Proceedings of the 51^{st} Hawaii International Conference on System Sciences | 2018

Introduction to Cyber Threat Intelligence and Analytics Minitrack: A Conceptual Three-Pronged Approach and Future Research Agenda

Kim-Kwang Raymond Choo
University of Texas at San Antonio, USA
raymond.choo@fulbrightmail.org

Ali Dehghantanha
University of Salford, UK
A.Dehghantanha@salford.ac.uk

Abstract

Technologies underpin almost every facet of our society, both online and offline (e.g. cyber-physical systems and Internet of Military Things). For example, a coordinated cyber and physical attack on our interconnected cyber-physical systems using both cyber (e.g. malware) and physical (e.g. improvised explosive devices) techniques could potentially cripple our critical infrastructure systems (e.g. in the event of a coordinated terrorist attacks). Thus, it is important to be able to defend against such threats in real-time, for example using cyber threat intelligence and data analytics approaches. This mini-track reports on existing state-of-the-art advances. We also present a conceptual three-pronged approach to protecting our cyber-physical infrastructure, and identify a number of potential research agenda.

1. Introduction

Cyber security threats are real due to the increasingly connected nature of our society. The seriousness of malicious cyber activities, for example, is echoed in the September 2017 media release of the Chairman of the U.S. Securities and Exchange Commission (SEC) [2]:

> *I recognize that even the most diligent cybersecurity efforts will not address all cyber risks that enterprises face. That stark reality makes adequate disclosure no less important. Malicious attacks and intrusion efforts are continuous and evolving, and in certain cases they have been successful at the most robust institutions and at the SEC itself. Cybersecurity efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery.*

The implementation of any cyber security and cyber resilience strategy will be dependent upon a number of factors such as the infrastructure sector and the level of participation required from the public sector, the private sector and other relevant stakeholders. However to ensure our cyber and national security and competitiveness, all relevant stakeholders in the public and private sectors have a primary responsibility to make detailed preparations to act against current and emerging threats, as well as to recover from a wide range of malicious cyber activities when they succeed (resilience).

With the digitalization of things, a significant amount of data is collected from different security monitoring solutions as well as systems that were compromised or have been used to facilitate an attack (e.g. a cloud server). Thus, advanced cyber threat intelligence and analytical techniques (e.g. threat intelligence, big data and machine learning techniques) are key to real-time detection and mitigation of cyber security incidents, and to the collection and analysis of cyber security incident related information. For example, one emerging research focus is cyber threat intelligence and analytics, which seeks to integrate and deploy different computing techniques such as big data analytics, sentiment analysis, artificial intelligence and machine learning to perceive, reason, learn and defend against advanced cyber attacks or advanced persistent threats, as well as facilitating the collection, preservation and analysis of evidence that may then be used to identify and prosecute the perpetrators.

There are parallels between cyber threat intelligence and analytics and intelligence analysis. The latter (intelligence analysis) involves a continuous cycle of tasking, collection, collation, analysis, dissemination and feedback [6].

In the next section, we will introduce the three papers in this mini-track. We will then present a conceptual three-pronged approach and outline potential research agenda in Section 3.

2. Cyber threat intelligence and analytics

Cryptographic solutions are generally used to secure our data and systems, as well as our communications. Similarly, Nanda *et al.* [5] from

URI: http://hdl.handle.net/10125/50577
ISBN: 978-0-9981331-1-9

University of Technology, Sydney in Australia presented a novel hybrid authentication model for geo location oriented routing in dynamic wireless mesh networks. The model is capable of supporting full authentication, quick authentication and new node authentication.

De Faveri, C., Moreira [3] from Universidade NOVA de Lisboa in Portugal presented a framework designed to generate adaptive deception-based defense strategies.

Bollmann *et al.* [1] from Naval Postgraduate School, USA presented an approach to increase the robustness and accuracy of anomaly detection without affecting system detection and response rates.

3. Future research agenda

The diversity of attack vectors and threat actors necessitates enhanced interdisciplinary and international knowledge base. Unsurprisingly, cyber threat intelligence and analytics is among one of the fastest growing interdisciplinary fields of research bringing together researchers from different fields such as digital forensics, political and security studies, criminology, cyber security, big data analytics, machine learning, etc. to detect, contain and mitigate advanced persistent threats and fight against malicious cyber activities (e.g. organized cyber crimes and state-sponsored cyber threats).

In Figure 1, we present a three-pronged framework to ensure the effective use of up-to-date cyber threat intelligence (broadly defined) in a combined top-down/bottom-up approach. This allows us to obtain situational awareness, make careful predictions about future trends in information and communications technologies (ICT) and scale of the threat landscape at both localized and international levels, the impact of malicious cyber activities on society, and to ensure that appropriate controls (e.g. resources and investment) are made to ensure the resilience of critical information infrastructure systems – e.g. in the form of national cyber security registers.

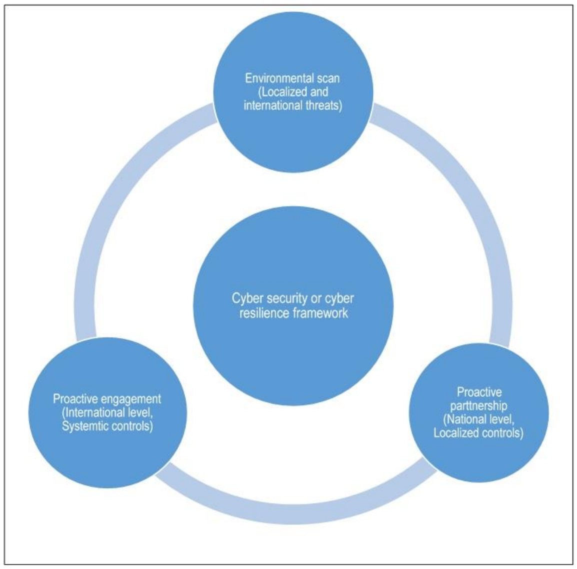

Figure 1: Conceptual cyber security or cyber resilience framework

National risk registers, as argued by Hagmann and Cavelty [4, p. 80], are valuable

> *tools for dealing with unknowability, or the limits of knowledge more generally, but they are not about making particular unexpected events – or catastrophes – actionable and governable. Instead, they are about the management of insecurity in the broadest sense, as they provide seemingly incontestable and neutral mechanisms by which danger potentials can be prioritized in a cost-effective way.*

An environmental scan would include a review of current information on existing and emerging cyber threats as such threats and windows of vulnerability evolve over time, partly in response to defensive actions or crime displacement. Although the speed of change in ICT development and adoption means that history may offer limited guidance about the future threat landscape, understanding the threat landscape is crucial to a country’s national and cyber security agenda.

ICT also create various interdependencies between different systems and between key critical infrastructure sectors in most technologically advanced countries, with many of the same technology-related risks affecting one or more of these sectors and in more than one country, and potentially lead to larger-scale and often unanticipated failures. In addition, the interdependencies may also result in mutual dependence between sectors and countries and complicate recovery efforts. Therefore, the oversight and governance of critical infrastructure resilience should involve all key stakeholders in the public sector, private sector and the research community at both the national and international levels. A proactive partnership will also result in collaboration and strategic alliances outside our borders for critical infrastructure resilience and help us to identify and prioritize current and emerging risk areas (including risk arising from unexpected and highly unpredictable causes – also known as “black swan” problem), and hence, achieving systemic resilience.

Thus, there are many research challenges that need to be addressed, and these challenges are not just technical challenges although we will only list some of the technical research challenges below:

- Detection and analysis of advanced threat actors tactics, techniques and procedures
- Application of machine learning tools and techniques in cyber threat intelligence
- Theories and models for detection and analysis of advanced persistent threats
- Automated and smart tools for collection, preservation and analysis of digital evidences
- Threat intelligence techniques for constructing, detecting, and reacting to advanced intrusion campaigns
- Applying machines learning tools and techniques for malware analysis and fighting against cyber crimes
- Intelligent incident response tools, techniques and procedures for contemporary technologies, such as cloud and cyber-physical systems
- Intelligent analysis of different types of data collected from different layers of network security solutions
- Threat intelligence in cyber security domain utilizing big data solutions such as Hadoop
- Intelligent methods to manage, share, and receive logs and data relevant to variety of adversary groups
- Interpretation of cyber threat and forensic data utilizing intelligent data analysis techniques
- Infer intelligence of existing cyber security data generated by different monitoring and defense solutions
- Automated and intelligent methods for adversary profiling
- Automated integration of analyzed data within incident response and cyber forensics capabilities.

References

[1] Bollmann, C., Tummala, M., McEachen, J., Scrofani, J., Kragh, M. 2018. Techniques to Improve Stable Distribution Modeling of Network Traffic. In Proceedings of 51st Annual Hawaii International Conference on System Sciences (HICSS 2018), IEEE.

[2] Clayton, J. 2017. Statement on Cybersecurity. Media Release 20 September, 2017. https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

[3] De Faveri, C., Moreira, A. 2018. A SPL Framework for Adaptive Deception-based Defense. In Proceedings of 51st Annual Hawaii International Conference on System Sciences (HICSS 2018), IEEE.

[4] Hagmann, J., Cavelty, M. D. 2012. National risk registers: Security scientism and the propagation of permanent insecurity. Security Dialogue 43(1), pp. 79–96

[5] Nanda, A., Nanda, P., He, X., Jamdagni, A., Puthal, D. 2018. A Novel Hybrid Authentication Model for Geo Location Oriented Routing in Dynamic Wireless Mesh Networks. In Proceedings of 51st Annual Hawaii International Conference on System Sciences (HICSS 2018), IEEE.

[6] Ratcliffe, J 2003. Intelligence-led policing. Trends & Issues in Crime and Criminal Justice 248, pp. 1–6