Cyber Systems – Their Science, Engineering, and Security Minitrack: Evolving Future Cyber Solutions

Chad Bollmann^, John Roth^, James Scrofani^, and Britta Hale*
^Department of Electrical and Computer Engineering
*Department of Computer Science
Naval Postgraduate School, Monterey, CA, USA
{cabollma, jdroth, jwscrofa, britta.hale}@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 involvement 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 attacks that we attempt to prevent. In 2020, just like 2019, the scale and population of successful attacks against cyber systems increased year-over-year. From an application perspective, reported vulnerabilities are now being weaponized in hours and days, and attack automation will continue to shrink this timeline. From a systemic health perspective, key services from internet giants such as Amazon and Microsoft were disabled by attacks for prolonged periods of time.

The practice of cyber is constantly-evolving as well, partially due to the increasing diversity of sub-systems connected to the Internet. The first widespread 5G implementations are being connected, which will pave the way in future years for massive industrial-internet-of-things (IIoT) deployments and increased reliance on low-latency, virtualized, edge-based applications.

To address this constant evolution, novel research must be willing to consider unusual approaches and be willing to challenge accepted "truths". As the field broadens, Research must also seek and integrate insights from other disciplines. And to mitigate the vulnerabilities added by connecting new services and systems (e.g., IIoT, 5G, critical infrasturce), cyber research should identify and develop new areas of practice.

2. Minitrack Papers

The papers in this minitrack apply the principles of scientific inquiry or engineering to diverse aspects of cyber security. Many have answered our call for re-examinations of typical approaches.

For instance, Safar et al. develop an immunological graph-based approach to detect self-propagating malware (e.g., worms such as *Blaster* and *WannaCry*) [1]. The authors leverage spectral graph theory and develop the strong node concept to measure the effects of a phantom node on network connectivity, permitting detection of worm propagation and identification of infected nodes. Using a combination of real-world network data and injected attacks, their MATLAB simulations show that their algorithm can detect 100% of infections between 1 – 6 seconds after a worm begins to spread from a compromised device.

Siebach and Giboney challenge the status quo architecture of authorization systems with their *Abacus* [2]. Their proposed system uses policies and attributes vice roles and groups and a push-centric approach to improve authorization accuracy and reduce latency. The authors have refined their system through real-world deployment and we hope for an update regarding lessons learned and best practices at HICSS 2022.

Through advancing a new methodology for quantifying cyber resilience, Llansó and McNeil address under-examined metrics essential to the effective practice of cyber defense [3]. Tying key organizational functions to assets and threat vectors, the authors propose a *systemic* assessment tool that advances the state of the practice and has potential to guide a defender's security design and response to both intentional and inadvertent cyber incidents. Organizations have limited budgets, and rigorous methods for the assessment and evaluation of resilience

URI: https://hdl.handle.net/10125/71465
978-0-9981331-4-0

are essential to making investments and decisions that mitigate the impacts of future cyber events.

Analyzing malware in a virtual environment (i.e., sandbox) is a key technique for identifying vulnerabilities and developing security patches. However, advanced malware can include protective functions designed to sense virtualization artifacts and change behavior when a sandbox is sensed. Norine et al. propose *smokescreen* [4], a proof-of-concept algorithm to deceive malware attempting to detect virtual environment artifacts such as temperature. The authors show that *smokescreen* intercepts a specific system call while incurring limited computational overhead (which could be an artifact in itself).

Finally, leveraging new signal propagation characteristics available with 5G (e.g., sparse channel state information), St. Germain and Kragh propose a novel physical layer method to increase mobile communications security and privacy [5]. Their approach uses a semi-supervised generative adversarial network to identify spoofing attempts based only on a device location's effect on channel state information. The proposed solution demonstrates very high accuracy at separations as little as 10 cm using MATLAB simulation and the DeepMIMO dataset.

3. Future Directions

Going forward, researchers should continue to challenge *insecurity* by examining theoretical foundations, novel technologies, and real-world limitations from different directions and with fresh sets of eyes.

Effective cyber security solutions require theoretical, conceptual, tutorial, and descriptive stepping stones. Additionally, in rapidly-evolving fields there is a constant need for the consolidation of previous work into state-of-the-practice meta-analyses that are digestible. Those types of papers will be of continuing interest to this minitrack, as will these more specific topics:

1. Preliminary results in cutting-edge, high-risk, high-reward cyber research
2. Cross-disciplinary approaches to cyber security
3. Cryptography, privacy, and security
4. Artificial and augmented intelligence
5. Traditional and predictive analytics
6. Modeling and simulation of cyber systems and risk
7. Software technology applications to cyber systems
8. Human-machine interaction and optimization
9. Data science and big data solutions
10. Securing the cloud
11. Cyber system adaptation, organization, and resilience

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

References

[1] J. L. Safar, M. Tummala, and J. C. McEachen, "Spectral graph-based cyber worm detection using phantom components and strong node concept," in *Proceedings of the 54th Hawaii International Conference on System Sciences, Koloa, Hawaii, USA, January 5 – 8, 2021.*

[2] J. A. Siebach and J. S. Giboney, "The abacus: A new architecture for policy-based authorization," in *Proceedings of the 54th Hawaii International Conference on System Sciences, Koloa, Hawaii, USA, January 5 – 8, 2021.*

[3] T. Llansó and M. McNeil, "Towards an organizationally-relevant quantification of cyber resilience," in *Proceedings of the 54th Hawaii International Conference on System Sciences, Koloa, Hawaii, USA, January 5 – 8, 2021.*

[4] C. Norine, A. Shaffer, and G. Singh, "Artifact mitigation in high-fidelity hypervisors," in *Proceedings of the 54th Hawaii International Conference on System Sciences, Koloa, Hawaii, USA, January 5 – 8, 2021.*

[5] K. St. Germain and F. Kragh, "Multi-subcarrier physical layer authentication using channel state information and deep learning," in *Proceedings of the 54th Hawaii International Conference on System Sciences, Koloa, Hawaii, USA, January 5 – 8, 2021.*