THE HACKER IS INSIDE THE COMPANY!

Instance-Based Learning & Its Application to Defend Against Insider Hacking

David Esquivel
Canutillo Independent School District, Canutillo, Texas, United States
davidjr.esquivel39@gmail.com

Shawn Trousdale
Ysleta Independent School District, El Paso, Texas, United States
shawntrousdale@gmail.com

Mohammad Ariful Islam Khan
The University of Texas at El Paso, El Paso, Texas, United States
mkhan16@utep.edu

Palvi Aggarwal
The University of Texas at El Paso, El Paso, Texas, United States
paggarwal@utep.edu

Deepak K. Tosh
The University of Texas at El Paso, El Paso, Texas, United States
dktosh@utep.edu

Abstract

This research was conducted by the authors while participating in the Cybersecurity Research Experience for Educators through Data Science (CREEDS), a Research Experience for Teachers (RET) summer program funded by the U.S. National Science Foundation at the University of Texas at El Paso (UTEP). The work explores the application of Instance-Based Modeling to understand the behavior of cyber attacker in order to ensure better defense. The study simulates the hacker choices among multiple targets with various reward/penalty structures. The fact that the common elements from human decision-making such as cognitive noise and memory decay influences the model has also been discussed. Ultimately, the authors propose strategies on how these techniques can be introduced in high school class rooms in order to make a bridge between advanced cybersecurity research and practical secondary math and computer science curricula.

CCS Concepts

• **Human-centered computing**; • **Human computer interaction (HCI)**; • **HCI theory, concepts and models**;

Keywords

cybersecurity, instance-based learning, cognitive modeling, human factors, high school education

ACM Reference Format:
David Esquivel, Shawn Trousdale, Mohammad Ariful Islam Khan, Palvi Aggarwal, and Deepak K. Tosh. 2024. THE HACKER IS INSIDE THE COMPANY!: Instance-Based Learning & Its Application to Defend Against Insider Hacking. In *The 25th Annual Conference on Information Technology Education (SIGITE '24), October 10–12, 2024, El Paso, TX, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3686852.3687084

SIGITE '24, October 10–12, 2024, El Paso, TX, USA

ACM ISBN 979-8-4007-1106-0/24/10
https://doi.org/10.1145/3686852.3687084

1 INTRODUCTION

Cybersecurity threats, nowadays put modern businesses and government organization in serious risk. Amongst various type of cyber-attacks, insider threats are difficult to detect but causes an institution enormous harm. In this paper, we adopt a novel approach of understanding and mitigating this type of threat by utilizing cognitive modeling approaches. Using cognitive models we have replicated attacker-behavior and thus, provided insights for better defensive strategies. On top of that, this research was conducted as a RET or Research Experience for Teachers and therefore, we shed light on some realistic techniques for introducing the above-mentioned advanced cyber defense methods to make student aware of not only various math and computer science concepts but also such cutting-edge research.

2 INSTANCE-BASED LEARNING MODELS

Recent developments in using instance-based cognitive models [1] to understand and replicate a hacker's behaviors, tendencies, and biases have provided an opportunity to provide defense from cyberattacks, both from outside and inside an organization's network. Cognitive modeling methods involve using Stackelberg Game Theory [2] and Instance-Based Learning. The aim is to maximize security with limited resources and use past instances to influence future actions. A framework is constructed here through straightforward methods to assist in determining factors that affect real-world decision-making.
These models use the following foundational principles:
Instances - An instance consists of situation, decision and utility that occurs at a specific time stamp under certain parameters.
Blended Value, Probability of Retrieval and Activation -The Instance-based Learning Theory or IBLT evaluates the attractiveness of the alternative options based on the results of similar past situations using a mechanism called Blending. All observed outcomes that arise from choosing a particular option are combined into a single blended value for each option. The blended value of option j is denoted as

$$V_j = \sum_{i=1}^{n} p_i x_i \tag{1}$$

where x_i is the value of the perceived outcome and p_i is the probability of retrieval of that outcome from memory. This probability

Table 1: – Target Information

Round	Target 1	Target 2	Target 3	Target 4	Target 5	Target 6
Round 1	[2, −1, 0.22]	[8, −5, 0.51]	[9, −9, 0.42]	[9, −10, 0.40]	[2, −6, 0.08]	[5, −5, 0.36]

indicates the likelihood of retrieving the specific instance from the memory.

Equation 1) demonstrates that an option's blended value is the sum of all observed outcomes (x_i) weighted by their probability of retrieval. Now at any trial t, the probability of retrieval of outcome i is determined by the activation of that outcome, which is represented by

$$P_{i,t} = \frac{e^{A_{i,\frac{t}{\tau}}}}{\sum je^{Aj,t/\bar{\tau}}} \tag{2}$$

where τ is defined as random noise and $\tau = \sigma \cdot \sqrt{2}$, σ is a free noise parameter. Equation 2)'s noise accurately depicts the variability involved in remembering prior events.

Finally, the activation of each outcome in memory depends upon a mechanism from ACT-R ((Adaptive Control of Thought - Rational) [3]. The activation of an outcome in a given trial is a function of the frequency of its occurrence and the time passed since each of these outcomes occurred. At each trial t, activation A of outcome i is

$$A_{i,t} = \sigma \ln\left(\frac{1-\gamma_{i,t}}{\gamma_{i,t}}\right) + MP \sum_{k} \text{sim}\,(v_k, c_k) + \ln \sum_{t_p \in \{1,\cdots,\ t-1\}} \left(t - t_p\right)^{-d} \tag{3}$$

where t_p represents each of the prior trial indexes where the result i was recorded, and d is a free decay parameter, which is a random draw from a uniform distribution limited between 0 and 1. The similarity between current and past instances can be calculated by defining the similarity function ($\text{sim}(v_k, c_k)$).

3 TASK DESCRIPTION

In this task, the IBL based cognitive model was presented with six targets presented in Table 1. Each of the targets had a reward/penalty structure and monitoring probability.

Here, 2, -1, and 0.22 represent the gain, the loss, and the probability. Quantitatively speaking, when a hacker chooses to attack a target or targets, that decision is influenced by the experience of reward and penalty, each varying in degree. Targets with relatively large reward / low penalty outcomes will influence the attacker to attack and vice versa. When paired with a monitoring probability, the attacker develops habits. The experiment was done by implementing a simple binary choice model [4] over a series of trials, and later transitioning it into a multiple-choice task (using PyIBL library in Python [5]). This was done by taking the conditions for two targets and duplicating them for six. Each of the targets was then updated to have a reward/loss structure and monitoring probability. We were able to verify that the model was working by placing a high reward on a target and running the IBL model. The model quickly identified the target and chose it consistently as to show us it knew the valuable target.

4 RESULTS

The results in Figure 1 reflect a modeled attacker's bias over 100 trials based on the selection amongst six targets. The results yield a bias toward selecting the Target B.

Figure 2 shows the effect of increasing noise on target selection. As the noise increases, less distinction in the preference of target selection can be observed. This indicates the randomness in decision-making. Lastly, in figure 3, we see that how the increase in decay impairs the model's inability to recall past success or failure. Higher decay leads to uniform target selection as the model forgets the past experiences more quickly.

5 INFLUENCING SECONDARY MATH & CS EDUCATION

The benefits of utilizing instance-based cognitive modeling to predict human behavior and bias in cybersecurity research (discussed briefly above) are credited to those involved at the highest levels of research. On the other hand, as teachers in the secondary education mathematics and computer science content areas participating in the UTEP's RET program, we began to explore opportunities within the high school classrooms to enhance instruction with newfound knowledge.

The reality that most students face with today's instruction is sometimes a lack of real-world or relevant application in their limited life experience. Even those students who can grasp content at a high-rate face challenges in this context. That being said, Mathematics is one of the courses that can be seen as too abstract for students to comprehend in a real-world situation. Math applications typically center around situations based on something other than the current situations students will see in their lifetime. However, with this project through the CREEDS program, teachers can find a variety of methods to tie into the mathematics classroom. Firstly, in Geometry, computers have a logical computation process. Therefore, spending time coding logic statements using Python to see the effects logic can have on computations is an applicable math skill students would enjoy. Secondly, in Algebra, we refer to various equation types, including exponential, logarithmic, etc. Showing students that IBL models use these basic equations to construct higher computations would allow students to see the applicable side of mathematics. Identifying the key features like growth vs. decay or domain vs. range would enable students to see their learning in action. Finally, the model explores probabilities that are based on an IBL model. Probability is usually for students stuck in the realm of cards and dice, but having a chance to see that probabilities can be calculated for computer models is an excellent learning opportunity. Furthermore, students can see the basic probability rules in action, such as adding up to 1 or being represented in various forms. Overall, the possible applications here are limitless and should be

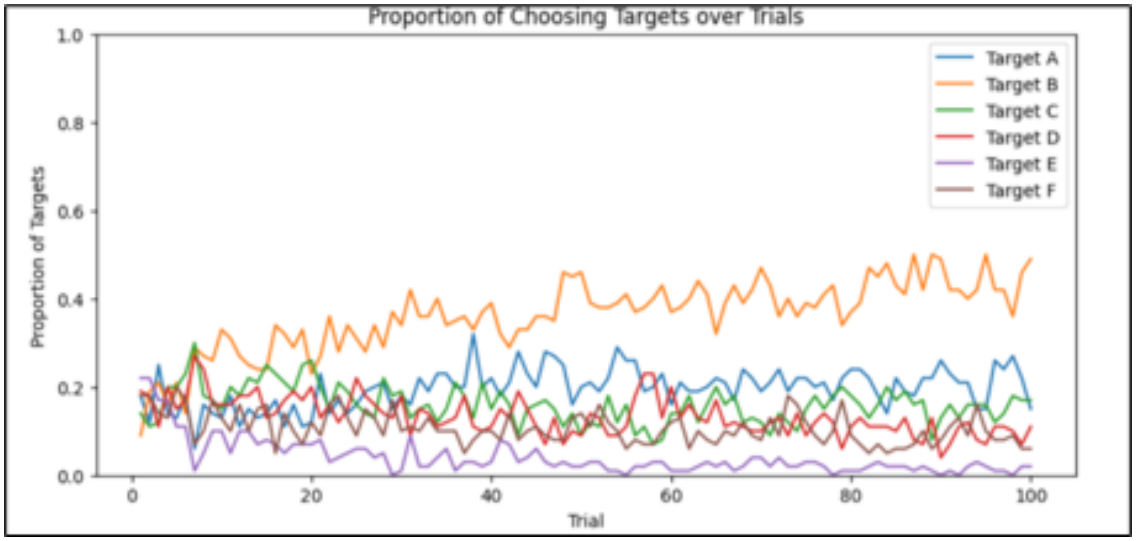

Figure 1: – IBL model action for 100 trials

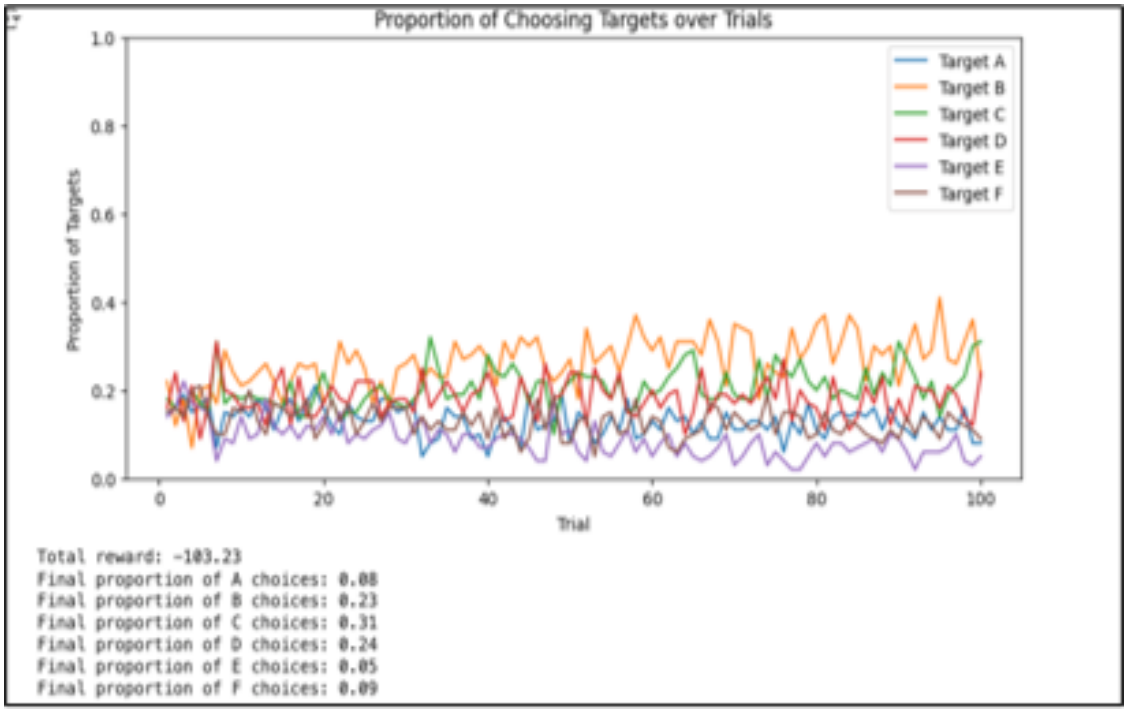

Figure 2: – Impact of noise on the model

dissected by math teachers everywhere to find a piece they can take back to their students.

On the other hand, the Computer Science curriculum in high school settings can challenge the most experienced teachers. Regardless of grade level, students bring varying degrees of self-taught knowledge of varying languages. This fact, paired with an abundance of inconsistency in the level of teacher mastery from campus to campus or even within a particular campus, can generate substantial learning obstacles in the classroom. Many teachers lean heavily on a "canned" curriculum to get through their instruction. Although the results do yield many students mastering beginner to intermediate levels of coding; however, there is a significant number of challenges when students are asked to apply learned skills to real-world application and problem-solving.

Through knowledge obtained during the RET Program, teachers are exposed to creative problem-solving strategies to initiate critical

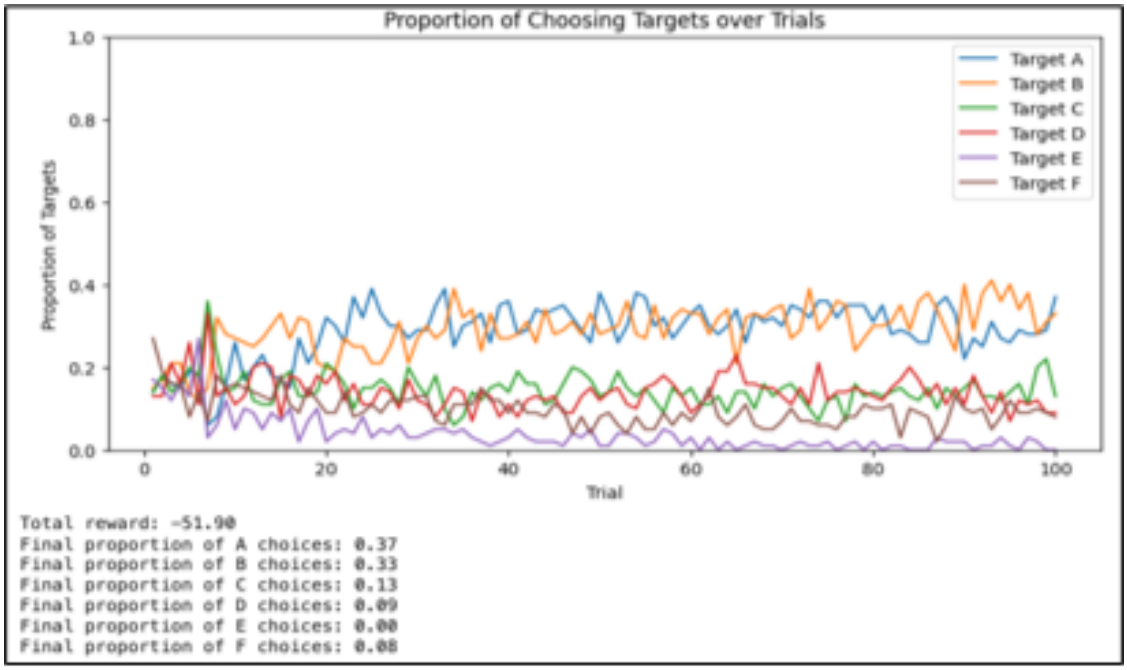

Figure 3: – Impact of decay

thinking. This leads to students having the opportunity to learn algorithmic thinking, a fundamental yet critical skill required to be successful in computer science, cybersecurity, and data science. Once a firm understanding of algorithmic thinking can be demonstrated, students can be introduced to aspects of cognitive modeling and how it relates to human behavior when faced with decisions that allow for rewards and penalties relative to their experiences. This also reinforces critical thinking and provides a supplementary opportunity to apply the already learned coding knowledge. Furthermore, students now have real-world scenarios that yield vast data sets that, when paired with appropriate modules and libraries, can graphically demonstrate the applied mathematical calculations. This enforces their knowledge on diverse data visualization techniques. To summarize, using these modeling tools of IBL, doors to critical and algorithmic thinking are unlocked for students to apply programming concepts and generate a robust understanding of what otherwise would be considered as some obscure data.

6 CONCLUSION

The research demonstrates the potential of IBL to understand and predict the decision-making process of hackers through simulation in order to devise effective cyber defense. Moreover, the integration of these advanced concepts into secondary education not only enables the students to gain practical understanding of math and computer science concepts but also makes them aware of advanced research regarding cyber defense techniques. To conclude, the output gained from the Research Experience for Teachers program and collaboration amongst the professors, Ph.D. students, and other teachers is noteworthy as advancements in cybersecurity research through cognitive learning models [6] can directly impact secondary student education in the classrooms.

Acknowledgments

We want to thank the National Science Foundation for sponsoring UTEP's CREEDS RET program (Award number #2206982). We also want to acknowledge the dedication, effort, and willingness of all those who have participated in the program to share knowledge. Dr. Palvi Aggarwal, Dr. Deepak Tosh, Dr. Martine Ceberio, Dr. William Robertson, and Mohammad Ariful Islam Khan were indispensable mentors and an inspiration to all those participating.

References

[1] Gonzalez, C., Lerch, J. F., & Lebiere, C. (2003). Instance-based learning in dynamic decision making. *Cognitive Science, 27*(4), 591-635. DOI: https://doi.org/10.1207/s15516709cog2704_2

[2] Maqbool, Z., Pammi, V. C., & Dutt, V. (2022). Computational modeling of decisions in cyber-security games in the presence or absence of interdependence information. In *Cybersecurity and Cognitive Science* (pp. 357-370). Academic Press. DOI: https://doi.org/10.1016/B978-0-323-90570-1.00005-X

[3] Anderson, J. R., Matessa, M., & Lebiere, C. (1997). ACT-R: A theory of higher level cognition and its relation to visual attention. *Human–Computer Interaction, 12*(4), 439-462. DOI: https://doi.org/10.1207/s15327051hci1204_5

[4] Lejarraga, T., Dutt, V., & Gonzalez, C. (2012). Instance-based learning: A general model of repeated binary choice. *Journal of Behavioral Decision Making, 25*(2), 143-153. DOI: https://doi.org/10.1002/bdm.722

[5] Carnegie Melon University (n.d.). *PYibl Documentation.* Retrieved [June 18th, 2024] from http://pyibl.ddmlab.com/.

[6] Cranford, E. A., Gonzalez, C., Aggarwal, P., Cooney, S., Tambe, M., & Lebiere, C. (2020). Toward personalized deceptive signaling for cyber defense using cognitive models. *Topics in Cognitive Science, 12*(3), 992-1011. DOI: https://doi.org/10.1111/tops.12513