Adversarial Thinking Module

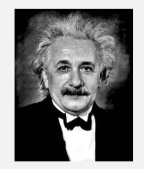
National Cybersecurity Curriculum Project

Seth Hamman, Ph.D., Ken Hopkinson, Ph.D.

Curriculum Highlights

Sternberg's Triarchic Theory and Adversarial Thinking

Analytical: How does the hacker's "book smarts" contribute to his hacking prowess?



Creative: How does the hacker's ability to make creative connections help him break into systems?

Practical: How does the hacker's ability to plan, strategize, and overcome obstacles contribute to his success?

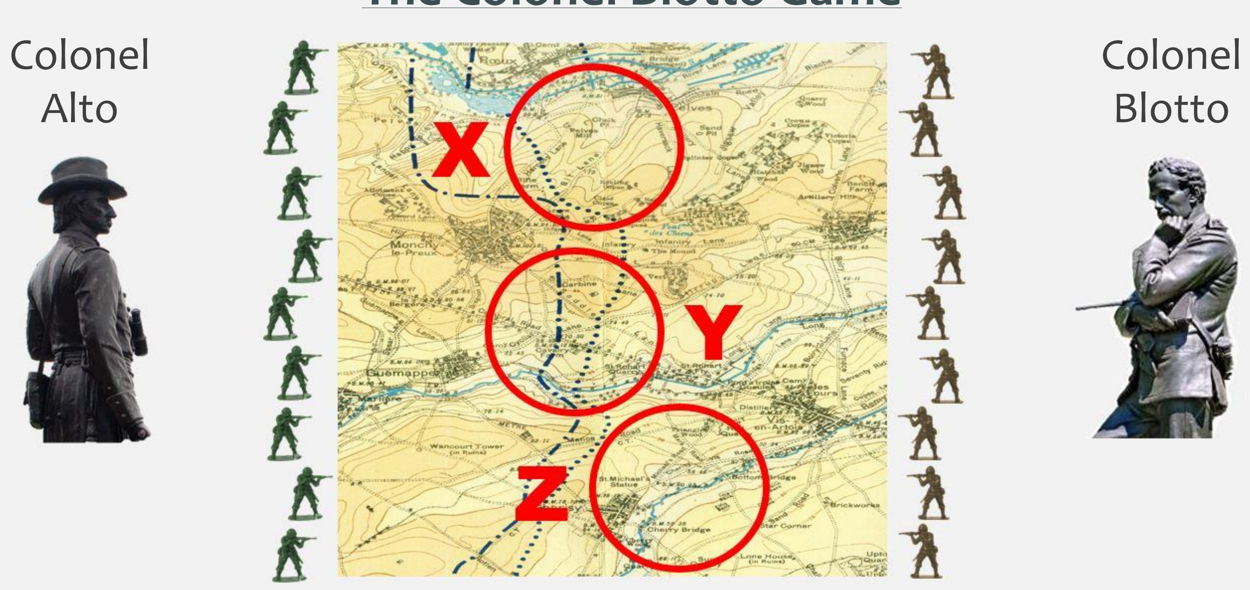
Adversarial Thinking Learning Outcomes

Component	Learning Outcome
Technological Capabilities	Understand computer networking protocols, low-level programming languages, and operating systems
Unconventional Perspectives	Identify unconventional uses of software and protocols that could be exploited by hackers
Strategic Reasoning	**Anticipate the strategic actions of hackers, including where, when, and how they might attack, and their tactics for evading detection**

Analytical vs. Behavioral Game Theory

	Analytical	Behavioral
Method	Deductive	Inductive
Approach	Theoretical	Empirical
History	1940's, Von Neumann	2000's, Camerer
Predictive	Many repeated-play games	Many one-shot games
Example	The Prisoner's Dilemma	The 2/3s Guessing Game
Key Concept	Nash Equilibrium	Level-k Reasoning

The Colonel Blotto Game



Overview

This curriculum module provides a basic introduction to adversarial thinking, game theory, and behavioral game theory to help develop cybersecurity students' abilities to anticipate the strategic actions of cyber adversaries, including where, when, and how they might attack, and their tactics for evading detection. The basic message of the module is that human adversaries are what differentiates cybersecurity from other technical disciplines such as computer science, and, therefore, the concept of **adversarial thinking is central to cybersecurity**. The goal of the module is to **produce enduring strategic-mindedness** in students who may otherwise tend to equate cybersecurity with technology-based best practices. This is a stand-alone, self-contained module, with no knowledge prerequisites. The module can be incorporated into virtually any university-level course. A syllabus, learning outcomes, assessment materials, instructor notes, PowerPoint slides, videos, and whole-class interactive exercises are included. This module has been experimentally validated and is the subject of two peer-reviewed journal articles.

Curriculum Package

3 Lessons of approximately 1 hour each
- Lesson 1: Intro to Adversarial Thinking
- Lesson 2: Intro to Game Theory
- Lesson 3: Intro to Behavioral Game Theory

Materials
- 68 PowerPoint Slides with extensive notes
- Assessment materials with step-by-step solutions
- **Custom videos** and video clips

Learning Outcomes
- Students will be able to illustrate the three components of adversarial thinking for cybersecurity.
- Students will be able to analyze a strategic scenario from a game theoretical perspective.
- Students will be able to apply level-*k* reasoning to derive playing strategies in strategic contests.
- **Students will be able to analyze cybersecurity from the strategic perspective of cyber adversaries.**

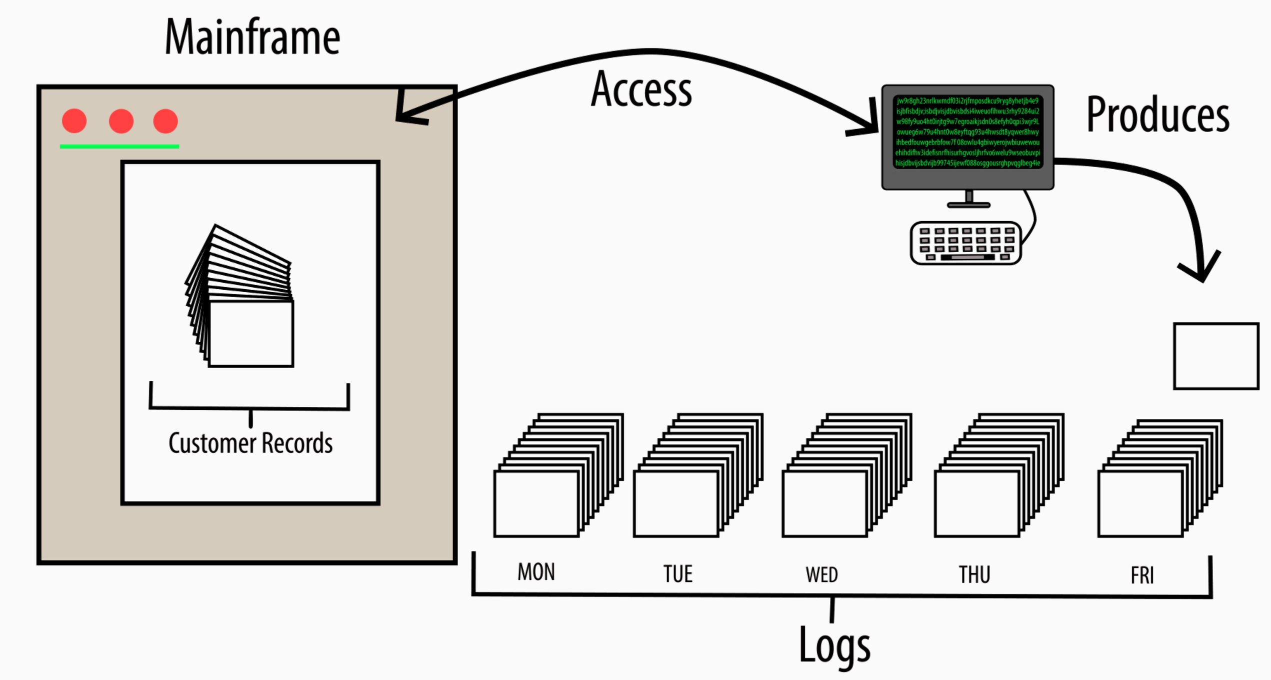
Exercises and Illustrations
- **Data Breach** – *a cyber-themed game used as a pretest-posttest assessment tool to measure the impact of the curriculum module on students' adversarial thinking abilities (see right panel)*
- **Illustrating Adversarial Thinking** – *a profile of the hacker described in Cliff Stoll's* The Cuckoo's Egg *is analyzed for the three components of adversarial thinking*
- **The Hacker's Dilemma** – *a cyber-themed retelling and analysis of the prisoner's dilemma game*
- **The Battle of Bismarck Sea** – *a real-life strategic military situation is analyzed with game theory*
- **Solomon's Wise Ruling** – *game theory is applied to this famous story to try and predict the ending*
- **The 2/3s Guessing Game** – *played together in class, this game illustrates the key differences between analytical and behavioral game theory, and the concept of level-k reasoning*
- **The Hide and Seek Game** – *a famous experimental game theory game illustrating focal point biases*
- **The Colonel Blotto Game** – *a game theoretical model of the scarce resource allocation problem faced in many real-life defense scenarios (see left panel)*
- **DDoS** – *a cyber-themed Colonel Blotto game is analyzed using level-k reasoning in multiple dimensions*

Recommended Readings

- S. Hamman and K. Hopkinson, "Teaching adversarial thinking for cybersecurity," *Journal of The Colloquium for Information System Security Education*, vol. 4, no. 1, pp.
- S. Hamman, K. Hopkinson, R. Markham, A. Chaplik, and G. Metzler, "Teaching game theory to improve strategic reasoning in cybersecurity students," *IEEE Transactions on Education*, vol. 60, no. 3, pp. 205-211, 2017.
- (many additional books, articles, and websites are cited in the slide notes)

The Data Breach Pretest-Posttest Assessment

This exercise measures students' adversarial thinking abilities. It tasks them with detecting an employee's attempt to exfiltrate customer records by strategically allocating log auditing man-hours. The exercise is scored against actual data collected from students cast in the role of the insider threat.



Daily Log Files	Mon	Tue	Wed	Thu	Fri
Value of Data	1	2	3	4	5
Log Auditing Hours (must sum to 100)	?	?	?	?	?

Lesson Summaries

Lesson 1
Adversarial thinking is central to cybersecurity
Adversarial thinking is the ability to embody the technological capabilities, the unconventional perspectives, and the strategic reasoning of hackers
Strategic reasoning for cybersecurity is the ability to anticipate the strategic actions of hackers, including where, when, and how they might attack, and their tactics for evading detection

Lesson 2
Game theory is the study of interdependent decision making between multiple players where each player strives to maximize his own utility
Real life strategic situations can be analyzed through the lens of game theory by identifying the players, the interdependent choices available to the players, and the utility preferences of the players
A player's game theoretical analysis proceeds by carefully examining the choices and outcomes from the perspectives of the other players

Lesson 3
For many strategic situations, behavioral game theory is a better predictor of a person's strategic actions than analytical game theory
Level-*k* reasoning is a helpful tool to use for strategic contests where each player must try to anticipate the actions of the other player
2 to 3 levels of level-*k* reasoning performs very well in most games