serene risc

SERENE-RISC Fall 2015 Workshop
October 28 & 29, 2015 | Canadian Museum of Nature
240 McLeod Street | Ottawa (Ontario)

Wednesday, October 28th	
8:00 – 9:00	**Registration and continental breakfast** – Barrick Salon
9:00 – 10:00	**Opening session keynote** – Barrick Salon • *Securing the Internet of Things* Mika Ståhlberg, *F-Secure*
10:00 – 10:30	**Networking break** – Barrick Salon
10:30 – 12:00	**Session 1 – Alternative Training Approaches: Cybersecurity Challenges and CTF Competitions** – Barrick Salon • *CTF in the enterprise: keys to a healthy relationship* Alexis Dorais-Joncas, *ESET* • *The Benefits of Cyber Security Simulation for Workforce Preparedness* Michael Garvin, *Symantec* • *Cyber Security Challenges for IT-Security Workforce Enhancement* Tom Levasseur, HackingAway.org & *CGI*
12:00 - 13:30	**Networking lunch & Knowledge mobilization discussion group** – Barrick Boardroom
13:30 - 15:30	**Session 2 – Data Breaches and Consumer Cybersecurity** – Barrick Salon • *Real-life breach dissected, exploring all sides of the story* Pascal Fortin, *GoSecure* • *A Measure of Transparency: Evaluating PIPEDA's New Data Breach Notification Requirements* Dr. Teresa Scassa, *University of Ottawa* • *Data Breach Response and Reporting: Best Practices for the Handling of Privacy Incidents* Joel Scott-Mignon, Office of the Privacy Commissioner
15:30 - 16:00	**Networking break** – Barrick Salon
16:00 – 17:30	**Session 3 – Critical Infrastructure Protection** – Barrick Salon • *"Innovation in ICS CyberSecurity" – Leading from the front on threat to Critical Cyber Infrastructure* Joe Cummins, *Red Tiger Labs* • *Cybersecurity: Gaps, Research Challenges, and Solutions* Dr. Ali Ghorbani, *University of New Brunswick*
17:30 – 19:00	**Networking Reception** – Rotunda
Thursday, October 29th	
8:00 – 9:00	**Registration and continental breakfast** – Barrick Salon
9:00 – 10:30	**Session 4 – Critical Infrastructure Protection** – Barrick Salon (registered participants only) • *Lessons from the Strategic Corporal - Implications for Cyber Incident Responders* Dr. Tiago de Jesus, Infrastructure Resilience Research Group (IRRG) • *CCIRC – Cyber Threats and ICS Vulnerabilities* François Turbide, *Canadian Cyber Incident Response Centre (CCIRC)*
10:30 – 11:00	**Networking break** – Barrick Salon
11:00 – 12:30	**Session 5 – The Next Generation of Cybercrime and Regulatory Strategies** – Barrick Salon • Second Generation Online Illicit Markets: The Role Of Canadians And The State Of Hacking Services Dr. David Décary-Hétu, *Université de Montréal* • Internet Intermediaries: Private Arbiters of Legality Dr. Natasha Tusikov, *Brock University*
12:30 - 14:00	**Networking Lunch** – Barrick Salon

@SERENE_RISC #SRcybersec

Opening presentation

Moderator: Benoît Dupont, SERENE-RISC, Université de Montréal

Mika Ståhlberg

Securing the Internet of Things

Internet of Things is coming. It may not be coming at the speed that you'd think if you just listen to the early adopters – but it's coming. The efficiency benefits for businesses are on a level that will make those unwilling or unable to implement IoT in their processes uncompetitive. Also, for consumers IoT brings tangible time-saving convenience to their daily lives. This means that eventually everyone will use some level of IoT even if they don't recognize it as such.

It's estimated that in just a few years a home may have even hundreds of connected devices. The volumes are completely different from the IT-era of devices. At the same time these devices have a direct link to your family's physical security as well as privacy: They are e.g. controlling your locks, controlling your car, as well as are recording audio and video of what's happening inside your home. Embracing the efficiency benefits IoT brings mean these devices will rapidly become critical to the operations of businesses and also to the infrastructure they are responsible for. As a result, IoT security and privacy are going to be important for consumers, businesses, and for critical infrastructure alike.

There's a lot of discussion and standardization work ongoing on the topic of protecting IoT. We also need to think about how to protect ourselves from IoT. Furthermore, it's important to have an active discussion on the threats as e.g. TLS encryption of in-transit data isn't a silver bullet that solves all issues. This talk presents insight on the current and future IoT threat landscape and the protection measures needed.

About the speaker

Mika Ståhlberg is the Director for Strategic Threat Research at F-Secure. Mika handles a diverse range of tasks that involve identifying emerging online threats, and uses his strong background in network security and malware protection to research and create strategies, technologies and products that help protect from these threats.

Session 1

Alternative Training Approaches: Cybersecurity Challenges and CTF Competitions

Moderator: Luc Dancause, Sapiens Conseils

Alexis Dorais-Joncas

CTF in the enterprise: keys to a healthy relationship

Capture the Flag (CTF) competitions have been a part of ESET's Montreal Research & Development office life since its inception in 2011. Over the years, ESET structured and integrated CTFs in its regular hiring campaigns and as an optional continuous training benefit for their employees.

In this presentation, Mr. Dorais-Joncas will share how they do it and how exactly their CTF policy benefits both ESET and their employees. The presenter will also share a few unexpected side effects from this great ongoing experience and the lessons learned along the way.

About the speaker

Hired by ESET in 2010, Alexis Dorais-Joncas worked as a Malware Researcher, then as Security Intelligence Team Lead. In 2015, Alexis Dorais-Joncas was appointed head of ESET's R&D branch office located in Montreal. He and his team focus on cutting edge malware research, network security and targeted attacks tracking in order to shed light on the latest trends and developments in the malware ecosystem and implement efficient countermeasures to allow ESET customers to be safer online. Alexis's team is also present at various international events to share ESET's latest research with the infosec community.

Michael Garvin

The Benefits of Cyber Security Simulation for Workforce Preparedness

Businesses and governments globally face a critical shortage of cyber security professionals, with recent estimates as much as 1 - 1.5 million by 2020, leaving us fighting an asymmetric battle with attackers. The increasing pace and scale of breaches calls out the need for continuous, hands-on preparation, a new model for skills assessment and development for professionals both entering and already in the workforce. For four years Symantec has been leveraging and delivering cyber security simulations such as the CyberWar Games - the gamification of skills assessment and development through the use of immersive, hands-on infrastructure and situations using realistic virtualized systems, networks and applications for attack, defense, incident response and more. In this talk we will share the background, execution, outcomes and futures of these efforts.

About the speaker

Michael Garvin is a Director, Security Simulation at Symantec corporation. Starting with Symantec in 2006 he is currently in the Cyber Security Services business unit. His responsibilities include live-fire cyber security skills assessment, development and practice through cyber exercises and ranges, Symantec's CyberWar Games, and product management for Symantec's Security Simulation offerings. Michael has over 20 years experience in information security and compliance, IT architecture and management, and systems administration, and is a CISSP, CISM and CGEIT.

Tom Levasseur

Cyber Security Challenges for IT-Security Workforce Enhancement

Canada needs more IT-security experts. This is well recognized by employers, public bodies and, unfortunately, the many Canadian victims of cyber crime. Many nation-wide initiatives are underway in other countries, but Canada's Cyber Security Strategy (2010) and the Action Plan to implement that strategy (2013) have no provisions to address the shortfall of qualified IT-security experts.

Cyber Security Challenges have proven to be an effective way of attracting new people - smart, energetic, motivated candidates – into the IT-security industry. Several types of cyber security challenges are flourishing in the US, though they are expensive to launch and operate. But practical, easy-to-launch and sustainable models that Canada could emulate have been running in Australia and the UK since 2011.

An effort was made in 2012 for Canada to keep up with our peers in this area, but it fell through due to lack of support. With government backing, private sector groups will be willing to join in a partnership. Is it time for us to catch-up? Can Canada show true leadership in this important area? A champion is needed.

About the speaker

Mr. Tom Levasseur has over 20 years' experience in IT and IT Security, from system and network admin, to Global R&D IT-Security Chief at Canada's largest high-tech company. This combination of deep technical skills and senior-level management experience gives him a unique perspective on today's cyber-threat landscape. Tom is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and holds Top Secret (Level III) security clearance from the Canadian Industrial Security Directorate (CISD). He received an MBA from McGill University, and a B.B.Admin, Information Systems, from Université Laval, Quebec City.

By day, Tom is a Vulnerability Analyst and Penetration Tester for a huge Canadian IT consulting firm. By night, he's fighting the forces of IT evil at HackingAway.org, running cyber security competitions, simulations, and training events for students, consultants, auditors and managers.

Thank you to our Gold Sponsor

InnovationWorks
Colliding ideas…sparking action

Session 2 — Data Breaches and Consumer Cybersecurity

Moderator: John Clare, Industry Canada

Pascal Fortin

Real-life breach dissected, exploring all sides of the story

There are many highly publicized major cyber security breaches available to study, but does the information available tell the whole story? We delve into a multi-billion dollar corporation's nightmare, and explore the many interesting but typically untold stories that unfold at the same time inside and outside of the corporation.

About the speaker

Pascal Fortin, MBA, CISA, CRISC, CRMA is the CEO of GoSecure Inc, a leading Canadian cyber security services provider. Throughout his 11 year tenure at GoSecure, he has been directly involved with several dozen major cyber security investigations in Canada and abroad. He holds undergraduate degrees in Computer Science and Finance from UQAM and an MBA from University of Sherbrooke.

Dr. Teresa Scassa

A Measure of Transparency: Evaluating PIPEDA's New Data Breach Notification Requirements

Media reports of corporate data security breaches suggest that such breaches are growing in number and that consumer personal information is sometimes put in significant jeopardy. In Canada, a sharp rise in the number of class action law suits for data security breaches reflects growing concern over failures to adequately protect personal information and the potentially serious consequences for those affected by a breach. The *Digital Privacy Act* of 2015 will introduce into Canada's private sector data protection legislation a data breach reporting requirement. Once regulations are in place and the Bill becomes law, organizations will be required to report breaches of data security safeguards to the Privacy Commissioner of Canada "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." This presentation will critically examine the new legislative provisions and will consider what they will contribute towards addressing the problem of data security breaches, where they may fall short, and what remains to be done.

About the speaker

Dr. Teresa Scassa is the Canada Research Chair in Information Law at the University of Ottawa, where she is also a professor at the Faculty of Law. She is the author of the book Canadian Trademark Law (2d edition, LexisNexis 2015), and co-author of Electronic Commerce and Internet Law in Canada, (CCH Canadian Ltd. 2012) (winner of the 2013 Walter Owen Book Prize), Law Beyond Borders: Extraterritorial Jurisdiction in an Age of Globalization (Irwin Law, 2014), and Canadian Intellectual Property Law: Cases, Notes and Materials (Emond Montgomery, 2013). She is co-editor of Intellectual Property for the 21st Century: Interdisciplinary Approaches (Irwin Law 2014). She is a past member of the External Advisory Committee of the Office of the Privacy Commissioner of Canada, and currently sits on the Canadian Government Advisory Committee on Open Government. She has written widely in the areas of intellectual property law, law and technology, and privacy.

Joel Scott-Mignon

Data Breach Response and Reporting: Best Practices for the Handling of Privacy Incidents

About the speaker

Joel Scott-Mignon is a Senior Privacy Investigator/Breach Response Officer with the Office of the Privacy Commissioner of Canada ("OPC"). Prior to joining the OPC's PIPEDA Investigations Branch, Joel obtained extensive experience with respect to privacy-related matters within the OPC working with both the Communications Branch and the Access to Information and Privacy Directorate. Joel has also gained federal public sector experience working on issues related to copyright and to cultural affairs within the Department of Canadian Heritage and to audit and evaluation during his time with the Department of Aboriginal Affairs and Northern Development Canada. Prior to joining the public service, Joel studied at the University of Ottawa, where he earned his Honours Bachelor of Arts degree with Specialization in Music as a result of his interest and experience with respect to the study, performance and tutelage of music.

Session 3

Critical Infrastructure Protection

Moderator: Paul Beesley, Ontario Provincial Police

Joe Cummins

"*Innovation in ICS CyberSecurity*" – Leading from the front on threat to Critical Cyber Infrastructure

SCADA Control System Operators and their Asset Owners face ever-growing challenges of discovering and managing vulnerabilities found within their current embedded controller networks. Existing risk assessment tools fall short of the needs to these environments, while the attacks against these systems is rapidly becoming commonplace.

Leveraging recent advances in the use of discreet electronic platforms and specifically crafted scripts, control systems can be effectively mapped, audited, and analyzed to determined efficacy of existing security controls and identification of weakness or vulnerabilities in existing architectures.

This presentation will guide the audience through past histories of toolkits and tradecraft used in the performance of Critical Infrastructure Protection assessments, trends and taboo's related to the current methodologies used to evaluate security measures, and the latest generation of technologies that are being leveraged to provide protection to the ICS ecosystem.

About the speaker

Joe Cummins has been active in the Information Security and Infrastructure Protection communities for over eight years. As a recognized leader in Cyber-Security and Industrial Automation Control Systems (IACS) Security, he has built a career on innovating the core processes and technologies that enable safe, secure and resilient networks of our modern society.

As the Founder and Principal Consultant for Red Tiger Labs, Joe performs Risk Management activities, Cyber Incident Response and Forensics, as well as leading innovation and development within Industrial Control Systems security across the globe. He has been a contributor to the development of services and products that effectively raise the standard of Cyber-Security within essential systems.

Drawing from his background in both Public and Private security sectors, jumpstarted by his service in the Canadian Forces, he now directs a number of Security and Intelligence projects designed to maintain the Cyber-Security of core Canadian infrastructure sectors.

Dr. Ali Ghorbani

Cybersecurity: Gaps, Research Challenges, and Solutions

The Information Security Centre of Excellence (http://www.iscx.ca) at the University of New Brunswick, Canada, is a broad based centre having both an education and research mandate. It provides interdisciplinary industry-sponsored and/or government funded R&D work within the area of cybersecurity, and is home to the Canadian Chapter of the Honeynet project and a number of large R&D projects with industry. The Centre also provides training opportunities for visiting scientists and students in an exciting, dynamic and challenging environment. We employ diverse research disciplines such as artificial intelligence, machine learning, data mining, and multi-agent systems to develop novel algorithms and techniques for information and network security.

Our current areas of R&D interests include, but not limited to, *intrusion detection and prevention, botnet detection and mitigation, malware analysis, mobile security, security big data analytics, security analysis and risk management, security visualization, and critical infrastructure protection*. This talk takes a look at some of the major research challenges and our contributions to these topics. At the end, I will provide an overview of our advanced threat intelligence platform utilizing security big data analytics and our malware analysis and botnet infiltration system.

About the speaker

Dr. Ghorbani has held a variety of positions in academia for the past 34 years, and is currently the Dean of the Faculty of Computer Science and the Founding Director of the Information Security Centre of Excellence (ISCX) at the University of New Brunswick. His current research focus is Network & Information Security, Complex Adaptive Systems, Critical Infrastructure Protection, and Web Intelligence.

Dr. Ghorbani is the co-inventor on 3 awarded patents in the area of Network Security and Web Intelligence and has published approximately 200 peer-reviewed articles during his career. His book, Intrusion Detection and Prevention Systems: Concepts and Techniques, was published by Springer in October 2010. Dr. Ghorbani has been a world leader in working with the research community to build benchmark datasets for testing and evaluating network security solutions. The most used dataset is called 'ISCX 2012 Intrusion Detection Evaluation Dataset' and has been used by more than 600 researchers and companies.

Session 4

Critical Infrastructure Protection

Moderator: Michele Mosca, Institute for Quantum Computing, University of Waterloo

Dr. Tiago de Jesus

Lessons from the *Strategic Corporal* - Implications for Cyber Incident Responders

With the rise of the Advanced Persistent Threat (APT) actors, which are often state-sponsored hackers dedicated to electronic espionage, the role of cyber incident responders has dramatically increased in complexity. It is no longer possible to adopt a simple strategy of cleaning up an infection and moving on. However, the skills profile of incident handlers has not changed since the glory days of the Internet worms. Today, the strategic position of companies is being put at risk by operational personnel, which often have little to no awareness of the strategic implications of their technical decisions. How do we make sure that incident handlers make the right decisions in this new environment? In recent decades, the military has gone through similar change and has dubbed this new reality the "strategic corporal". While initially designed for a warfighting role, the military has been increasingly relied upon for operations other than war, such as peacekeeping, disaster relief and nation building. In response to these new operational requirements they have adapted their skill sets to reflect the new challenges they face. In this talk we will present the solutions put forward by the military and how they can be applied to cyber incident responders.

About the speaker

Mr. de Jesus completed an undergraduate degree in mathematics and physics at l'Université de Montréal before going to the University of British Columbia to obtain a Masters in theoretical physics. He later went to McGill University, where he received a PhD in nano-electronics. After his doctorate, he went to Bay Street to work in the financial sector before co-founding two high-tech start-up companies. He later came to Ottawa to pursue a career in National Security. He joined the RCMP's National Security program where he worked as a Senior Intelligence Researcher. There he became the program's subject matter expert in cyber threats to Canada's critical infrastructures before leading the newly formed national security cyber unit. During this time he worked on national security criminal investigations. He was also responsible for setting up and managing science and technology projects, including Canada's first research project in SCADA security.Today, he is a Senior Advisor and the Deputy Project Manager at NRCan's National Energy Infrastructure Test Center (NEITC), where he is responsible for developing and delivering hands-on cyber security training exercises to security professionals from the Energy and Utilities Sector, among other responsibilities.

François Turbide

CCIRC – Cyber Threats and ICS Vulnerabilities

About the speaker

Mr. Turbide has over twenty-five years' experience in the information technology field. He has spent the last eighteen years involved in all aspects of information technology security, first as an operational responsibility, in teaching, consulting and since 2010 as a technical analyst at the Canadian Cyber Incident Response Centre (CCIRC) where he is responsible for the industrial control systems portfolio.

Session 5 Moderator: Christian Leuprecht, Royal Military College of Canada

David Décary-Hétu

Second Generation Online Illicit Markets: The Role Of Canadians And The State Of Hacking Services

First generation online illicit markets were launched in the 1990s and 2000s and were hosted on online discussion forums, newsgroups and Internet Relay Chat (IRC) chatrooms. They offered mainly stolen financial information and hacking services. Over the past five years, second generation online illicit markets – known as *cryptomarkets* – have appeared and provide their participants with a much higher level of operational security. This increased security is due to the use of anonymous connections using the Onion Router (Tor), anonymous payments through the use of virtual currencies like bitcoins and lower victimization rates through the use of escrow payments and automated feedback systems. Cryptomarkets are used to offer many illicit products but focus mainly on drugs and hacking services. The aim of this presentation will be to describe the current state of cryptomarkets, particularly those where Canadians are present as vendors. The market share of Canadian vendors will be analyzed as well as the type of products they offer. This presentation will also adopt a more global point of view to analyze the hacking services that are offered on cryptomarkets. These online platforms are more and more used to selling malware and Trojans and provide a better level of security for the participants that use them.

About the speaker

David Décary-Hétu is an Assistant Professor at the School of Criminology of the University of Montreal and a regular researcher at the International Centre For Comparative Criminology (ICCC). He has worked at the School of Criminal Sciences at the University of Lausanne, a leading institution in forensic science. His work focus on online illicit markets, more particularly on those that offer drugs, stolen financial information, hacking services and stolen intellectual property products such as books, movies and software. He currently has two funded projects that seek to better understand the impact of second generation online illicit markets on the illicit drug industry.

Natasha Tusikov

Internet Intermediaries: Private Arbiters of Legality

Internet intermediaries, such as Google and PayPal, play an increasingly important role in the regulation of a range of complex social problems, including child pornography and online sales of tobacco. Since 2010, these intermediaries have also become gatekeepers for prominent multinational rights holders of intellectual property like Nike and Nokia. In contrast to their previous efforts, however, intermediaries are working with rights holders through non-legally binding enforcement agreements. These efforts are global, rapid, and, because they do not involve court orders, are largely undertaken in secret. The paper argues that a small group of mostly U.S.-based Internet firms has, along with rights holders, constructed a global, extra-legal, private enforcement regime that is becoming a *de facto* standard globally. Research is based on over fifty interviews with Internet firms, rights holders, private security companies and government officials in the United States.

About the speaker

Natasha Tusikov is an assistant professor in the department of sociology at Brock University. She received her Ph.D. in sociology from the Regulatory Institutions Network at the Australian National University, an inter-disciplinary institute specializing in the study of regulation and governance. She has been a postdoctoral research fellow at the Baldy Centre for Law and Social Policy at the State University of New York in Buffalo. Her research examines the intersection among law, technology, and regulation, with a particular focus on regulation by Internet intermediaries. Prior to undertaking her dissertation, Natasha worked as a civilian researcher with the Royal Canadian Mounted Police in the areas of cybercrime, money laundering, fraud, and transnational organized crime.

serene risc

SERENE-RISC Fall 2015 Workshop
October 28 & 29, 2015 | Canadian Museum of Nature

Thanks to our SERENE-RISC Partners

CGI

DRDC | RDDC
technologyscience technologie

ESET ENJOY SAFER TECHNOLOGY™

ITAC
INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ACTI
ASSOCIATION CANADIENNE DE LA TECHNOLOGIE DE L'INFORMATION

NCE RCE

nurun services conseils

Public Safety Canada | Sécurité publique Canada

Symantec

TRTech

Université de Montréal

www.serene-risc.ca