Introduction to The Science and Engineering of Cyber Systems Minitrack: Evolving Future Cyber Solutions

Chad Bollmann, John Roth, and James Scrofani
Department of Electrical and Computer Engineering
Naval Postgraduate School, Monterey, CA, USA
{cabollma, jdroth, and jwscrofa}@nps.edu

Abstract

Cyber security is a multi-functionary area of practice; effective solutions are difficult because of the diverse range of expertise required and the impact of fallible humans. The impact and number of successful attacks grows every year even while cyber security spending grows at a double-digit annual rate. To fundamentally improve the state of cyber security, research must consider cross-disciplinary techniques and investigate novel paths; incremental progress is unlikely to fundamentally improve the state of the practice.

1. Introduction

“Cyber” is a loaded word that continually evolves, much like the multi-functionary combination of disciplines to which it applies. Effective cyber security solutions must account for diverse as well as practical considerations, so useful research must harness insights from multiple disciplines and offer a path towards solutions vice admiring problems. To address the evolving nature of cyber, novel research must be willing to consider unusual approaches and be willing to challenge accepted “truths”.

2. Minitrack Papers

The papers in this minitrack apply the principles of scientific inquiry or engineering to diverse aspects of cyber security, answering our calls for the unusual and practical.

Through re-examining the mathematical foundations of Turing computation, Fiske challenges the acceptance of status quo implementations of hardware and software that can lead to stability problems [1]. Instabilities manifest as “bugs” that can be exploited by attackers to hijack benign processes. Fiske presents novel directions for future research that could address foundational computing flaws that are the cause of many current security issues.

Kanth et al. develop a proof-of-concept solution that leverages Ethereum blockchain technology to protect system logs [2]. Logs provide a record of processes and actions upon which most modern security systems and forensics methods depend; advanced attackers will alter logs after gaining control of a system to hide their actions or obfuscate their intentions.

Finally, accounting for the real-world implications of periodically-deployed and air-gapped computing systems as well as limited pools of highly-skilled technology workers, Plot et al. develop a prototype automated security scanning tool [3]. Their work provides a thorough review of current security solutions and develops an expandable, open-source alternative controlled through a graphical user interface.

3. Future Directions

As these three papers show, we must challenge *insecurity* from multiple directions through considering theoretical foundations, novel technologies, and real-world limitations.

While effective cyber security solutions must be practical and multi-functionary, achieving this end state requires theoretical, conceptual, tutorial, and descriptive research stepping stones. Additionally, in rapidly-evolving fields there is a constant need for the consolidation of previous work into state-of-the-practice chunks that are digestible.

A partial list of continuing topics of interest to this minitrack and cyber security in general includes:

1. Preliminary results in cutting-edge, high-risk, high-reward cyber research
2. Cross-disciplinary approaches solutions
3. Human-machine interaction optimization
4. Scalable blockchain solutions

URI: https://hdl.handle.net/10125/64561
978-0-9981331-3-3

5. Big data
6. Artificial and augmented intelligence security agents
7. Traditional and predictive analytics
8. Security and risk modeling and simulation
9. Privacy and security
10. System adaptation, organization, optimization, and resilience

The challenges will continue to evolve; so must our research and methodology.

References

[1] M. S. Fiske, "Toward a mathematical understanding of the malware problem," in *Proceedings of the 53rd Hawaii International Conference on System Sciences, Wailea, Hawaii, USA, January 7 – 10, 2020.*

[2] V. Kanth, A. McAbee, M. Tummala, and J. C. McEachen, "Collaborative intrusion detection leveraging blockchain and pluggable authentication modules," in *Proceedings of the 53rd Hawaii International Conference on System Sciences, Wailea, Hawaii, USA, January 7 – 10, 2020.*

[3] J. Plot, A. Shaffer, and G. Singh, "Cartt: Cyber automated red team tool," in *Proceedings of the 53rd Hawaii International Conference on System Sciences, Wailea, Hawaii, USA, January 7 – 10, 2020.*