Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

GTEC SPECIAL EDITION | OCTOBER 2016

IN THIS EDITION

CSE AT GTEC 2016

QUANTUM COMPUTING AND THE SECURITY OF PUBLIC KEY CRYPTOGRAPHY

LEVERAGING BLOCKCHAIN FOR THE GOVERNMENT OF CANADA

MOBILE SECURITY: USING GC MOBILE DEVICES ON PUBLIC NETWORKS CAN BE RISKY

IT SECURITY LEARNING CENTRE NEWS

ABOUT THIS NEWSLETTER

SUBSCRIBE

CONTACT US

WE ARE CYBER SECURITY

For the fifth year in a row, CSE will be participating in the Government Technology Exhibition and Conference (GTEC), which will be held November 1-3 at the Shaw Centre in Ottawa.

Government departments are subject to millions of cyber intrusion attempts every day. Hackers, criminals, foreign states and others are constantly probing government systems and networks looking for vulnerabilities. CSE continues to play a critical role in shaping the future of cyber security in Canada, which has influenced our message for this year's booth: "We Are Cyber Security."

As CSE celebrates its 70th anniversary, we continue our commitment to integrating technologies that enable secure business, and in turn, secure GC information and networks against present and future cyber threats. We encourage you to stop by our booth to learn more about how CSE works with our partners such as Shared Services Canada (SSC) and the Treasury Board of Canada Secretariat (TBS), as well as industry and academia to collaborate on identifying evolving cyber threats and building solutions to mitigate them.

We encourage you to benefit from GTEC and register for the CSE-led speaker sessions, which include a panel of multi-disciplinary experts discussing the threat posed by the advent of Quantum Computing, and the potential benefits for securing GC services with blockchain. Following each session you can join our speakers, as well as other subject matter experts, in our booth to discuss topics ranging from mobility to tailored training.

Originally signed by

Scott Jones
Deputy Chief, IT Security

cse-cst.gc.ca/en/its

This document is for official government use only. Guidance contained within should not be considered comprehensive and all encompassing.

CYBER JOURNAL

GTEC SPECIAL EDITION – OCTOBER 2016

VISIT CSE AT THE GTEC TRADESHOW EXHIBIT

Shaw Centre Ottawa
Booth 307

"ASK THE EXPERT" SESSIONS AT THE CSE BOOTH

WEDNESDAY, NOVEMBER 2

Risk Management	10:00 – 11:15
Learning Pathways	11:15 – 12:30
Quantum	12:30 – 13:45
COMSEC/TEMPEST/EMSEC	13:45 – 15:30

THURSDAY, NOVEMBER 3

Supply Chain Integrity	10:00 – 11:15
Top 10 Implementation	11:15 – 12:30
Blockchain	12:30 – 13:45
Securing Mobile Communications	13:45 – 15:30

Exhibition Showroom - Booth 307

GTEC SPEAKING SESSIONS

Joe Waddington, Director General Cyber Protection
Chair of the Quantum-Safe Cryptography Panel
11:00 a.m., November 2 – Room 212

Quantum computing is no longer a distant notion; government, industry and academia are directing an increasing amount of resources into all aspects of this technology. Although quantum computing will undoubtedly bring great advantages to all areas of life, this opportunity will also put at risk the confidentiality of Canadian information. Quantum-Safe Cryptography represents cryptographic methods that will not be vulnerable to this dramatic increase in computing methodology. A quantum-safe strategy will ensure that the necessary protection measures will be in place when needed. This is no small goal, as this reality will take significant resources, collaboration and partnerships between government, industry, academia and standards bodies. In this session, members from these sectors will share their approaches.

Nadia Diakun-Thibault, Senior Advisor Emerging Technologies
Blockchain
11:45 a.m., November 3 – Room 211

Join this session to get a succinct overview of cryptocurrencies and Blockchain. The session will focus on services that in the near future could be delivered by government through decentralized distributed ledgers with security assurance. This technology has the potential of reducing the costs of delivering basic services and mitigating the complexity of advanced services. Examples include digital signatures and identity, passport services, voting, election finance disclosure, personalized industry services, procurement and national income distribution. This session will balance the 'disruptive' truths with 'constructive' actions that good governance and political stewardship can deliver.

Register for the GTEC Conference in order to attend these speaking sessions.

CYBER JOURNAL

GTEC SPECIAL EDITION – OCTOBER 2016

QUANTUM COMPUTING AND THE SECURITY OF PUBLIC KEY CRYPTOGRAPHY

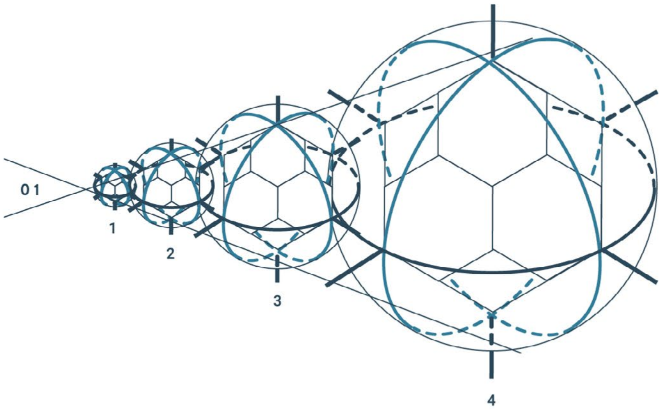
PUBLIC-KEY CRYPTOGRAPHY

Today, public-key cryptography (PKC) is used to protect a wide range of information and services. Using today's computers, it could potentially take decades to centuries to break PKC encryption.

PKC is used in:

- Credit Card Transactions
- Digital Cash
- E-commerce
- Encrypted E-mails
- Encrypted File Transfer
- Instant Messaging
- On-line Banking
- Secure Voting
- Secure Web sites

THE QUANTUM CHALLENGE



Within the next several decades, quantum computers may be able to solve specific complex problems exponentially faster than today's classical computers.

Once viable, a future quantum computer could potentially be used to easily break today's strongest PKC encryption in minutes.

WHAT ARE WE DOING ?

To ensure private and sensitive Canadian information is protected, CSE will be doing the following:

- Developing quantum-safe solutions;
- Working in partnership with Government of Canada, academia, industry and standards organizations on quantum and quantum-related technologies.

Register online to learn more and attend CSE's Quantum-Safe Cryptography Panel at GTEC 2016.

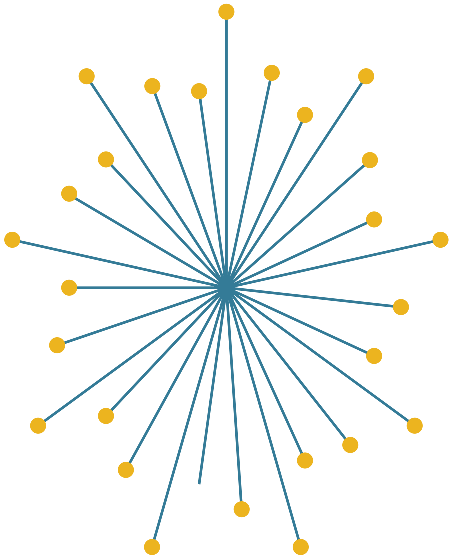
CYBER JOURNAL

GTEC SPECIAL EDITION – OCTOBER 2016

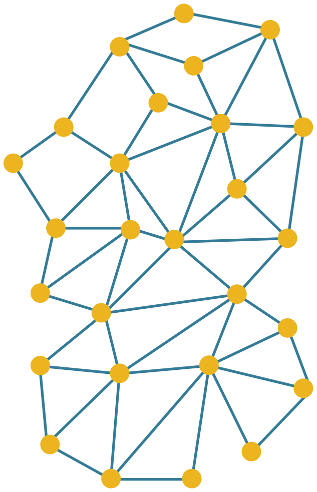
LEVERAGING BLOCKCHAIN FOR THE GOVERNMENT OF CANADA

Mention the cryptocurrency Bitcoin, and you will get varying reactions. Like any new technology, it takes time for people to understand how it works. Although Bitcoin has been used for illegal purposes, in and of itself, it is neither good nor bad.

Bitcoin's true value is not found in the activities for which it is used, but rather in the technology upon which it is based: blockchain. One of the more recent digital technologies, blockchain facilitates transactions between two parties without using intermediaries and extends beyond peer-to-peer exchanges. Instead of carrying out transactions in the traditional manner, whereby trust between the parties is established by the approval of an overarching central body, blockchain ensures that no single user controls the system. It is, instead, based on the concept of a distributed ledger that is updated and maintained by thousands of nodes on a network of computers. Further, the blockchain technology provides a method for secure transactions; any tampering attempts are immediately apparent and get flagged on the chain.



CENTRALIZED



DISTRIBUTED

The blockchain technology could be important in the context of services that the GC provides to Canadians, as it could be leveraged to protect the privacy of Canadians while delivering federal services, e.g., passport renewals. Having legacy information already on file would greatly reduce delivery time. Moreover, blockchain could provide a means of sharing data with provinces, independent researchers and industry.

To learn more about blockchain and its security implications for the Government of Canada, attend the GTEC speaker session **Government Services on the Blockchain** by CSE's Nadia Diakun-Thibault, Senior Advisor Emerging Technologies.

MOBILE SECURITY: USING GC MOBILE DEVICES ON PUBLIC NETWORKS CAN BE RISKY

Mobile devices such as smart phones and tablets are now being used by GC employees to boost productivity and efficiency. However, when GC employees take these devices outside the office and connect to unknown and possibly untrusted networks, there is an increased risk of compromise to GC information and networks.

A compromise may result in outages, downgrades in system performance, lost productivity, costly recovery efforts and damage to the reputation of the GC. Mobile devices use commercial cellular or Wi-Fi networks for internet access, but the GC does not have control over the security of these networks and they are considered susceptible to additional threats.

To help mitigate the risks of using untrusted networks, GC departments can secure their communications channels by enforcing VPN connections to GC networks and systems and by ensuring that only trusted Wi-Fi access points are used. Departments can also employ Mobile Device Management (MDM) technologies to secure, monitor, manage and support mobile devices within a network.

Departments can also apply strong mobile device policies and strive to implement the best practices to enhance the departmental security posture. These policies and best practices will facilitate the convenience of using a mobile device in a secure fashion.

Visit the CSE Wireless and Mobility Web site for additional advice and guidance on securing your mobile devices.

IT TRANSFORMATION PLAN – SHARE YOUR THOUGHTS

Contributed by Shared Services Canada

Shared Services Canada (SSC) is currently undertaking public consultations to seek feedback from Canadians, federal public servants, client departments and industry on its IT Transformation Plan. The plan is a roadmap to modernize the GC's IT infrastructure and the way it delivers services to departments and agencies. These services include e-mail, data centres, networks and workplace technology devices.

The GC is inviting you to share your ideas. Visit our Web site before October 31, 2016, to share your thoughts and feedback. Your input will help shape the GC's IT Transformation agenda.

SSC proudly reaches its 5th anniversary milestone on November 15, 2016. Stop by our booth at GTEC and celebrate this milestone with us.

Visit SSC at the Government Centre of Excellence at the GTEC Exhibition Showroom, November 2-3. Booth 315.

Visit CSE's Web site to read about our new IT security advice and guidance publication renewal.

Executive

Publications aimed at the strategic-level decision maker explaining the importance of IT security from a business process optimization, compliance, and financial point of view.

UNCLASSIFIED

IT SECURITY RISK MANAGEMENT IN THE GOVERNMENT OF CANADA

Departmental Responsibility

Authority to Operate is the business owner's approval to allow a project, program, facility, or system to operate using a particular set of safeguards within an acceptable level of residual risk.

Build and Strengthen

Canada

Management

Publications aimed at IT security management outlining the importance of IT security from a program delivery point of view by providing more in-depth explanations.

UNCLASSIFIED

MANAGEMENT SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

SECURING THE ENTERPRISE FOR MOBILITY
ITSM.80.001
July 2016

Canada

Practitioner

Publications aimed at the IT security professional explaining specific IT security issues at the technical level.

UNCLASSIFIED

PRACTITIONER SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

USER AUTHENTICATION GUIDANCE FOR INFORMATION TECHNOLOGY SYSTEMS
ITSP.30.031 V2
August 2016

Canada

Awareness

Publications that every GC employee can benefit from focusing on general IT security concepts.

UNCLASSIFIED

Using Your Mobile Device Securely

Mobile Threat Environment

Did you know?
Technology exists that a hacker can use to turn on and control your device – without your knowledge.

Who is Being Targeted?

HOW?

Canada

IT SECURITY LEARNING CENTRE LEARNING PATHWAYS

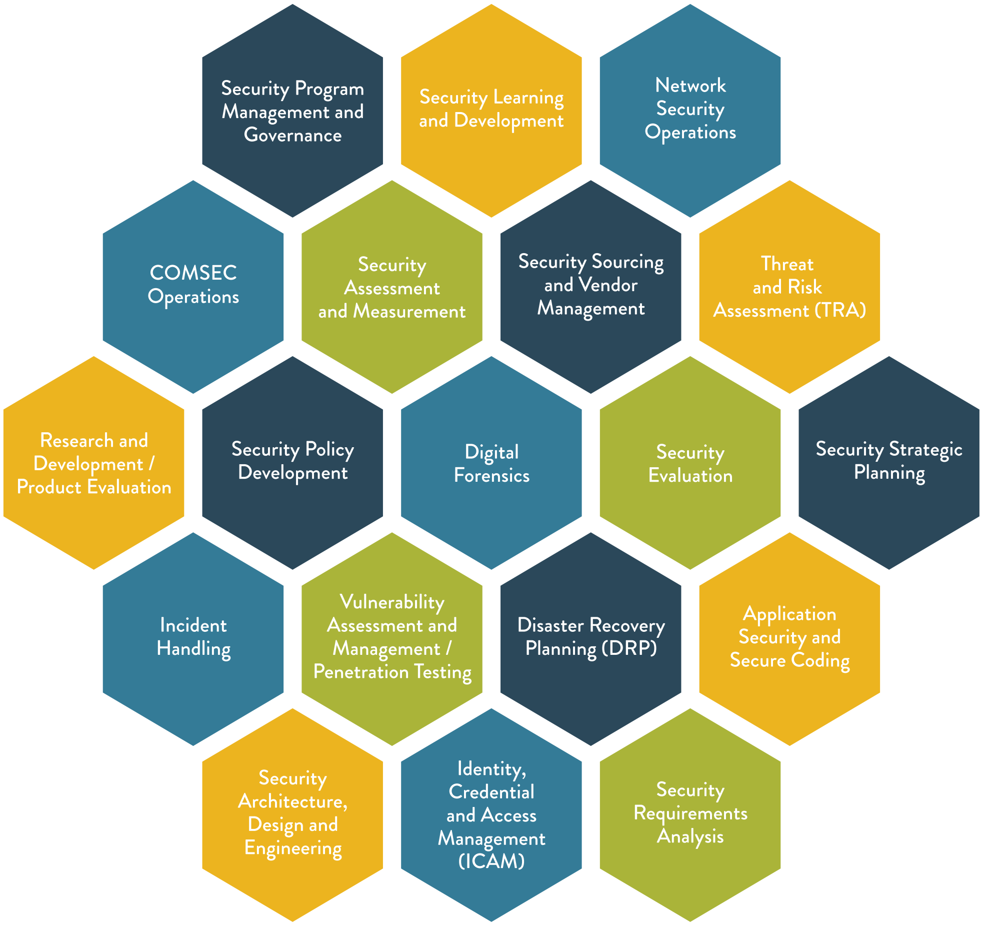
The IT Security Learning Centre (ITSLC) Learning Pathways were developed to help IT security practitioners, supervisors and managers identify learning activities that will reinforce career development in the functions that support GC departmental IT security activities.

Through this new approach, the ITSLC has created a more advanced and specialized curriculum that will assist GC COMSEC and IT security specialists achieve a higher level of knowledge and enhanced skill sets.

For more information on the ITSLC Learning Pathways, visit us at GTEC for our **Ask the Expert** session.

WEDNESDAY, NOVEMBER 2, 2016 | 11:15 – 12:30

www.cse-cst.gc.ca/en/page/itslc-learning-pathways



- Security Program Management and Governance
- Security Learning and Development
- Network Security Operations
- COMSEC Operations
- Security Assessment and Measurement
- Security Sourcing and Vendor Management
- Threat and Risk Assessment (TRA)
- Research and Development / Product Evaluation
- Security Policy Development
- Digital Forensics
- Security Evaluation
- Security Strategic Planning
- Incident Handling
- Vulnerability Assessment and Management / Penetration Testing
- Disaster Recovery Planning (DRP)
- Application Security and Secure Coding
- Security Architecture, Design and Engineering
- Identity, Credential and Access Management (ICAM)
- Security Requirements Analysis

AUTHENTICATING THE FUTURE

Contributed by Treasury Board of Canada Secretariat

As collaboration continues to increase throughout the GC towards enterprise consolidation, the Internal Centralized Authentication Service initiative is another example of the efforts that the GC is undertaking to address a common requirement for accessing GC enterprise applications.

The Treasury Board of Canada Secretariat (TBS), Shared Services Canada (SSC) and CSE are working with industry to develop this service, which will provide a secure, centralized authentication capability for users. This service is intended to improve user experience by providing single sign-on for all enterprise applications, to enhance security and to reduce costs. Join TBS, SSC and CSE at the Government Centre of Excellence at GTEC as they explain how you, the GC employee, will benefit from this new initiative.

Visit TBS at the Government Centre of Excellence at the GTEC Exhibition Showroom, November 2-3. Booth 321.

CYBER JOURNAL

GTEC SPECIAL EDITION – OCTOBER 2016

Federal Safety,
Security, and Intelligence
CAREER FAIR
#secureyourcareer
NOVEMBER 17TH, 2016
11am – 7pm
Shaw Centre
Ottawa

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT practitioners and stakeholders and is published on a periodic basis. This publication reflects the CSE IT security commitment to share information, advice and guidance with the broader GC community to help departments and agencies better protect themselves from cyber threats. The aim is to highlight key security issues and stimulate discussion about security within your department. In addition, the newsletter profiles key products and services offered by CSE with information on how you can leverage them to help your GC organization. Security awareness throughout an organization is an essential element to improving the GC's security posture. As such, we encourage you to share this information within your organization.

SUBSCRIBE

To be notified of future releases,
contact: itsclientservices@cse-cst.gc.ca

CONTACT US

For general advice and security guidance support, contact:

✉ itsclientservices@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-7654**

To contact the Cyber Threat Evaluation Centre:

✉ ctec@cse-cst.gc.ca

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ comsecclientservices@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-8495**

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ cmac-camc@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-8600**

For education and training services, contact the IT Security Learning Centre:

✉ its-education@cse-cst.gc.ca

☎ **General Inquiries: (613) 991-7110**