Cybersecurity Methodology for Specialized Behavior Analysis

Edgar Padilla[1(✉)], Jaime C. Acosta[2], and Christopher D. Kiekintveld[1]

[1] The University of Texas at El Paso, El Paso, TX 79968, USA
e-padilla@live.com
[2] CCDC Army Research Laboratory, Adelphi, MD 20783, USA

Abstract. Analyzing attacker behavior and generating realistic models to accurately capture the realities of cybersecurity threats is a very challenging task for researchers. Psychological personality and profiling studies provide a broad understanding of personality traits, but lack a level of interactive immersion that enables observers to collect concrete cybersecurity-relevant behavioral data. Participant's intricate actions and interactions with real computer systems are seldom captured in any cybersecurity studies. Our work focuses on capturing human actions and decisions to provide an empirical basis for these types of models. We provide a practical methodology that helps bridge the gap between theory and practice by facilitating construction, experimentation, and data collection for repeatable and scalable human experimentation with realistic cybersecurity scenarios. While our methodology is platform agnostic, we describe state of the art technologies that may be used to satisfy the objectives of each of the stages of the methodology.

Keywords: Cybersecurity · Attacker profiling · Methodology

1 Introduction

Prevailing literature on cybersecurity behavioral analysis is limited to basic psychological profiles. Although there is an abundance of work related to behavioral analysis and personality profiling in psychology, these works mainly focus on profiling attackers using the results of surveys taken by non-technical participants [1]. Most of these studies originate from speculative actions and responses to questions. Participants are typically drawn from Amazon Mechanical Turk (AMT), in which the target population does not possess technical or cybersecurity training and qualifications [1–3]. The resulting datasets and models built from these studies fail to capture interactions of attackers and defenders with real systems and networks.

Presently, cybersecurity datasets that enable analysis and model generation are incomplete or unavailable. This is in part due to the sensitive nature of forensic data resulting in non-releasable information associated with real attacks [4].

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2021
Published by Springer Nature Switzerland AG 2021. All Rights Reserved
S. Goel et al. (Eds.): ICDF2C 2020, LNICST 351, pp. 237–243, 2021.
https://doi.org/10.1007/978-3-030-68734-2_14

After compromise, organizations do not commonly publish details about incidents risking it could lead to loss of revenue [5]. If released, datasets are altered e.g., removed network packet payloads and anonymization. This may result in loss of valuable information for researchers [6]. Frequently these datasets do not contain ground truth such as tools and configurations employed. Furthermore, participants' technical proficiency, psychological characteristics, and demographic information is often not documented or made available.

Our approach combines solutions to the shortcomings presented in psychology and computer forensics when compiling experimental data. In summary, our work described here brings forth the following objectives:

1. Guidelines for valid and experimental datasets that are aimed at bridging the gap between technical experiments and psychological profiling by enabling the generation of an effective dataset.
2. A mechanism that incorporates elevating participants' technical skills, which can be expensive and difficult to recruit otherwise.
3. While the methodology is platform agnostic, we provide a set of state-of-the-art tools and frameworks that can be used to implement a system to meet the research objectives.

2 Related Work

An abundant number of psychological studies pursue to profile cybersecurity attackers based on high-level traits. These profiles include motivation, personality traits, and propensity to commit a crime among others. These studies are not technical in nature but directed towards technical participants [5,7]. Most models developed from these studies are built from answers to hypothetical questions in an attempt to characterize participants [1]. Nonetheless, hypothetical answers may not capture participant actions when interacting with real computer systems. Our methodology aims on capturing these key missing interactions.

In McClain et al., an experimental procedure is presented similar to our research method where participants are trained and raised to a proficiency level before conducting a technical experiment. These experiments generate datasets that capture detailed interactions between participants and computer systems including keystrokes, network traffic, and process trees [8]. Nonetheless, their approach does not scale well. A preliminary implementation of this methodology allows a large number of remote participants using a web browser. Similarly, Acosta et al. also developed a novel data collection system, ECEL, and platform for hosting exercises focused on penetration testing and other cybersecurity analyst tasks [9]. Our approach is similar to [8,10], however we refrain from educating participants with live instructors. This approach may lead to inconsistent teaching across the sample population.

3 Methodology Design

We developed a methodology that improves upon prevailing mechanisms for collecting human behavioral information such as AMT. Existing methods do not

capture interactions between cybersecurity experts and information systems. We propose bridging this gap by targeting participants with minimal technical background. These participants are trained to fulfill the particular needs of an experiment. A well-tuned experimental setup and trained participants, we believe, can compensate for the need of experienced and expensive ones. This novel cybersecurity methodology consists of five stages: Questionnaires, Theoretical Education, Practical Education, Experimentation, and Model Creation/Validation (See Fig. 1).

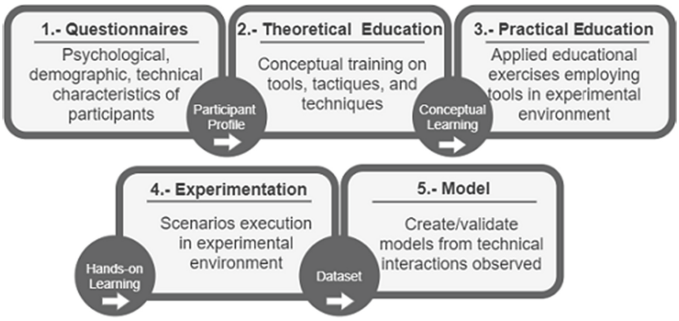

Fig. 1. Five-stage methodology for training, experimenting, and collecting technical cybersecurity data.

3.1 Questionnaires

A fundamental stage in our methodology is to collect participants' ground truth. With these questionnaires, researchers can inquire about psychological, demographic, and similar characteristics. This facilitates capturing participant inherent features to build robust participants' profiles [1]. This is not intended to inquire about any hypothetical actions an attacker or defender might carry out.

3.2 Theoretical Education

Education is a critical stage in our methodology. During this stage, researchers can recruit participants with basic cybersecurity knowledge and then train them on specific concepts, tasks, and tools employed during an experiment. Even though we work with novice participants, they can provide powerful insights into human behavior such as propensity towards certain actions. This involves their cognitive processes of selection across multiple alternatives including spontaneous actions and reactions [11]. Our methodology does not serve the purpose of gathering data from domain experts, but instead looks at human behavior such as decision making on scenarios with high technical complexity. We elevate the participants' skill level required for a technical study as opposed to simplifying an experiment and considerably diminishing its impact and relevance

of its findings. This allows researchers to abstain from formulating assumptions where participants are asked hypothetical or abstract questions and consequently obtain hypothetical and high level answers that are later unrealistically mapped to higher complexities in real-world scenarios. Instead, we gather information from informed beginners connected to the cybersecurity domain such Computer Science students and IT professionals, and turn them into qualified participants.

3.3 Practical Education

Our methodology emphasizes an educational model where practical instruction is a cornerstone for learning cybersecurity. Practical education ought to be directed toward aiding participants to improve understanding of concepts and tools. Complementing integration of theoretical concepts and development of practical experience to reinforce learning in preparation for an experiment. This stage promotes practical teaching of cybersecurity at an operational level [12].

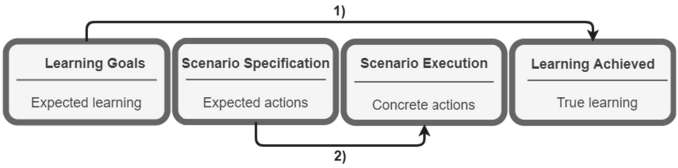

Fig. 2. Relationship between 1) theoretical and 2) practical learning effectiveness with respect to their anticipated outcomes.

We adapted Millar and Abrahams [10] stages of teaching and learning effectiveness for cybersecurity tasks and scenarios into four stages: Learning Goals, Scenario Specification, Scenario Execution, and Learning Achieved (See Fig. 2). The *Learning Goals* stage aims to clearly define the scope of the learning plan. Artifact design ought to be driven by type of expected audience, technical complexity, and experiment's goals. Interactive content, videos, and supplemental lesson notes can be options for effective learning artifacts. Next, the *Scenario Specification* stage defines the desirable tactics and techniques participants should follow during an experiment. Scenario configurations are meticulously defined and act as the authoritative source of content for the practical education section of this paper. Practical exercises must be designed to complement theoretical education to achieve a comprehensive grasp of concepts. *Scenario Execution* is concerned with the actual actions performed by participants during an experiment. These actions are the result of the quality of educational methods, particularly practical education leading up to this stage. Also, actions are influenced by the experiment's design and complexity, as well as the performance metrics known to participants. Finally, *Learning Achieved* is the credible learning attained. We measure practical education effectiveness contrasting intended

activities (Scenario Specification) and actual activities performed by participants (Scenario Execution). Similarly, we compare Learning Goals with Learning Achieved to assess effectiveness of theoretical learning [13]. For our experimentation methodology, we are primarily interested in the relationship between Scenario Specification and Scenario Execution. Learning efforts are centered on short term goals addressing technical requirements allowing participants to competently progress through the experimental scenarios. Theoretical lessons and practical activities must be constantly evaluated employing small focus groups to measure their effectiveness where revisions must trigger an increase in learning performance [13].

3.4 Implementation and Experimentation

At present time, availability of valid, complete, and labeled cybersecurity data constraint research efforts. This unmet data demand raises the need for experimental frameworks and testbeds that accurately emulate cybersecurity scenarios. Nonetheless, sophisticated testbeds are complex and expensive to build. For this reason, during the scenario design time, deciding on implementation options such as emulation versus simulation is of the utmost importance. On the one hand, simulations only reproduce external visible behavior from a model. This is more efficient and inexpensive, but fails to capture low level interactions. On the other hand, emulation do reproduce low level interactions. Emulation increases system development and complexity, in addition to greater computational resources. Nonetheless, emulation allows a more comprehensive experimental settings where forensic level interactions can be recorded and analyzed. Sandia National Laboratory developed a cyber-physical testbed that combines simulation and emulation in an attempt to alleviate implementation costs [14].

Our methodology lays novel groundwork for an experimental framework. We propose tools for accessibility, portability, and scalability of a framework. Complex technical studies may require human subjects to be physically present for training and participation [10]. Similar to AMT, a web-based tool, we propose Apache Guacamole to increase accessibility to participants. Moreover, we propose the Common Open Research Emulator (CORE) as the center of our experimental environment. CORE facilitates the creation of network scenarios and supports connecting emulated networks seamlessly to real ones [15].

3.5 Model Creation/Validation

The final stage in this methodology is to create and validate new or existing models from the experimental data collected. The goal of decision-making models is to reasonably predict actions from cybersecurity actors. Performance metrics must be defined to evaluate the validity of models [16]. Models are not expected to always be correct, but as complexity increases, must yield reasonable answers to our questions. [17]. This stage is open to any research area, such as psychology and mathematics, to create and validate their own models.

4 Conclusions and Future Work

A central issue for developing realistic models is data availability revolving around the human aspects of decision-making in a valid cybersecurity context.

Existing data does not provide context for researchers to account for cybersecurity actor's intentions, technical skills, psychological traits, and demographics. Additionally, predominant research methods do not capture realistic interactions among cybersecurity actors. Similarly to the scarcity of valid data, cybersecurity professionals are difficult to find and expensive to recruit when conducting technical studies.

We have defined a five-stage methodology that works around inadequate sources of qualified cybersecurity participants. Our methodology elevates the skills of novice technical students and professionals to an acceptable proficiency turning them into more suitable participants. This leveling enables participants to complete realistic exercises using tools and techniques that mimic those used by field professionals.

Moreover, we recommend tools and software, laying the groundwork for an experimental framework and testbed. We believe it is well-suited for experiments that observe decision-making phenomena, not skill level, associated with humans in technical environments.

Future work involves validating this methodology with a larger pool of participants in a formal setting. We also plan to perform a study and collect associated data to determine what human factors influence decision making, at the reconnaissance phase, when scanning a computer network. An in-depth analysis will involve extrapolation of salient features and patterns in the data.

Acknowledgement. This research was sponsored by the U.S. Army Combat Capabilities Development Command Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Combat Capabilities Development Command Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

References

1. Gaia, J., et al.: Psychological profiling of hacking potential. In: Proceedings of the 53rd Hawaii International Conference on System Sciences (2020)
2. Basak, A., et al.: An initial study of targeted personality models in the FlipIt game. In: Bushnell, L., Poovendran, R., Başar, T. (eds.) GameSec 2018. LNCS, vol. 11199, pp. 623–636. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01554-1_36
3. Gutierrez, M., et al.: Evaluating Models of Human Behavior in an Adversarial Multi-Armed Bandit Problem (2019)
4. Abbott, R.G., et al.: Log analysis of cyber security training exercises. Proc. Manufact. **3**, 5088–5094 (2015)

5. Crossler, R.E., et al.: Future directions for behavioral information security research. Comput. Secur. **32**, 90–101 (2013)
6. Shiravi, A., et al.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput. Secur. **31**(3), 357–374 (2012)
7. Seebruck, R.: A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model. Digit. Invest. **14**, 36–45 (2015)
8. McClain, J., et al.: Human performance factors in cyber security forensic analysis. Proc. Manufact. **3**, 5301–5307 (2015)
9. Acosta, J.C., et al.: A platform for evaluator-centric cybersecurity training and data acquisition. In: MILCOM 2017–2017 IEEE Military Communications Conference (MILCOM). IEEE (2017)
10. Abrahams, I., Millar, R.: Does practical work really work? a study of the effectiveness of practical work as a teaching and learning method in school science. Int. J. Sci. Educ. **30**(14), 1945–1969 (2008)
11. Karat, J., Dayton, T.: Practical education for improving software usability. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (1995)
12. Wang, H., et al.: Construction of practical education system for innovative applied talents cultivation under the industry-education integration. In: Proceedings of the 5th International Conference on Frontiers of Educational Technologies (2019)
13. Millar, R., Abrahams, I.: Practical work: making it more effective. School Sci. Rev. **91**(334), 59–64 (2009)
14. Hahn, A., et al.: Cyber-physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans. Smart Grid **4**(2), 847–855 (2013)
15. Networks and Communication Systems Branch. Common Open Research Emulator (CORE) — Networks and Communication Systems Branch. https://www.nrl.navy.mil/itd/ncs/products/core. Accessed 15 April 2020
16. Law, A.M.: How to build valid and credible simulation models. In: 2008 Winter Simulation Conference. IEEE (2008)
17. Sargent, R.G.: Verification and validation of simulation models. In: Proceedings of the 2010 Winter Simulation Conference. IEEE (2010)