Bernie Murphy

The Digital Age Creates One of the Greatest Challenges in the History of Policing

Digital technologies have impacted on police investigations in four key areas: 1)An overwhelming and unmanageable demand has been created for the recovery of digital evidence from the myriad of devices now entrenched in every aspect of our lives; 2) The Internet provides another treasure trove of evidence, but one that comes with its own difficult series of unique problems including attribution, retrieval from foreign jurisdictions, privacy issues, security of policing networks etc.; 3) Communications technologies have changed in a revolutionary manner and investigative techniques related to lawful access legislation are not able to keep pace; 4) Police agencies are in possession of masses of highly sensitive data and must ensure that internal data systems and practices meet the highest security standards. Further, law enforcement has a key role to play in ensuring cybersecurity across society.

Some of the topics to be discussed in this presentation will expound on above illustrating the enormity of this problem and will discuss metrics related to police investigations such as numbers and measurements related to digital forensics (and the exponential growth in demand for digital forensics) and difficulties in measuring various types of cybercrime (Identity theft, computer hacking, child pornography). Proposed strategies to address these problems will be discussed, including various forms of engagement with the broader community: academia, private sector, and other government agencies.

About the speaker

Bernie Murphy has been with the OPP for 27 years. He started his career in Nipigon Detachment in Northwestern Ontario and has since worked in a number of specialized investigative roles including physical surveillance, forgery, major frauds and homicide. He has worked in management roles as a Major Case Manager in Criminal Investigation Branch, Director of Anti-Rackets Branch and as Director of Strategic Management at the Alcohol and Gaming Commission of Ontario.He is currently the Director of the OPP's Behavioural, Forensic and Electronic Services.

He is also a liaison with the OPP's Workplace Discrimination and Harassment Program and is a Deputy Aide de Camp for the Lieutenant-Governor of Ontario.

He sits on the Executive of the OPP Commissioned Officers Association and has been the Association's Director on the Board of the Friends of The OPP Museum since 2012.

Thanks to our SERENE-RISC Partners

CGI
DRDC | RDDC technologysciencetechnologie
ESET ENJOY SAFER TECHNOLOGY™
NCE RCE
Symantec
TRTech
Université de Montréal
VFAC

October 21 & 22, 2014 | Ottawa Convention Centre | 55 Colonel By Drive | Ottawa

Tuesday

11:30 - 13:30 — **Registration and Welcome Lunch**
OCC Rideau Canal Atrium Alcove – 2nd Floor

13:30 - 14:00 — **Opening presentation** - Room 205
- *The evolution of the threat landscape and emerging challenges*
  Nart Villeneuve, FireEye

14:00 - 15:30 — **Session 1 – What can we learn from large information security surveys?**
- *The Global State of Information Security Survey 2015*
  Salim Hasham, PwC
- *2014 TELUS-Rotman Security Study*
  Walid Hejazi, Rotman School of Business

15:30 – 16:00 — **Networking break**
OCC Rideau Canal Atrium Alcove – 2nd Floor

16:00 – 17:30 — **Session 2 – New approaches in metrics collection and sharing**
- *Global Cybercrime event data exchange*
  Peter Cassidy, Anti-Phishing Working Group
- *Towards a science of Digital Public Health: A clinical study of risk factors leading to malware infections*
  José Fernandez, Polytechnique Montréal

17:30 – 19:00 — **Networking reception**
OCC Rideau Canal Atrium Alcove – 2nd Floor

Wednesday

8:00 – 9:00 — **Registration and continental breakfast**
OCC Rideau Canal Atrium Alcove – 2nd Floor

9:00 – 10:30 — **Session 3 – The current cybersurveillance landscape** - Room 201
- *Targeted Digital Threats against Civil Society: An overview of the evolving landscape from the Citizen Lab*
  Ron Deibert, University of Toronto
- *Does the State Belong in the Computers of the Nation? Legal Developments in Cybersurveillance*
  Craig Forcese, University of Ottawa
- *Hacking the Slovak National Security Authority aka case "nbusr123"*
  Peter Kovac, ESET

10:30 – 11:00 — **Networking break**
OCC Rideau Canal Atrium Alcove – 2nd Floor

11:00 – 12:30 — **Session 4 – Assessing data breaches and underground data markets**
- *The 2014 Verizon Data Breach Investigations Report*
  Suzanne Widup, Verizon
- Underground Market 101: Pricing Stats and Schemas
  Loucif Kharouni, Trend Micro

12:30 - 14:00 — **Networking Lunch**
OCC Rideau Canal Atrium Alcove – 2nd Floor

14:00 - 16:00 — **Session 5 – Government efforts in data collection and investigations**
- *Canadian Anti-Spam Act and Spam Reporting Centre*
  Lynne Perrault, CRTC
- *CCIRC, Canadian Cyber Incident Response Centre & Cyber Security in Canada*
  Gwen Beauchemin, CCIRC
- *The Digital Age Creates One of the Greatest Challenges in the History of Policing*
  Bernie Murphy, Ontario Provincial Police

16:00 – 17:00 — **Informal Networking** – Location to be announced

Opening presentation

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

Nart Villeneuve

The evolution of the threat landscape and emerging challenges

While the term Advanced Persistent Threat (APT) increasingly appears in the headlines as the numbers of major data breaches spirals upward, there are many misconceptions surrounding APT activity. The current threat landscape features a broad array of bad actors. On one end, there are highly focused attackers, believed to be sponsored on some level by nation-states, and on the other end there are "commodity" cybercriminals that indiscriminately compromise thousands of systems around the globe. This presentation will provide an overview of the advanced attacks facing government and industry in Canada. However, the presentation focuses on the evolution threat landscape and the challenges this creates for those seeking to understand both the context and significance of the spectrum of threats we now face as well as the technical indicators network defenders use to track and combat cyber-attacks.

About the speaker

Nart Villeneuve is a Sr. Intelligence Researcher at FireEye where he focuses on cyber-espionage, targeted malware attacks, botnets and the criminal underground. Nart has conducted in-depth investigations of malware-based espionage networks and continues to monitor numerous targeted attack campaigns with an emphasis on building threat intelligence by developing indicators that can be used to identify the tools, tactics, and procedures used in targeted attacks. Prior to joining FireEye, Nart's research at Trend Micro and the University of Toronto led to the discovery and documentation of multiple cyber-espionage networks and in-depth reports on cybercrime networks as well; the resulting papers are available at http://www.nartv.org/writing/

Session 1

What can we learn from large information security surveys?
Moderator: Bill Munson, Information Technology Association of Canada (ITAC)

Salim Hasham

The Global State of Information Security Survey 2015

Security breaches are on the rise, and it is no surprise to find that as the number of information security incidents continues to mount, so do financial losses.

Survey respondents in 2014 report that the number of detected incidents soared to a total of 42.8 million, a 48% leap over 2013. This increase comes at great cost: Total financial losses attributed to security compromises increased 34% over 2013.

Cyber risks will never be completely eliminated. Today, organizations must remain vigilant and agile in the face of a continually evolving threat landscape. Find out why your organisation should consider implementing a risk-based approach to security that prioritises your most valuable assets and proactively addresses your most relevant threats.

About the speaker

Salim has over a decade of experience in technology and business consulting, including the delivery of complex large-scale transformational engagements spanning the areas of security, strategy, governance, organizational design, M&A, performance and cost management, information management, and risk and regulatory matters.

Originally from the PwC UK firm, Salim led engagements across financial services, technology, telecommunications, government and defence industries, having worked extensively in Europe, North America, Asia and the Middle East.

Salim is leader of the GTA information security practice and national leader for security strategy and management, emerging security technology, cyber security and the identity management practices. Working closely with executives, he assists them in enabling business transformation in the cyber age, developing security as a competitive advantage, managing risk, protecting personal and corporate reputation, brand and financial integrity and crisis management.

Session 5

Government efforts in data collection and investigations
Kerry Patterson-Baker, Symantec

Lynne Perrault

Canadian Anti-Spam Act and Spam Reporting Centre

About the speaker

Lynne Perrault is the Director of Electronic Commerce Enforcement at the CRTC. She is responsible for ensuring that the CRTC enforcement responsibilities designated under the new Canadian Anti-Spam legislation (CASL) are met. She joined the CRTC in December 2010. Ms. Perrault previously held the position of Executive Director of the National Cyber-Forensics and Training Alliance Canada (NCFTA Cda) for three years prior to joining the CRTC. Concurrently, Ms. Perrault was a Computer Forensics Officer in the Electronic Evidence Unit (EEU) of the Competition Bureau, which is an independent Canadian law enforcement agency that investigates complaints and monitors businesses for fair practices. Formerly, she worked as Case Officer in the Fair Business Practices branch at the Competition Bureau conducting both criminal and civil investigations resulting in enforcement efforts. She has more than 20 years of rich experience in forensic case management, electronic evidence seizure, open source investigations, interviewing and statement taking, fraud investigations, infringing intellectual property and competitor Intelligence, policy development and negotiated settlements. In the past, Ms. Perrault led the 2nd largest investigative firm in Ontario, expanding into three other provinces within 5 years. As a respected leader and young entrepreneur, she was twice recognized as one of Ottawa's top 40 executives under 40 in 1997 and 1999 and nominated for Young Entrepreneur of the Year in 1998.

Gwen Beauchemin

CCIRC, Canadian Cyber Incident Response Centre & Cyber Security in Canada

CCIRC is Canada's National Cyber Emergency Response Team, or CERT. Learn what CCIRC services are and what areas of technical expertise on which it focuses as well as the role CCIRC has within the Canadian context. We will also share situational awareness of Canada's cyber security, elaborating on trends as well as how Canada is positioned in relation to other world leaders.

About the speaker

Gwen is the Director of the Canadian Cyber Incident Response Centre (CCIRC) at Public Safety Canada, which she joined in the January 2014. Prior to CCIRC, in September 2009, Gwen was posted to the Canadian High Commission, Canberra Australia, as a Senior Counsellor. Prior to that posting, from 2002-2009, she was a Director at Communications Security Establishment (CSE), where she led teams in a variety of roles the IT Security Branch and the Chief Information Office, including an assignment at Public Safety Canada in 2006-7 in the Canadian Cyber Security Task Force. Prior to the Federal Public Service, Gwen held a variety of roles including managing Verification teams, Portfolio Management, Software Release Manager, Project Manager, Team Leader Sustainability and software developer with Bell Northern Research and later, Nortel Networks, where she worked on a variety of products including voice recognition applications, multi-media broadband design and network operations center products. Gwen holds an Honours Bachelor of Computer Science, Carleton University.

Session 4

Assessing data breaches and underground data markets
Stephen Marsh, University of Ontario Institute of Technology

Suzanne Widup

The 2014 Verizon Data Breach Investigations Report

Based on forensic evidence collected from over 50 partner organizations as well as the Verizon caseload, the 2014 Verizon Data Breach Investigation Report (DBIR) presents a rare and comprehensive view into the world of corporate cybercrime. Now in its' seventh year of publication, this research has been used by thousands of organizations to evaluate and improve their security programs. The presentation will discuss the evolution of results over the 7 years of data and delve into the people, methods and motives that drive attackers today to better inform your own security program.

About the speaker

Suzanne Widup is a member of the Verizon RISK Team, and a co-author of the Verizon Data Breach Investigations Report. She spends quality time hunting for publicly disclosed data breaches for the VERIS Community Database. Suzanne has 20 years of IT experience, including unix system administration, information security engineering and digital forensics in large enterprise environments. She holds a B.S. in Computer Information Systems and an M.S. in Information Assurance. Suzanne is the author of Computer Forensics and Digital Investigation with EnCase Forensic v.7

Twitter @SuzanneWidup

Loucif Kharouni

Underground Market 101: Pricing Stats and Schemas

Online fraud has long since moved from being a mere hobby to a means for cybercriminals to earn a living. Daily we see lots of activity in social networks, blogs and forums, but this is the part of the internet visible to everyone.

There is another side to the internet however - its criminal underbelly - and here just like on the blogs and forums, communication is key. In this talk we will cover the principles of underground information exchange, ways to secure money/goods in underground transactions and basic cyber hierarchy.

We will also talk about underground products and services. Crypt services, DDoS attacks, Traffic resale, Bulletproof servers, SMS Fraud, Spam services and Credit card Hijack- these will be covered with pricing comparisons shown over the last 2-3 years. We will go through the typical pricing steps of a criminals attack - from buying software, all the way to monetize the volumes of infected victims.

http://www.linkedin.com/in/loucifk

About the speaker

Loucif Kharouni is a Senior Threat Researcher with Trend Micro's Forward Looking Threat Research Team. He has been working in the computer security industry for over 13 years. He has extensive tracking down latest threats campaigns. His current interests include expertise in open source intelligence gathering (OSINT), tracking down cyber criminal, targeted attacks, banking Trojan, PoS malware as well as tracking down cyber criminals and activity.He participated as a speaker in various conferences on cyber crime activity such as Cert EE, VB, TakeDown Con and ToorCon.

Walid Hejazi

2014 TELUS-Rotman Security Study

Since 2008, the Rotman School of Management together with TELUS have surveyed over 2,500 companies operating in Canada, providing significant clarity on the state of IT security in Canada. A security responsible scale is developed which encompasses four key best practices (1) strong focus on risk management (2) retaining the right skills (3) effective policies and governance and (4) employee education. We find that regardless of whether enterprises say 'yes' or 'no' to innovation, those that rate higher on the security responsible scale experience more security success. Canadian companies that embrace business-enabling innovations and are 'security responsible' can simultaneously realize productivity gains and cost savings through innovations like 'bring your own device,' social networking and cloud computing while maintaining a high level of security success.

About the speaker

Walid Hejazi, PHD has been a Professor of Business Economics and International competitiveness at the University of Toronto's Rotman School of Management for 20 years, and an Academic Director at the school. He teaches global business strategy to MBA / EMBA students and executives. He has published over 50 articles in academic peer reviewed journals and has published extensively in mainstream magazines and websites such as the Banker magazine, the Globe and Mail, National Post, Maclean's Magazine, opecnanada.org, and many others. He is the recipient of several teaching and research awards, most recently for a paper that highlights the importance of the English language in doing business internationally. Since 2008, he has worked closely with TELUS on studying the state of IT security in Canada. The annual study is now in its 6th year.

Session 2

New approaches in metrics collection and sharing
Moderator: Kush Gidda, BCE Corporate Security

Peter Cassidy

Global Cybercrime event data exchange

Cybercrime event data informs a number of interventions and subsequent metrics to help responders manage cybercrime and other cybersecurity incidents but animation of a routinized system for development and maintenance of cybersecurity metrics, which by definition must operate globally, faces a development curve challenged by the need to forge consensus in policy and law, industrial convention, technical standards and durable definitions of measurable and recordable cybersecurity events. Each dimension has a number of issues to resolve before cybersecurity event metrics provide the kind of actionable data that is provided by our global weather forecasting system, the public agency and private sector maritime piracy reporting schemes and the kind of public health case data that informs the seasonal flu vaccination program managed by the World Health Organization. We're at an inflection point in which cyber events will have to be exchanged routinely like weather data, maritime piracy info andepidemiological case data, in order to animate broad defensive systems for cyber like we have for weather, piracy at sea and the flu. Still, to do that presents a number of challenges in mounting that development curve.

About the speaker

Peter Cassidy is secretary general and co-founder of the APWG, largest and most influential coalition combating Internet crime, having cultivated the organization since 2004 into an internationally recognized authority on electronic crime with more than 2000 member institutions worldwide. Mr Cassidy is a product development consultant, software designer, industrial analyst and widely published writer, speaker and commentator on information security, white collar crime and electronic crime who has been investigating the intersection of security technologies, electronic commerce, public policy and financial crime for decades in his many capacities. Mr. Cassidy has spoken as an intervenor and consulting expert to the European Commission, the Council of Europe Convention on Cybercrime, The Organization of American States, the United Nations Office of Drugs and Crime and the Commonwealth of Nations' Cybercrime Initiative. His patents span technologies for detection of crime over internetworks and for pricing premiums for ecommerce insurance policies and bonds. LinkedIn: http://tinyurl.com/mdoo26v

José Fernandez

Towards a science of Digital Public Health: A clinical study of risk factors leading to malware infections

The success of malicious software (malware) attacks often depend upon both technical and human factors. Most mass-market and targeted attacks depend on user actions such as clicking on drive-by-download web sites or opening email attachments. In addition, even the most security conscious users are vulnerable to zero-day exploits and even the best security mechanisms can be circumvented by poor user choices. While there has been significant research addressing the technical aspects of malware attack and defense, there has been much less research reporting on how human behavior interacts with both malware and current malware defenses.

To try to shed some light on this issue, we performed at Polytechnique Montreal a 4 month-long field study, conducted in a fashion similar to the clinical trials used to evaluate medical interventions and pharmaceutical drugs. This study involved 50 subjects whose laptops were instrumented to monitor possible infections and gather data on user behavior. Although the population size was limited, this initial study produced some intriguing, non-intuitive insights into the efficacy of current defenses, particularly with regards to the technical sophistication of end users. In this presentation, we will describe the methodology employed, present some of the results obtained and discuss lessons learned from the design and worldwide-first conduction of an experiment of this type in computer security. Joint work with Lalonde Levesque, F., Somayaji, A. & Chiasson, S.

About the speaker

Dr. Fernandez is an associate professor in the Department of Computer & Software Engineering at Polytechnique Montreal. He heads the Laboratory for Information Security Research (SecSI) and his main area of research is computer security. His current research interests include malware, cybercrime, cyber warfare, security of SCADA systems, security product testing methodologies, and security and integration of logical and physical access control systems. He has several years of professional experience as a practitioner of Information Security in both industry and government. He holds Bachelor's degrees in Mathematics and Computer Science and Engineering from MIT, a Master's in Cryptology from the University of Toronto, and a Ph.D. in Quantum Computing from the Université de Montréal.

Session 3

The current cybersurveillance landscape
Moderator: Jean-Louis Tiernan, Canadian Security Intelligence Service

Ron Deibert

Targeted Digital Threats against Civil Society: An overview of the evolving landscape from Citizen Lab

For over a decade, the Citizen Lab at the Munk School of Global Affairs, University of Toronto has researched and documented information controls that impact the openness and security of the Internet and that pose threats to human rights. We collaborate with universities, advocacy organizations, and independent researchers around the world in conducting our research, and employ a "mixed methods" approach, which combines technical investigations with field research, and legal and policy analyses. I will provide an overview of one of the Citizen Lab's main projects: the "Targeted Threats" research. Civil society organizations face a growing spectrum of online threats, including Internet filtering, denial-of-service attacks, and targeted malware. The Targeted Threats project seeks to gain a better understanding of the technical and social nature of digital attacks against civil society groups and the political context that may motivate them.

About the speaker

Ron Deibert, (OOnt, PhD, University of British Columbia) is Professor of Political Science, and Director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is an interdisciplinary research and development hothouse working at the intersection of the Internet, global security, and human rights. He was one of the authors of the Tracking Ghostnet cyber espionage , and co-editor of three major volumes with MIT Press: Access Denied (2008), Access Controlled (2010), and Access Contested (2011). He is the author of Parchment, Printing, and Hypermedia: Communications in World Order Transformation (New York: Columbia University Press, 1997), and Black Code: Surveillance, Privacy, and the Dark Side of the Internet. (Signal/McClelland & Stewart/Random House, 2013). In 2013, he was appointed to the Order of Ontario and awarded the Queen Elizabeth II Diamond Jubilee medal, for being "among the first to recognize and take measures to mitigate growing threats to communications rights, openness and security worldwide."

Craig Forcese

Does the State Belong in the Computers of the Nation? Legal Developments in Cybersurveillance

Over the last year and a half, the Snowden disclosures have drawn unprecedented attention to signals intelligence agencies, including Communication Security Establishment Canada. At the same time (and Perhaps not coincidentally) Canadian courts have issued decisions that bootstrap Canadian privacy and 'search and seizure' rules into the cyber age. The law in this area is not yet fully settled, but prevailing trends point to robust constitutional protections for on-line conduct. These developments have implications for both the state, and for those private sector entities on whose systems electronic communication takes place. In this talk, I set out some of these changes and speculate as to how they may affect the world of cybersurveillance.

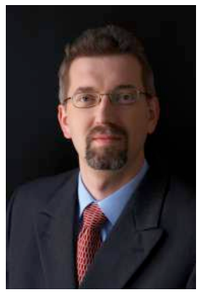
About the speaker

Craig Forcese is an associate professor at the Faculty of Law (Common Law Section), University of Ottawa. He teaches public international law, national security law, administrative law and public law/legislation. Much of his present research and writing relates to national security, human rights and democratic accountability. Recently, he has focused on law and national security surveillance, especially intelligence-sharing between security services and cybersurveillance.

He is the author of National Security Law: Canadian Practice in International Perspective (Irwin Law, 2008) and co-editor of Human Rights and Anti-terrorism (Irwin Law, 2008). He is also co-author of International Law: Doctrine, Theory and Practice (Irwin Law, 2007, 2d Ed 2014) and Laws of Government: The Legal Foundations of Canadian Democracy (Irwin Law, 2005, 2d Ed 2011) and co-editor of Public Law: Cases, Commentary and Materials (Emond Montgomery, 1st Ed 2006; 2d Ed 2011).

Prior to joining the law school faculty, Craig practiced law with the Washington D.C. office of Hughes Hubbard & Reed LLP for two years, specializing in international trade and commercial law. He has a B.A. from McGill, an M.A. from the Norman Paterson School of International Affairs, Carleton University, an LL.B. (summa cum laude) from University of Ottawa and an LL.M. from Yale University.

He is a member in good standing of the bars of Ontario, New York and the District of Columbia.



Peter Kovac

Hacking the Slovak National Security Authority aka case "nbusr123"

In 2007, the computer systems of the Slovak National Security Authority have been compromised. Hackers targeted an unpatched security flaw in NSA's webmail to gain access to further systems. Description of the hack was published on underground server and picked up by mainstream media. The key to the hack was user account "nbusr" with weak password "nbusr123" forgotten on the system since its delivery by the third party supplier.

Based on the public information and available court records, prosecution's failure to produce conclusive evidence to connect virtual identities of the hackers and two accused young males is analyzed. Limited capabilities of the criminal justice system to deal with highly technical matters were a major factor contributing to the prosecution failure.

About the speaker

Peter Kovác studied medicine (1996) and law (2002) at the Comenius University in Bratislava. In 1996–2009 he has worked as lecturer and senior lecturer at the Institute of Forensic Medicine at the Medical Faculty of Comenius University. Since 2002 he also worked as senior lecturer at the Department of Criminal Law and Criminology at the Faculty of Law of Trnava University. In 2005 he defended Ph.D. thesis in criminal law focused on problems of euthanasia and criminal liability. Also in 2005 he joined ESET a Slovak security software vendor as an in-house counsel. In 2012 he was appointed associate professor for criminal law at the Faculty of Law of Trnava University. His research focus is cybercrime and expert witnessing in criminal proceedings.