A User Experience Study of MeetingMayhem: A Web-Based Game to Teach Adversarial Thinking

Shan Huang, JiWoo Lee, Chenyan Zhao, Geoffrey L. Herman,

Marc Olano, Linda Oliva, Alan Sherman

Contributions

Motivation

ADVERSARIAL THINKING IS *IMPORTANT* FOR EVERYONE!!

CREATE AN *ENGAGING* WAY FOR STUDENTS *WITH* *LIMITED TECHNICAL BACKGROUND*

Adversarial Thinking

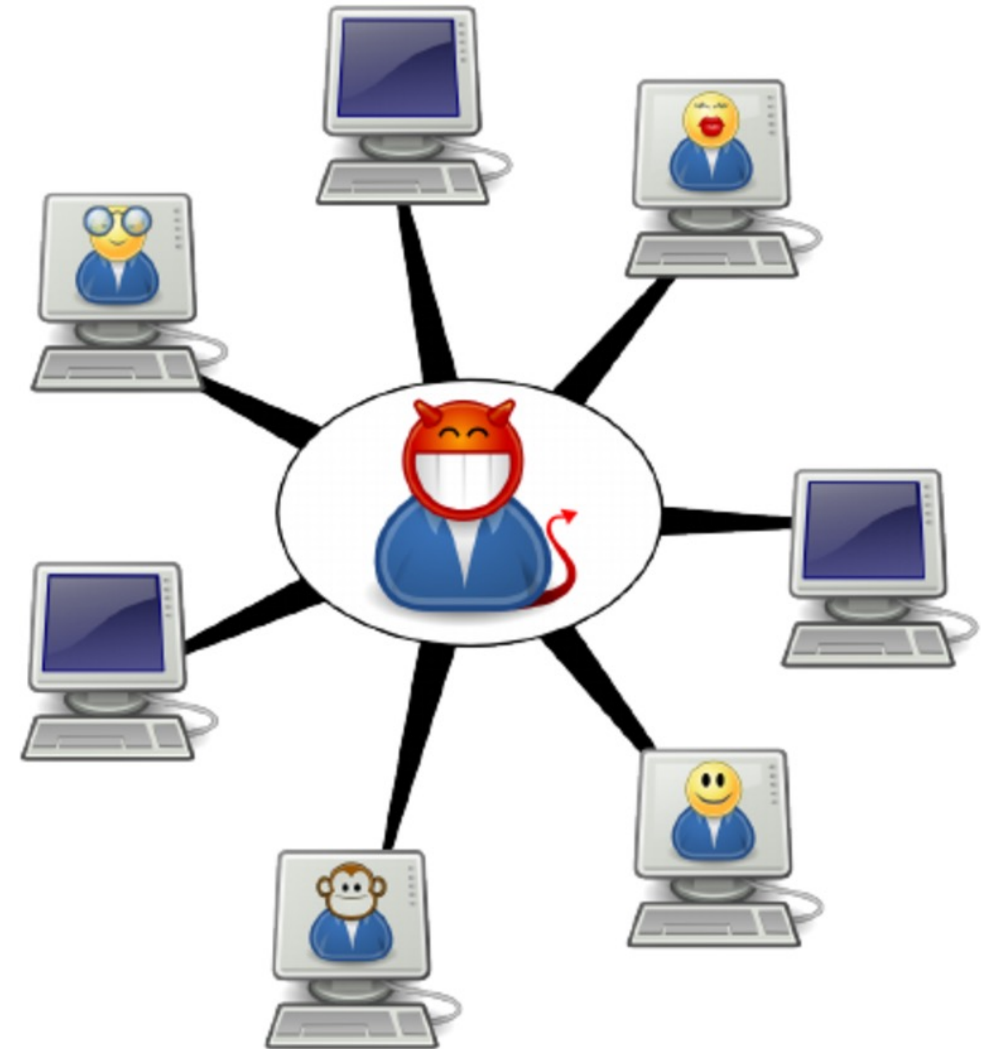**Vague Definition:** "Thinking as hackers"

Formal Definition: Reasoning about the *adversary's actions and goals* under *certain system rules* and *operational environments*

Dolev-Yao Model

- A strong network intruder model

- Realistic deployment

- Used by others in teaching adversarial thinking

Game Introduction

Agents' Goal: Agree on time + location

Adversary:

- Legitimate communicants

- Authorized access to the network

- Modify non-cryptographically protected messages

- Delete messages

Cryptographic Tools

Symmetric Encryption
- Encrypts or decrypts the message with a *shared symmetric key*
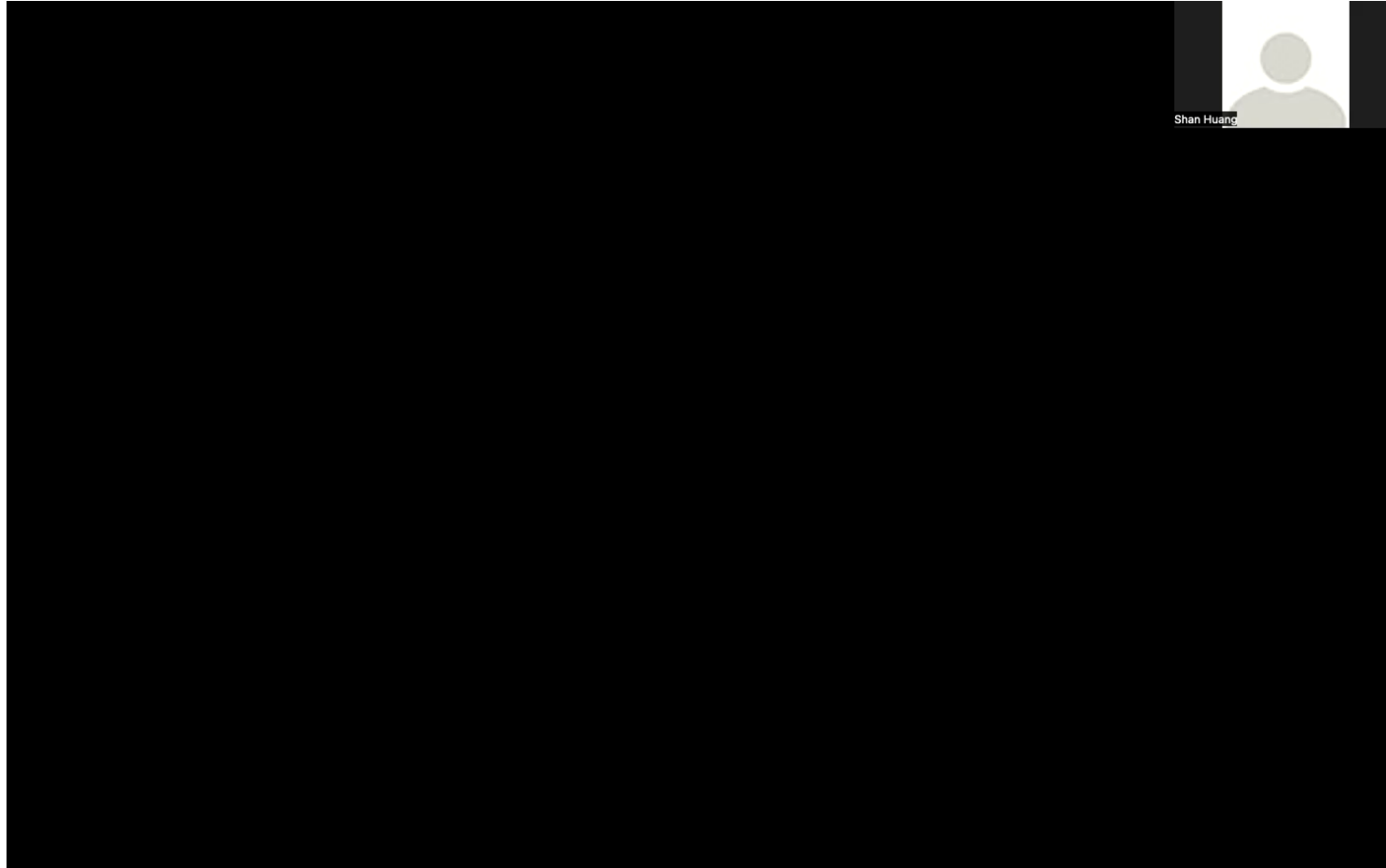
Asymmetric Encryption
- Encrypts message with *recipient's public key*
- Decrypts message with *sender's private key*

Signature
- Authenticate the identity of the sender of a message with *sender's private key*

Demo Video

https://drive.google.com/file/d/1qS60l-LdD0yz3RTlnQIJqNd7x94ehmRD/view?usp=sharing

Learning Objectives

LO1
- Identify dangers of computer network communications

LO2
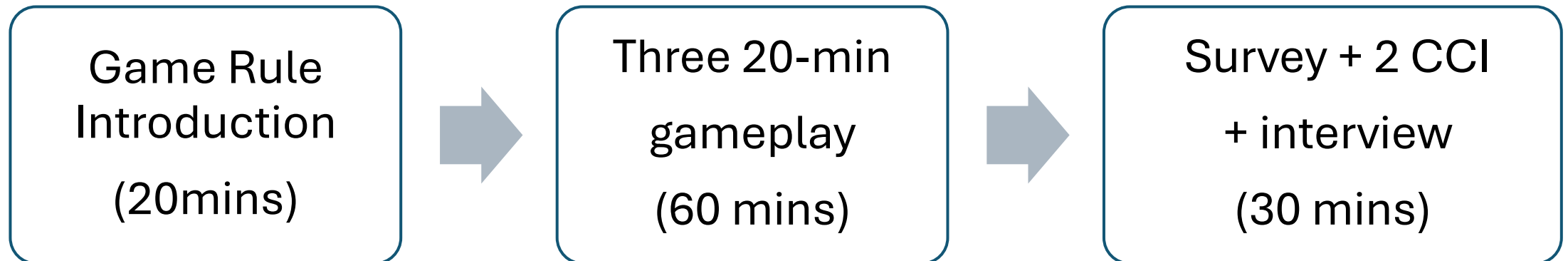- Describe the capabilities of a Dolev-Yao adversary

LO3
- Apply cryptographic primitives to mitigate dangers: symmetric encryption, asymmetric encryption, and digital signature

Data Collection

Recruitment Requirement (9) :

- ❑ College students greater than 18
- ❑ No prior knowledge in cybersecurity

Preliminary Study Set up:

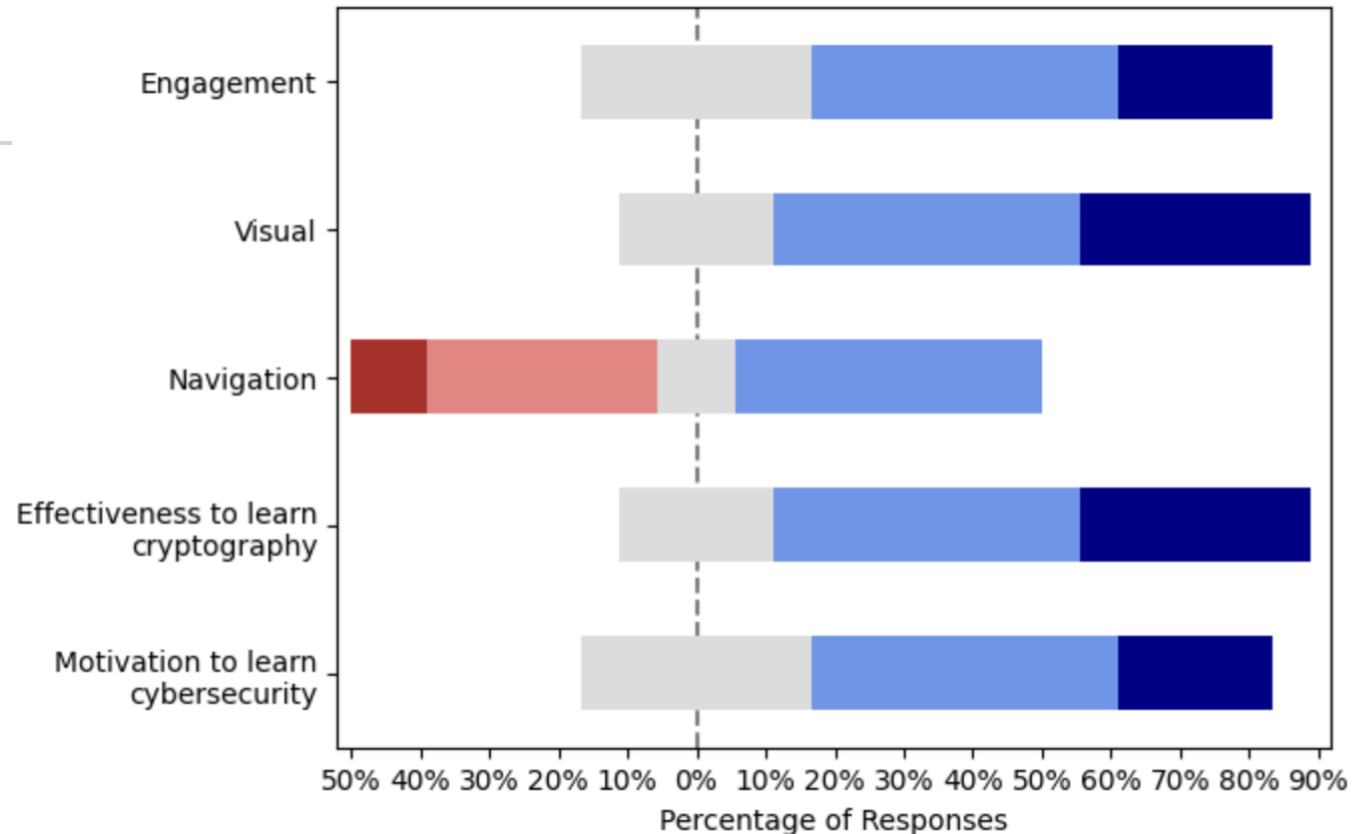| Game Rule Introduction (20mins) | → | Three 20-min gameplay (60 mins) | → | Survey + 2 CCI + interview (30 mins) |

Survey Result

Students rate **high** on

- Visual (4.11)
- Engagement (3.89)
- Motivation (3.89)
- Effectiveness (4.11)

Students rate **low** on

- Interface design (2.89)

Focus Group Result (LO1): Identify the dangers of communicating through a computer network

🔒 High usage of symmetric encryption to protect messages

👄 "There's so much [the] adversary can do with the message before it even gets to the other person, it makes it basically impossible to communicate."

Focus Group Result (LO2): Describe the capabilities of a Dolev-Yao adversary

Frustration with few and slow response from others

Realize it is caused by the adversary has to process and manipulate every message.

Focus Group Result (LO3): Applying three cryptographic tools

All students eventually use encryption to protect messages

Use symmetric encryption more frequently
Asymmetric encryption appears to be harder to understand

Creation of own authentication instead of using signature
Assign different codes to different participants.

Future Work

Chatbox Interface

- Like social media chat application
- More Compact

Level-based game design

- One cryptographic tool at a level
- Reduce cognitive load

Tutorial System

- Replace current presentation
- Automation