CREEDS RET 2024

Team PsyberSecurity Lab
Faculty Mentor: Dr. Palvi Aggarwal
Student Mentor: Mohammad Ariful Islam Khan (Arif)
About the Mentors

Faculty Mentor:
- Dr. Palvi Aggarwal (Assistant Professor, Department of Computer Science)
- Research interests: Cybersecurity, Cognitive modeling, Human-machine teaming, Cyber education, Human-AI interaction
- Director of the Psyber Security Lab

Student Mentor:
- Arif
- PhD Student in the CS department
- Research areas: Human factors in cybersecurity, Cyber education, Human-machine teaming
- Doctoral Research Associate at the Psyber Security Lab
95% of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index
PsyberSecurity Lab (Contd.)

- Interdisciplinary research lab focused on human factors in cybersecurity
- Combines expertise from computer science, cognitive science, and psychology

**Research areas:**
- Cognitive modeling of cybersecurity decision-making
- Human-machine teaming for cybersecurity tasks
- Cybersecurity education and training
- Human-AI interaction in cybersecurity contexts
Research Focus: Human-Like Models in Cybersecurity

Source: The Decision Lab
Research Focus: Human-Like Models in Cybersecurity

- **Cognitive Science and Cognitive Modeling**
  - Understands mental or cognitive processes for perception, learning, memory, thinking, problem-solving, and decision-making.
  - Builds computer simulations to predict and explain human behavior.

- **Key Cognitive Processes:**
  - **Attention**: Focusing on specific stimuli.
  - **Language**: Understanding and expressing thoughts.
  - **Learning**: Synthesizing new information.
  - **Memory**: Encoding, storing, and retrieving information.
  - **Perception**: Taking in sensory information and responding.
  - **Thought**: Engaging in decision-making and problem-solving.
Cognitive Modeling Process
Applications Areas

Applications of Cognitive Modeling:

- **Predicting Human Behavior**: Simulates how people act in various scenarios (numerous fields such as education, finances, healthcare and so on).

- **Understanding Cognitive Processes**: Insights into attention, memory, and decision-making.

- **Enhancing Human-Machine Interaction**: Anticipates user needs and behaviors for effective Human-Machine Teaming.

- **Some notable sectors**:
  - **Healthcare**: Improves diagnosis and treatment plans by modeling patient behavior.
  - **Education**: Enhances learning by understanding student cognitive processes.
  - **Marketing**: Predicts consumer behavior and improves personalized marketing strategies.
Cognitive Modeling (Contd.)

Cognitive Modeling in Cybersecurity:

- **Simulating and understanding human behavior**: Models strategies and behaviors of cyber attackers, users or defenders.
- **Improving Decision-Making**: Designs better decision-support systems. Also, facilitates the design of effective defensive measures.
- **Training and Education**: Provides realistic scenarios and feedback for training.
- **Policy Development**: Aids in formulating effective security policies by predicting human responses.
Adaptive Defense: Tracking Adversary in Cyber Situations

1) Adversary Interacts with System
2) Cog Model Observes Adversary Interactions
3) Cog Model Informs Adaptive Defense
4) Automated Defense Deployed

Adaptive Defense is More Robust Against Future Attacks

Cog Model Accurately Predicts Adversary Behavior, etc.
Projects

Predicting End-Users in Phishing Classification Task

Prior history

From: john.lennon@gmail.com
To: Alice <alice@sec2ram.net>
Subject: Funny Dog Video
Body: Click here to see cute puppies!

Click

New emails

#1
From: jenny.garcia@gmail.com
To: Alice <alice@sec2ram.net>
Subject: Help the dogs
Body: Click the video to learn about how you can help the dogs.

Does Not Click

#2
From: David <david@sec2ram.net>
To: Alice <alice@sec2ram.net>
Subject: RIP. Fix the spreadsheet.
Body: Thanks for the help. Here is a cute video about dogs that I think you will love!

Click

#3
From: David <david@me.com>
To: Alice <alice@sec2ram.net>
Subject: Help the dogs
Body: Click the video to learn about how you can help save the dogs.

Click

Predicting Attackers in Insider Attack Game

(A) Screenshot of IAG interface

Round 1
Attacks Left: 25
Click on a computer you want to access
SCORE: 0

An analyst is watching 40% of the time.
9 Stars
-10 Stars

(B) Example signal message

38% of time this computer appears as "monitored" the analyst is NOT present. Do you want to access this computer?

Yes
No
Program Structure (Overview)

- **Duration**: 6 weeks
- **Format**: Weekly thematic lectures and hands-on labs
- **Topics covered**:  
  - Python programming basics  
  - Data analysis fundamentals  
  - Cognitive modeling with PyIBL  
  - Cybersecurity basics  
  - Capstone projects (team and individual)
Week 1 - Python Programming Basics

- Introduction to Python
- Data structures
- Control flows
- Functions
- Libraries and modules

**Activities:**
- Coding exercises
- Daily challenges
- Mini-projects
Week 1 (Contd.) - Data Analysis Fundamentals

- Introduction to Pandas
- Data visualization with Matplotlib
- Basic statistical analysis

**Activities:**
- Hands-on sessions
- Real-world dataset analysis
- Weekly project
Week 2-3 - Cognitive Modeling with PyIBL

- Core concepts of Instance-Based Learning (IBL)
- Introduction to PyIBL
- Modeling decision-making processes
- Understanding how these models assist us in strengthening defense

**Activities:**
- Hands-on modeling sessions
- Working on several projects (e.g. modeling decisions in binary choice tasks)
- Plotting and observing the data obtained through the modeling tasks
- Insights and group discussions
Week 4 - Cybersecurity Basics

- **Cyber hygiene**: Digital defense habits.
- **Password security**: Strong, unique passwords.
- **Phishing awareness**: Spotting fake emails/messages.
- **Social engineering**: Deception tactics for online info gathering.

**Activities:**
- Discussions
- Quizzes
- Simulated exercises
Week 5-6 - Capstone Projects

- **Team project:** Cybersecurity problem modeling with IBL
- **Individual project:** Teaching module on a cybersecurity topic related to human factors

**Activities:**
- Final research project development
- Working on the poster
- Preparation for the Presentations
- Feedback sessions
Assessment and Outcomes

- Weekly evaluations
- Capstone project evaluation

**Skills gained:**
- Python programming
- Data analysis
- Cognitive modeling of decision making
- Cybersecurity concepts related to human factors
- Teaching materials developed
Conclusion (Key Takeaways)

▪ Empowering Cyber-Aware Education
  ➢ Incorporates human-centric cybersecurity principles
  ➢ Fostering cyber awareness and responsible online behavior

▪ Cognitive Modeling for Cyber education
  ➢ Leverages Instance-Based Learning (IBL)
  ➢ Simulates human decision-making in cybersecurity
  ➢ Facilitates effective cyber education strategies

▪ Interactive Cybersecurity Learning
  ➢ Experiential learning on human aspects
  ➢ Prepares students for real-world cyber threats
Excited to learn from you guys too!

Thank You...