Program

Presenters' Bios & Abstracts

SERENE-RISC Spring 2017 Workshop

April 26 & 27, 2017

Sofitel Montréal

serene • risc

Supported by:

Canada Research Chair in Cybersecurity

Wednesday, April 26th	
8:00 – 9:00	**Registration and continental breakfast** – Picasso
9:00 – 10:15	**Opening session keynote** – Picasso • *Anonymous and the Politics of Leaking* Gabriella Coleman, *McGill University*
10:15 – 10:45	**Networking break** – Foyer
10:45 – 12:15	**Session 1 – Infrastructure Security** – Picasso • *Understanding the Simplicity Behind IoT Botnets : A Case Study of a Social Media Fraud Provider* Masarah Paquet-Clouston, *GoSecure* • *Security and AI: A Bayesian Approach* Evgeny Naumov, *Delve Labs* • *Security in virtualized infrastructures: A networking perspective* Ashraf Matrawy, Carleton University
12:15 - 13:45	**Networking lunch** – Picasso
13:45 - 15:00	**Session 2 – Online Fraud Prevention (In Camera)** – Picasso • *Trends in Cyber Fraud* Christian Leuprecht, *Royal Military College of Canada* • *Cybercrime Knows No Borders* Dominic Arpin, *Global Affairs Canada* • *Panel discussion* Rita Estwick, *Canada Post* Lesley Ahara, *Royal Canadian Mounted Police* Jacques Boucher, *Reitmans* Pierre-Luc Pomerleau, *Banque Nationale* Denise Portugaise, *Canada Post*
15:00 - 15:30	**Networking break** – Foyer
15:30 – 17:00	**Session 3 – Bitcoins** – Picasso • *Bitcoin, the Gateway Virtual Currency?* Aaron Gilkes, *Royal Canadian Mounted Police* • *Cryptocurrencies in Canada: Legal status and public policy considerations* Gabriel Ngo, *Finance Canada* • *Assessing the Money Laundering and Terrorist Financing Risks of Emerging Payment Technologies* Evangeline Ducas, *Financial Transactions and Reports Analysis Centre of Canada (Fintrac)*
17:00 – 17:30	**Pre-Cocktail Presentation** – Picasso • Marie-Josée Hébert, *Université de Montréal* • Harout Chitilian, *Ville de Montréal* • Jean-Sébastien Pilon, *Desjardins*
17:30 – 19:00	**Networking Cocktail Reception** – Foyer
Thursday, April 27th	
8:00 – 9:00	**Registration and continental breakfast** – Picasso
9:00 – 10:15	**Session 4 – Big Data and Privacy** – Picasso • *Data and Criminology: Research from the UK* Matthew L. Williams, *Cardiff University* • *Security Analytics* Nicolas Christin, *Carnegie Melon University*
10:15 – 10:45	**Networking break** – Foyer
10:45 – 12:15	**Session 5 – The Next Generation of Cybercrime and Regulatory Strategies** – Picasso • *Tech & Privacy: Protecting against Unreasonable Search and Seizure in the Context of Cell Phone Searches* Anne-Marie McElroy, *Defence Lawyer* • *L'État de la cybercriminalité pour la Sûreté du Québec* Christian Dumas, *Sûreté du Québec* • *Collaboration in the fight against cybercrime* Marc-Étienne Léveillé, *ESET*
12:15 - 12:45	**Closing Remarks** – Picasso
12:45 - 14:30	**Networking Lunch** – Picasso

Opening presentation

Moderator: Jeremy Clark, SERENE-RISC - Concordia University

Gabriella Coleman

Anonymous and the Politics of Leaking

In this talk Dr. Gabriella Coleman will provide a history of Anonymous' crucial role in establishing a novel style of hacking-for-leaking: public disclosure hacks. In contrast to traditional whistle-blowing—instigated by insiders who possess intimate awareness of wrongdoing and access to documents that can prove it—a public disclosure hack is led by an outsider-hacker or group of them. Driven to seize documents by a suspicion of misconduct and endeavoring to secure incriminating evidence to establish it, these explorers gain unlawful entry to an organization's computer systems to gain, exfiltrate, and distribute documents. If the published contents spur reporting from journalistic or activist publics, its status may be said to switch from a dump to a public interest leak. Some of the questions to be addressed in the lecture are, What are the properties of the public disclosure hack? What separates it from the other varieties of hacks, leaks, and breaches and other classes of whistleblowing proliferating today? Why is this tactic propagating now, when many of the material components and ideological conditions had already been in place for this sort of covert operation to have cropped up earlier?

About the speaker

Gabriella (Biella) Coleman holds the Wolfe Chair in Scientific and Technological Literacy at McGill University. Trained as an anthropologist, her scholarship explores the intersection of the cultures of hacking and politics, with a focus on the sociopolitical implications of the free software movement and the digital protest ensemble Anonymous. She has authored two books, Coding Freedom: The Ethics and Aesthetics of Hacking (Princeton University Press, 2012) and Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous (Verso, 2014).

Session 1

Infrastructure Security
Moderator: David Décary-Hétu, SERENE-RISC – Université de Montréal

Masarah Paquet-Clouston

Understanding the Simplicity Behind IoT Botnets: A Case Study of a Social Media Fraud Provider

Last Fall, the Mirai large-scale attacks on several important websites, such as Twitter, Spotify and Reddit, made the headlines for several weeks. This was one of the first registered global attack made by a botnet running on IoT systems. Since then, IoT botnets and the potential threats they represent have been much discussed in the media. This presentation aims at presenting one specific IoT botnet that receives less media coverage due to its innocuous activity: social media fraud, yet represents the same type of menace. This IoT botnet is dubbed Linux/Moose and runs on embedded systems, such as routers and IP cameras. It uses the infected devices, mainly on Instagram, as proxies to conduct social media fraud, which is the process of creating fake likes and follows on targeted accounts. The presentation will explain how the botnet spreads and operates, but also how the illegal activities are monetized. It will demystify the public's perception of IoT botnets, explaining the simplicity behind the Linux/Moose technical scheme and illegal activities. Simple solutions to protect consumers against IoT botnets will be presented, along with the latest public initiatives.

About the speaker

Masarah is a security researcher at GoSecure, a consultancy firm specializing in cybersecurity services for the public and private sector. She is also a member of the council for the NorthSec conference. Using her economic and criminological backgrounds, she specializes on the study of market dynamics behind illegal online activities, such as ransomware or social media fraud. Her goal is to understand complex social problems emerging from technological innovation and help society overcome them. She has presented at various international conferences such as Black Hat Europe, Botconf, the International Society for the Study of Drug Policy and the American Society of Criminology. Besides doing scientific research, she's passionate about programming, defending online privacy and discussing politics.

Evgeny Naumov

Security and AI: A Bayesian Approach

The rapid rise in the number and ubiquity of internet services and internet-facing devices has increased pressure to automate cybersecurity monitoring. However, vulnerabilities discovered by automated solutions per scan can number in the thousands and beyond, still placing a considerable burden on security teams to confirm and address each manually. To overcome this problem, the ever-growing repertoire of machine learning methods can be brought to bear. However, the complexity of the data, the often modest number of training examples, and the requirement for customer anonymity make this a challenging task for existing machine learning techniques.

This talk describes the false positive problem outlined above, and gives an introductory overview of the principles and methods of machine learning that can be applied to solve it. In particular, it focuses on Bayesian methods and their specific applicability to challenging security data.

About the speaker

Evgeny Naumov graduated from the University of Waterloo with a degree in mathematical physics, and went on to pursue a Master's degree in computer science at McGill University with a focus on machine learning. He is particularly interested in the application of new machine learning technologies to challenging practical problems. He currently works at Delve Labs, a Montreal startup specializing in automated cybersecurity solutions.

Ashraf Matrawy

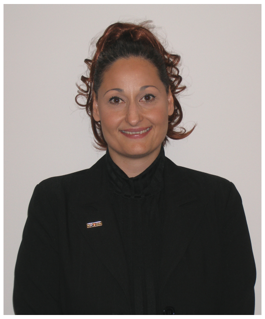
Security in virtualized infrastructures: A networking perspective

For economic, technical, and environmental reasons, there is a very strong trend towards virtualizing computing infrastructures and relying less on private computing infrastructures. This trend utilizes information infrastructures that are built using virtualization techniques while taking advantage of very rapid advances in networking technologies. In addition to the promise of cost reduction and higher resource utilization, this trend is expected to expedite the creation process of new computing services. This area is of tremendous importance to innovation in Canada. This talk explores the security of virtualized infrastructures from a computer networking perspective. The use of software to define and manage networks using SDN (Software Defined Networking) in these virtualized infrastructures is expected to have an impact on security. A brief overview of the state-of-the-art research in this area will be presented.

About the speaker

Dr. Ashraf Matrawy is an Associate Professor in the School of Information Technology at Carleton University. He leads the Next Generation Networks research group (http://ngn.sce.carleton.ca/). His main research interests are software defined networking, security of mobile networks, and security and privacy of the Internet of Things. He is a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and a licensed Professional Engineer in Ontario. Dr. Matrawy also served as a consultant in industry and for government departments.

Session 2 **Online Fraud Prevention**



Rita Estwick

About the session chair

In her capacity as Director, Enterprise Security Development at Canada Post, Rita is responsible for mitigating risks and creating positive customer experiences through collaborative partnerships, education and awareness and security thought leadership.

Throughout her career at Canada Post, Rita has established strategic partnerships with both the business and law enforcement communities where she has placed an important focus on information-sharing and preventative strategies to support risk and fraud reduction. Highly regarded for her ground-breaking efforts in the security community, Rita is a frequent speaker at educational conferences.

Rita has been recognized twice on the cover of Canadian Security Magazine and was recently awarded the inaugural Loss Prevention Lifetime Achievement Award from Retail Council of Canada.

Christian Leuprecht

Trends in Cyber Fraud

This presentation discusses trends in cyber fraud, the mounting challenges such fraud poses, and the difficulties of attribution, prosecution and recovery of funds.

About the speaker

Christian Leuprecht is Professor of Political Science at the Royal Military College of Canada and Senior Fellow at the Macdonald Laurier Institute. He holds a Governor-in-Council appointment to the governing Council of the Natural Sciences and Engineering Research Council of Canada, is president of the International Sociological Association's Research Committee 01: Armed Forces and Conflict Resolution, and a United Nations Security Structure Expert. He is cross-appointed to the Department of Political Studies and the School of Policy Studies at Queen's University where he is also a fellow of the Institute of Intergovernmental Relations and the Queen's Centre for International and Defence Policy. An expert on security and defence, political demography, and comparative federalism and multilevel governance, he is regularly called as an expert witness to testify before committees of Parliament.

Dominic Arpin

Cybercrime Knows No Border

Cybercrime knows no border and can only be addressed through effective international cooperation. Mr. Arpin will give a brief overview of Canada's and of the international community's efforts to increase this cooperation (in particular through the Council of Europe's "Budapest" Convention on Cybercrime), of the remaining challenges (mutual legal assistance procedures, issues of jurisdiction, trans-border access to data, extra-territoriality, encryption, etc.) as well as of Canada's international cyber capacity building programmes.

About the speaker

Dominic Arpin (LL.B., Université du Québec à Montréal, 1990; Quebec Bar, 1991; M.A. International Relations, Université Laval, Québec, 1997) worked as an international policy advisor for the Department of Canadian Heritage and for UNESCO, Paris, prior to joining the Department of Foreign Affairs and International Trade in 2001. In Ottawa, Mr. Arpin has worked in the Legal Bureau (Humanitarian Law), as well as with divisions covering conflict prevention, peace keeping and international security issues. Mr. Arpin first assignment abroad was at the Mission of Canada to the European Union, Brussels. He also served at the Joint Delegation of Canada to the North Atlantic Council (NATO), Brussels, as a senior political officer . Most recently, Mr. Arpin was the politico-military counsellor at the Canadian Delegation to the OSCE, Vienna, where he contributed, among other things, to the negotiation of a first international set of cyber confidence building measures. Since last fall, Mr. Arpin is the cybercrime coordinator in the International Crime and Terrorism Division, Global Affairs Canada.

Lesley Ahara

About the speaker

Inspector Lesley Ahara joined the Royal Canadian Mounted Police (RCMP) in July, 1996 and was posted to beautiful British Columbia (BC) in Coquitlam, a suburb outside of Vancouver. She spent eight years in BC performing general duties, school liaison and full-time mountain bike duties. In 2004, she was transferred to Ontario, where she transitioned from uniformed duties to plain clothes duties in federal policing as a Financial Crime investigator in the Greater Toronto Area (GTA).

In 2007, Insp. Ahara was promoted to the rank of Corporal in Financial Crime. In 2009, she joined the 2010 G8-G20 Joint Intelligence Group (JIG) Information Intelligence Management Team (IIMT). In 2011, Insp. Ahara was promoted to the rank of Sergeant in Milton, Ontario as the Non-Commissioned Officer in charge of Intelex, an Information and Intelligence exchange unit within the RCMP's Criminal Intelligence Branch.

In November 2014, she became a Commissioned Officer and achieved the rank of Inspector moving to the RCMP's National Headquarters in Ottawa, Ontario, to work alongside one of their Deputy Commissioners. In April 2016, Lesley moved on to Federal Policing where she is currently the Officer-in-Charge at the Federal Coordination Centre managing several Financial Crime portfolios including the Canadian Anti-Fraud Centre (CAFC).

Jacques Boucher

About the speaker

Currently Director of Loss Prevention for Reitmans Canada Ltd, responsible for inventory losses, investigations and security equipment in all stores belonging to the Reitmans group of companies, M. Boucher began his career has a police officer with the RCMP. He has served as Director of loss prevention and security for Provigo, as Manager, Loss Prevention and Security at Costco and, previously, at The Bay. He currently serves on the board of Échec au Crime Québec (Crime Stoppers) and as Director of the board of the RGSI (Regroupement des gestionnaires en sécurité Interne). In 2007, he was awarded the National assembly medal for service to the population.

Pierre-Luc Pomerleau

About the speaker

Pierre-Luc Pomerleau currently leads National Bank of Canada's Corporate Security and Fraud Risk Management division which includes Corporate security investigations, Physical Security as well as the Fraud Strategy & Data Analytics teams.

Pierre-Luc holds a Bachelor in Criminology from Université de Montréal and a MBA from the Université de Sherbrooke. He is currently pursuing a PhD in Business Administration with specialization in Homeland Security and Leadership Policy at Northcentral University. He also holds the CPP, PSP, PCI, CFE, CAMS, CCCI & CFCI certifications. Since 2015, he has been the President of the Montreal ACFE Chapter. In October 2016, Pierre-Luc was awarded an honorary diploma by Université de Montréal School of Criminology for his exemplary contribution to the advancement of society.

He has more than 12 years of experience leading teams within the Canadian Fraud & Risk Management landscape with a concentrated focus in Corporate Security, Internal Investigations, Payment card Fraud as well as Fraud Strategy.

Denise Portugaise

About the speaker

Denise Portugaise is a CPA who has had a vast career at Canada Post for over 28 years. She is currently the General Manager of Customer Relationship Support, a portfolio which includes all billing and invoicing, customer account management and collections, payment processing, international settlements, claims and cash management for all 6,500 postal outlets across the country. Denise previously led Canada Post's Anti-Money Laundering and Terrorist Financing detection team where she conducted forensic analysis of money order activity across the country and was responsible for the Corporation's Whistleblowing portfolio.

Today, she also co-chairs, along with the General Manager of the Corporation's Security and Investigation team, the Canada Post Fraud Prevention Steering Committee whose mandate is to raise awareness of fraud threats and risks for the company and mitigate these by supporting effective prevention and detection programs and action plans.

Denise is an avid golfer, who is married to her perfect golfing partner and they have two grown sons.

Session 3

Bitcoins
Moderator: Jeremy Clark, SERENE-RISC - Concordia University

Aaron Gilkes

Bitcoin, the Gateway Virtual Currency?

Is Bitcoin (BTC) a gateway virtual currency? Will using BTC lead to more sinister or otherwise naughty behaviour online? There seems to be four prevailing groups of BTC users : Technology enthusiasts, Libertarians, Speculators and Criminals. I will be focusing on Law Enforcement's experiences with BTC as well as the past, current and future perceived challenges of the movement towards fully digital commerce..

About the speaker

A former student of Concordia University, Aaron has worked in the financial sector as an insurance broker and financial planner before becoming a police officer with the Royal Canadian Mounted Police in 2011. He originally worked as a proceeds of crime investigator targeting multiple forms of money laundering including the infractions facilitated by virtual currencies. He now works as a cybercrimes investigator within the Montreal RCMP Integrated Technical Crimes Unit where He investigates both traditional cybercrimes and cyber facilitated crimes.

Gabriel Ngo

Cryptocurrencies in Canada: Legal status and public policy considerations

Bitcoin (BTC) has often been referred to as "nerd money". However, since the first BTC transaction in 2009, the decentralized cryptocurrency has become more popular and is becoming widely available with more users and merchants adopting the cryptocurrency every day. This presentation will provide a high-level taxonomy of cryptocurrencies and discuss BTC's inherent properties that make it appealing to both law-abiding citizens and bad actors. This presentation will also touch on BTC's status in the current legal environment and the broader public policy implications of BTC and its underlying technology.

About the speaker

Gabriel has over 15 years of combined experience in both the financial services industry and the public sector as a senior advisor and adjudicator. He is a subject matter expert on Canada's framework for anti-money laundering (AML), combating the financing of terrorism (ATF/CFT), and financial intelligence (FININT).

Through his public service experience in both operations and policy, he has developed key skills in providing strategic advice, leading horizontal Government-wide initiatives, Parliamentary and public affairs, and developing and implementing legislative and regulatory amendments.

He has developed a professional expertise in financial sector policy, regulatory compliance, administrative monetary penalties (AMP) regimes, and financial technology (FinTech).

Gabriel holds a Bachelor of Commerce (B.Com.) from the Telfer School of Management and a Juris Doctor (LL.B./J.D) from the University of Ottawa. He has also completed formal training in adjudications at Osgoode Hall Law School.

Evangeline Ducas

Assessing the Money Laundering and Terrorist Financing Risks of Emerging Payment Technologies

Rapid advancements in financial technology – or "fintech" – are quickly changing the way we use and think about money. This includes both the use of technologies outside of the traditional regulated financial system, such as cryptocurrencies, and the financial innovations developed by banks, such as mobile wallets. This talk will provide a high level overview of FINTRAC's mandate as it pertains to understanding the money laundering and terrorist financial risks associated with these new technologies. It will focus specifically on the vulnerabilities of cryptocurrencies to abuse for money laundering and terrorist financing, as well as the investment and experimentation in distributed ledger technologies across the formal financial sector.

About the speaker

Evangeline is a Strategic Intelligence Analyst at the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) where she focuses primarily on assessing the vulnerabilities of emerging financial technologies to abuse for money laundering and terrorist activity financing in both domestic and international settings. Evangeline has previously worked as a Policy and Program Analyst at Global Affairs Canada in the Economic Growth and International Financial Institutions Division, and as a Business Manager at Investors Group's Outaouais Regional Office. Evangeline holds an Honours Bachelor of Arts degree in Political Science from Queen's University and is nearing the completion of a Master's in Public Administration at Carleton University.

Session 4

Big Data and Privacy

Moderator: David Décary-Hétu, SERENE-RISC – Université de Montréal

Matthew L. Williams

Big Data and Criminology: Research from the UK

The role of "Big Data" in criminological research and practice has begun to receive attention. In the UK the Economic and Social Research Council has invested £64M into the Big Data Network for the Social Sciences. The Social Data Science Lab at Cardiff University forms part of this Network and studies the utility of new forms of data, such as social media communications, in research on crime and security. This presentation will provide an overview of the work of the Lab and will present results from one of its recently completed studies funded by the ESRC and Google, that examined the use of Twitter data to identify and model the propagation of hate speech following a terrorist attack.

About the speaker

Matthew Williams holds the Chair in Criminology at the School of Social Sciences, Cardiff University. He is Director of the Economic and Social Research Council (ESRC) Social Data Science Lab and Director of the ESRC Centre for Cyberhate Research and Policy, both at Cardiff. He conducts research and writes extensively on the topics of Big Data and Criminology, Cybercrime, Cyber Security and Hate Speech on Social Media. In the UK he has been awarded funds by the ESRC, EPSRC, Home Office, Metropolitan Police Service, Department of Health, Google and Airbus to study the role of Big Data in Crime and Security. In the US, with the RAND Corporation he was recently awarded a $800K DoJ National Institute for Justice grant to study hate speech online and its relationship to offline hate crimes in Los Angeles County.

Nicolas Christin

Security Analytics

The speaker will advocate the need for an interdisciplinary research agenda, termed "Security Analytics," which combines network measurements and large-scale data analysis. Using case studies (online sale of unlicensed pharmaceutical drugs, and anonymous marketplaces), He will describe how longitudinal, large-scale measurements and data analysis reveal important economic and structural properties of a priori complex criminal ecosystems, which can be used to motivate intervention policies.

About the speaker

Nicolas Christin is an Associate Research Professor at Carnegie Mellon University, jointly appointed in the School of Computer Science and in Engineering & Public Policy. He is affiliated with the Institute for Software Research, and a core faculty in CyLab, the university-wide information security institute. He also has courtesy appointments in the Information Networking Institute and the department of Electrical and Computer Engineering. He holds a Diplôme d'Ingénieur from École Centrale Lille, and M.S. and Ph.D. degrees in Computer Science from the University of Virginia. He was a researcher in the School of Information at the University of California, Berkeley, prior to joining Carnegie Mellon in 2005. His research interests are in computer and information systems security; most of his work is at the boundary of systems and policy research. He has most recently focused on security analytics, online crime modeling, and economics and human aspects of computer security. His group's research won several awards including Honorable Mention at ACM CHI 2011 and 2016, Best Student Paper Award at USENIX Security 2014, and Best Paper Award at USENIX Security 2016 and at ACM CHI 2017. He equally enjoys field measurements and mathematical modeling.

Session 5

Investigation and Prosecution and Defence of Cybercrimes
Moderator: Jeremy Clark, SERENE-RISC - Concordia University

Anne-Marie McElroy

Technology & Privacy: Protecting against Unreasonable Search and Seizure in the Context of Cell Phone Searches

As technology develops, so too does the way that crimes are being investigated and prosecuted. The Charter of Rights and Freedoms continue to apply, regardless of the nature of the evidence and how it is obtained. However, evolution in technology and its use has forced Canadian courts to adapt legal tests in order to balance an individual's rights under the Charter with police investigative powers.

The Charter states that every person has the right to be free from unreasonable search and seizure. However, a search of a cell phone invokes a much higher privacy interest than the search of another personal item. In response, the Supreme Court of Canada modified the pre-requisites for the police to execute a reasonable search on a cell phone. It also recently heard arguments about whether a person can have a reasonable expectation of privacy in sent text messages, and whether the police need judicial authorization before seizing messages from a recipient device.

These cases show how the courts are slowly working to address the implications of these changes in the use of technology, attempting to interpret the Charter within the framework of privacy rights that accompany evolving technology.

About the speaker

Anne-Marie McElroy is a criminal defence lawyer and sole practitioner. After completing her undergrad in Sociology and Contemporary Studies at the University of King's College and Dalhousie in Halifax, Anne-Marie returned to her hometown of Ottawa to study law. Anne-Marie articled with Shore Davis Hale and was called to the bar in 2010. She went on to practice at Hale Criminal Law Office before joining May & Konyer. In August of 2015, she founded McElroy Law, where she practices exclusively criminal law. Anne-Marie is a director for the Defence Counsel Association of Ottawa and a member of the Community Adult Justice Network. Her blog won a 2015 Canadian Law Blog Award (Clawbie) for Best New Blog and a 2016 Clawbie for Best Practitioner Blog.

Christian Dumas

L'état de la cybercriminalité pour la Sûreté du Québec

Dans cette présentation, le Sergent Christian Dumas dressera un portrait de la cybercriminalité pour la Sûreté du Québec et abordera les principaux défis et enjeux auxquels font face les forces policières en matière de cybercriminalité en 2017. Il présentera ensuite le résumé d'une enquête d'envergure menée au cours des deux dernières années qui a mené à l'arrestation de 18 suspects liés à l'exploitation sexuelle des enfants sur Internet.

À propos du conférencier

Le Sergent Christian Dumas est membre de la Division des enquêtes en cybercriminalité et vigie des médias sociaux, au sein du Service des projets d'enquêtes spécialisées de la Sûreté du Québec. Il est responsable de la coordination, de la formation, de la recherche et développement, ainsi que de l'équipe de vigie des médias sociaux. Il s'implique donc dans les divers domaines touchés par le phénomène, tant en gestion qu'au niveau des opérations, du judiciaire, du renseignement, de la formation et prévention, le tout dans le but d'optimiser et d'harmoniser les meilleures pratiques de son organisation.

Avec 18 ans d'activité à la Sûreté du Québec, M. Dumas possède un bagage de diverses formations spécialisées et ateliers notamment au Collège canadien de police et à l'École nationale de police du Québec ainsi qu'une expérience variée en enquête de crimes majeurs et d'exploitation sexuelle des enfants sur internet, en interrogatoire vidéo et témoignage, en cyber-surveillance et infiltration virtuelle.

Marc-Étienne Léveillé

Bridging malware research and Law Enforcement in the fight against cybercrime

Good malware researchers have a deep understanding of the technical details and infrastructure of the malware families they study. They do not, however, have the power to stop criminals from pursuing their business. While exposing a threat or taking down its infrastructure could temporarily mitigate it, malicious groups are known to be able to continue their activity nonetheless. Identifying and prosecuting the conspirators is a more long-term solution but law enforcement must be involved.

Our team has worked with multiple law enforcement agencies including the FBI and the RCMP to initiate or collaborate in cybercrime investigations. Sometimes collaboration leads to tangible results, sometimes it does not. In this presentation, we will share our experience and suggest how we can do a better job at helping one another.

About the speaker

Marc-Etienne has been a malware researcher at ESET since 2012. He specializes in malware attacking unusual platforms, whether it's fruity hardware or software from south pole birds. Lately, Marc-Etienne was mostly reverse engineering server-side malware to discover their inner working and operation strategy. His research led to the publication of the Operation Windigo white paper that won Virus Bulletin's Péter Szőr Award for best research paper in 2014.

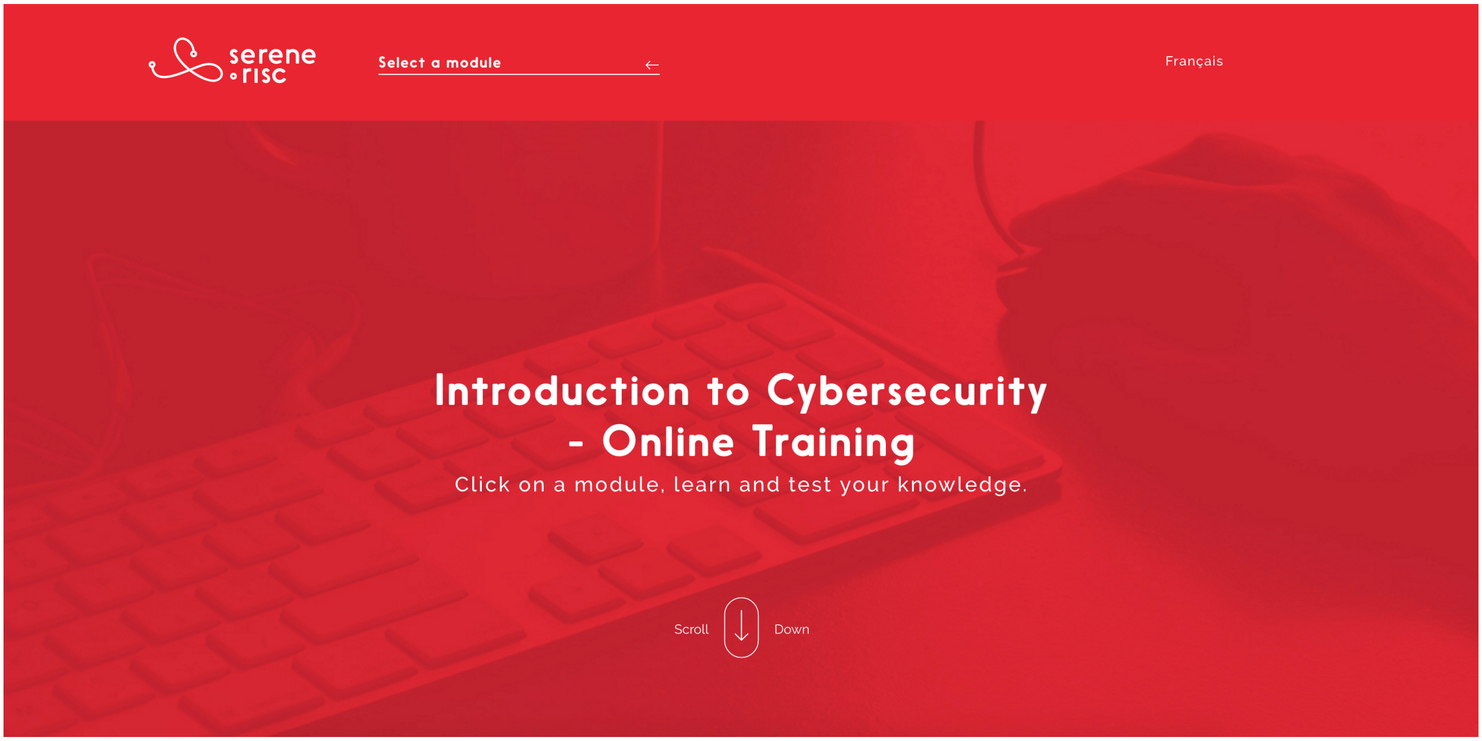
Outside his day job, Marc-Etienne enjoys designing challenges for the NorthSec CTF competition. He is also a co-organiser of the MontréHack monthly event. He presented at multiple conferences including CSAW:Threads, CARO Workshop and Linuxcon Europe. When he's not one of the organizers, he loves participating in CTF competitions like a partying gentleman. Outside the cyberspace, Marc-Etienne plays the clarinet and read comics. He tweets sporadically at @marc_etienne_.

Help us to improve the SERENE-RISC Workshop

Please take a minute to complete the Workshop survey, which you can find in your participant package, and drop it at the registration table. Thank you!

Notes:

WWW.CYBERSEC101.CA



Introduction to Cybersecurity - Online Training

Click on a module, learn and test your knowledge.

Six months after its launch, the online training package designed by SERENE-RISC has benefited almost 30,000 online users and is offered on-site by more than 100 trained librarians and community centre leaders. Cybersec101.ca is an excellent resource to share when non-experts ask how to be safer online!

Save the date:
SERENE-RISC Fall 2017 Workshop
October 25 – 26, 2017 – Ottawa (Ontario)

NCE RCE

Université de Montréal

serene
risc