia, Aug. 7, 2019.
- Mo Chen, "Reachability-Based Robotic Safety and Reinforcement Learning," *Alberta Machine Intelligence Institute (Amii) invited seminar*, Edmonton, AB, Apr. 25, 2019.
- Mo Chen, "Safety in Autonomy via Reachability," *Stanford Robotics Seminar*, Stanford, CA, USA, May 18, 2018.
- Mo Chen, "Differential Games: Practical Safety-Critical Applications," *The Center for Information Technology Research in the Interest of Society (CITRIS)/CITRIS People and Robots (CPAR) Control Theory and Automation Symposium*, Santa Cruz, CA, USA, Apr. 27, 2018.

Selected Publications

[J1] Mo Chen, Sylvia L. Herbert, Haimin Hu, Ye Pu, Jaime Fisac, Somil Bansal, SooJean Han, Claire J. Tomlin. "FaSTrack: a Modular Framework for Real-Time Motion Planning and Guaranteed Safe Tracking." *IEEE Transactions on Automatic Control*, to appear.

[J2] Sandeep P. Chinchali, Scott C. Livingston, Mo Chen, Marco Pavone, "Multi-objective optimal control for proactive decision-making with temporal logic models," *International Journal of Robotics Research*, 2019.

[C1] Seth Siriya, Minh Bui, Arrvindh Shriraman, Mo Chen, Ye Pu, "Safety-Guaranteed Real-Time Trajectory Planning for Underwater Vehicles in Plane-Progressive Waves," *IEEE Conference on Decision and Control*, 2020.

[C2] Xubo Lyu, Mo Chen, "TTR-Based Rewards for Reinforcement Learning with Implicit Model Priors," *IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2020.

[C3] Payam Nikdel, Mo Chen, Richard Vaughan, "Recognizing and Tracking High-Level, Human-Meaningful Navigation Features of Occupancy Grid Maps," *Proceedings of the Conference on Computer and Robot Vision*, 2020.

[C4] Anjian Li, Somil Bansal, George Giovanis, Varun Tolani, Claire J. Tomlin, Mo Chen, "Generating Robust Supervision for Learning-Based Visual Navigation Using Hamilton-Jacobi Reachability," *Proceedings of the Learning for Dynamics and Control Conference*, 2020.

[C5] Juan Chacon, Mo Chen, Razvan C. Fetecau, "Safe Coverage of Compact Domains For Second Order Dynamical Systems," *Proceedings of the IFAC World Congress*, 2020.

[C6] Anjian Li, Mo Chen, "Guaranteed-Safe Approximate Reachability via State Dependency-Based Decomposition," *Proceedings of the American Control Conference*, 2020.

Curriculum Vitae – 7 years

Greg Mori
Professor School of Computing Science 8888 University Drive Burnaby, BC V5A 1S6, Canada

Email: mori@cs.sfu.ca
Web: http://www.cs.sfu.ca/~mori
Tel.: +1 (778) 782 7111
Fax: +1 (778) 782 3045

1 Background

1.1 Education

2004 Ph.D. in Computer Science
Department of Electrical Engineering and Computer Sciences
University of California at Berkeley
Thesis: Detecting and Localizing Human Figures
Advisor: Jitendra Malik

1999 Hon. B.Sc. in Computer Science and Mathematics with HighDistinction
University of Toronto

1.2 Employment History

06/2018 - current Research Director
RBC Borealis AI Vancouver

09/2015 - current Professor
School of Computing Science, Simon Fraser University

05/2015 - 04/2018 Director
School of Computing Science, Simon Fraser University

12/2014 - 05/2015 Visiting Scientist
Google Inc., Mountain View, CA

09/2010 - 08/2015 Associate Professor
School of Computing Science, Simon Fraser University

1.3 Awards since 2013

ICCV Helmholtz Prize, IAPR MVA Most Influential Paper over the Decade Award, Discovery Accelerator Supplement, Award for Service to the Research Community

2 Research

2.1 Research Program

My research is in computer vision, and is concerned with developing algorithms that automatically interpret images and videos, particularly those containing people.

2.2 Most Significant Research Contributions

Human Action Recognition, Human Pose Estimation, Breaking Visual CAPTCHAs, Applications of Vision-based Activity Monitoring

2.3 Publications

A complete list of publications can be found here https://www.cs.sfu.ca/~mori/mori_cv.pdf

3 Teaching

3.1 Award

Excellence in Undergraduate Teaching Award 2006

This award is handed out annually by the SFU Undergraduate Computing Science Student Society (CSSS) to Computing Science faculty to recognize their efforts in teaching undergraduate courses in our department. I received this award in 2006.

3.2 Graduate Student Supervision

Summary of graduate student senior supervisory duties:

Ph.D.		M.Sc.		Total
Active	Complete	Active	Complete	
11	11	2	34	58

3.3 Undergraduate Student Supervision

I have supervised research projects by undergraduate students working under the NSERC Undergraduate Student Research Award (USRA) program, directed studies courses (CMPT 415/416), and directly via research assistantships (RA).

3.4 Course Teaching at Simon Fraser University

For each of my courses I maintain a webpage with lecture slides, homework assignments, and other course material. These webpages are linked from my webpage: `http://www.cs.sfu.ca/~mori`.

3.5 Other Teaching

- Statistical and Structural Recognition of Human Actions: Tutorial at European Conference on Com- puter Vision (ECCV) 2010, Ivan Laptev and Greg Mori
- Emerging Topics in Human Activity Recognition: Tutorial at Computer Vision and Pattern Recognition (CVPR) 2014, Michael Ryoo, Ivan Laptev, Sangmin Oh, and Greg Mori

Abbreviated C.V. – Oliver Schulte

Academic Positions

- Current: Professor, School of Computing Science, Simon Fraser University
- Assistant Professor, University of Alberta, 1997-2001

Education

- Ph.D. - Logic and Computation – Carnegie Mellon University 1997
- M.Sc. – Logic and Computation - Carnegie Mellon University 1994
- B.Sc. – Computer Science – University of Toronto 1992

Awards and Selected Grants (last five years)

- Inference, Learning, and Population Size: Projectivity for SRL Models. Manfred Jaeger and Oliver Schulte (2018). *StarAI Workshop @IJCAI.* Best Paper Award.
- Model-based Outlier Detection for Object-Relational Data. Sarah Riahi and Oliver Schulte (2015). *IEEE SSCI 2015,* pp. 1590-1598. Best Student Paper Award.
- NSERC Strategic Project award. Project Title: Reinforcement Learning for Sports Analytics. Amount: $500K/3 years, success rate 20%. Our company partner is SportLogiq. My co-applicant is Pascal Poupart (Waterloo).
- NSERC Discovery and Accelerator award ($36K/year, $40K/year). One of 125 national awards. The Accelerator awards provide substantial and timely additional resources to maximize the impact of outstanding research programs.
- Blue Ribbon Service Award from the International Joint Conference on Artificial Intelligence (2016). IJCAI is the leading AI conference.

Refereed Research Papers (last five years)

Conference Papers (main archival publication mode in computer science)

AR = Acceptance Rate

C1. Inverse Reinforcement Learning for Team Sports: Valuing Actions and Players. Yudong Luo, Oliver Schulte, and Pascal Poupart (2020). Proceedings IJCAI. AR: 12%. In Press.
C2. Cracking the Black Box: Distilling Deep Sports Analytics. Xiangyu Sun, Jack Davis, Oliver Schulte, Guiliang Liu (2020). Proceedings ACM Knowledge Discovery and Data Mining (KDD). AR: 16%. In press.
C3. A Complete Characterization of Projectivity for Statistical Relational Models. Manfred Jaeger and Oliver Schulte (2020). Proceedings IJCAI. AR: 12%. In Press.
C4. Yan, J. N, Schulte, O., Zhang, M., Wang, J., & Cheng, R. "SCODED: Statistical Constraint Oriented Data Error Detection." Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data, pp. pp. 845-860. AR: 27%
C5. Deep Generative Probabilistic Graph Neural Networks for Scene Graph Generation. Khademi M and Schulte O. (2020). Proceedings AAAI, pp. 11237-11245. AR 20.6%.
C6. Dynamic Gated Graph Neural Networks for Scene Graph Generation. Mahmoud Khademi and Oliver Schulte (2019). *Asian Conference on Computer Vision,* LNCS 11366, pp. 1–17.

Abbreviated C.V. – Oliver Schulte

C7. Toward Interpretable Deep Reinforcement Learning with Linear Model U-Trees (2018). Guiliang Liu, Oliver Schulte, Wang Zhu and Qingcan Li. *Proceedings European Conference on Machine Learning, ECML* pp. 414-429.
C8. G. Liu and O. Schulte (2018). Deep Reinforcement Learning in Ice Hockey for Context-Aware Action Values and Player Evaluation. Proceedings IJCAI, pp.3442-3448.
C9. O. Schulte and S. Gholami (2017). Locally Consistent Bayesian Network Scores for Multi-Relational Data. Proceedings IJCAI, pp.2693-2700.
C10. O. Schulte, Z. Zhao, M. Javan, and P. Desaulniers (2017). Apples-to-Apples: Clustering and Ranking NHL Players Using Location Information and Scoring Impact. MIT Sloan Sports Analytics Conference, Boston, MA, USA.
C11. F. Riahi and O. Schulte (2016). Propositionalization for Unsupervised Outlier Detection in Multi-Relational Data. FLAIRS-29. Proceedings International Florida Artificial Intelligence Research Society Conference, Key Largo, FL, USA, pp.448-453.
C12. F. Riahi and O. Schulte (2015). Model-Based Outlier Detection for Object-Relational Data. IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, pp.1590-1598. *Best Student Paper Award.*
C13. Z. Qian and O. Schulte (2015). FactorBase: Multi-relational model learning with SQL all the way. *Proceedings Data Science and Advanced Analytics (DSAA)*, pp. 1--10.
C14. K. Routley and O. Schulte (2015). A Markov Game Model for Valuing Player Actions in Ice Hockey. Proceedings Uncertainty in Artificial Intelligence (UAI 2015), pp.782-791.

Journal Papers

J1. Riahi, F. & Schulte, O. (2020), 'Model-based exception mining for object-relational data', *Data Mining and Knowedge. Discovery* **34**(3), 681--722.
J2. Schulte, O. & Qian, Z. (2018), 'FACTORBASE: multi-relational structure learning with SQL all the way', *International Journal of Data Science and Analytics* **7(4)**, 1--21.
J3. Schulte, O. (2018), 'Causal Learning with Occam's Razor', *Studia Logica* **107(5)**, 991--1023.
J4. O. Schulte, M. Khademi, S. Gholami, Z. Zhao, M. Javan, and P. Desaulniers, "A Markov Game Model for Valuing Actions, Locations, and Team Performance in Ice Hockey," Data Mining and Knowledge Discovery, vol.31, no.6, pp.1-23, 2017.
J5. D. Beaudoin, O. Schulte, and T.B. Swartz, "Biased Penalty Calls in the National Hockey League," Statistical Analysis and Data Mining: The ASA Data Science Journal, vol.9, no.5, pp.365-372, 2016.
J6. Schulte, O.; Qian, Z.; Kirkpatrick, A. E.; Yin, X. & Sun, Y. (2016), 'Fast learning of relational dependency networks', *Machine Learning*, 1--30.

Supervision (last 6 years, including active students)

- 6 M.Sc., 3 Ph.D. Students
- Kurt Routley received an award for the *best Canadian AI Master's Thesis* of 2015 from the Canadian Artificial Intelligence Association for his work on hockey analytics.

Service

- Co-organizer, Vancouver Hockey Analytics Conference, 2016 and 2018.
- Coordinator, Organizing Committee, Workshop on New Perspectives in Relational Learning. Banff International Research Station. 42 participants. May 2015.

Uwe Glässer

School of Computing Science, Simon Fraser University, BC, Canada

Employment History

- Professor, School of Computing Science, 2009/9–current
- Dean *pro tem* of the Faculty of Applied Sciences, 2015/7–2016/12
- Associate Dean for Graduate Studies, Research and Industrial Liaison, Faculty of Applied Sciences, 2015/3–2015/6
- Acting Dean of the Faculty of Applied Sciences, 2014/10–2015/2
- Associate Dean for Graduate Studies, Research and Industrial Liaison, Faculty of Applied Sciences, 2013/11–2014/9
- Director, School of Computing Science, SFU, 2006/1–2009/4

Professional Training in Industry

- Microsoft Research, Foundations of Software Engineering Group, Redmond, WA, USA, 2000/10–2001/10
- Telecommunication Standardization on behalf of the International Telecommunication Union, ITU-T Study Group 10, Geneva, Switzerland, 1998/10–2001/2

Educational Background

- Habilitation (postdoctoral qualification), Computer Science, Paderborn University, Germany, 1999
  Thesis title: *Analysis and Validation of Formal Requirement Specifications in Model-Based Engineering of Concurrent Systems*
- Doctorate (Dr. rer. nat.), Computer Science, Paderborn University, 1992 (***summa cum laude***)
  Thesis title: *A Distributed Implementation of Flat Concurrent Prolog on Message-Passing Multiprocessor Systems*
- M.Sc. (Diploma), Computer Science, Paderborn University, 1987
  Thesis title: *Graph algorithms for structural testability analysis of VLSI circuit designs (in German)*

Awards

- 2015 Faculty of Applied Sciences Excellence Award for Service, May 2015

Patents

- U.S. Patent: *High level executable network abstract machine*
  Publication no. US 7149678 B2, Date: Dec. 12, 2006, Co-inventors: Y. Gurevich, M. Veanes, Uwe Glässer
  Microsoft Corp., Redmond, WA, USA

Teaching and Curriculum Development

- Cybersecurity, undergraduate and graduate courses, 2017–2020
- Software Engineering Foundations, undergraduate and graduate courses, 2002–2015
- Software Project Management Methodologies, undergraduate and graduate courses, 2002–2015

Research Interests

- Cyber security analytics, Cyber situational awareness, Cyber risk management
- Maritime Intelligence and Security, Behavioral analytics
- Crime data and criminal network analysis
- Time series analysis and forecasting
- Formal semantic foundations

Research Laboratories

Principle investigator and founder of the Software Technology Lab (STL) in Computing Science and the Public Safety & Security High Performance Computing Lab (sHPC), a highly secure computing cluster and data storage integrated with SFU Cedar and jointly funded by the Canada Foundation for Innovation, the British Columbia Knowledge Development Fund and Simon Fraser University

Scientific Publications

Cybersecurity

- Mohammad A. Tayebi, Uwe Glässer, and David B. Skillicorn, Editors. Open Source Intelligence and Cyber Crime - Social Media Analytics. *Lecture Notes in Social Networks*, Springer, 2020.
- Zahra Zohrevand and Uwe Glässer. Dynamic Attack Scoring using Distributed Local Detectors. In Proceedings of the *45th International Conference on Acoustics, Speech, and Signal Processing*, 2892-2896, Barcelona, IEEE Signal Processing Society, 2020.
- Zahra Zohrevand, Uwe Glässer, Mohammad A. Tayebi, Hamed Yaghoubi Shahir, Mehdi Shirmaleki, and Amir Yaghoubi Shahir. Deep Learning Based Forecasting of Critical Infrastructure Data. In Proceedings of the *2017 ACM Conference on Information and Knowledge Management*, pages 1129–1138, Singapore, November (2017).

Maritime Security

- Saeed Arasteh, Mohammad A. Tayebi, Zahra Zohrevand, Uwe Gässer, Amir Yaghoubi Shahir, Parvaneh Saeedi, and Hans Wehn. Fishing Vessels Activity Detection from Longitudinal AIS Data. In Proceedings of *ACM SIGSPATIAL'20, International Conference on Advances in Geographic Information Systems*, Seattle, WA, USA (2020).
- Amir Yaghoubi Shahir, Mohammad A. Tayebi, Uwe Glässer, Tilemachos Charalampous, Zahra Zohrevand, and Hans Wehn. Mining Vessel Trajectories for Illegal Fishing Detection. *2019 IEEE International Conference on Big Data*, Los Angeles, CA, USA, 1917–1927 (2019).
- Hamed Yaghoubi Shahir, Uwe Glässer, Amir Yaghoubi Shahir, and Hans Wehn. Maritime Situation Analysis Framework: Vessel Interaction Classification and Anomaly Detection. In Proceedings of the *2015 IEEE International Conference on Big Data*, Santa Clara, CA, IEEE, pages 1279–1289 (2015).

Predictive Policing

- Mohammad A. Tayebi and Uwe Glässer. Social Network Analysis in Predictive Policing: Concepts, Models and Methods. Lecture Notes In Social Networks, Springer, October, 2016.
  DOI https://doi.org/10.1007/978-3-319-41492-8 **(11,000$^+$ copies sold.)**
- Mohammad A. Tayebi, Uwe Glässer, Martin Ester, and Patricia L. Brantingham. Personalized Crime Location Prediction. *European J. of Applied Mathematics*, The Mathematics of Crime and Security, vol. 27, 422–450, Cambridge University Press (2016).
- Mohammad A. Tayebi, Martin Ester, Uwe Glässer, and Patricia L. Brantingham. Spatially Embedded Co-offence Prediction Using Supervised Learning. In Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 1789–1798, NYC, USA, ACM (2014).

CoreASM Toolset

- Roozbeh Farahbod, Vincenzo Gervasi, Uwe Glässer. Executable formal specifications of complex distributed systems with CoreASM. *Science of Computer Programming*, Elsevier, 79(1):23–38 (2014).

Mohammad Ali Tayebi

CONTACT INFORMATION

Software Technology Lab,
School of Computing Science,
Simon Fraser University,
8888 University Drive, Burnaby,
BC, Canada, V5A 1S6

tayebi@cs.sfu.ca
+1 - 778 862 4664

WORK EXPERIENCE

- **University Research Associate**, School of Computing Science, Simon Fraser University, 2019 - Present
- **Postdoctoral Research Fellow**, School of Computing Science, Simon Fraser University, 2016 - 2019
- **Software Engineer and Algorithm Designer**, Sepanta R&D Foundation, Tehran, Iran, 2005 - 2007

EDUCATION

Simon Fraser University, Burnaby, British Columbia, Canada
Ph.D. Computing Science, 2008 - 2015
- Thesis Title: "Predictive Models for Public Safety Using Social Network Analysis"

Amirkabir University of Technology, Tehran, Iran
M.Sc. Computer Science, 2005 - 2008
- Thesis Title: "Knowledge Extraction from Social Media Using Link Analysis"

University of Tabriz, Tabriz, Iran
B.Sc. Computer Science, 2000 - 2005

PUBLICATIONS

Peer-reviewed Books and Book Chapters

- **Mohammad A. Tayebi**, Uwe Glässer, David B. Skillicorn, Editors. Open Source Intelligence and Cyber Crime - Social Media Analytics. Lecture Notes in Social Networks (LNSN), Springer, 2020 (in print).
- **M. A. Tayebi** and U. Glässer. Social Network Analysis in Predictive Policing – Concepts, Models and Methods. Lecture Notes in Social Networks (LNSN), Springer, 2016.
- P. L. Brantingham, M. Easter, R. Frank, U. Glässer, and **M. A. Tayebi**. Co-offending Network Mining. in *U. Kock Wiil (ed.), Counterterrorism and Open Source Intelligence*, Lecture Notes in Social Networks, Vol. 2, Springer, pp. 73–102, 2011.
- U. Glässer, **M. A. Taybei**, P. L. Brantingham, and P. J. Brantingham. Estimating Possible Criminal Organizations from Co-offending Data, *Public Safety Canada*, Ottawa, Canada, 2012. (Resulted in invited keynote of *Organized Crime Summit* in Vancouver, November 2012)

Peer-reviewed Journal and Conference Publications

- Amir Yaghoubi Shahir, **Mohammad A. Tayebi**, Uwe Glässer, Tilemachos Charalampous, Zahra Zohrevand, and Hans Wehn, Mining Vessel Trajectories for Illegal Fishing Detection. In *Proceedings of the 2019 IEEE International Conference on Big Data (BigData'19)*, Los Angeles, USA, 2019.
- Z. Zohrevand, U. Glässer, **M. A. Tayebi**, H. Y. Shahir, M. Shirmaleki and A. Y. Shahir. Deep Learning Based Forecasting of Critical Infrastructure Data. In *Proceedings of the*

26th Conference on Information and Knowledge Management (CIKM'17), pp. 1129–1138, Singapore, 2017.

- **M. A. Tayebi**, U. Glässer, P. L. Brantingham, and H. Y. Shahir. SINAS: Suspect Investigation Using Offenders' Activity Space. In *Proceedings of European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD'17)*, pp. 253–265, Skopje, Macedonia, 2017.
- Z. Zohrevand, U. Glässer, H. Y. Shahir, **M. A. Tayebi**, and R. Costanz. Hidden Markov Based Anomaly Detection for Water Supply Systems. In *Proceedings of the 2016 IEEE International Conference on Big Data (BigData'16)*, pp. 1551-1560, Washington D.C., USA, 2016.
- **M. A. Tayebi**, U. Glässer, M. Ester, and P. L. Brantingham. Personalized crime location prediction. *European Journal of Applied Mathematics*, vol. 27, pp. 422–450, Cambridge University Press, 2016.
- **M. A. Tayebi**, M. Ester, U. Glässer and P. L. Brantingham. Spatially Embedded Co-offence Prediction Using Supervised Learning. In *Proceedings of 20th Knowledge Discovery and Data Mining (KDD'14)*, pp. 1789–1798, New York City, USA, 2014.
- **M. A. Tayebi**, R. Frank and U. Glässer. Understanding the Link Between Social and Spatial Distance in the Crime World. In *Proceedings of ACM SIGSPATIAL Conference on Advanced in Geographic Information Systems (SIGSPATIAL'12)*, pp. 550–553, Redondo Beach, USA, 2012.
- **M. A. Tayebi**, M. Jamali, M. Ester, U. Glässer, and R. Frank. CrimeWalker: A Recommendation Model for Suspect Investigation. In *Proceedings of ACM Conference on Recommender Systems (RECSYS'11)*, pp. 173-180, Chicago, USA, 2011.
- **M. A. Tayebi**, L. Bakker, U. Glässer and V. Dabbaghian. Locating Central Actors in Co-offending Networks. In *Proceedings of Conference on Advances in Social Network Analysis and Mining (ASONAM'11)*, Kaohsiung, Taiwan, pp. 171–179, 2011.
- **M. A. Tayebi**, S. M. Hashemi and A. Mohades, B2Rank: An Algorithm for Ranking Blogs Based on Behavioral Features. In *Proceedings of International Conference on Web Intelligence*, pp. 104-107, Silicon Valley, USA, 2007.

Academic Experience

Service

- Program Co-chair, International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI), 2016 (San Francisco), 2017 (Sydney), 2018 (Barcelona), 2019 (Vancouver), 2020 (The Hague)
- Sudent Volunteer Co-Chair, ACM Conference on Recommender Systems, Vancouver, 2018

Reviewer for Journals

- Social Network Analysis and Mining (SNAM), Journal of Information Science, IEEE Intelligent Systems, International Journal of Information Technology and Decision Making (IJITDM), Knowledge and Information Systems (KAIS)

Instructor

- Security Testing and Evaluation, Simon Fraser University, Canada, Fall Semesrter, 2019
- Database Systems II , Simon Fraser University, Canada, Summer Semesrter, 2018
- Introduction to Data Mining, Ontario Provincial Police, Canada, 2017
- Programming principles, Tabriz Azad University, Iran, 2005

Khaled Diab, PhD
University Research Associate
School of Computing Science
Simon Fraser University

Email : kdiab@sfu.ca
http://www.sfu.ca/~kdiab

Education

- **Simon Fraser University** — Burnaby, BC
  PhD in Computer Science — *Jan. 2014 – Aug. 2019*
- **Cairo University** — Cairo, Egypt
  BSc in Computer Engineering — *Sep. 2006 – May 2011*

Research Interests

- Multimedia networking; Computer network programmability; Datacenter networking; Cloud computing

Research Experience

- **Simon Fraser University** — Burnaby, BC
  University Research Associate — *Sep. 2019 – Present*
  - **Research**: Affiliated with the network systems lab, my research spans multiple areas such as multicast forwarding and routing, network service chaining, multimedia streaming and cloud gaming.
  - **Teaching**: I develop and teach system-related courses such as advanced computer networking and network and system security.
  - **Service**: I co-designed the cybersecurity stream for the school professional master program.
- **Simon Fraser University** — Burnaby, BC
  Research Assistant — *Jan. 2014 – Aug. 2019*

  My research focused on developing algorithms and testbeds for building traffic-engineered multimedia distribution systems. Specifically, I worked on designing efficient algorithms to stream multiview videos, building new CDN architectures and developing new multicast forwarding systems.
- **Qatar Computing Research Institute** — Doha, Qatar
  Research Assistant — *Feb. 2012 – Oct. 2013*

  I worked in the Distributed Systems lab to address problems such as dynamic sharing of GPUs in cloud systems, real-time 3D video retargeting and 3D video streaming system. I also contributed to the development of a large-scale infrastructure for executing NLP workloads.

Industry Experience

- **Mentor Graphics** — Cairo, Egypt
  Software Development Engineer — *Aug. 2011 – Jan. 2012*

  Building an IDE for hardware engineers and developers.
- **Cairo Microsoft Innovation Center** — Cairo, Egypt
  Research Intern — *Summer 2010*

  I developed a frontend for the lab's morphological analyzer engine. I also implemented some backend features for the morphological analysis engine.

Publications

- **K. Diab**, C. Lee and M. Hefeeda *Oktopus: Service Chaining for Multicast Traffic* (Under submission)
- **K. Diab** and M. Hefeeda *Efficient Multicast Forwarding* (Under submission)
- M. Hegazy, **K. Diab**, M. Saeedi, B. Ivanovic, I. Amer, Y. Liu, G. Sines and M. Hefeeda *Content-aware Video Encoding for Cloud Gaming*. In Proc. of ACM MMSys'19. [Best Student Paper Award]
- **K. Diab** and M. Hefeeda *Joint Content Distribution and Traffic Engineering of Adaptive Videos in Telco-CDNs*. In Proc. of IEEE INFOCOM'19,
- **K. Diab** and M. Hefeeda *MASH: A Rate Adaptation Algorithm for Multiview Video Streaming over HTTP*. In Proc. of IEEE INFOCOM'17.

- K. Calagari, T. Elgamal, **K. Diab**, K. Templin, P. Didyk, W. Matusik and M. Hefeeda *Depth Personalization and Streaming of Stereoscopic Sports Videos*. In ACM Trans. Multimedia Comput. Commun. Appl. 12, 3, Article 41 (March 2016).
- K. Calagari, K. Templin, T. Elgamal, **K. Diab**, P. Didyk, W. Matusik and M. Hefeeda. *Anahita: A System for 3D Video Streaming with Depth Customization*. In Proc. of ACM MM'14.
- **K. Diab**, T. Elgamal, K. Calagari and M. Hefeeda. *Storage optimization for 3D streaming systems*. In Proc. of ACM MMSys'14.
- **K. Diab**, M. M. Rafique and M. Hefeeda. *Dynamic sharing of GPUs in cloud systems*. In Proc. of IPDPS Workshops and PhD Forum (IPDPSW'13).

Patents

- MM. Rafique, M. Hefeeda and **K. Diab**, *Graphics processing unit controller, host system, and methods*, 2018, United States US9875139B2.

Graduate Students Supervised (last one year)

(Note: serving on their supervisory committees)

- Carlos Lee, MSc (Expected: August 2020)
- Parham Yassini, MSc (Expected August 2021)

Mentoring Experience (last five years)

- Trevor Gale, Undergraduate (May 2019 – August 2019)
- Qiao Chen, Undergraduate (August 2016 – January 2017)

Teaching Experience

Instructor

Fall 2020: Computer Networking II

Spring 2020: Systems and Network Security

Fall 2019: Multimedia Systems

Professional Service

Program Committee

2020: IEEE INFOCOM

External Reviewer

Journals: ACM TOMM, IEEE/ACM ToN, IEEE TMM, IEEE TCSVT

2020: ACM Multimedia

2019: ACM Multimedia, ACM Multimedia Systems, ACM Multimedia Asia

2017: ACM Multimedia, ACM NOSSDAV

2015: ACM Multimedia, ACM Multimedia Systems

Thesis Committee

2020: Carlos Lee (Supervisor), Amgad Ahmed (Chair)

Recognitions and Awards

- Best Student Paper Award for *Content-aware Video Encoding for Cloud Gaming*, ACM MMSys 2019.
- ACM Student Research Competition Travel Award, ACM SIGCOMM 2017
- Travel scholarship, the ACM 50th Celebration of the Turing Award, ACM SIGMM 2017
- Computing Science Graduate Fellowship, Simon Fraser University, Spring 2017
- Graduate Fellowship, Simon Fraser University, Fall 2017

Dr. W. Nick Sumner

Associate Professor
School of Computing Science
Simon Fraser University

Cell: 1-778-873-8021
E-mail: wsumner@sfu.ca
Homepage: http://www.cs.sfu.ca/~wsumner

Education

2013	Ph.D.	Computer Science	Purdue University, IN, USA
2005	B.Sc. B.A.	Computer Science German	Hope College, MI, USA

Research Interests

I am interested in using program analysis and machine learning to automate and assist developers in producing secure, efficient, and correct software systems. This specifically includes:

- Using testing and program transformation to harden software systems against attack
- Automated techniques to assist in debugging and understanding real world systems

Recent Publications

24 total refereed conference publications.
Google Scholar page including estimated citations, etc.: http://bit.ly/2jkHUsM.
Publications below are from the last 7 years.
Names of authors who were students at the time of publication have been underlined.

Recent Articles in Refereed Conference Proceedings

1. Golnaz Gharachorlu and **Nick Sumner**.
   Pardis: Priority Aware Test Case Reduction. FASE 2019.
   Acceptance Rate: 32%
2. Golnaz Gharachorlu and **Nick Sumner**.
   Avoiding the Familiar to Speed Up Test Case Reduction. QRS 2018.
   Acceptance Rate: 19%
3. Naveen Vedula, Arrvindh Shriraman, Snehasish Kumar, and **Nick Sumner**.
   NACHOS: Software-Driven Hardware-Assisted Memory Disambiguation for Accelerators. HPCA 2018.
   Acceptance Rate: 21%
4. Snehasish Kumar, **Nick Sumner**, Vijayalakshmi Srinivasan, Steven Margerm, and Arrvindh Shriraman.
   NEEDLE: Leveraging Program Analysis to Analyze and Extract Accelerators from Whole Programs. HPCA 2017.
   Acceptance Rate: 22%
5. Snehasish Kumar, **Nick Sumner**, and Arrvindh Shriraman.
   SPEC-AX and PARSEC-AX: Extracting Accelerator Benchmarks from Microprocessor Benchmarks. IISWC 2016.
   Acceptance Rate: 30%
6. Snehasish Kumar, Vijayalakshmi Srinivasan, Amirali Sharifian, **Nick Sumner**, and Arrvindh Shriraman.
   Peruse and Profit: Estimating the Accelerability of Loops. ICS 2016.
   Acceptance Rate: 24%
7. Yonghwi Kwon, Dohyeong Kim, **Nick Sumner**, Kyungtae Kim, Brendan Saltaformaggio, Xiangyu Zhang, and Dongyan Xu.
   LDX: Causality Inference by Lightweight Dual Execution. ASPLOS 2016.
   Acceptance Rate: 22%
8. Robert D. Cameron, Nigel Medforth, Dan Lin, Dale Denis, **Nick Sumner**.
   Bitwise Data Parallelism with LLVM: The ICgrep Case Study. ICA3P 2015.
   Acceptance Rate: 36%
9. Dohyeong Kim, Yonghwi Kwon, **Nick Sumner**, Xiangyu Zhang, and Dongyan Xu.
   Dual Execution for On the Fly Fine Grained Execution Comparison. ASPLOS 2015.
   Acceptance Rate: 17%
10. Dohyeong Kim, **Nick Sumner**, Xiangyu Zhang, Dongyan Xu, and Hira Agrawal
    Reuse-Oriented Reverse Engineering of Functional Components from x86 Binaries. ICSE 2014.
    Acceptance Rate: 20%

11. **Nick Sumner** and Xiangyu Zhang.
Identifying Execution Points For Dynamic Analyses. ASE 2013.
Acceptance Rate: 23%
12. Zhongshu Gu, **Nick Sumner**, Zhui Deng, Xiangyu Zhang and Dongyan Xu.
DRIP: A Framework for Purifying Trojaned Kernel Drivers. DSN 2013.
Acceptance Rate: 22%
13. **Nick Sumner** and Xiangyu Zhang.
Comparative Causality: Explaining the Differences Between Executions. ICSE 2013.
Acceptance Rate: 19%

Research Funding

Amounts are cash contributions in CAD. NSERC is the National Science and Engineering Council of Canada.

1. NSERC Discovery Grant
Role: Principal Investigator
Project Title: Automated explanations for debugging
Total Funding: $150,000 **Awarded:** 2014
Annual Funding: $25,000 **Duration:** 2014-2020 (5+1 years)
2. NSERC Discovery Grant
Role: Principal Investigator
Project Title: Learning rich input structure for software debugging and defence
Total Funding: $120,000 **Awarded:** 2020
Annual Funding: $24,000 **Duration:** 2020-2025 (5 years)
3. Mitacs Accelerate
Role: Joint Investigator
Project Title: High Performance Regular Expression Matching Using Parallel Bit Stream Technology
Total Funding: $15,000 **Awarded:** 2013
Annual Funding: $15,000 **Duration:** 2013-2014
4. Mitacs Accelerate
Role: Joint Investigator
Project Title: Chain Certs: Development of a platform for organizational authenticity certificates creation
Total Funding: $15,000 **Awarded:** 2019
Annual Funding: $15,000 **Duration:** 2019

Student Supervision

Student Progress

PhD		MSc		Total	
Active	Graduated	Active	Graduated	Active	Graduated
2	1†	0	4	2	5

† One substantially co-supervised PhD student.

PhD Students

Active (Start Date, Name, Thesis Topic)

1. 2017. Shadi Romani. Program understanding for smart contracts.
2. 2015. Golnaz Gharachorlu. Machine learning for compiler correctness.

Graduated (Graduation Date, Name, Thesis Topic, Position)

1. 2017. Snehasish Kumar†. Program analysis for hardware specialization. Google.

MSc Students

Graduated (End Date, Name, Thesis Topic, Position)

1. 2019. Shreeasish Kumar. Automated hardening of interactive security systems. Amazon.
2. 2019. Himahansi Fernando. Mining approaches to fault localization.
3. 2017. Ali Arab. Evaluating modern mutation analysis approaches for C programs. PhD SFU.
4. 2016. Mehrnoosh Ebrahimipour. Pruning undefined behavior from mutation analysis. Apple.

Ouldooz Baghban Karimi

Email: ouldooz@sfu.ca Cell: 604.345.8442 Web: https://www.cs.sfu.ca/~oba2

Education

PhD Computing Science, Simon Fraser University (SFU), Burnaby, BC, Canada, ***A+ CGPA*** (2013)
Thesis: Efficient Resource Utilization in Advanced Wireless Networks, **Advisor:** Jiangchuan Liu

MSc Computer Engineering, Iran University of Science and Technology, Tehran, Iran, ***A+ CGPA*** (2006)
Thesis: Adaptive End-to-End QoS for Multimedia over Heterogeneous Wireless Networks
Advisor: Mahmood Fathy

BSc Computer Engineering, University of Tehran, Tehran, Iran (2003)

Certifications
PMP Project Management Professional, Project Management Institute (PMI) (2016)
ISW Instructional Workshop (2020)

Experience

Simon Fraser University (Surrey, BC, Canada)

Lecturer, School of Computing Science (March 2019 – Now)
Chair, Computing Science Diversity Committee (June 2019 – Now)
President, Academic Women (June 2021 – Now)
Co-Director, Invent the Future (AI4ALL SFU) (April 2019 – August 2020)

Ciena (Remote - Vancouver, BC, Canada)

Lead Systems Engineer (SE 3), CSNE & SE&I, Solution Integration (Feb 2017 – March 2019)

- Led on a cross-functional team from engineering, PLM, solution architecture, and CTO office for successful delivery of service virtualization proof of concept for Vectors 2018 (NFV, orchestration, IoT, machine learning at the edge, edge & cloud computing, and SD-WAN) **Customer feedback: 4.76 out of 5 (22 International Telcos)**
- Designed, developed, and presented technical Proof of Concept and solution introductions to North American, South American, Asian, and European telcos and channel partners (virtualized edge, distributed NFV, orchestration, wireless, routing, firewall, and SD-WAN)
- Designed and delivered performance analysis of third-party and commercial off-the-shelf solutions
- Designed and delivered internal engineering trainings, TOIs, workshop, and lab modules **Workshop attendee feedback: 4.62 out of 5**

Software Engineer (SE 2), Packet R&D (August 2015 – Feb 2017)

Cyan (Currently BluePlanet, acquired by Ciena - Vancouver, BC, Canada)

Software Engineer (Dec 2013 – August 2015)

- Designed and implemented data model (MOF) and resource manager (Python) for Z-series products software features (MPLS-TP, EMS)

Tellabs (Richmond, BC, Canada)

Intern, R&D (Oct 2012 – Feb 2013)
Designed and built a Smart Debugger PoC for network log and real-time data analysis and diagnosis of routing and forwarding modules of 9200 series routers

Started **Novel Design** (Tehran, Iran, 2004-2008), and **WiFier Network** (Vancouver, BC, Canada, Oct 2012- Nov 2013).

Selected Publications

JOURNAL ARTICLES:

[J1] **Lightweight User Grouping with Flexible Degrees of Freedom in Virtual MIMO**
Ouldooz Baghban Karimi, Milad Amir Toutounchian, Jiangchuan Liu, Chonggang Wang, *IEEE Journal on Selected Areas in Communications (**IEEE JSAC**)*, Vol. 31, Issue 10, pp. 2004-2012, Oct 2013

[J2] **Seamless Wireless Connectivity for Multimedia Services in High Speed Trains**
Ouldooz Baghban Karimi, Jiangchuan Liu, Chonggang Wang, *IEEE Journal on Selected Areas in Communications* (***IEEE JSAC***), Vol. 30, No. 4, May 2012

[J3] **Multicast with cooperative gateways in multi-channel wireless mesh networks**
Ouldooz Baghban Karimi, Jiangchuan Liu, Zongpeng Li, *Elsevier Ad-Hoc Networks*, October 2011

[J4] **Adaptive end-to-end QoS for multimedia over heterogeneous wireless networks**
Ouldooz Baghban Karimi, Mahmood Fathy, *Elsevier Journal of Computers and Electrical Engineering* Vol. 36, Issue. 1, pp. 45-55, 2010

CONFERENCE ARTICLES:

[C5] **Power-Efficient Resource Utilization in Cellular Multimedia Multicast,** Ouldooz Baghban Karimi, Jiangchuan Liu, Zhi Wang, IEEE International Conference on Mobile Ad-Hoc & Sensor Networks (IEEE MSN), China, 2015

[C6] **Optimal Collaborative Access Point Association in Wireless Networks**, Ouldooz Baghban Karimi, Jiangchuan Liu, Jennifer Rexford, International Conference on Computer Communications ***(IEEE INFOCOM)***,Toronto, Canada, April 2014

[C7] **Power Efficient High-Quality Multimedia Multicast in LTE Wireless Networks**, Ouldooz Baghban Karimi, Jiangchuan Liu, IEEE International Conference on Mobile Adhoc and Sensor Systems ***(IEEE MASS),*** Spain, 2011

[C8] **The Trajectory Exposure Problem in Location-Aware Mobile Networking**, Li Ma, Jiangchuan Liu, Limin Sun, Ouldooz Baghban Karimi, IEEE International Conference on Mobile Adhoc and Sensor Systems ***(IEEE MASS),*** Spain, 2011

[C9] **Multicast in Multi-Channel Wireless Mesh Networks**, Ouldooz Baghban Karimi, Jiangchuan Liu, Zongpeng Li, ***IFIP networking*** 2010 proceedings, Chennai, India, 2010

[C10] **Availability Measurement in Peer to Peer Network Management Systems**, Ouldooz Baghban Karimi, Saleh Yousefi, Mahmood Fathy, Mojtaba Mazoochi, IEEE International Conference on Digital Information Management, London, UK, 2008

[C11] **Availability in Management P2P Networks**, Ouldooz Baghban Karimi, Saleh Yousefi, Mahmood Fathy LNCS proceedings of Asia-Pacific Network Operations and Management, China, 2008

[C12] **Adaptive End-to-End QoS for Multimedia over Heterogeneous Wireless Networks**, Ouldooz Baghban Karimi, Mahmood Fathy, Computer Society of Iran Computer Conference, Iran, 2008

[C13] **Application Level Wireless Multi-level ECN for Video and Real-time Data**, Ouldooz Baghban Karimi, Mahmood Fathy, Saleh Yousefi, IEEE International Conference on Networking, Mauritius, 2006

[C14] **Improvements on Active Resource Management for Differentiated Services Domain,** Ouldooz Baghban Karimi, Shahram Jamali, Mahmood Fathy, Morteza Analouie, IST2005 proceedings, Iran, 2005

[C15] **Dynamic Resource Management in Differentiated Services Domain**, Shahram Jamali, Ouldooz Baghban Karimi, Morteza Analouie, Mahmood Fathy, Computer Society of Iran Computer Conference proceeding, Iran, 2006 (In Persian)

SHORT ARTICLES & POSTERS:

[P16] Project-based Learning of Web Systems Architecture, C. Kerslake, O. Baghban Karimi, ITiCSE 2021

[P17] Power Efficient Scalable Video Multicast in LTE Wireless Networks, GHC, 2011

[P18] Seamless Wireless Connectivity in High-Speed Vehicles, GHC 2011

[P19] Multimedia Transmission in Wireless Networks, ACM CRA-W Grad Cohort, Boston, 2011

Igor Shinkar

CURRENT POSITION: *Assistant Professor* at *Simon Fraser University*
HOMEPAGE: https://www.cs.sfu.ca/~ishinkar/
EMAIL: ishinkar@sfu.ca

EDUCATION

2016 - 2018 Postdoctoral Scholar
Department of Electrical Engineering and Computer Sciences at UC Berkeley

2014 - 2016 Post-Doctoral Associate
Courant Institute of Mathematical Sciences, New York University

2010 - 2014 Ph.D. in Mathematics and Computer Science
Weizmann Institute of Science, Faculty of Mathematics and Computer Science
Advisor: *Prof. Irit Dinur*
Thesis: *On Local-to-Global Phenomena in Large Combinatorial Objects*

2007 - 2009 M.Sc. in Mathematics and Computer Science
Weizmann Institute of Science, Faculty of Mathematics and Computer Science
Advisor: *Prof. Irit Dinur*
Thesis: *Intersecting Families and Independent Sets in Graphs*

2001 - 2005 B.Sc. in Mathematics
Tel-Aviv University, Faculty of Exact Sciences, School of Mathematics

PUBLICATIONS

Refereed Conference Publications

[C17] **On Local Testability in the Non-Signaling Setting**
Alessandro Chiesa, Peter Manohar, Igor Shinkar
The 11th Innovations in Theoretical Computer Science Conference (ITCS 2020).

[C16] **Relaxed Locally Correctable Codes with Nearly-Linear Block Length and Constant Query Complexity**
Alessandro Chiesa, Tom Gur, Igor Shinkar
ACM-SIAM Symposium on Discrete Algorithms (SODA 2020).

[C15] **String Matching: Communication, Circuits, and Learning**
Alexander Golovnev, Mika Göös, Daniel Reichman, Igor Shinkar
International Conference on Randomization and Computation (RANDOM 2019).

[C14] **Probabilistic Checking against Non-Signaling Strategies from Linearity Testing**
Alessandro Chiesa, Peter Manohar, Igor Shinkar
The 10th Innovations in Theoretical Computer Science Conference (ITCS 2019).

[C13] **Sorting Networks On Restricted Topologies**
Indranil Banerjee, Dana Richards, Igor Shinkar
45th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2019).

[C12] **Testing Linearity against Non-Signaling Strategies**
Alessandro Chiesa, Peter Manohar, Igor Shinkar
Conference on Computational Complexity (CCC 2018).

[C11] **A Graph-Theoretic Approach to Multitasking**
Noga Alon, Daniel Reichman, Igor Shinkar, Tal Wagner, Jonathan D. Cohen, Biswadip Dey
Thomas L. Griffiths, Sebastian Musslick, Kayhan Özcimder
Neural Information Processing Systems 30 (NIPS 2017) - *oral presentation*.

[C10] **On Axis-Parallel Tests for Tensor Product Codes**
Alessandro Chiesa, Peter Manohar, Igor Shinkar
The 21st International Workshop on Randomization and Computation (RANDOM 2017).

[C9] **An $\tilde{O}(n)$ Queries Adaptive Tester for Unateness**
Subhash Khot, Igor Shinkar
The 20th International Workshop on Randomization and Computation (RANDOM 2016).

[C8] **On Percolation and NP-hardness**
Huck Bennett, Daniel Reichman, Igor Shinkar
The 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016).

[C7] **On Hardness of Approximating the Parameterized Clique Problem**
Subhash Khot, Igor Shinkar
The 7th Innovations in Theoretical Computer Science (ITCS 2016).

[C6] **The Complexity of DNF of Parities**
Gil Cohen, Igor Shinkar
The 7th Innovations in Theoretical Computer Science (ITCS 2016).

[C5] **Zero-Fixing Extractors for Sub-Logarithmic Entropy**
Gil Cohen, Igor Shinkar
The 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015).

[C4] **Direct Sum Testing**
Roee David, Irit Dinur, Elazar Goldenberg, Guy Kindler, Igor Shinkar
The 6th Innovations in Theoretical Computer Science (ITCS 2015).

[C3] **A Bi-Lipschitz Bijection between the Boolean Cube and the Hamming Ball**
Itai Benjamini, Gil Cohen, Igor Shinkar
The 55th Annual Symposium on Foundations of Computer Science (FOCS 2014).

[C2] **Two-Sided Error Proximity Oblivious Testing**
Oded Goldreich, Igor Shinkar
The 16th International Workshop on Randomization and Computation (RANDOM 2012).

[C1] **On the Conditional Hardness of Coloring a 4-Colorable Graph with Super-Constant Number of Colors**
Irit Dinur and Igor Shinkar
The 13th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX 2010).

Journal Publications

[J13] **Multitasking Capacity: Hardness Results and Improved Constructions**
Noga Alon, Jonathan D. Cohen, Thomas L. Griffiths, Pasin Manurangsi, Daniel Reichman
Igor Shinkar, Tal Wagner, Alexander Yu
SIAM Journal on Discrete Mathematics, 34(1), 885–903, 2020.

[J12] **An Entropy Lower Bound for Non-Malleable Extractors**
Tom Gur, Igor Shinkar
IEEE Transactions on Information Theory, 66(5), 2904–2911, 2019.

[J11] **On Percolation and NP-hardness**
Huck Bennett, Daniel Reichman, Igor Shinkar
Accepted to Random Structures & Algorithms, 2017.

[J10] **On Lipschitz Bijections between Boolean Functions**
Shravas Rao, Igor Shinkar
Accepted to Combinatorics, Probability and Computing, 2016.

[J9] **Direct Sum Testing**
Roee David, Irit Dinur, Elazar Goldenberg, Guy Kindler, Igor Shinkar
Accepted to SIAM Journal on Computing (SICOMP), 2016.

[J8] **A Counterexample to Monotonicity of Relative Mass in Random Walks**
Oded Regev, Igor Shinkar
Electronic Communications in Probability, 21 (2016), paper no. 8.

[J7] **A Tight Upper Bound on Acquaintance Time of Graphs**
Omer Angel, Igor Shinkar
Graphs and Combinatorics, 32(5), 1667–1673, 2016.

[J6] **A Bi-Lipschitz Bijection between the Boolean Cube and the Hamming Ball**
Itai Benjamini, Gil Cohen, Igor Shinkar
Israel Journal of Mathematics, 212(2), 677—703, 2016.

[J5] **Two-Sided Error Proximity Oblivious Testing**
Oded Goldreich, Igor Shinkar
Random Structures & Algorithms, 48(2), 341–383, 2016.

[J4] **Excited Random Walk with Periodic Cookies**
Gady Kozma, Tal Orenshtein, Igor Shinkar
Annales de l'Institut Henri Poincaré, 52(3), 1023–1049, 2016.

[J3] **On the Acquaintance Time of a Graph**
Itai Benjamini, Igor Shinkar, Gilad Tsur
SIAM Journal on Discrete Mathematics, 28(2), 767–785, 2014.

[J2] **A Note on Subspace Evasive Sets**
Avraham Ben-Aroya, Igor Shinkar
Chicago Journal of Theoretical Computer Science, 2014, Article 9, 1–11, 2014.

[J1] **Greedy Random Walk**
Tal Orenshtein, Igor Shinkar
Combinatorics, Probability and Computing, 23(2), 269–289, 2014.

Manuscripts

[P3] **Meyniel Extremal Families of Abelian Cayley Graphs**
Fatemeh Hasiri, Igor Shinkar
Available at arXiv:1909.03027, 2019.

[P2] **On Mappings on the Hypercube with Small Average Stretch**
Lucas Boczkowski, Igor Shinkar
Available at arXiv:1905.11350, 2019.

[P1] **On Coloring Random Subgraphs of a Fixed Graph**
Igor Shinkar
Available at arXiv::1612.04319, 2018.

*The list of publications has conference/journal overlaps.

TEACHING

SPRING 2020 **CMPT 706 - Design and Analysis of Algorithms for Big Data**
Simon Fraser University

SPRING 2020 **Probabilistically Checkable Proofs - informal course**
Simon Fraser University

FALL 2019 **CMPT 125 - Introduction to Computing Science and Programming II**
FALL 2020 *Simon Fraser University*

SPRING 2019 **CMPT 409/CMPT 815 - Approximation and Randomized Algorithms**
FALL 2019 *Simon Fraser University*

FALL 2017 **Instructor** in **Coding Theory**
UC Berkeley (co-teaching with Tom Gur)

SPRING 2017 **Instructor** in **Probabilistically Checkable and Interactive Proof Systems**
UC Berkeley (co-teaching with Alessandro Chiesa)

FALL 2016 **Instructor** in **Property Testing**
UC Berkeley (co-teaching with Alessandro Chiesa)

FALL 2015 **Instructor** in **Data Structures**
SPRING 2016 *Courant Institute of Mathematical Science, New York University*

FUNDING

2019 NSERC DISCOVERY GRANT: 140,000 CAD FOR 5 YEARS
2019 NSERC EARLY CAREER RESEARCH GRANTS SUPPLEMENT: 12,500 CAD

ORGANIZING ACTIVITIES

SPRING 2019 - CURRENT **CS Theory Seminar** at *Simon Fraser University*

SPRING 2019 - CURRENT **CS Student Theory Seminar** at *Simon Fraser University*

2014 - 2016 **CS Theory Seminar** at *Courant Institute of Mathematical Science, NYU*

RECREATIONAL ACTIVITY

FALL 2019 - SPRING 2020 **Weekly math club for children in 4th-5th grades**
at *Leigh Elementary School, Port Coquitlam, BC, Canada*

FALL 2014 - FALL 2016 **Mentoring talented high school graduates.**
Projects included:
- Artificial Intelligence algorithms
- Image Compression algorithms

Curriculum Vitae

Dr Andrei Bulatov / Professor / Computing Science

Educational Background

1995 Ph.D. Mathematics, Institute of Mathematics and Mechanics, Ural Branch, Russia

1991 M.Sc. Mathematics, Ural State University, Russia

Employment History at Academic Institutions

09.2012 - Current	Professor, Computer Science, SFU
09.2008 – 08.2012	Associate Professor, Computer Science, SFU
08.2004 – 08.2008	Assistant Professor, Computer Science, SFU
08.2002 – 08.2004	Research Officer, Computer Science, Computing Laboratory, The University of Oxford
09.1997 – 07.2002	Associate Professor, Mathematics and Computer Science, Ural State University, Ekaterinburg, Russia
09.1993 – 08.1997	Assistant Professor, Mathematics, Ural State University

Current Research Interests

- Constraint Satisfaction problems. Algorithms, structure, and complexity issues for finite constraint satisfaction problems, counting problems, and related combinatorial problems

- Graph homomorphisms and isomorphisms. Properties, algorithms and theory of homomorphisms of graphs and other relational structures

- Clone Theory and Universal Algebra. Clones of operations and relations, algebraic and combinatorial properties of clone lattices, structure of finite algebras, etc.

Selected Recent Publications

I published more than 50 journal papers and about 50 papers in conference proceedings. These include

- (with A. Dadsetan): Counting homomorphisms in plain exponential time. ICALP 2020, to appear.

- (with M. Backens, L.A. Goldberg, C. McQuillan, S. Zivny): Boolean approximate counting CSPs with weak conservativity, and implications for ferromagnetic two-spin. Journal of Computing Science and Systems, 109: 95-125 (2020)

- Constraint satisfaction problems over semilattice block Mal'tsev algebras. Information and Computation, 268 (2019)

- A short story of the CSP dichotomy conjecture. LICS, 2019

- (with P. Mayr, Á. Szendrei): The Subpower Membership Problem for Finite Algebras with Cube Terms. Logical Methods in Computer Science 15(1) (2019)

- Constraint satisfaction problems: complexity and algorithms. SIGLOG News 5(4): 4-24 (2018)

- (with R. Briceño, V. Dalmau, and B. Larose):
Dismantlability, Connectedness, and Mixing in Relational Structures. ICALP 2019: 29:1-29:15
- A Dichotomy Theorem for Nonuniform CSPs. FOCS 2017, 319-330 (Best Paper Award)

- Constraint satisfaction problems over semilattice block Mal'tsev algebras, LICS 2017, p.1-11

- (with M. Kozik, P. Mayr, M. Steindl): The subpower membership problem for semigroups. IJAC 26(7): 1435-1452 (2016)

- Graphs of relational structures: restricted colours. In Proceedings of LICS 2016.

- Conservative constraint satisfaction re-revisited. J. of Comp. and System Sci., 82(2), 2016, 347-356

- Counting Constraint Satisfaction Problems. In the Proceedings of the International Congress of Mathematicians, Seoul, Korea, August 13-21, 2014, vol 4, p. 321-342

- (with D.Marx) Constraint Satisfaction Parameterized by Solution Size. SIAM J. Comput. 43(2): 573-616 (2014)
- The complexity of the counting constraint satisfaction problem. J. ACM 60(5): 34 (2013)
- (with M.E. Dyer, L.A.Goldberg, M.Jerrum, C.McQuillan) The expressibility of functions on the boolean domain, with applications to counting CSPs. J. ACM 60(5): 32 (2013)
- (with D.Marx) Constraint satisfaction parameterized by solution size, In ICALP 2011
- (with D.Marx): Constraint satisfaction problems and global cardinality constraints. Commun. ACM 53(9): 99-106 (2010)
- (with D. Marx) The complexity of global cardinality constraints. LICS 2009, p.343-352

Recent Grants

2020-2025	NSERC Discovery grant, $320K
2015-2020	NSERC Discovery grant, $215K

Graduate Students

I have supervised 6 PhD students and 12 MSc students

Awards, Honors and Scholarships

2017	Best Paper award:	48th Annual IEEE Symposium on Foundations on Computer Science (FOCS 2017)
2013	Best Paper award:	43rd Annual International Symposium on Multiple-Valued Logic (ISMVL 2013)
2004	Best Paper award:	Algorithmic Learning Theory, 15th International Conference (ALT 2004)
2002	Best Paper award:	43rd Annual IEEE Symposium on Foundations on Computer Science (FOCS 2002)

Appendix 6 Budget for the proposed program (financial and personnel)

Program Cost

A. Instructional costs

Most faculty members teaching courses for Cybersecurity will also teach courses for other programs so the cost has been included proportionally.

Course instructors are generally supported by Teaching Assistants.

B. Staffing

The new program, together with other master programs, will be supported by dedicated administrative staff and the Program Director. Cost for administration will be shared between programs.

C. Equipment and lab

IT support and technical equipment is also shared with the other master programs.

The school will also require a new lab to run the Cybersecurity Professional Computer Science program. The new lab will be shared between the other master programs (Professional Master in Big Data, MSc in Visual Computing, MSc in Cybersecurity) that the School aims to offer concurrently, so 1/3 of the set-up cost of the lab has been included in this budget.

D. Other expenses

Expenses for recruitment, marketing and retention have been included in the budget.

Proposed tuition and other program fees including a justification

The tuition fee structure is based on a per term (not per unit) fee of $9,000 (CAD) per term for domestic students and $12,500 (CAD) for international students. Please note that the same per-term fee applies to the industrial internship term as well. We expect most students to graduate in four terms, but, in cases where additional terms are required for program completion, a continuing fee is assessed for each additional term. The continuing fee is half the normal tuition per term.

Total tuition cost for domestic students (4 terms): $36,000 (CAD)

Total tuition cost for international students for (4 terms): $50,000 (CAD)

	TOTAL	Term 1	Term 2	Term 3	Annual fee (3 terms)
Domestic	$36,000	$9,000	$9,000	$9,000	$27,000
International	$50,000	$12,500	$12,500	$12,500	$37,500

1. **Revenue**

The Revenue is based on 3 terms (annual revenue), for enrolment numbers (see enrolment plan)

Enrollment revenue	**Year 1**	**Year 2**	**Year 3**
Domestic	$472,500.00	$659,137.50	$672,320.25
International	$656,250.00	$924,309.29	$964,643,75
TOTAL	**$1,128,750.00**	**$1,583,446.79**	**$1,636.964.00**

2. **Overall budget**

	Year 1	Year 2	Year 3
Program Expenses	$ 614,830.00	$ 626,300.00	$ 553,488.00
Program Revenue	$ 1,128,750.00	$ 1,583,446.79	$ 1,636,964.00
Net Income	$513,920.00	$1,042,196.79	$1,202,120.75