Cyber Security for Current and Future IoT and Ubiquitous Computing Systems

Dr.-Ing. Monika Freunek, Catalyst Fellowship Program, 2022/2023, Rogers Cybersecure Catalyst, Toronto Metropolitan University, Toronto, Ontario, Canada

Final report 15/09/2023

Rogers Cybersecure Catalyst Research Fellow: **Dr.-Ing. Monika Freunek**
Lighthouse Science Consulting and Technologies Inc., Nova Scotia, Canada
Contact and further information: The author can be reached under monika.freunek@tmu.ca and monika.freunek@lighthouse-sct.com

I. Executive Summary

This final report covers the research project "Cyber Security for Current and Future IoT and Ubiquitous Computing Systems" of the inaugural Rogers Cybersecure Catalyst Research Fellowship program. Major findings of the project and recommendations on the cyber security of the Internet of Things (IoT) are discussed. In summary, IoT cybersecurity is both as critical and urgent as immature, especially from a research perspective.
Cybersecurity is a network profession and one of the disciplines that require the most interdisciplinary collaborations, not only between professional disciplines, but also between academia and industry. During the Catalyst Fellowship program, an intense and fruitful exchange has been established between the Fellows, the Academic Director and the Catalyst Community, both on research as on general cybersecurity topics. The second part of this report reflects the role of the Fellowship program both on the research outlined above and the cybersecurity community as a whole. During this collaboration several themes have been reoccurring. From both perspectives, establishing and funding of interdisciplinary networks and long term collaborations between operations, education and research across academia, industry and the public sector are recommended. Cybersecurity research requires both scientific and cross-disciplinary operational understanding. In order to accelerate successful implementation of solutions in practice, cybersecurity research funding needs to be both available and adapted to this requirement.

II. The IoT - an essential infrastructure unseen and unsecured

Background and Motivation

The initial vision of the IoT had foreseen an area of silent computing, where computers of all sizes would quietly perform various functions, often without their users even being aware of their presence [1]. This vision has been fully achieved. However, the quite nature of IoT devices seems also to expand to their visibility from a security perspective. And despite their truly pervasive and ubiquitous scale of today, the cybersecurity level of IoT devices is generally low, independent from how critical or sensitive the function and the data of a device are.
While cybersecurity has been established by now as an operational necessity and requirement in classical IT environments, cybersecurity measures and often even the existence of IoT devices within an environment is regularly neglected. However, the level of criticality of IoT systems meets or exceeds the one of classical IT systems in many applications. IoT devices physically interact with their environment, they measure and control municipal water treatment systems, they shut down power in energy utilities, enable fuel flow in gas stations, track food inventories in grocery stores, locate emergency vehicles, and control irrigation and feeding in agriculture. They also log heart rates, monitor our doorsteps and homes, provide control decision data for our cars, and listen in our personal conversations. In short, IoT systems keep our nations running. If they fail or provide wrong or manipulated data, the damage can be significant. IoT cybersecurity is now regularly identified as one of the highest risks to impact the economy, the national security and the life quality of individuals, and losses resulting from hacks easily range in the million dollar scale [2-7].
Yet, where other systems of similar criticality are subject to standards, regulations, and fail-safe design requirements, IoT devices are generally not [8]. Attempts to improve IoT security have been isolated and mostly focused on very narrow application areas, sometimes even limited to specific products or specifications. In addition, many regulatory approaches remain recommendations, putting safety aware manufacturer at a competitive disadvantage. Hence, the majority of IoT devices and applications remains unaddressed and the devices that are covered are quickly outdated.

III. Assessing IoT Security – Methods, Major Findings and Recommendations

Research Scope and Methods

IoT cybersecurity is a critical topic of a vast scope with an urgent need to act. The goal of this project was to gain a solid understanding of the current state and future development of IoT cybersecurity to then identify major areas of action to achieve the quickest impact in the most critical areas from a Canadian perspective.

In IoT cybersecurity, complex scientific research needs to be coupled with operational realities and needs. The most promising technical solution will not succeed, if regulatory aspects or psychological factors are neglected. In order to reflect this, this project consisted of four pillars:

a) Assessment of the state of the art in IoT security from a technological perspective today and in the near future based on a literature study of scientific publications, technological reviews, industry studies and patents

b) Assessment of existing standards and regulations based on regulatory studies and scientific publications

c) Investigation of physical limits to achievable IoT security based on scientific publications and theoretical modeling

d) Real world feedback via discussions and interviews with 20 experts and professionals from cybersecurity, critical infrastructures, operation and management.

Major Results and Recommendations

The research consistently showed an almost paradox current approach to IoT systems and an urgent need to advance IoT cybersecurity research and data, some of it on a fundamental level. Within the constraints of the brevity of this report, major findings will be summarized in the following.

I) The IoT is here to stay

On all levels of society, the IoT truly has become an ubiquitous and a permanent institution.

IoT systems are widely in use and frequently considered indispensable. Their benefits made them a necessity of today for private and public life, ranging from simple comfort functions, productivity, and participation in today's society to critical infrastructures. Since long, deployment of IoT devices has been the default decision for all applications.

Once laws are established, they often remain unchanged over decades. Thus, in general, technologies have to achieve a certain maturity and scale of societal impact to be considered in legislation. This critical threshold has recently been recognized for the IoT, and regulations and laws are being established all over the world, including in Canada.

Recommendation: The likely existence and use of IoT devices should be reflected accordingly, such as in organizational security policies, the legislature, or education.

II) The IoT is unsafe, often fundamentally

The IoT is unsafe, often in very basic aspects, some of which are inherent to IoT design.

A general and strong consensus was identified throughout the scientific and technical literature and the interviews, that both the current and the achievable security of IoT devices is low up to a degree where it is not considered realistic to trust IoT devices today or in the future. This is solidified by the theoretical model, where already the size of the attack surface makes a breach the most probabilistic outcome. In addition, some characteristics of IoT devices such as low computing resources or the frequently open physical exposure of the devices limit applicable security measures.

Recommendation II a: The use and the design of IoT application should include risk assessment and mitigation. In some applications, IoT devices might not be recommendable or require fail-safe design measures, such as a redundancy solution in case of a device function failure.

Recommendation II b: Available security measures, such as the use of sufficient passwords, should be applied. In addition, see recommendations IV, V and VI.

III) What is an IoT device?

There is a lack of standard or consensus definitions of IoT devices in technical and regulatory solutions and the public perception, even among experts.

Available definitions of what constitutes an IoT system are vague and heterogeneous to the degree of uncertainty from all perspectives investigated within this project. This limits the development and evaluation of security goals and measures from a technical perspective and the development and application of effective legal tools and standards.

Recommendation III: Standardized definitions of what constitutes an IoT device are required both on a national and an international level. When several definitions are required, a sufficient coverage needs to be achieved.

IV) IoT cybersecurity is about elephants in the room

Well-known measures of technically relatively low efforts could mitigate the risk for the majority of breaches, but are rarely mandatory.

The majority of publicly known IoT breaches can be categorized into a few scenarios of technically relatively low effort, such as attacks on routers and cameras and/or taking advantage of insecure passwords [7]. Major vulnerabilities in mobile data transmission systems are public knowledge [8]. And although IoT devices come with inherent constraints to their achievable security, even the applicable best practices out of cybersecurity are rarely in place or legally required.

Voluntary IoT cybersecurity measures bring security-oriented manufacturers in a competitive disadvantage. The existing legal and regulatory approaches are either highly specific or very broad both in their definition of IoT devices and the required measures, thus limiting their practical applicability and impact. In alignment with these findings, the interviews showed a strong consensus on the need for mandatory standards in the form of laws and sector wide regulations as well as public awareness campaigns.
Recommendation IV: An adaption of the legal and regulatory environment as well as public awareness campaign are recommended to make use of the already available and highly effective measures.

V) Specific solutions for specific scenarios – challenges for IoT cybersecurity research
Many IoT cybersecurity solutions are tailored to specific scenarios and narrow in their scope. This limits effective protection measures, such as applicability of many automated tools.
Current IoT cybersecurity research focuses on selected topics of limited general applicability. The majority of solutions are based on hard- or software centered approaches including artificial intelligence. Few research covers network protection, physical measures, or the impact of emerging technologies such as quantum computing.
While this fundamental research is necessary, there is a gap between the requirements of funding structures to address the high impact challenges of IoT cybersecurity and the existing cybersecurity research funding. Classical research funding encourages work of single disciplines on isolated research questions, where IoT cybersecurity research requires the possibility for interdisciplinary collaboration and equal involvement of Academia, Industry and the Public Sector. The lack of standard definitions and the prevalence of proprietary solutions in IoT systems aggravate the situation.
Recommendation V: In order to achieve a near-term significant impact on the IoT cybersecurity situation, cross-disciplinary research projects with a strong collaboration between the Public Sector, Academia and Industry for selected priority application fields are advised.

VI) Is it you, Mirai?
A lack of current systematic and trustworthy IoT malware inventories hinders effective research and security measures.
Depending on the source, the same malware can be found under various names or not all, and the few available sources need to be evaluated individually for their credibility and completeness [9]. Hence, own research in a constantly changing environment is required for a current taxonomy. More research and official credible sources that report, classify and track IoT malware in a standardized manner, are needed.
Recommendation VI: Establishing a standardized official IoT malware reporting such as the Common Vulnerabilities and Exposures database CVE is recommended.

VII) How safe is safe?
Currently, there is no standardized procedure to evaluate and compare the cybersecurity of IoT devices in Canada.
Without shared security metrics, no user is able to evaluate a security rating given by a manufacturer. Users interested in trying to understand who has access to their devices and their data quickly reach the limits, and sometimes even manufactures themselves might not have a full understanding of the real flow of data. Manufacturers willing to increase the security level of their products face competitive disadvantages due to higher sale prices while not being able to promote their products due to lack of standard comparative metrics.
Recommendation VI: The development of standard security metrics for IoT cybersecurity in Canada is recommended.

VIII) The IoT brings foreign affairs home.
There is a stark contrast between the current level of insecurity of IoT devices and the potential impact of their failure on a national scale. IoT are part of critical infrastructures and as such targets of strategic relevance. Citizens and organizations alike need appropriate measures in place, including empowerment for security and education.
The global character of many IoT products and their potential use for espionage or military applications place them into the context of military strategy and its role in national and international law. In recent years, military framework has shifted to classify cyber attacks, especially those causing a significant physical impact, as potential triggers for the opportunity for physical and other military retaliation measures within international law. The function of many IoT devices is the direct interaction with physical parameters or their measurements, where falsified or missing data can have disastrous effects. Yet, unlike in other critical applications the legal framework does not reflect the strategic role of IoT cybersecurity, for example, by requesting fail-safe design of critical functions or even reflecting the possibility of a failure of an IoT device at all. Where mandatory regulations are in place, the limited enforcement options of national and international law in cyberspace pose an ongoing challenge. As the development of solutions will likely be a long term and international effort, risks mitigation measures should be developed before.
Recommendation III: The strategic role of the IoT at the interplay of national and international law and foreign affairs should be reflected in technology, industry and regulations and standards.
Recommendation IV: Where laws cannot be in place, failure management for critical IoT is highly recommend to be included in the legislation, for example requiring critical applications to include redundancy solutions consisting of separate technologies or manual fallback options.

IV. Reflections on the Cybersecure Catalyst Research Fellowship on this Project - The Role of Networks, Research and Funding in Cybersecurity

The Rogers Cybersecure Catalyst Research Fellowship has enabled this work and the research on this topic as presented within this report. The organizational and professional support from all members of the Cybersecure Catalyst and from all Fellows of the fellowship program has been a major contribution to the success of this project, as well as the outstanding expertise within the Catalyst and its professional networks.
The Fellowship Hour was held every two weeks for two hours, and provided a platform for exchange, development, and networking. Besides being a time for research updates and administrative matter, current cybersecurity topics were discussed, connections established, and feedback and ideas exchanged. Often, the combination of the perspectives from industry and academia was fruitful for this exchange. Despite the different scopes of the overall topics of the fellows, the wish to establish, extend and maintain a strong cyber security network is shared and perceived as beneficial to the Canadian cybersecurity landscape. A research exchange as such is highly valuable. In general, the wish for networking, exchange and learning in the cybersecurity community was high. Regular platforms such as research colloquii, professional events and alumni networks, and the continuous use of virtual and hybrid forms could assist in establishing this exchange on a long-term base and also to expand the network.
The outreach of the Fellowship has been remarkable with more than three joint publications resulting out of three webinars, and several other publications. In general, the funding provided for research more on an inaugural level, where the required depth and focus of a more profound research project was identified.
Three topics reoccurred during the Fellowship both within the project presented in this report and in the exchange and collaboration of the Fellowship as a whole: the generally immature state of cybersecurity research, the limited access to cybersecurity research funding, and the need for interdisciplinary collaboration between disciplines and academia and industry. As these three aspects seem of interest not only for the Catalyst itself, but also with views on the general Canadian cybersecurity, they are outlined in more detail below.

Establishing networks and interdisciplinary collaboration with research and industry
The Fellowship provided plenty of opportunities for an exchange of disciplines, as Fellows were from technical and humanities background, and also equally represented both the academic and industrial perspective. During the discussions in the Fellowship hour, the joint publications, and the webinars with outstanding external experts the need to bridge these the worlds and to establish exchange and collaboration was a reoccurring theme.
As no other discipline, cybersecurity can be seen as a puzzle where lacking pieces such as important insights from professional perspectives, operational realities within industries, psychological effects or technical boundaries regularly become attack vectors. And while cybersecurity solutions might be available from research and industry, the methods to fully implement them into practice often lack coordination and knowledge about each other realities. Improving and establishing collaboration is therefore strongly recommended within Canada, be it through research as with the Catalyst, enabling networking or collaboration opportunities.

Accelerating the State of Cybersecurity Research and its Impact
Cybersecurity is an emergent research discipline, and its scope is still relatively limited when compared to similar fields. On a closer look, the majority of existing cybersecurity research focuses on selected technical topics, in some of which cybersecurity is only one application fields of many. All of this limits the real scope of cybersecurity research and its maximal impact on real systems even further.
Cybersecurity has a massive backlog in research even within its fundamentals, and especially when leaving out projects on highly specified applications that cannot easily be applied to real cybersecurity environments. The covert nature of cybersecurity aggravates this. Few research work aims for the realities of cybersecurity operation with its complex environment. Given the critical nature of secure computing for today's society, it is highly recommended to increase funding for cybersecurity in general and to widen the scope of the research itself with a focus on the complex interdisciplinary environment, cybersecurity represents.

Access to Funding for Cybersecurity Research,
During this project and together with the Fellows, several areas have been identified that require follow up or even initial research, yet appropriate funding could not be identified during the Fellowship. Currently, funding for cybersecurity research represents a minority of available funding opportunities and not all options display the realities of required funding. Despite the identified research needs and their urgency with regards to the importance of the topics, progress is hindered, and existing knowledge lacks the means for implication.

It is important to outline the role of industrial research and cybersecurity start-ups within the cybersecurity community, for which classical funding is not designed for. It is highly recommend to investigate how funding models could look like that enable both fundamental and application oriented cross-disciplinary collaboration work.

V. Acknowledgements

This work has been enabled by funding from the Rogers Cybersecure Catalyst and the strong and constructive support from many individuals. The Fellow would like to sincerely thank the academic director Prof. Marcus Santos and the fellow researchers Prof. Reza Samavi, Prof. Rasha Kashef, Prof. Burcu Bulgurcu, Dr. Jeff Schwartzentruber and AJ Khan for the strong support and the fruitful exchange. Much has been learned. The author would also like to thank her outstanding students Alexandra Rombos and Jorge Cavalho for their enthusiast and hard work and their valuable contributions.
The author would like all Fellows, Prof. Marcus Santos, Charles Finley, Sumit Bathia, Trysh Dyl, Anita Schrettlen, Juliana Scharrer, Randi Purse, Prof. Ali Miri, Prof. Sylvain Leblanc, Dr. Tiago de Jesus, Suman Roy, Herbert Saurugg, Dr. Simon Erb, Torben Keck and Oliver Doleski, for their valuable contributions and time, who all shaped this project. It has been an honor. The author would also like to thank Rolf Müller for the valuable discussions on military strategy in the context of cyberwar.

VI. Bibliography

[1] Weiser, M. (1991). The computer for the 21st Century. Scientific American, 265(3), 75-84.
[2] Cremer, F., et al., Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap. Risk Insur. Issues Pract., 47(3), 2022, pp. 698-736.
[3] Radanliev, P., et al., Future developments in cyber risk assessment for the internet of things, Computers in industry, 102, 2018, pp. 14-22.
[4] The Global Risks Report 2020, 15th Edition, World Economic Forum, Geneva, Switzerland.
[5] The Global Risks Report 2022, 17th Edition, World Economic Forum, Geneva, Switzerland.
[6] National Cyber Threat Assessment, Canadian Center for Cyber Security, Communications Security Establishment, Ottawa, Canada, 2023.
[7] Evaluation Study of Protection Needs for Smart Metering in Switzerland – "Studie Schutzbedarfsanalyse Smart Metering Schweiz" [German and French], AWK Group, final report for the Federal Office of Energy, Bern, Switzerland, June 2016, p.15 .
[8] Freunek, M., The Internet of Things exposes us all to the biggest cyber threats, Toronto Star, 20-03-2023, accessed 15-09-2023.
[9] Freunek, M., Rombos, A., History and Taxonomy of IoT malware. In: Freunek, M. (Editor), IoT Cybersecurity in Critical Infrastructures, Elsevier, 2024, under preparation.