Towards a Smart Grid Community of Practice

Smart Grid Cybersecurity Symposium Report

Eric Fowler
DRDC – Centre for Security Science

Defence Research and Development Canada

Reference Document

DRDC-RDDC-2016-D056

October 2016

Abstract

This report captures the efforts of the Defence Research and Development Canada's Centre for Security Science (DRDC CSS) e-Security Portfolio Manager in building a community of practice for smart grid cybersecurity out of Smart Grid Canada's Cybersecurity Symposium. It (a) highlights the key areas of discussion of the Symposium, and (b) details the steps taken and progress made in forming a new community of practice.

Significance to Defence and Security

A smart grid community of practice tied to DRDC CSS' e-Security Portfolio will allow for better communication and collaboration between DRDC CSS and various partners in government, in the private sector, and in academia in order to build projects that will realise a more secure development of next generation smart grid technologies in Canada.

Résumé

Le présent rapport fait état des efforts déployés par le gestionnaire du portefeuille de sécurité électronique du Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (CSS RDDC) afin d'établir une communauté de pratique pour assurer la cybersécurité du réseau électrique intelligent à la suite du colloque sur la cybersécurité de SmartGrid Canada. Il vise deux objectifs : a) souligner les principaux sujets de discussion dans le cadre du colloque et b) expliquer les mesures prises et les progrès réalisés pour créer une nouvelle communauté de pratique.

Importance pour la Défense et la Sécurité

Une communauté de pratique pour la cybersécurité du réseau électrique intelligent jumelée au portefeuille de sécurité électronique du CSS RDDC permettra d'améliorer les communications et la collaboration entre le CSS RDDC et divers partenaires du gouvernement, du secteur privé et du milieu universitaire afin d'élaborer des projets en vue d'assurer un développement plus sécurisé des technologies des réseaux électriques intelligents de la prochaine génération au Canada.

1 Introduction

1.1 Aim

The aim of this report is two-fold. First, it is meant as a reference document for the Defence Research and Development Canada's Centre for Security Science (DRDC CSS) e-Security Portfolio. This Portfolio has the mandate to create communities of practice around issues related to cybersecurity, especially looking to the future of that field. Through communities of practice, DRDC CSS can better identify capability gaps and find project partners for key areas of concern. This report captures the steps taken and progress made at the Smart Grid Canada's Cybersecurity Symposium in forming a new community of practice around this next generation smart grid technology.

Second, it includes a concise overview of the key discussions by Smart Grid Canada's expert panelists. This will provide a start point for further research related to cyber threats and vulnerabilities in Canada as part of a strategic-level environmental scan that will ultimately contribute to DRDC CSS's project-risk alignment.

2 Report

2.1 Background

The 6th annual Smart Grid Canada conference was held at the Westin Hotel in Montreal, Quebec supported by a number of sponsors, including Hydro Quebec and Schneider Electric. Smart Grid Canada is unique in that it is the only national, smart grid-focused industry association in Canada advocating for national and provincial smart grid development. A smart grid is a power grid equipped with various meters and appliances that allow for automated production, control, and distribution of energy. The annual conference typically deals with technical challenges and opportunities related to their topic of choice—for example, the 2015 conference focused on the active consumer (e.g., real-time feedback, dynamic power pricing, and architecting the grid for the new energy consumer), grid resiliency (e.g., the predictive grid, the automation of conservation for predictable energy savings, and technologies that go beyond the smart grid), and interoperability of various grid and grid-related technologies. This year's conference stands out because it marks the first time a side symposium has been added devoted to cybersecurity. Previously, a large gap in the conference was identified and this new symposium has been added, hosted jointly by Deloitte Canada and the Department of National Defence (DND) through DRDC CSS.

2.1.1 e-Security Portfolio Objectives

Members of Smart Grid Canada have expressed the ambition that this symposium will continue to be a regular event at the annual conference in order to develop an awareness, understanding, and community around cybersecurity. In the continued implementation of this symposium, one of the objectives is to improve connections among those working towards the security of this next generation technology in order to ensure that best practices of system assessment and defence will be shared, guaranteeing that the smart grid in Canada develops with an appropriate consideration of the cybersecurity concerns.

In furthering this objective, the DRDC CSS e-Security Portfolio Manager with the assistance of an analyst:

- presented the Canadian national security view of cybersecurity;
- gauged the interest and reception to building a community of practice around smart grid cybersecurity to add to the communities in place (finance, telecommunications, supervisory control and data acquisition (SCADA)); and
- opened discussions with regards to current DRDC e-security projects and potential future projects.

2.2 Areas of Discussion

The workshop was divided into four discrete complimentary subjects, each with presentations, a panel, or both. These subjects were:

- Canadian National Security View on Cybersecurity;
- Canadian Utility View of Cybersecurity;
- Canadian Industry Views on Cybersecurity Trends and Opportunities; and
- Upcoming Evolutions that could Impact Utilities.

The bulk of the symposium was in the three related perspective discussions, which shared a formula of first identifying the threat as determined by the sector in some depth and later developing solutions. The focus here was, as introduced by Smart Grid Canada, to “grasp the depth of the problem and set a roadmap for the future” in the transition of utilities from a “dumb” environment to one connected on all fronts.

2.2.1 Content

Though presenters used different tools to introduce the threat, all demonstrated that it is significant and urgent. For this presenters relied on explaining common attack vectors in a generalised way, introducing exploitation statistics, walking through case studies, or exploring hypotheticals. Of particular note is the case study of the Ukrainian BlackEnergy hack, which resonated with the audience because of their own relationship to industrial control systems in the energy sector. In the December 23rd attack highly sophisticated cyber threat actors exploited vulnerabilities in the information and operational networks of the Prykarpattyaoblenergo company. Two presenters (Emile Khan, North American Electric Reliability Corporation (NERC) Auditor; and Jean Le Duc, Hydro Canada) used this case study to explain the current environment, especially with regards to security standards and the implications of the convergence of operations technology and information technology (OT-IT convergence). Extreme case studies such as this act as both a catalyst and focal point for discussion, which can be beneficial to understanding and provide a host of lessons learned. In discussing the concerns of cybersecurity in other industries—banking and air transportation—there were either many smaller examples or the panelists had to rely solely on hypothetical disasters.

An interesting conversation occurred regarding the motivation of actors during the “Other Industry” panel when an audience member proposed that any actor targeting such critical infrastructure as the energy grid or air transportation must be driven by political motivations. There was emphatic pushback from the panelists. First, it was asserted that rampant ransomware in the medical industry is an example of the criminal monetization of critical services which is equally applicable in the utilities. Second, one panelist insisted that one of their greatest concerns is “expert hackers” or “hacker-researchers”, very skilled individuals or groups aiming to be the first to prove a conceptual exploitation.

Not represented here is the amount of very practical suggestions made throughout the course of the day for security practitioners in the utilities world. These range from very basic guidelines on dynamic monitoring or social engineering awareness to specific suggestions on penetration testing sequences and contingency planning.

The day ended with a series of forward-looking researchers presenting concepts and insights in order to generate insights on trends in the field. The presentations ranged from very specific, such as Alex McEachern's demonstration of hardware vulnerabilities in the power grid to very general, such as Duncan Stewart's quick spin through the technology, media, and telecommunications futurology work at Deloitte. As a result of this presentation, Duncan Stewart will be visiting DRDC CSS to deliver a presentation.

2.3 Towards a Community of Practice

To wrap up the symposium, Hassan Farhangi of the British Columbia Institute of Technology and Rodney Howes of DRDC CSS expressed the need to build a Community of Practice for utilities cybersecurity. Interest or confirmation of partnership was expressed by:

- Smart Grid Canada;
- Siemens Canada;
- Hydro-Québec;
- BC Hydro and Power Authority;
- Hydro One;
- British Columbia Institute of Technology;
- University of Toronto;
- École Polytechnique de Montréal; and
- a number of additional companies, academics, and government groups.

It must also be noted that the room dedicated to the conference was set up to accommodate an estimated 60 guests but surpassed capacity by roughly 20 people. The popularity of this event was commented on multiple times by the organisers and demonstrates the receptivity of the smart grid community to cybersecurity. Much discussion was generated by Hassan Farhangi's presentation on the necessity for a formal community of practice. DRDC CSS has entered a partnership with Dr. Farhangi as he takes the lead in organising this community.

3 Conclusion

Given that 2016 is the first year that Smart Grid Canada decided to include a full day cybersecurity symposium, this event must be considered a success. The scope and quality of expert-level presentations is fitting of a long-running symposium, the reception of the community lead to a room over capacity to the surprise of the organizers, and important first steps were made with regards to developing a community of practice. The key for the future will be maintaining this momentum and following through to ensure the continuation of this symposium in future conference and the building of relationships in line with DRDC CSS's goals of developing a community of practice for the security of this next generation technology in Canada.

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Towards a Smart Grid Community of Practice : Smart Grid Cybersecurity Symposium Report

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Fowler, E.

5. DATE OF PUBLICATION (Month and year of publication of document.)

October 2016

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

12

6b. NO. OF REFS (Total cited in document.)

0

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Reference Document

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2016-D056

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report captures the efforts of the Defence Research and Development Canada's Centre for Security Science (DRDC CSS) e-Security Portfolio Manager in building a community of practice for smart grid cybersecurity out of Smart Grid Canada's Cybersecurity Symposium. It (a) highlights the key areas of discussion of the Symposium, and (b) details the steps taken and progress made in forming a new community of practice.

Le présent rapport fait état des efforts déployés par le gestionnaire du portefeuille de sécurité électronique du Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (CSS RDDC) afin d'établir une communauté de pratique pour assurer la cybersécurité du réseau électrique intelligent à la suite du colloque sur la cybersécurité de SmartGrid Canada. Il vise deux objectifs : a) souligner les principaux sujets de discussion dans le cadre du colloque et b) expliquer les mesures prises et les progrès réalisés pour créer une nouvelle communauté de pratique.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Smart Grid; Cybersecurity; Community of Practice.