UNIVERSITY OF CALIFORNIA, IRVINE

BERKELEY · DAVIS · IRVINE · LOS ANGELES · MERCED · RIVERSIDE · SAN DIEGO · SAN FRANCISCO   SANTA BARBARA · SANTA CRUZ

DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
3436 ENGINEERING HALL
IRVINE, CALIFORNIA 92697-2625

PHONE: (949) 824-8147
EMAIL: yshoukry@uci.edu
April 15, 2023

Dear Evaluation Committee,

It is with great pleasure that I nominate the paper named "A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music", which is published in ACM CCS, 2022 for the 11th Annual Best Scientific Cybersecurity Paper Competition. I am providing below the scientific contribution of the paper and explaining why this paper merits the award in point-by-point fashion.

- The nominated paper demonstrates how an attacker can disrupt the normal behavior of a negative pressure room (NPR) by using simple music that may lead to leak of pathogens from a bio-safety labs or infectious hospitals. This unconventional attack model brings attention to the critical importance of bioweapon and bioterrorism preparedness, particularly in the post-COVID era. The paper effectively demonstrates how an attacker could target the differential pressure sensors within an NPR, potentially resulting in the spread of infectious diseases. Overall, the findings underscore the pressing need for increased vigilance and security measures in safeguarding against such threats to national security.

- The technical contribution of this paper is significant and insightful. The authors have discovered that the differential pressure sensors commonly used in negative pressure rooms possess resonant frequencies within the audible range. This finding is quite important in a sense that the attacker can use these resonance frequencies to design malicious music to create resonance in differential pressure sensors, resulting in an overshooting in the differential pressure sensor's normal pressure readings. This overshooting in the differential pressure sensors reading can fool the building management systems (BMSs) so that the negative pressure room turns its negative pressure to a positive one, creating an environment for a potential leak of deadly microbes from negative pressure rooms. By highlighting the potential for deadly microbes to leak from negative pressure rooms, the paper draws attention to the critical need for robust security measures to protect public health and safety.

- Last of all, which is the most important, this paper shows that the attacker can adversarially control the forged pressure in differential pressure sensors by using the malicious music. Moreover, this paper also shows that the attacker can also simultaneously attack multiple negative pressure rooms in a facility just by attacking a single differential pressure sensor. This concept makes the attack model of the paper stronger compered to attacking a single negative pressure room.

Given the critical insights outlined in this paper, this paper is very relevant for today's safety-critical systems where unorthodox attack can happen in the physical domain that could compromise the cyber domain. With the rise of sophisticated cyber threats, the findings of this study provide valuable information that can help to safeguard against potential security breaches. Based on its significant contributions, I strongly believe that this paper deserves to be considered as a top contender in the Cybersecurity Paper Competition. Therefore, I am honored to nominate this paper for your careful consideration.

Sincerely,

Yasser Shoukry
Assistant Professor
Resilient Cyber-Physical Systems Lab
EECS, University of California, Irvine

Brief Bio: Yasser Shoukry is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of California, Irvine where he leads the Resilient Cyber-Physical Systems Lab. Before joining UCI, he spent two years as an assistant professor at the University of Maryland, College Park. He received his Ph.D. in Electrical Engineering from the University of California, Los Angeles in 2015. Between September 2015 and July 2017, Yasser was a joint postdoctoral researcher at UC Berkeley, UCLA, and UPenn. His current research focuses on the design and implementation of resilient, AI-enabled, cyber-physical systems and IoT. His work in this domain was recognized by the Early Career Award from the IEEE Technical Committee on Cyber-Physical Systems in 2021, the NSF CAREER Award in 2019, the Best Demo Award from the International Conference on Information Processing in Sensor Networks (IPSN) in 2017, the Best Paper Award from the International Conference on Cyber-Physical Systems (ICCPS) in 2016, and the Distinguished Dissertation Award from UCLA EE department in 2016. In 2015, he led the UCLA/Caltech/CMU team to win the NSF Early Career Investigators (NSF-ECI) research challenge. His team represented the NSF- ECI in the NIST Global Cities Technology Challenge, an initiative designed to advance the deployment of Internet of Things (IoT) technologies within a smart city. He is also the recipient of the 2019 George Corcoran Memorial Award from the University of Maryland for his contributions to teaching and educational leadership in the field of CPS and IoT.