

Adversarial Thinking

How to Think Like a Hacker



Frank H. Katz

fkatz@georgiasouthern.edu

Dept. of Information Technology

Allen E Paulson College of Engineering &
Computing





ABSTRACT

It's Not Enough to Teach Tech

- Yes, cybersecurity requires teaching technical tools such as firewalls, VPNs, IDS/IPS, packet sniffers
- But it requires more than that.
 - It requires understanding hacker motivations
 - It requires learning how hackers think, how to try to stay one step ahead of them

Thinking Like a Hacker

- Developing the student's abilities to “anticipate the strategic actions of cyber adversaries, including where, when, and how they might attack, and their tactics for avoiding detection.”

Objective

- Describes content and implementation of a 6 hour, 15 minute (5 class sessions) module in Adversarial Thinking in a Network Security course (IT 4336)
- Describes the students' perceptions of the value & importance of the module
- Describes statistical results of Pretest-Posttest assessment of an exercise to measure their understanding.



INTRODUCTION

CLARK – Cybersecurity Labs and Resour Knowledge Bae

The screenshot shows a web browser window with the following elements:

- Browser Tabs:** Google, MyGeorgiaSouthern, Homepage - IT-2531, Inbox (4) - fkatz@geor..., Tasks by main, Toold..., Google Keep, Home | CLARK.
- Address Bar:** clark.center/home
- Navigation:** Search..., Sign in, Register.
- Header:** CLARK logo.
- Main Content:** A blue-tinted background image of a person presenting. Text reads: "Effective cybersecurity curriculum at your fingertips." Below this is a search bar: "Search Learning Objects by author, title, or keywords". To the right of the search bar are links for "Browse all" and a "SEARCH" button.
- Taskbar:** Windows taskbar with search, task view, and various application icons (Edge, File Explorer, Mail, Chrome, Firefox, Word, Excel, Calculator, PDF, PowerPoint). System tray shows 3:30 PM on 10/8/2019.



What it contains

- Cybersecurity curriculum on a variety of subjects, both technical and non-technical
- In a variety of instructional formats:
 - Nano and micromodules (one class session or even less than one session)
 - Modules: several class sessions
 - Units: several weeks
 - Entire courses

Adversarial Thinking

CLARK

Adversarial Thinking

Contribute

FILTERS [Clear all filters](#)

RESULTS (9) [Clear Search](#) FILTERS SORT

Collection

- Security Injections
- NSA NCCP
- CS
- GenCyber
- CAE Community
- Secure Coding Community
- Intro To Cyber

Length

- Nanomodule
- Micromodule
- Module
- Unit
- Course

Level

- Elementary
- Middle
- High
- Undergraduate
- Graduate
- Post Graduate
- Community College
- Training

Guidelines

- NCWE KSA c

Adversarial Thinking
NSA NCCP
Seth Hamman | Cedarville University
Updated Oct 2, 2018
This curriculum module provides a basic introduction to adversarial thinking, game theory, and behavioral ga...

Varying the costs of attack and defense on a network
NSA NCCP
Susan Campbell | University Of Maryland
Updated Apr 15, 2019
This simulation of an adversarial situation between hackers (attacking a network) and analysts (defending a n...

Threat and Risk Analysis
Secure Coding Community
Laurie Williams | North Carolina State University At Raleigh
Updated Sep 26, 2019
Security requirement analysis is a critical process in software development to better understand threats and r...

Cybersecurity: Cyber Technology; Future Considerations
NSA NCCP
John Heslen | Augusta University
Updated Apr 3, 2019
This final nanomodule of the course "Introduction to Strategic Cybersecurity" discusses topics for students to...

https://clark.center/details/susanc/Varying the costs of attack and defense on a network

Type here to search

3:41 PM
10/8/2019

Adversarial Thinking

The screenshot shows a web browser window with the following elements:

- Browser Tabs:** Google, MyGeorgiaSou, Homepage - IT, Inbox (5) - fkat, Tasks by main, Google Keep, Adversarial Thin, New Tab.
- Address Bar:** clark.center/details/shamman/Adversarial%20Thinking
- Page Header:** CLARK logo, search bar containing "Adversarial Thinking", and "Contribute" button.
- Module Title:** Adversarial Thinking
- Author:** Created by Seth Hamman - Cedarville University
- Update:** Updated 10/2/18 [View the changelog](#)
- Rating:** ☆☆☆☆☆ [Write a review](#)
- Category:** Module
- Logos:** Cedarville University and NSA NCCP
- Description:**

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 premise 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. It contains three lessons of approximately one hour each. The module can be incorporated into virtually any university-level course. This module has been experimentally validated and is the subject of two peer-reviewed journal articles (cited in the syllabus).
- Right Panel:** "DOWNLOAD NOW" button, "SAVED TO YOUR LIBRARY!" message, "76 saves" and "32 downloads" statistics, "Attribute this Object" section with a link to the module and a CC BY 4.0 license icon, and a "Share" section with social media icons for Facebook, Twitter, LinkedIn, Email, and Print.
- Taskbar:** Windows Start button, search bar, and various application icons (e.g., Edge, File Explorer, Mail, Chrome, Firefox, Word, Excel, Calculator, PDF Reader, PowerPoint). System tray shows date and time: 3:54 PM 10/8/2019.



Why Teach Adversarial Thinking?

- Throughout our cyber curriculum at Georgia Southern, there are various references to the “hacker mindset”
- Hacker motivations could be financial, demonstrate ability, just because it’s an exciting challenge
- “To protect systems . . . we need to temporarily adopt thinking of malevolent hacker . . . Developing this way of thinking must be part of . . . educating cybersecurity professionals.” (A. McGettick, 2013, cited in Hamman and Hopkinson)

Why Teach Adversarial Thinking?

- Requirement for students to be able to “identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk” is now part of the NSA-CAE Non-Technical Core – Cyber Threats Knowledge Unit (KU)
- Thus teaching adversarial thinking fulfills a requirement for designation or redesignation as a CAE

Teaching the Module

- Taught to IT 4336 Network Security students (21)
- Spring 2019
- Note that the authors of the module believe that it be taught in a face-to-face class, not online.
- Indeed, given that almost all of the exercises are collaborative in nature, in small ad-hoc groups of 3 to 4 students, working in real time on the exercises, it would be difficult, if not impossible, to teach this module online



LESSON 1: INTRODUCTION TO ADVERSARIAL THINKING

Components of Lesson 1

- Data Breach Exercise Pretest. This will be discussed later
- Definition of terms introduced in the module
 - Bounty
 - Bad Guys
 - Barriers
 - Adversarial Thinking
 - Cognitive psychology
 - Sternberg's Triarchic Theory of cognitive intelligence
- Learning outcome: students will be able to analyze cybersecurity from strategic perspective of adversaries

Triarchic Theory / Adversarial Thinking

- Cognitive psychology: “study of higher mental processes, such as attention, language use, memory, and perception, problem solving, and thinking to more precisely define what it means to think like a hacker.” (Hamman, Lesson 1 slides)
- **Sternberg’s Triarchic Theory** of cognitive intelligence: three distinct aspects of the intellect
 - Analytical (book smarts)
 - Creative (ability to make new & unique connections)
 - Practical (ability to plan, strategize, & accomplish goals)
 - How these 3 affect the activities of a hacker
- “Adversarial thinking is the ability to embody the technological capabilities, the unconventional perspectives, and the reasoning of hackers” (Hamman, Lesson 1 slides)



LESSON 2: INTRODUCTION TO GAME THEORY

Components of Lesson 2

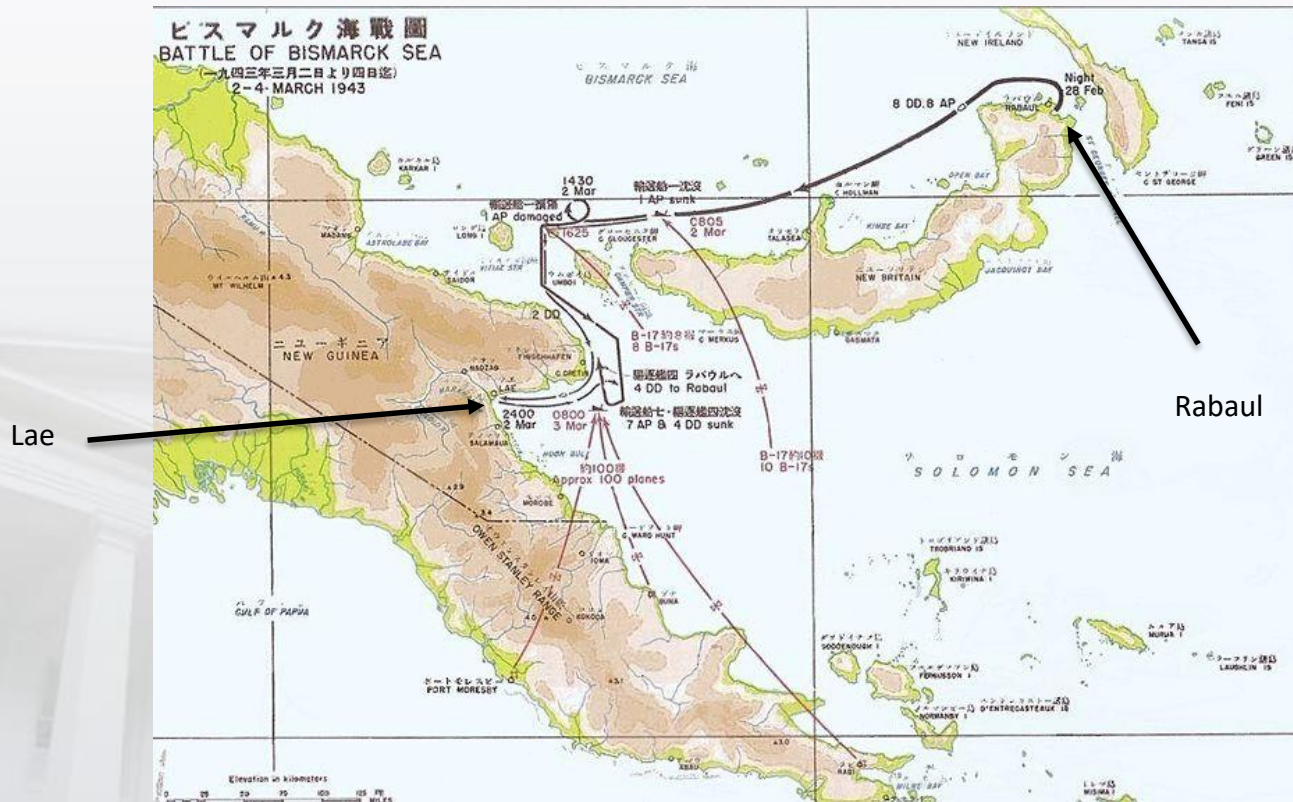
- Exercises employed to teach students how game theory could be used to prevent an adversary from hacking a system
 - These were group exercises
 - **Battle of Bismarck Sea (WW2, Pacific Theater, 1942)**
 - Hacker's Dilemma (based on the Prisoner's Dilemma – who rats out the other prisoner)
 - King Solomon's Wise Ruling
- Learning outcome: students will be able to analyze a strategic scenario from a game theory perspective

Definitions

- ***Game Theory***: a mathematically rigorous approach to analyzing strategic contests (not games of skill or chance). Study of *interdependent* decision making between multiple *players* where each player strives to maximize his *utility*. (Hamman, Lesson 2 slides)
- ***Players***: actors in the game
- ***Interdependent choices***: final outcomes for each player are dependent on *other* player's choices
- ***Utility preferences***: ordering of outcomes for each player from least desirable to most desirable

Battle of Bismarck Sea

- World War II, 1943. In map below, Japanese movements in black, allies in red

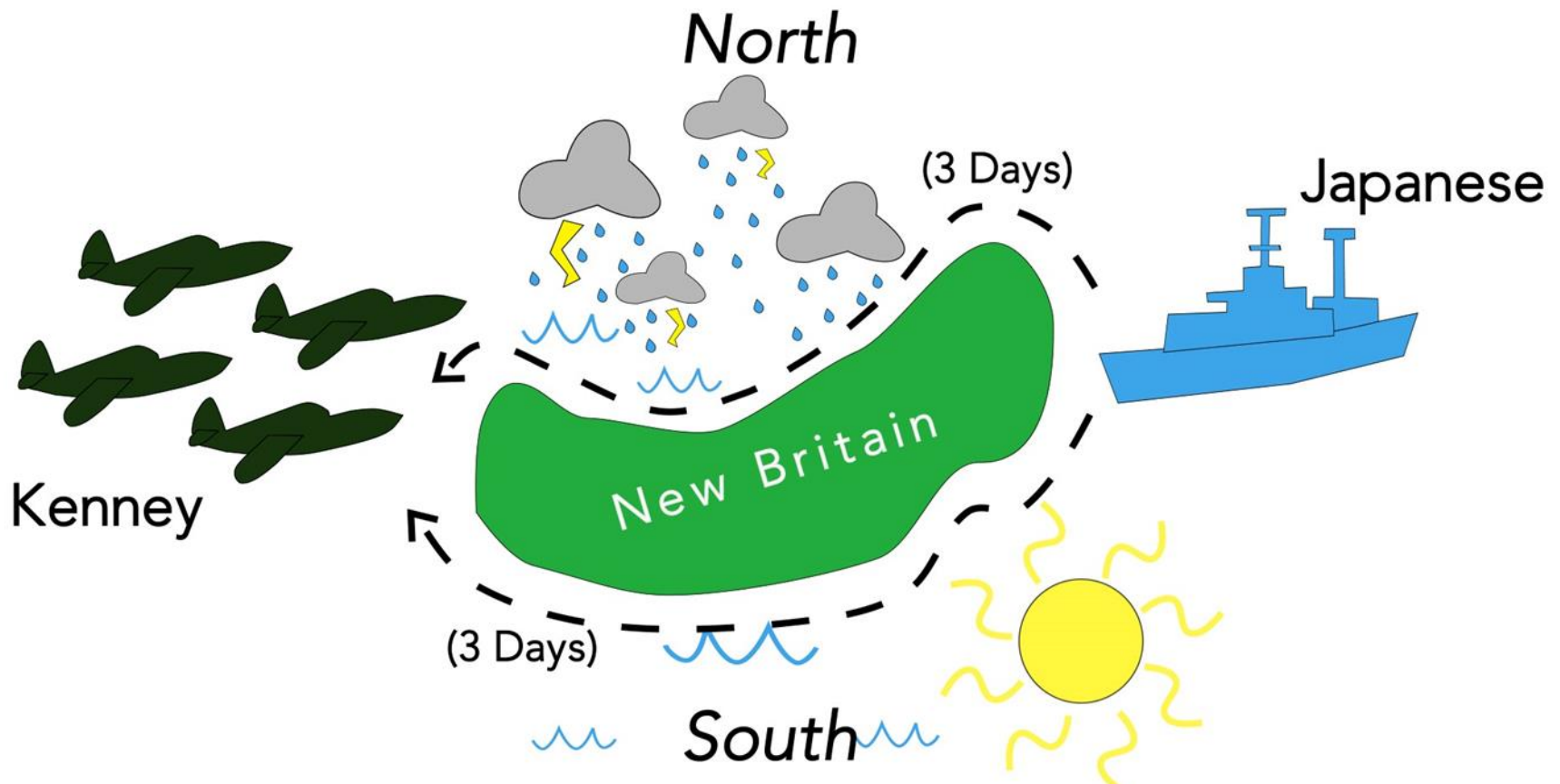


Lae

Rabaul

Battle of Bismarck Sea

- A more simple version



Interdependent Choices / Utility Preferences

- What are the interdependent choices?
 - Gen. Kenney: perform reconnaissance north or south of the island
 - Japanese commander: sail north or south of the island
- What are the utility preferences?
 - Not all students got this right
 - Correct answer is that this is directly tied to number of days of bombing of Japanese fleet by allied aircraft
 - Ends up a zero-sum game
- Students were asked to make a “normal form game grid”
- Combination of Kenney, N, S and Japanese, N, S, where numbers represent days of bombing

Grid and Dominated Strategy

		Japanese	
		N	S
Kenney	N	2	2
	S	1	3

		Japanese	
		N	S
Kenney	N	2	2
	S	1	3

Application to Cybersecurity

- Defending a computer network
- Knowing a vulnerability in a computer network, determining the optimal location (dominating strategy) to place an IDS



LESSON 3: INTRODUCTION TO BEHAVIORAL GAME THEORY

Analytical vs Behavioral Game Theory

- *Player perfect rationality* – players behave perfectly rationally to the nth degree when making strategic choices
- Difference between *analytical game theory* and *behavioral game theory*
- 2/3s guessing game
- Related to behavioral game theory because
 - It has interdependent choices, whole numbers between 1 and 100
 - It has utility preferences, losing and winning

2/3s Guessing Game

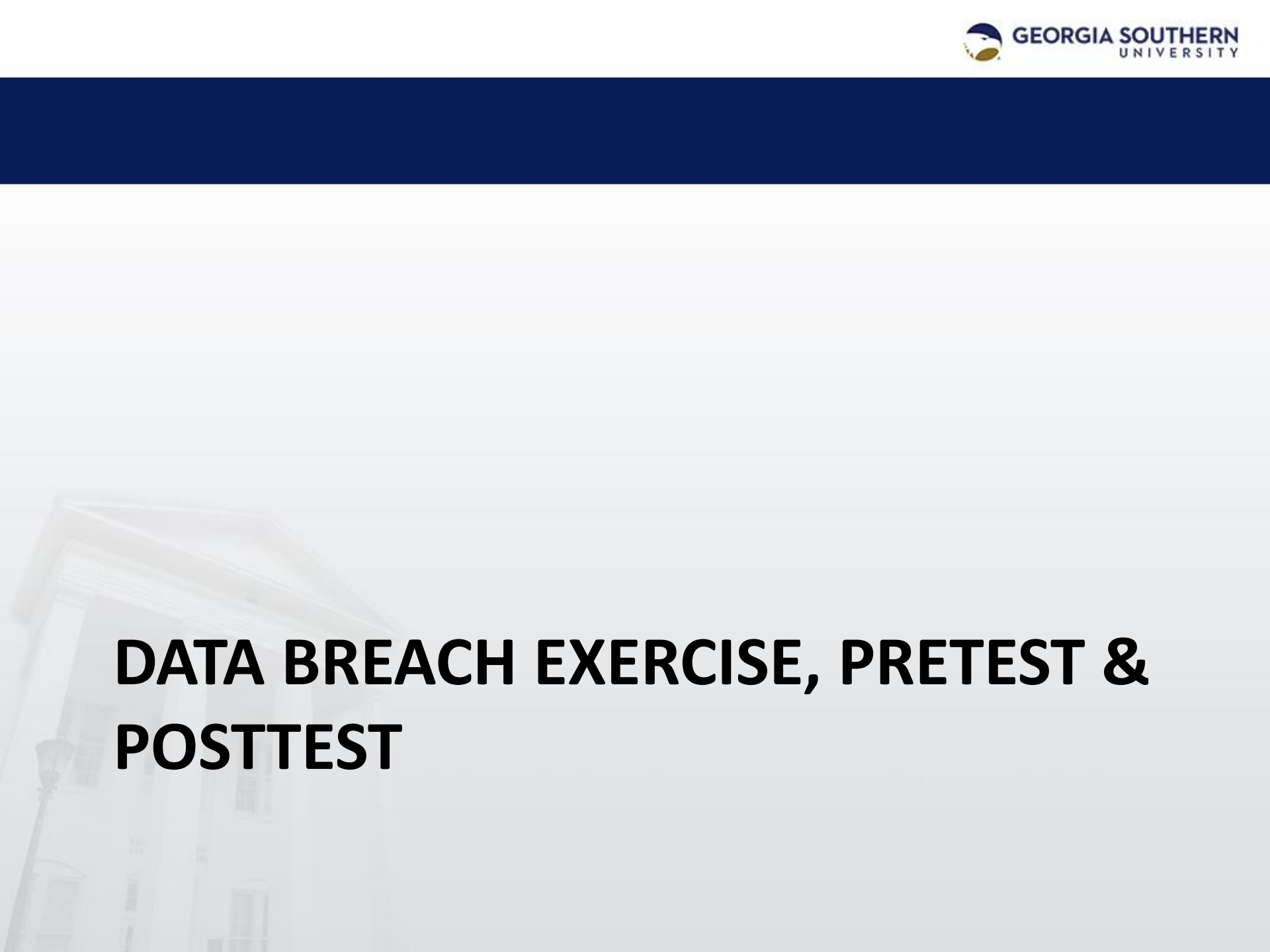
- Analysis of this game depends on *dominated strategies* - highest calculated number could only be 67, but that would depend on each student choosing 100
- So all numbers between 68 & 100 are dominated strategies, and should never be chosen
- So re-do game in light of this. Max is now 67, & everyone chose *that*, 2/3 of that is 45.
- So now all numbers between 45 and 67 are dominated strategies.
- To what level (level- k) will we continue this downward?

2/3s Guessing Game & Level- k reasoning

- Process itself is called *successive elimination of dominated strategies*.
- In *analytical game theory*, this would continue “all the way to the bottom,” with players exhibiting *player perfect rationality*, with players using a strict logical analysis
- But people don’t behave that way. In other games used in this particular module, there are only one or two successive eliminations of dominated strategies, and then equilibrium is reached
- That level where equilibrium is reached is known as **Level- k reasoning**

Application to Cybersecurity

- Adversary finds a vulnerability in your network, you discover that vulnerability, so you protect that.
- Then he finds another vulnerability, so you protect that
- As defenders, cybersecurity professionals must determine how many layers, or levels, of security they are willing to implement and pay for to defend against each potential adversary and mitigate each potential vulnerability
- At some point, cost of defending against a possible exploit with a very low probability of occurring becomes prohibitive



DATA BREACH EXERCISE, PRETEST & POSTTEST

Scenario

- Scenario describes a large company using an old, but well-entrenched mainframe. It cannot be properly secured, so every weekend, company runs a large migration job that clears data off the mainframe onto a more secure server
- Company is concerned that an insider might copy all the customer data off mainframe & sell it on black market
- Although they can't technically prevent this, they regularly audit the log files
- In future, they'll allocate 100 man hours per week to the task of auditing the daily logs

Scenario

- Company collects about same amount of data every day, so database grows linearly throughout the week
- DB starts fresh every Monday morning because of weekend migration job
- Assume nbr of hours allocated to inspecting particular day's job = likelihood of detecting an attack on that day
- So if X hours are assigned to reviewing a day's logs, & an insider attacks on that day, probability of detecting the insider is X%.
- Also assume if insider is detected, threat will be eliminated resulting in a "reward" = 10 pts for the company.

Scenario

- Each student has been hired as a cybersecurity consultant
- Job of each is to allocate the 100 man hours over the five daily log files, ensuring that integer percentages add up to 100
- Each student had to describe their reasoning
- Authors provided detailed instructions for scoring exercise, scored against actual data they had collected from 33 computer science undergraduate students who had participated in role of attackers

Control Set

- Attackers' data considered the control set.
- About $\frac{1}{2}$ of attackers chose Wednesday, about $\frac{1}{3}$ chose Tuesday, $\frac{1}{6}$ chose Thursday, none chose Monday or Friday

	Monday	Tuesday	Wednesday	Thursday	Friday
Percent of Attacks	0%	36%	46%	18%	0%
Value of Day	1	2	3	4	5

Formula for Scoring

- First half accumulates pts in proportion to detecting an attack on a particular day, with reward being 10 pts
- Second half deducts pts in proportion to their likelihood of not detecting an attack on a particular day
- Final score is sum of these values over all five days
- a_i = %age of attackers who choose day i ; d_i = %age of hrs allocated by the defender on day i ; v_i = value of day i ; R = reward for detecting the attacker

$$\sum_{i=1}^{|Days|} a_i(d_i * R) + a_i((1 - d_i) * -v_i)$$

Formula for Scoring & Results

- In example, total is -0.292. In Excel workbook provided, raw scores are normalized to values between 0 and 100.
- So in this example, student's final score is 42.3. Not to be interpreted as a percentage grade. But higher scores indicate stronger adversarial thinking abilities.
- So the posttest score should be $>$ pretest score
- Actual data bore this out. Data for 21 students showed that 16 out of 19, or 84.2% of the class, showed an increase pre- to posttest
- *p-value* of sample t-test in Excel between paired pre- and posttest scores was 0.0012361, indicating results were statistically significant, & improvement in mean pre- and posttest was as expected



SURVEY AND CONCLUSIONS

Survey Results

- Survey consisted of 17 statements, all on Strongly Agree to Strongly Disagree spectrum. Here are a selected few.

Survey Question	Percent Responding Strongly Agree / Agree
After being exposed to Lesson 1, I feel that I understand the overall concept of Adversarial Thinking and how it applies to hacking.	87.5%
I understand Sternberg's Triarchic Theory (related to cognitive psychology) and how it helps me understand how hackers think.	81.3%
The Battle of the Bismarck Sea exercise helped me understand the basics of Game Theory	75.0%
Participating in the 2/3 Guessing Game exercise helped me understand the concept of successive elimination of dominated strategies	62.5%
Participating in the 2/3 Guessing Game exercise helped me understand level-k reasoning as it applies to Behavioral Game theory	56.3%
Performing the DDoS exercise helped me understand the concepts of strategic resource allocation and level-k reasoning	68.8%
I feel that the entire Adversarial Thinking module was beneficial to my understanding of how a hacker thinks, and how to defend against a hacker.	87.8%
I feel that the time spent on Adversarial Thinking, versus the time that would have been spent on studying Network Security, was worth the inclusion of Adversarial Thinking in the course	68.8%

Conclusions

- Module improved student's adversarial thinking capabilities
- Being able to think like a hacker, they are better able to understand how to allocate defensive assets to protect an organization
- Survey showed students felt that they benefited from the module
- Since this ought to be taught in classroom setting, rather than teach this in our 4000 level Ethical Hacking course, which is often taught online, we might opt to teach this in our 2000 level intro course open to any student. In that way, it might become a "hook" into non-cyber students to get them to take our complete cyber curriculum