Reflections on the Annual CPI Conference

The University of Waterloo Cybersecurity & Privacy Institute (CPI) held its annual conference on October 5th and 6th, consisting of several presentations and panel discussions, which highlighted the rich interdisciplinary research pursued by CPI members and offered valued insights from invited speakers. Attendees were presented with state-of-the-art research by CPI members and visiting researchers on methods designed to enhance cybersecurity and individual privacy as well as on societal level issues.

After a welcome by Charmaine Dean (Vice President, Research and International), and a summary of the state of the Institute from N. Asokan (Executive Director, CPI), the conference began with a talk on ‘The Erosion of Social Capital Online and How We Can Revive It’, by Neil Desai (Vice President of Magnet Forensics and Senior Fellow at the Centre for International Governance Innovation-CIGI). Magnet Forensics offers digital investigation solutions for public safety agencies and enterprises. These state-of-the-art tools are used by public safety agencies to recover and analyze digital evidence relevant to criminal investigations. They are also used by enterprises for incident response to fraud, ransomware, insider threats, and other cybersecurity events.

Desai noted the numerous difficulties, including a talent shortage, that are impacting the ability of agencies to keep up with the growing complexity of cybercrime. This is especially worrisome, Desai said, because cybercrime is now being facilitated by the technological evolution in encryption, the Dark Web, AI, and cloud computing. However, technology also presents opportunities to develop trust with public safety agencies and innovations in public policy, both of which should be pursued.

The next discussion was from Diogo Barradas, Assistant Professor at the Cheriton School of Computer Science. His talk, ‘Are We Safe in the “Internet from Space?”’, focused on the implications of providing enhanced global connectivity through satellites. However, satellites’ wide beam ranges imply that such links are extremely susceptible to long-range eavesdropping attacks, despite the use of encryption. Professor Barradas’ talk covered some of the latest trends in the research and literature, which was followed by an explanation of how eavesdropping can result in an analysis of metadata from satellite internet links, with the potential for compromising individual privacy.

The first day’s events concluded with a panel discussion of the cybersecurity talent gap facing the country, as well as globally. Panelists included:

Facilitator:

- Anindya Sen - Associate Director, CPI - Director; Professor at the Department of Economics - UWaterloo

Panelists:

- Ken Barker - Director of ISPIA - University of Calgary
- Deborah Clark-Forster - Senior Account Executive, Ministry of Economic Development, Job Creation and Trade - Province of Ontario
- Sanjeev Gill - Associate Vice President of Innovation and Executive Director of WatSPEED - UWaterloo
- Ryan Westman - Sr. Manager, Threat Intelligence - eSentire Threat Response Unit

The discussion highlighted the importance of renewed government support, closer ties with industry partners and academic institutions, such as the University of Waterloo, all focusing on how to address the cybersecurity talent gap. Referencing the rising average costs and frequency of ransomware attacks, panelists stressed that significantly more HQP are needed to stem this rising tide of cybercrime, and that industry and academia needed to work together to create effective and constantly updated educational opportunities for people to fill these crucial roles in cybersecurity and privacy fields. Also of note was the concept that careers in these areas require strong promotional efforts in conjunction with lucrative salaries in order to attract the necessary interest from future students. A description of this panel's talking points was written by University Media Relations and is available here.

To end the first day of the conference, attendees were treated to an informative and enjoyable event centering on the poster presentations by UWaterloo graduate students, which was a very strong showcase of the seminal research being pursued in the university. The students were enthusiastic and clearly enjoyed the opportunity to present and discuss their work within an in-person environment.

The second day opened with an awards ceremony in which winners of CPI Graduate Excellence Scholarships, as well as CPI Undergraduate Awards, were recognized. Hossam ElAtali was presented an award for their poster on 'BliMe: Verifiably Secure Outsourced Computation with Hardware-Enforced Taint Tracking'.

The first talk of the day, 'The Lasting Challenges in Cybersecurity and Opportunities to Disrupt Them', was given by Andrew Walenstein, Director of Security Research and Development at BlackBerry. Walenstein noted that despite Machine Learning being first employed commercially to block malware prior to the first release of Windows 95, malware still thrives today. Organizations face significant challenges from system intrusions, exploits of network-facing services, credentials misuse, and the ever-present spam. Walenstein put forward an explanation, consistent with game theory, where enhanced technological defenses incentivize attackers to break new defenses. Given this context, Walenstein's talk focused on potential methods that could be used to address cybersecurity challenges faced by the research and education communities.

This was followed by a panel discussion on the National Cybersecurity Consortium (NCC).
Panelists included:

Facilitator:

- N. Asokan (Executive Director of CPI)

Panelists:

- Ken Barker - Director of ISPIA - University of Calgary
- Charles Finlay - Executive Director of Rogers Cybersecure Catalyst - Toronto Metropolitan University

The NCC is a consortium of different universities with expertise in cybersecurity that has received $80 million to lead Canada's Cyber Security Innovation Network (CSIN). The objective of this funding is to help foster a strong national cyber security ecosystem in Canada and enable it to become a global leader in cyber security. The funding is intended to stimulate collaboration between academia, the private sector, not-for-profit sectors, and other levels of government from across Canada, leading to research and development, increased commercialization, and developing skilled cyber security talent.

The panelists described their original vision and the multi-year process of discussions and interactions with various stakeholders that led to the formation of NCC and its successful bid to lead CSIN. In the lively Q&A that followed, the panelists reiterated NCCs intent to grow its membership and welcomed potential new members to reach out to NCC.

The next talk, ‘Differential Privacy: Potential and Limitations’, was given by Professor Ninghui Li, from the Department of Computer Science at Purdue University, also a member of the Centre for Education and Research in Information Assurance and Security. Differential Privacy (DP) has been increasingly accepted as the de facto standard for data privacy in the research community, and its use is slowly becoming more widespread, as DP is being applied to increasingly more application domains. Professor Li’s talk explored the potential and limitations of DP by analyzing its guarantee of privacy. The main insight from this discussion was that the requisite level of privacy is subjective and determined by legal and ethical considerations chosen by different communities.

The final individual talk of the conference was by Professor Guang Gong of the Department of Electrical and Computer Engineering at the University of Waterloo. Her talk, ‘How Practical is zkSNARK Enabled Blockchain Privacy?’, focused on the applicability of ‘zkSNARK’ as a way to enhance Blockchain privacy. Blockchain technology is attracting considerable interest as a possible solution to many applications in finance, healthcare, and supply chain management. zkSNARK is based on zero-knowledge proof systems and is the acronym for **z**ero-**k**nowledge **S**uccinct **N**on-interactive **AR**gument of **K**nowledge. Noted benefits of this application are that it does not leak information and is also computationally efficient. Professor Gong then discussed specific evidence regarding the performance of Polaris, a new version of zkSNARK that is considered to be transparent, universal, and plausibly post-quantum secure, making it a promising vehicle for further development. Her research is currently focused on investigating the efficacy of Polaris in supply chain management.

The conference concluded with a panel discussion on ‘Data Collection and Effective Public Policy’. The panel was moderated by Ian Goldberg, Professor of the Cheriton School of Computer Science. Panelists included:

- Lyall King (Director of Risk Mitigation Programs - Canadian Centre for Cyber Security)
- Kelly O’Hearn (Senior Advisor, Promotion, Business Advisory Directorate - Office of the Privacy Commissioner of Canada, Government of Canada)
- Nicolas Papernot (Assistant Professor of Electrical and Computer Engineering, UToronto)
- Anindya Sen (Associate Director, CPI – Director and Professor at the Department of Economics – UWaterloo)

Kelly O’Hearn began by outlining the role of OPC; they look at how Federal departments and the commercial private sector manage personal information and performing investigations and audits when necessary. Additionally, they promote cybersecurity and privacy practices, and actively give advice and recommendations to businesses on their privacy management programs, with the overall goal to enhance Canadians control over their personal information. O'Hearn stressed the importance of PIPEDA in relation to data collection policy, also detailing the importance of meaningful and informed consent for Canadians in reference to their data and privacy, encouraging people to view the important legislation being discussed in Bill C-27.

Lyall King then expanded on the role of CCCS; namely, it is part of the Communications Security Establishment (CSE), which is Canada's national cryptologic agency. CSE's mission is twofold: firstly, to provide information for the intelligence mission of the organization in response to the Government of Canada's intelligence requirements, and secondly, to also protect information. King pointed to the impact of COVID as a major switch to working from home, as well as a shift to cloud infrastructure and the elevation of cyberthreats as a result. Further focus was centred on state actors as well as cybercriminals, with concerns not only around maintaining security to avoid ransomware attacks etc., but to counteract attacks on infrastructure etc., that may weaken a nations ability to function. Industrial espionage and threats to IP were discussed, as well as various other cyberthreats to day-to-day life, including the significant cyber incident that impacted the critical I.T system supporting health care providers in Newfoundland and Labrador, and the Canada Post malware attack that exposed the data of 950,000 Canadians.

Nicolas Papernot continued the discussion with a concise presentation on the 'Limitations of De-identification: the Case of K-anonymity', which focused a bit more technically on the different definitions of what it means to have a privacy preserving analysis. Prior definitions include de-identification, the idea being to try to process data to remove what is considered to identify particular individuals. De-identification has been abandoned for about a decade and instead researchers are working on techniques to provide and improve differential privacy. Papernot discussed challenges, strengths, and weaknesses within DP moving forward, stressing that it is superior to de-identification, but challenges do remain.

CPI's own Anindya Sen then presented his talk entitled, 'How to Enhance Innovation , Privacy, and Data Protection Through the Artificial Intelligence and Data Act'. Initially touching on Bill C27 and its aims to regulate the development and the use of AI in Canada, which defines that it is the federal government's responsibility, and establishes an AI and Data Commissioner. Sen asserts that this is exciting because Europe is still working on its artificial intelligence act, hence Canada is being an innovator in this space. As the bill seeks to enact rules which are intended to improve public trust of AI systems and protect Canadians, this will also help stimulate innovation in a data-driven economy. He also makes two policy recommendations: firstly, to have clear opt out mechanisms for individuals when their data is collected. Secondly, in order to reassure individuals from a trust perspective, Canada should establish an AI advisory unit or an ombudsman, for example. Sen's salient point is that if people are struggling with the idea that through aggregation their data is protected, they require reassurance from an established third party to assuage their concerns.

A Q&A period followed, with Ian Goldberg querying Kelly O'Hearn about the details of the new tribunal proposed as part of Bill C27; whether it is intended that if a company doesn't like the ruling of the OPC they may appeal to this tribunal, as a quicker alternative to federal court. O'Hearn responded that it was intended to streamline that process, also touching on the recourse available when entities outside of Canada, corporate or otherwise, are found to have mismanaged or otherwise impacted Canadian data.

Continuing with this theme, an audience member posited that the Privacy Act is trying to locally govern an issue that is global in nature and expressing concern about how the Act can effectively protect the Canadian citizen when the technology used is not governed by any authority. O'Hearn replied that the Privacy Act only deals with federal government agencies; Service Canada, CRA, the CBSA etc., and how those departments manage your personal information. In reference to third-party businesses, PIPEDA stipulates that if an organization is working with a third-party business, as in processing out to another country or another country is storing information, that business which controls the information is still required to make sure that there is a comparable level of protection of information. If that's not happening, regardless of the technology that's used, there are experts at the OPC performing analyses on different types of technology; that would be something to raise to their attention and for the OPC to investigate.

Lyall King added that there are different models in terms of encouraging companies to protect data, using the 'carrot and stick' analogy. On the one hand there is legislation and how we can regulate the space and the use of data, and conversely, the approach of building communities of understanding and promoting best practices.

As a closing remark, Ian Goldberg raised the highly relevant if not moderately uncomfortable point that human error, and lack of effort in maintaining digital hygiene, is often a major component of how cyberattacks are enabled. He stressed that blaming individuals is not the answer however, underlining that it is unfair to rely on people to be far more fastidious than they have any reasonable ability to be, and noting that the technologists that have made these horribly insecure systems for a long time must bear some responsibility as well.

In summary, the annual conference was extremely successful and well-received, as it offered a blend of insights that touched on all the core mandates of UWaterloo and CPI. Firstly, attendees were exposed to contemporary research being conducted by faculty members from Waterloo and other universities. Secondly, the conference succeeded in gaining key insights on technology development and societal implications from the perspective of industry leaders. Thirdly, policymakers were given a platform to discuss issues impacting society and recent legislative changes related to cybersecurity and privacy, along with associated implications. Finally, graduate students were given the opportunity to present their research. Next year's conference is expected to consist of an extra day, to give CPI members the opportunity to present findings from their own research.

The webpage for this conference is available on CPI's website here.