Canadian Supercomputer Threat Assessment and Potential Responses
Date: Dec, 5 2018

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

KEY EVENTS

Four key events are addressed in this briefing note. Key event one is the announcement in April and May 2017 of two supercomputers being launched in Canada (Graham at University of Waterloo; Cedar at Simon Fraser University) and a third (Niagara at The University of Toronto)[1] using Compute Canada's Resources Allocation. Key event two is the announcement that Huawei Canada is building Graham's operating system.[2] Key event three, CSIS is warned, by the US Senators (Rep. Sen Marco Rubio and Dem. Sen Mark Warner), about the possibility of China and Russia spying on Canada. Key event four, the United States has reportedly banned sales of Huawei products on US military bases.[3, 4, 5]

This is briefing note is particularly relevant as Compute Canada is now preparing for the 2019 resource allocation - as there may be a raised / elevated security risk of economic espionage intellectual property theft, and abusing education access privileges which needs to be considered.[6]

[1] Compute Canada. (2018, March 05) Canada's most powerful research supercomputer niagara fuels canadian innovation and discovery. Retrieved https://www.computecanada.ca/featured/canadas-most-powerful-research-supercomputer-niagara-fuels-canadian-innovation-and-discovery/

[2] Feldman, M. (2017, April 23) Canada Is Quietly Adding 10 Petaflops to Its Network of Academic Supercomputers. Retrieved https://www.top500.org/news/canada-is-quietly-adding-10-petaflops-to-its-network-of-academic-supercomputers/

[3] Collins, K. (2018, May 02). Huawei, ZTE phones will no longer be sold on US military bases. Retrieved https://www.cnet.com/news/pentagon-reportedly-bans-sale-of-huawei-and-zte-phones-on-us-military-bases/

[4] Bronskill, J. (2018) Security agencies warn of foreign espionage threat to company networks. Retrieved https://www.cbc.ca/news/politics/security-agencies-warn-espionage-networks-1.4919962?fbclid=IwAR0GxsX5M_i1TB5H_aUmbmIul9qlCkwA6JxeXha-QzAE0j1mVgFALlEC40E

[5] Ibid

[6] SFU Innovates Staff (2018) SFU's Supercomputer Cedar to be part of Compute Canada's 2019 Resource Allocation Competition. Retrieved http://innovates.vpr.sfu.ca/story/sfus-supercomputer-cedar-be-part-compute-canadas-2019-resource-allocation-competition

NATURE OF DISCUSSION

This briefing note will explore the potential risk of foreign nationals accessing Canadian innovation and research linked to healthcare data, artificial intelligence, and data modeling. In particular, focusing on supercomputing systems known as Cedar and Graham. This briefing note will use a kill chain model to demonstrate a prior case example of how Ruopeng Liu allegedly stole data about the manufacturing of metamaterials from Dr. David Smith's Duke University lab,[7] which specialized in research regarding "invisibility cloaking technology".[8] That technology may have then been used by Liu to create a startup company called Kuang Chi Science in Shenzhen China that is now worth approximately $6 billion[9] and linked to Chinese military product development using similar low radar visibility metamaterials.

The note will then outline how a similar attack vector can be used in Canada to target Canadian supercomputing projects and associated research hosted on the supercomputer network.

This note will also introduce open source articles and commentary which support the need for a cybersecurity assessment be conducted with a specific focus on supercomputing contracts currently at Compute Canada and CFI innovation funding. These contracts include contributions by Lenovo and Huawei.

Indications of security risk are noted in the following examples: Lenovo to pay $7.3m for installing adware in 750,000 laptops[10], installation of a microchip on Elemental computers (developed in China by Supermicro)[11] deployed inside U.S. Department of Defence data centres, and China's government ability to directly influence Chinese company operations.[12]

This briefing note will then address the possible connection between Huawei and supercomputing risks in Canada. The final issue addressed in this briefing note will outline a potential attack that may involve compromising an individual with access to any of the computers connected to the Arbutus network. By spoofing the credentials of one of these targets, attackers may gain access to the computers computational power. This access may be gained through users who are active teaching faculty and may become a target of opportunity for a potential attacker.

---

[7] McFadden, C. et al. (2018, July 24) Education or espionage? A Chinese student takes his homework home to China. Retrieved https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881

[8] Ibid

[9] Ibid

[10] Waqas. (Nov 28, 2018). Lenovo to pay $7.3m for installing adware in 750,000 laptops. HackRead. Retrieved from https://www.hackread.com/lenovo-to-pay-fine-for-installing-adware-in-laptops/

[11] Robertson, J., & Riley, M. (Oct 4, 2018). The big hack: How China used a tiny chip to infiltrate U.S. companies. Bloomberg Businessweek. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[12] U.S. House of Representatives (Oct 8, 2012). Investigative report on the U.S. National Security Issues posed by Chinese telecommunications companies Huawei and ZTE.

BACKGROUND

Two potential attack vectors against supercomputing are possible: the human vector, and the technological vector. The human vector is potentially a foreign national student and the technological vector is a spoofing attack.

Human Vector: A potential attack under the kill-chain model could be demonstrated as follows. A university student conducts reconnaissance (by becoming a trusted member of a research project thus gaining access to the computer network), gathering information on potential targets and technical specifications (server details, operating systems used, vulnerability to malware, etc). Having gathered the data, the student would then gain access to the network, through the use of legitimate credentials for the purpose of stealing data (a/k/a weaponization of access privilege). Once system access has been obtained, the student would then steal the research data set. The data is then moved to a foreign nation and potentially converted into military products for a foreign government.

Technological Vector: "A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls."[13] A spoofing attack to compromise Cedar could be feasible if potential attackers are able to identify researchers with access to that network. In 2018, a list containing more than 400 names associated with research projects that utilized Cedar computing resources was made available online[14]. This list could potentially provide a number of targets for identity theft and spoofing, which are then converted into login credentials via keylogging software or other backdoor access.

Listed names include researchers from across Canada in a variety of fields and topic interests. Some of whom are active teaching faculty at their respective institutions. Attackers may pose as students, in order to send infected files possibly disguised as assignment submissions or other seemingly legitimate documents containing keyloggers or other spyware. In this way, the user can be compromised and attackers can access to the system. Once Cedar is compromised, it could then be vulnerable to a malware upload; potentially resulting in disruption to system or a potential backdoor access to the system being implemented.

Implications of these attacks. Analysis of the Compute Canada 2018 project data requests reveals research allocation projects which included artificial intelligence and big data analytics. These projects may be relevant to Canadian Armed Forces and Canadian police services who are currently using or exploring the role of AI and big data modeling in order to combat dark web activities. Furthermore, such a research framework is also being pursued at various Canadian universities. This target rich environment is similar to the security risk at Duke University.

Previous Supercomputer hacks. Similar supercomputer hacks have occurred and demonstrate there are vulnerabilities which can be exploited.

In 1999, a 15 year old boy known as C0mrade caused a 21-day shutdown after hacking NASA computers and invading Pentagon systems. In June 1999, he accessed 13 computers at the Marshall Flight Space

[13] veracode.com Spoofing Attack: IP, DNS & ARP. Retrieved https://www.veracode.com/security/spoofing-attack
[14] 2018 Resource Allocations Competition Results. Retrieved https://www.computecanada.ca/research-portal/accessing-resources/resource-allocation-competitions/rac-2018-results/

Centre and downloaded $1.7 million worth of NASA proprietary software that supports the space station's environment. Between August and October 1999, he entered the computer network run by the Defence Threat Reduction Agency (DTRA) through a router in Dulles, VA., and intercepted DTRA email and 19 usernames and passwords of employees, which included 10 on military computers. [15]

In 2013, Andrew James Miller was able to gain access to the supercomputers used at National Energy Research Scientific Computing Center in the Lawrence Berkeley National Lab California. He was arrested by the FBI when he attempted to sell root access to the supercomputers to an undercover FBI agent via an online chat platform. Selling unauthorized access to a government supercomputer would have enabled the purchaser to easily compromise information resources for the US Department of Energy.[16] These information resources are similar to the Compute Canada project list related to the energy sector.

In 2014, a New Zealand based weather supercomputer named Fitzroy was hacked from an IP that was reportedly traced back to China. Paul Buchanan, a former policy analyst for the US Secretary of Defense, noted that the attack followed similar Chinese patterns and may have been searching for back doors to other government computers including computers with access to Five Eyes network[17]. Fitzroy's operators were confident that the hackers did not get beyond the supercomputer.

Based on these case studies, the impact of these hacks are summarized as threats against intellectual property, compromised infrastructure security, and a loss of confidence in academic institutions' ability to adequately protect national security based research.

While searching for historical cases of supercomputers being hacked, there is evidence that supercomputers may also provide a solution. In 2018, a potential countermeasure against hacking powered by current or future supercomputers was announced. A team from Monash University is claiming to have "devised the world's leading post-quantum secure privacy preserving algorithm – so powerful it can thwart attacks from supercomputers of the future"[18]. This algorithm allows for the secure transfer of data, as well as the preservation of user privacy. Furthermore, it was noted that "...even in the existence of the future powerful quantum computer - which can easily break the current security algorithms such as RSA - HCash is still secure, and user privacy remains preserved,"[19].

Huawei. In the past some Chinese companies have reportedly been connected to incidents involving compromised computer security. In particular the microchip found in Supermicro was connected to

---

[15] Wilson, C. (Sept 22, 2000). 15-Year-Old Admits Hacking NASA Computers. Retrieved from https://abcnews.go.com/Technology/story?id=119423&page=1

[16] Goodin, D. (2013, August 28). Hacker pleads guilty to charges he sold "magic passwords" to sensitive networks. Retrieved https://arstechnica.com/information-technology/2013/08/hacker-pleads-guilty-to-charges-he-sold-magic-passwords-to-sensitive-networks/

[17] Richmond, B. (2014, May 29) Who Hacked the Most Powerful Weather Computer in the Southern Hemisphere? Retrieved https://motherboard.vice.com/en_us/article/bmjjxm/who-hacked-the-most-powerful-weather-computer-in-the-southern-hemisphere

[18] Monash University. (2018, July 18). World-first program to stop hacking by supercomputers. Retrieved from https://www.monash.edu/it/about-us/news-and-events/latest/articles/2018/world-first-program-to-stop-hacking-by-supercomputers

[19] Ibid

supercomputing mother boards.[20] Currently there are security concerns about Huawei as a cybersecurity threat have been expressed by US and Five Eyes intelligence community. As reported in the Globe and Mail (2018), Canada "does not allow Huawei to bid on federal government contracts." The contracts for Graham and Cedar supercomputers are funded by Canadian Innovation Fund, which is a federally funded agency to implement and manage research which benefits Canadians. This funding is linked to Computing Canada, Cedar and Graham supercomputing, and Huawei Canada. Given that Canada does not allow this bidding, there are still concerns that "the Shenzhen-based firm (Huawei Canada) has established relationships with leading research universities in Canada to create a steady pipeline of intellectual property to underpin its market position in 5G technology".[21]

CSE - Security Review - University Responsibilities to Address Huawei Canada Impact on Risk.

The detaining and possible extradition of Ms. Wanzhou Meng (Chief Financial Officer of China's Huawei Technologies) by Canadian officials in December 2018 may raise concerns or speculations about the extent of Huawei Canada's influence on Canadian national security, in particular 5G telecommunications design and implementation. As noted above, these concerns can be dated to 2012 in the U.S. and 2013 in Canada with CSE providing

> "advice and guidance to mitigate supply-chain risks in telecommunications infrastructure upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei," ....The...."testing is called the Security Review Program. Risks could affect equipment ranging from private cellular phones to large communications networks, corporations and governments"[22]

This kind of testing can be used to inform risk management issues and tasks which are identified as a condition of funding by the CFI funding guidelines. These guidelines can be traced back to 2013 and have evolved to address a variety of risk management issues. For example,

1. Innovation Canada at Section 5.1.1 (p. 24) recognizes the need to ensure the institution deals with 5.1.3 Special requirements for certain types of infrastructure projects The institution must ensure that researchers follow existing guidelines and adhere to the requirements for their research facility. In signing the Institutional agreement, the institution agrees to conform to these guidelines.[23]

---

[20] Robertson, J. & Riley, M. (2018, Oct 04) The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Retrieved https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[21] Fife, R. & Chase, S. (2018, Sept 07) Ottawa probes Huawei equipment for security threats. Retrieved https://www.theglobeandmail.com/politics/article-cse-says-canada-tests-chinas-huawei-equipment-for-security/

[22] ibid.

[23] Innovation Canada. (May 2013). Policy and program guide. Toronto, ON

2. Compute Canada and CFI Grant recognize the need for managing the funding and also the need to ensure the CC can "review options for hosting, operating, and maintaining the infrastructure to provide the highest quality and most cost effective total solution. Compute Canada can leverage its existing CFI-funded data centres, technical, and staffing investments to provide extremely high quality and cost-effective operations and maintenance of systems as part of the national platform, meeting a variety of uptime and security requirements. [24]

Innovation Canada provides "best practices" insight into risk-based management approach to ensure the funding project is well managed. Included in that document is specific mention that some projects will require more oversight than others. This is addressed in the proposal development and internal review stages.

> The internal vetting process ensures that project risks that may hinder success have been identified (e.g. potential for significant delays and cost escalations or insufficient capital and operating funds) and that mitigating measures, including any oversight activities, have also been discussed.[25]

Innovation Canada also recognizes the need for additional oversight of large or complex projects which includes oversights such as "scope and issues" and requires those receiving funding to have clear definition of roles and responsibilities to ensure "Improved risk management during project implementation and mitigation of adverse impacts" (if any).[26, 27]

Based on the information found in open sources, the following points are noted.

1. The national security threat from Chinese telecommunication companies can be traced back to 2012 and 2013.
2. Canadian government agencies were actively looking at this threat.
3. Universities who are involved in supercomputing projects have risk management mandates and responsibilities, and
4. There is a track record of three Chinese telecommunication companies who are currently involved in litigations which are directly related to national security concerns in Canada.

---

[24] CFI Grant Proposals. (2018). Grant Support. Retrieved from https://www.computecanada.ca/research-portal/grant-support/cfi-grant-proposals/

[25] Innovation Canada. (2017). Risk-based management approach. Retrieved from https://www.innovation.ca/awards/sharing-good-practices/risk-based-management-approach

[26] Innovation Canada (2016). Additional oversight for large or complex projects. Retrieved from https://www.innovation.ca/awards/sharing-good-practices/additional-oversight-large-complex-projects

[27] Innovation Canada. (2017). Clear definition of roles and responsibilities, and collaboration from key stakeholders at all stages of a CFI project. Retrieved from https://www.innovation.ca/awards/sharing-good-practices/clear-definition-roles-and-responsibilities-and-collaboration-key

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Increased security reviews and oversights are necessary to protect Canadian researchers and their intellectual property. SFU has a long established history of working with federal and provincial contracts. Is there an opportunity to provide additional security? And if so, what kind of security and at what costs?

Increased siloed security around military and public safety research. As noted previously that access via researcher credentials can potentially lead to a compromise of national security, the research allocation projects that share a relationship with law enforcement models may be susceptible to such a compromise. For example, SFU is conducting various research projects concerning artificial intelligence and as mentioned above, artificial intelligence is a field rich for attack[28]. In addition, with some projects potentially sharing a close relationship with the military, the risk is further increased. Is it now critical requirement to have a Chief Security Officer for all supercomputing projects answering to an external governance body?

Double Edged Challenge. British Columbia has a large international student population and is actively engaged around the world on a variety of academic initiatives. While this is promoting global partnerships, it is essential there be sufficient safeguards in place to protect Canadian interests. How do we promote international cooperation while also protecting Canada's intellectual property?

[28] Ibid