HUMAN-OUT-OF-THE-LOOP SWARM-BASED IOT NETWORK PENETRATION TESTING BY IOT DEVICES

Thomas Schiller

School of Modeling Simulation and Training
University of Central Florida
3100 Technology Pkwy
Orlando, FL, USA
schiller@knights.ucf.edu

Sean Mondesire

Institute for Simulation and Training
University of Central Florida
3100 Technology Pkwy
Orlando, FL, USA
sean.mondesire@ucf.edu

EXTENDED ABSTRACT

Technology and digital-based services are an integral part of today's life to personal and business networks. One of these networks gained attention in the last years due to its growth rate: networks of Internet-of-Things (IoT) devices. A smart home network is expected to consist of over 30 devices per person by 2030. (Al-Sarawi et al. 2020)

On the one hand, IoT devices in such environments are prone to cyber-attacks and can be a security risk. (e.g., Neshenko et al. 2019, Florez Cardenas, Mateo and Acar, Gabriel 2021) Penetration testing (pen-testing) is one way to deal with such a risk and to test IoT devices for possible vulnerabilities. On the other hand, IoT devices, such as in smart home environments, are often computationally capable. Smart TVs or smart fridges, as examples, are equivalent in computational power to micocomputers like a Raspberry Pi. Further, they often run fully functional operating systems, which makes them capable of running state-of-the-art network services and actions. These two aspects combined make IoT devices possible targets for attacks and actors of security pen-testing simultaneously. Using IoT devices as pen-testing devices appears feasible in view of the fact that IoT devices in a smart home are often only used for a fraction of a time and could use spare computational power for other tasks. An example would be a smart washing machine which is only used for a few hours a week and is idle for the rest of the time.

Traditionally, pen-testing is a highly structured and human-based activity. (Shebli and Beheshti 2018) Aspects of pen-testing can be automated. However, human-in-the-loop and human-on-the-loop are the standards for pen-testing scenarios. Human-out-of-the-loop and, therefore, autonomous pen testing is done in research environments but still in an early state (e.g. Standen, Maxwell and Lucas, Martin and Bowman, David and Richer, Toby J. and Kim, Junae and Marriott, Damian 2021, Campbell 2022). Research gaps are the multi-agent for swarm-based pen-testing and pen-testing by IoT devices themselves. This work-in-progress will target this gap and evaluate the feasibility and performance of swarm-based pen-testing of IoT devices by IoT devices.

To conduct this research, a network simulator is currently in development. This constructive multi-agent simulator will be published under MIT license and is also used by other research currently in progress. The simulator can simulate a network of agents (network devices) with a simplified pen-testing action space. Agents can detect active devices, open ports, and active services in the network and perform pen-testing ac-

ANNSIM'23, May 23-26, 2023, Mohawk College, ON, CANADA; ©2023 Society for Modeling & Simulation International (SCS)

tions on these devices. Detected vulnerabilities are reported to the simulation environment and can be used to analyze applied algorithms and tactics. Currently, the simulator includes a single-agent linear pen-testing agent mimicking human pen-testing behavior and a multi-agent swarm-based pen-testing non-optimized algorithm utilizing queues. A nature-based optimization algorithm utilizing Particle Swarm Optimization (PSO) is in development. This work aims to compare the performance and feasibility of these three algorithms on a simulated smart home /24 subnet network and on the scale of a larger /20 subnet smart building, e.g., an office building. Results so far show the superiority of the queue-based swarm algorithm over the linear pen-testing algorithm and the detection of simulated vulnerabilities on a smart home level for both algorithms.

Near-term, this work can lead to establishing multi-agent and swarm-based distributed pen-testing in research. Long-term, this work can lead to safer smart homes and IoT networks and the use of existing resources to achieve this goal without adding to existing infrastructure and hardware.

Keywords: IoT, penetration testing, swarm, autonomous, cybersecurity

REFERENCES

Al-Sarawi, S., M. Anbar, R. Abdullah, and A. B. Al Hawari. 2020. “Internet of things market analysis forecasts, 2020–2030”. In *2020 fourth world conference on smart trends in systems, security and sustainability (WorldS4)*, pp. 449–453.

Campbell, R. G. 2022, May. *Autonomous Network Defence Using Multi-Agent Reinforcement Learning and Self-Play*. Master of Science, San Jose State University, San Jose, CA, USA.

Florez Cardenas, Mateo and Acar, Gabriel 2021. “Ethical Hacking of a Smart Fridge : Evaluating the cybersecurity of an IoT device through gray box hacking”. Backup Publisher: KTH, School of Electrical Engineering and Computer Science (EECS) Issue: 2021:451 Pages: 46 Series: TRITA-EECS-EX.

Neshenko, N., E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. 2019. “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations”. *IEEE Communications Surveys & Tutorials* vol. 21 (3), pp. 2702–2733.

Shebli, H. M. Z. A., and B. D. Beheshti. 2018, May. “A study on penetration testing process and tools”. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pp. 1–7. Farmingdale, NY, IEEE.

Standen, Maxwell and Lucas, Martin and Bowman, David and Richer, Toby J. and Kim, Junae and Marriott, Damian 2021, August. “CybORG: A Gym for the Development of Autonomous Cyber Agents”. arXiv:2108.09118 [cs].

AUTHOR BIOGRAPHIES

THOMAS SCHILLER, M.A. is an active member of the German Armed Forces and a 2nd-year student of Modeling and Simulation (MS) at the School of Modeling Simulation and Training at the University of Central Florida (UCF). His research interest is in cybersecurity and military simulation. His email address is schiller@knights.ucf.edu.

SEAN MONDESIRE, PH.D. is an Assistant Research Professor of Big Data Analytics and Cybersecurity at the University of Central Florida’s (UCF) Institute of Simulation and Training. His research specialties are machine learning and big data analytics, focusing on autonomous decision-making, high-performance computing for simulation-based training and education, and predictive modeling of large-scale, dynamic systems. His email address is sean.mondesire@ucf.edu.