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

Chad Bollmann^, James Scrofani^, and Britta Hale*
^Department of Electrical and Computer Engineering
*Department of Computer Science
Naval Postgraduate School, Monterey, CA, USA
{cabollma, jwscrofa, britta.hale}@nps.edu

## Abstract

*There is tremendous pressure to build and operate cyber systems ever-faster and at increasing scales to meet the demands of growing populations. Thus, we continue to increase the number and role of critical systems connected to a kluged and insecure Internet architecture. But cyber systems are a multi-functionary areas of practice, so secure and resilient methods of scaling are difficult because of the diverse range of expertise required and the involvement of fallible humans. To fundamentally improve the state of cybersecurity, research must consider cross-disciplinary techniques and investigate novel paths; incremental progress is unlikely to fundamentally improve the state of the practice.*

## 1. Introduction

This mini-track continues to evolve, much like the "organism" it attempts to improve. As 5G becomes present and Beyond 5G is appearing on the horizon, humans are proposing to connect themselves constantly to the Internet and delegate increasing amounts of responsibility to cyber systems. Vehicles, sleep trackers, autonomous systems: They all propose to transport, influence, or protect and serve our lives, but now in (near) real-time. At the same time, these applications all depend on us as scientists and engineer to make them more secure, more reliable, and faster.

Experimentation on and engineering of cyber systems is the focus of this minitrack, and we are continually seeking novel, rigorous research which evolves with the leading edge of the converging technologies that form cyberspace. Certain technologies require incremental refinement to accommodate new applications and improve performance while ensuring backwards compatibility. But to radically change the status quo, which is required to "fix" security (and numerous other problems), researchers must be willing to consider non-traditional approaches and challenge paradigms that persist from things that *used* to be true, such as millimeter wave and autonomy.

## 2. Minitrack Papers

This year's papers, along with unaccepted submissions, ran the gamut from fundamental hardware security improvements to privacy protection to service improvement. Key themes of this year's accepted papers were a rigorous design process as well as the use and analysis of experiments to validate the proposed solutions.

In the area of security, Das et al. propose an enhancement to the Honeywords project to improve security through cyber deception [1]. The authors leverage Merkle trees with a novel implementation algorithm to expand the population of deceptive password hashes in a server database while halving the required storage space and roughly maintaining computational overhead. Anadalibi et al., our best paper nominee, design and validate an algorithm to anonymize browser fingerprints in order to protect online privacy [2]. They propose and evaluate multiple anonymization methods against spoofing detection (i.e., de-anonymization) algorithms in order to identify the optimal algorithm in terms of both anonymity and impersonation (of a human). Anyone capturing a trace of the spurious DNS connections made when they open a Facebook or Gmail page, for instance, realizes this a pressing concern.

In terms of automation, Canan et al. explore the use of probability theory to improve the interaction between humans and artificial intelligence (AI) machine agents [3]. By developing a methodology to quantify the information gain from human-machine interactions, they attempt to show the potential utility of quantum probability theory to reduce uncertainty and make human-machine interaction more successful. Riley et al. attempt to improve the adaptation and self-organization capabilities of fleets of unmanned aerial systems (i.e., drones) to solve complex field problems [4]. In a proven

URI: https://hdl.handle.net/10125/80255
978-0-9981331-5-7

modeling environment, they show that their proposed learning models can increase expected success rates by more than 20%, even under adverse conditions. Similarly, Moghaddam et al. assess the ability to improve quality-of-service through enhanced adaptive control architectures in smart (electrical) grids [5]. They test their approach to minimizing over-current situations on a physical smart grid and find that their experimental scheme reduces response time to unsafe situations, typically by 18 – 52%.

Finally, to enable cyber systems at scale, the performance of distributed systems (e.g., IoT/IIoT) must be improved through adaptation. Middleware, which permits centralized, homogeneous systems to interact with heterogeneous devices, is essential to the rapid and resilient operation of distributed systems. Brandão and Rosa extend an existing middleware framework with additional transport and application layer protocols to add security, functionality, and adaptability [6]. Their tests show that the proposed gMidArch framework adds flexibility while improving response time under both low and high processing loads as compared to common existing frameworks.

## 3. Future Directions

Going forward, it is our job as researchers to challenge cyber system insecurity and fragility by examining theoretical foundations, novel technologies, and real-world limitations from different directions and with fresh sets of eyes.

We will continue to emphasize this core attribute going forward, and expect the minitrack's future papers to advance the state of cyber systems practice through rigorous experimental design, execution, and analysis of results. Dykstra provides an excellent overview of cyber experiment design and execution, including examples [7].

Papers pushing boundaries through testable hypotheses will be of continuing interest to this minitrack, particularly in the following areas:

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. Autonomous networked systems and sensors
5. Implementations of edge intelligence
6. Modeling and simulation of cyber systems and risk
7. Software technology applications to cyber systems including next-generation network and security protocols
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] K. Das, J. Jafarian, E. Dincelli, E. Gethner, and T. Bekman, "Honeytree: Making honeywords sweeter," in *Proceedings of the 55th Hawaii International Conference on System Sciences, Lahaina, Hawaii, USA, January 3 – 7, 2022.*

[2] V. Andalibi, E. Azer, and L. J. Camp, "Criteria and analysis for human-centered browser fingerprinting countermeasures," in *Proceedings of the 55th Hawaii International Conference on System Sciences, Lahaina, Hawaii, USA, January 3 – 7, 2022.*

[3] M. Canan, M. Demir, and S. Kovacic, "A probabilistic perspective of human-machine interaction," in *Proceedings of the 55th Hawaii International Conference on System Sciences, Lahaina, Hawaii, USA, January 3 – 7, 2022.*

[4] I. Riley, B. McKinney, and R. F. Gamble, "Improving the expected performance of self-organization in a collective adaptive system of drones using stochastic multiplayer games," in *Proceedings of the 55th Hawaii International Conference on System Sciences, Lahaina, Hawaii, USA, January 3 – 7, 2022.*

[5] M. Moghaddam, E. Rutten, and G. Giraud, "Hierarchical control for self-adaptive iot systems: A constraint programming-based adaptation approach," in *Proceedings of the 55th Hawaii International Conference on System Sciences, Lahaina, Hawaii, USA, January 3 – 7, 2022.*

[6] D. C. Brandão and N. S. Rosa, "Multiple transport protocols in an adpative rpc-based framework," in *Proceedings of the 55th Hawaii International Conference on System Sciences, Lahaina, Hawaii, USA, January 3 – 7, 2022.*

[7] J. Dykstra, *Essential cybersecurity science: build, test, and evaluate secure systems*. O'Reilly Media, Inc., 2015.