THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

Knowledge that will change your world

Dynamic Cognitive Game CAPTCHA Usability and Detection of Streaming-Based Farming

Manar Mohamed, Song Gao, Nitesh Saxena, and Chengcui Zhang

University of Alabama at Birmingham

Outline

- Introduction
- Dynamic Cognitive Game Captchas (DCG)
- Usability Study
- Streaming-based Relay Attack Study
- Stream Relay Attack Detection
- Discussion

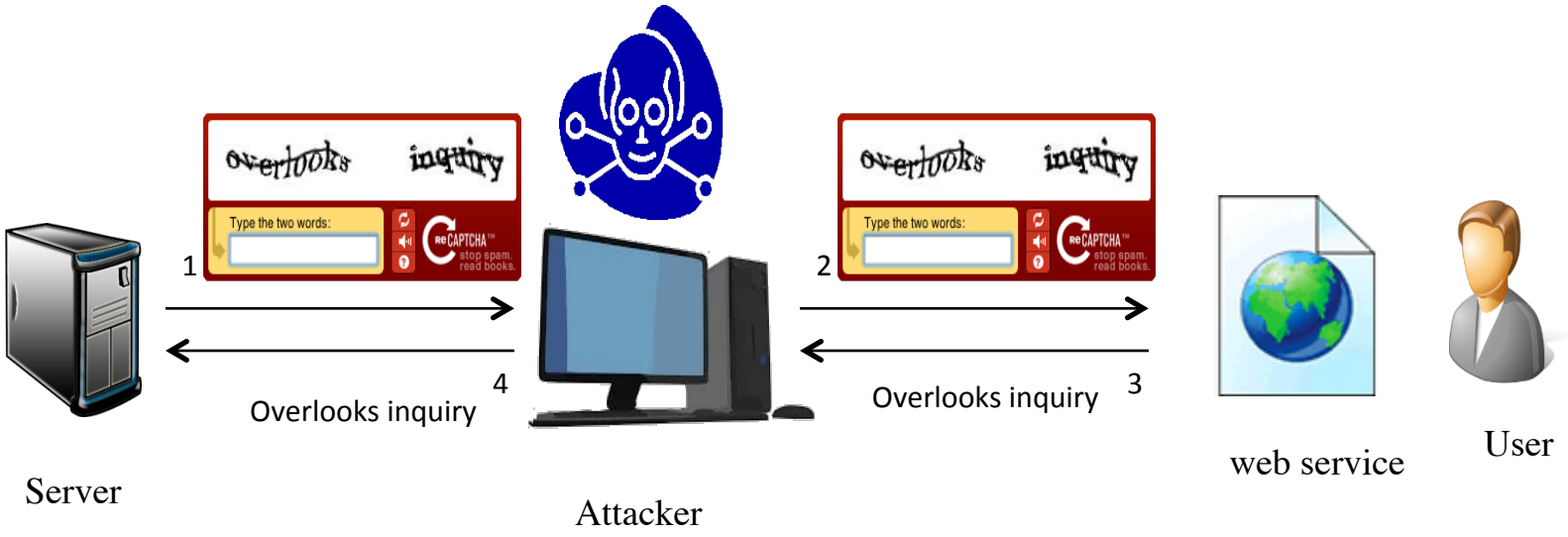
Introduction

- CAPTCHA is a test that can differentiate humans from malicious computer programs.

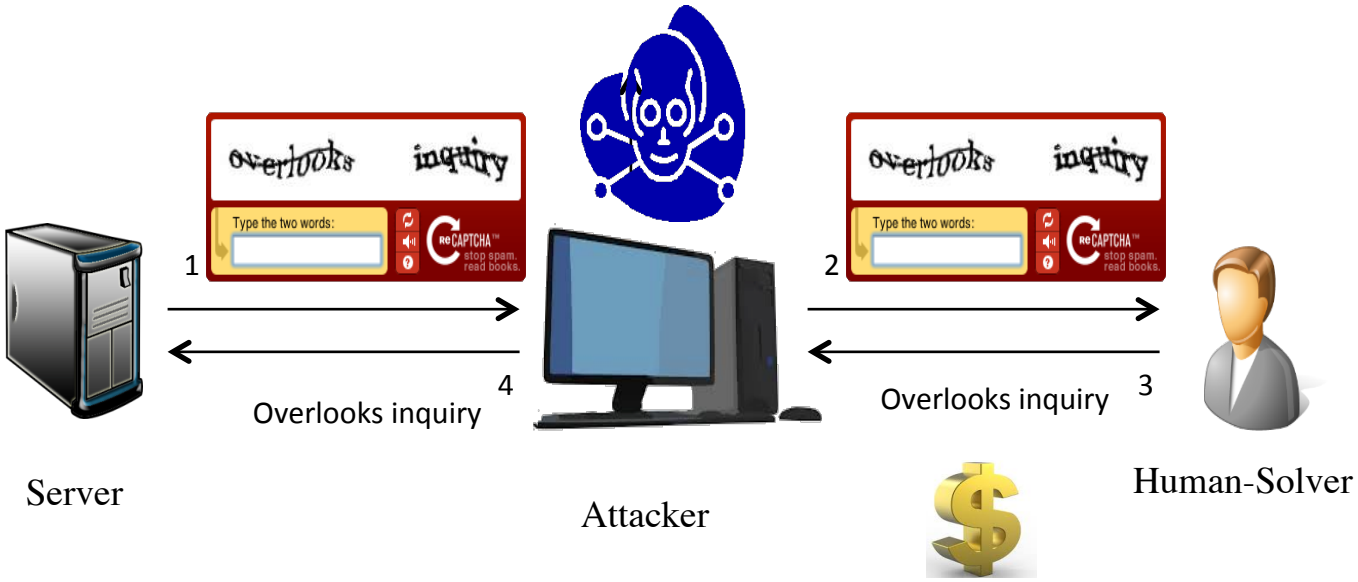
Attacks on CAPTCHA

- **Automated attacks:** utilize image processing algorithms
- **Relay attacks:** utilize human intelligence of third-party, remotely located human-solvers
  - opportunistic
  - sweatshops

Relay Attack (Opportunistic)



Relay Attack (Sweatshops)



Why Relay Attack?

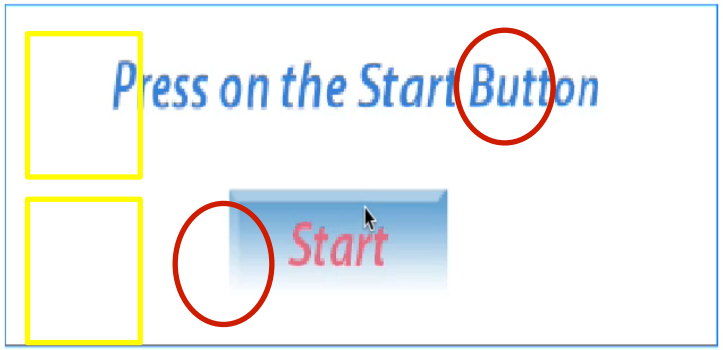
- Developing automated attack programs with human-like accuracy very complicated and costly
- For example, Paid solvers solve up to 1000 captchas for $1
- Relay attack more effective and economical than automated attack
- Unfortunately, most existing CAPTCHAs are easily and routinely broken using relay attacks

Dynamic Cognitive Game captchas (DCG)

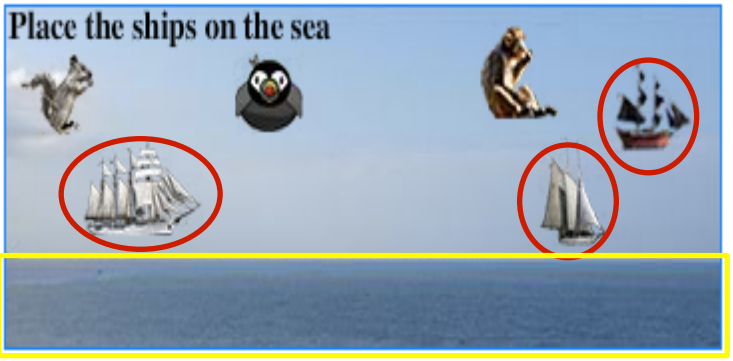
- Challenges user to perform *game*-like *cognitive* task, interacting with a series of *dynamic* images
- Interactive and dynamic in nature, and may offer some level of resistance to relay attacks
- Commercially offered by a startup named 'Are You a Human'

DCG Example Instances

Parking Game



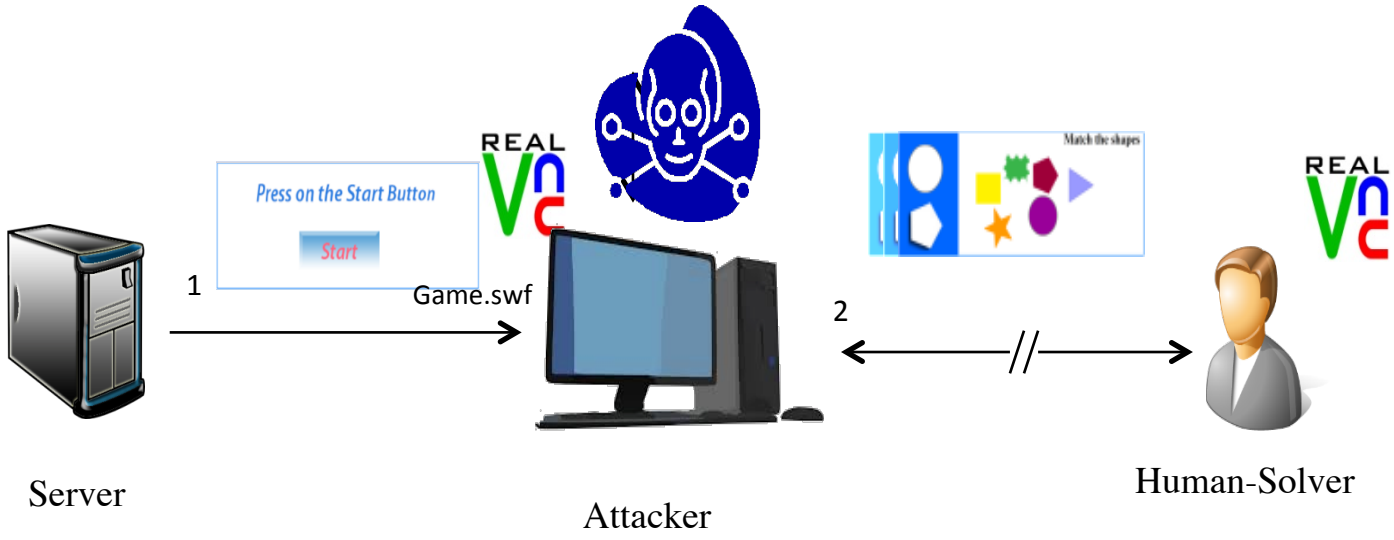
Shape Game



Ships Game

Animal Game

DCG Stream Relay Attack



Our Contributions

1. DCG Usability Study
   - Hypothesis: games quite easy for legitimate humans
2. Stream Relay Attack Study
   - Hypothesis: latency degrades game play performance of solvers (unlike legitimate humans)
3. Stream Relay Attack Detection
   - Behavioral differences in game play allows for detection

Usability Study

- 40 Amazon Mechanical Turk (Mturk) workers recruited
- MTurk workers provided with 4 DCG captchas in succession
- The performance metrics -- game completion time, number of object-drags, and number of clicks -- were recorded
- A survey used at the end of experiment to record the experience of the solvers
- The survey contains the 10 System Usable Scale (SUS) standard questions, each with 5 possible responses

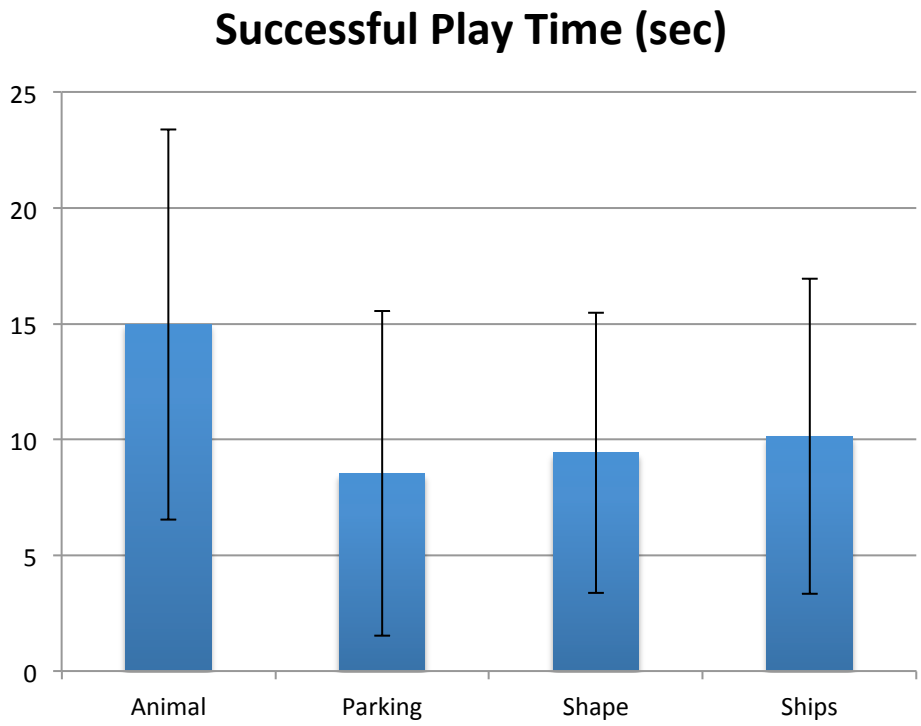
Stream Relay Attack Study

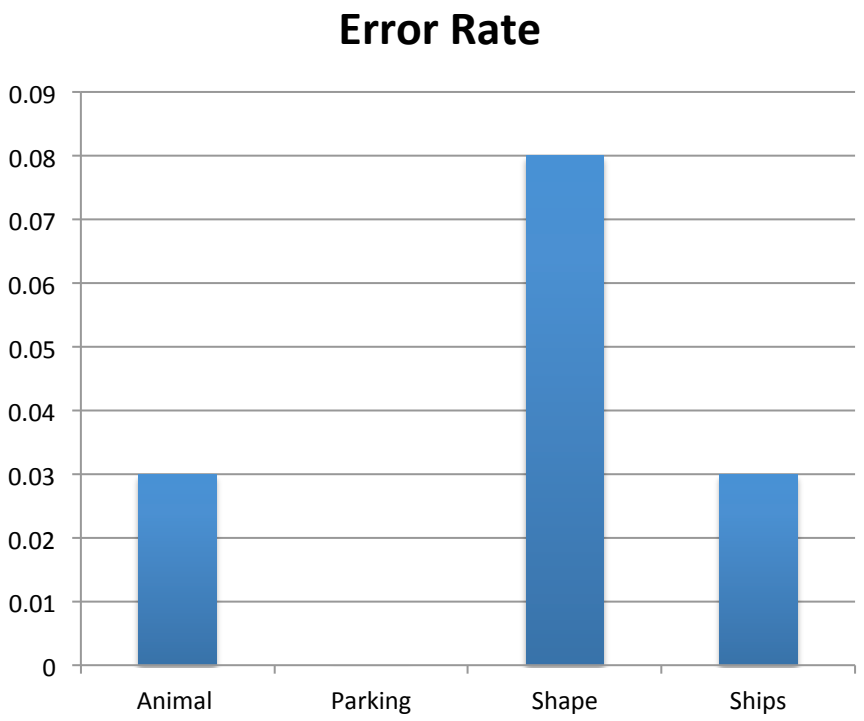
- Performed with MTurk workers
- MTurk workers were asked to connect to a computer residing in UAB and connected to UAB wireless network through a VNC application
- The workers were asked to fill demographics form, play 4 DCG CAPTCHAs followed a SUS survey

Stream Relay Attack Settings

- **High-Latency Relay:** The attacker reside in US while the solvers are residing outside the US
- **Small Game Relay:** The attacker relays a reduced size game to minimize latency effects
- **Low-Latency Relay:** The attacker launches the attack from a machine that is in close proximity to the solvers
  - attacker and solvers both in the US

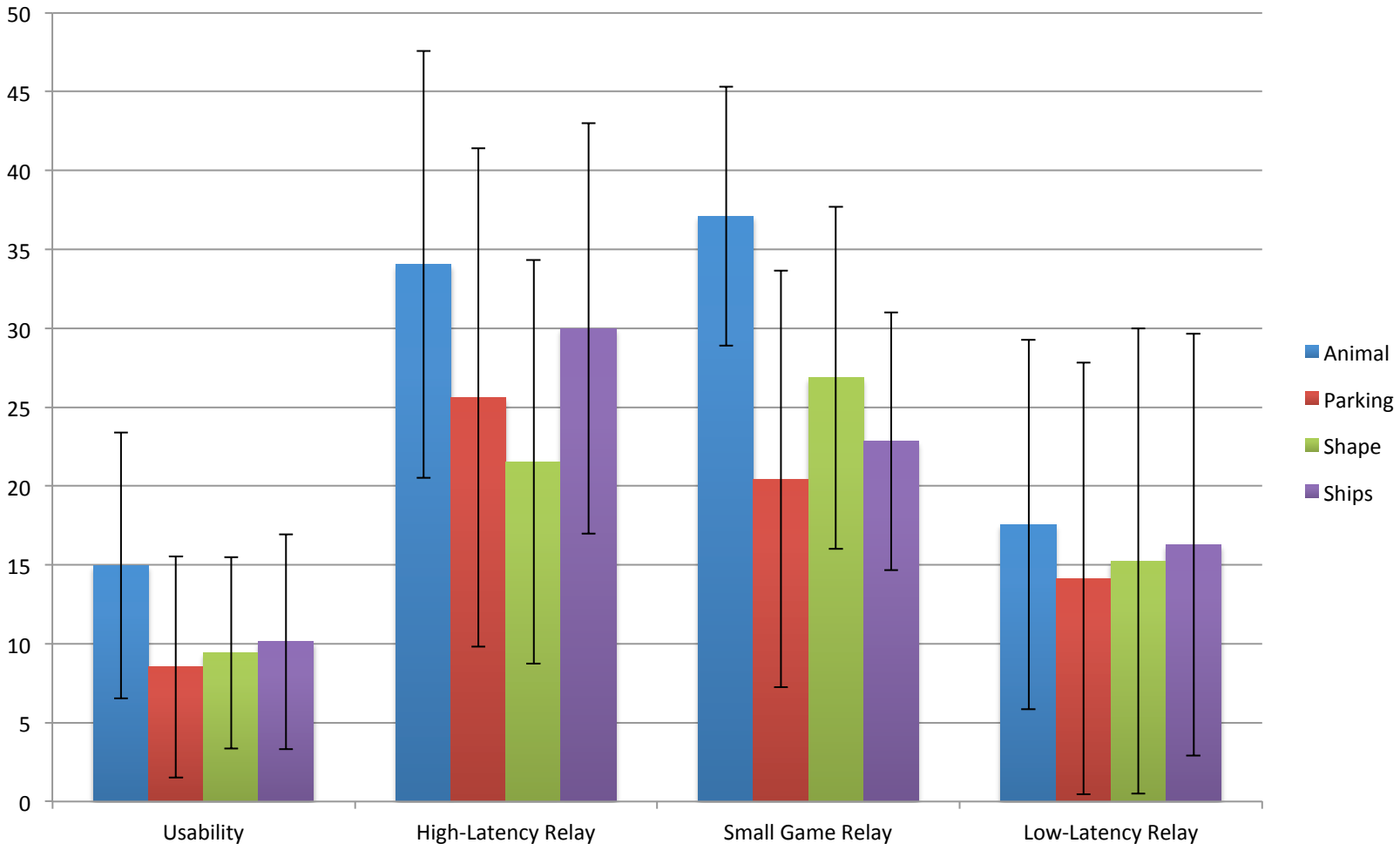
Results
Usability Study



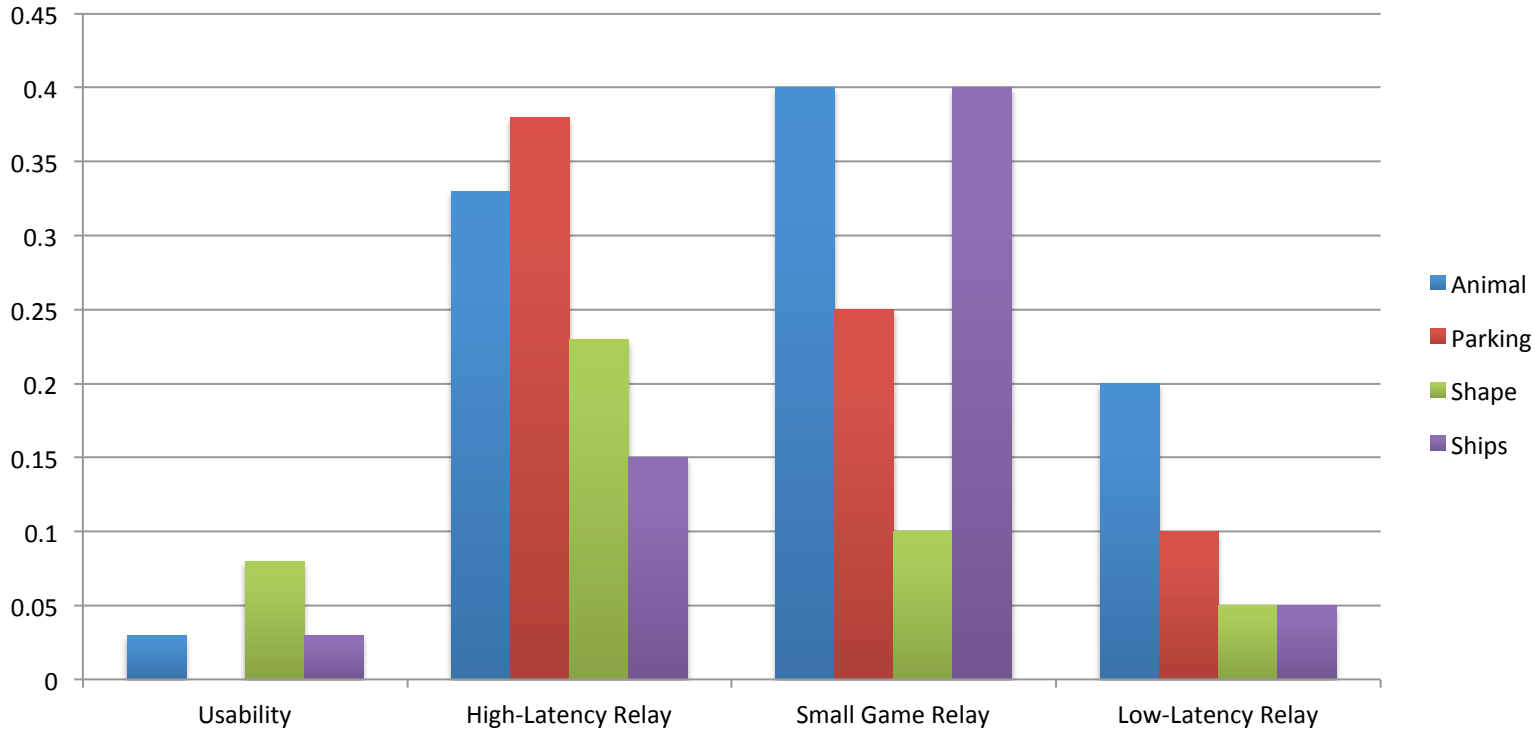


Results

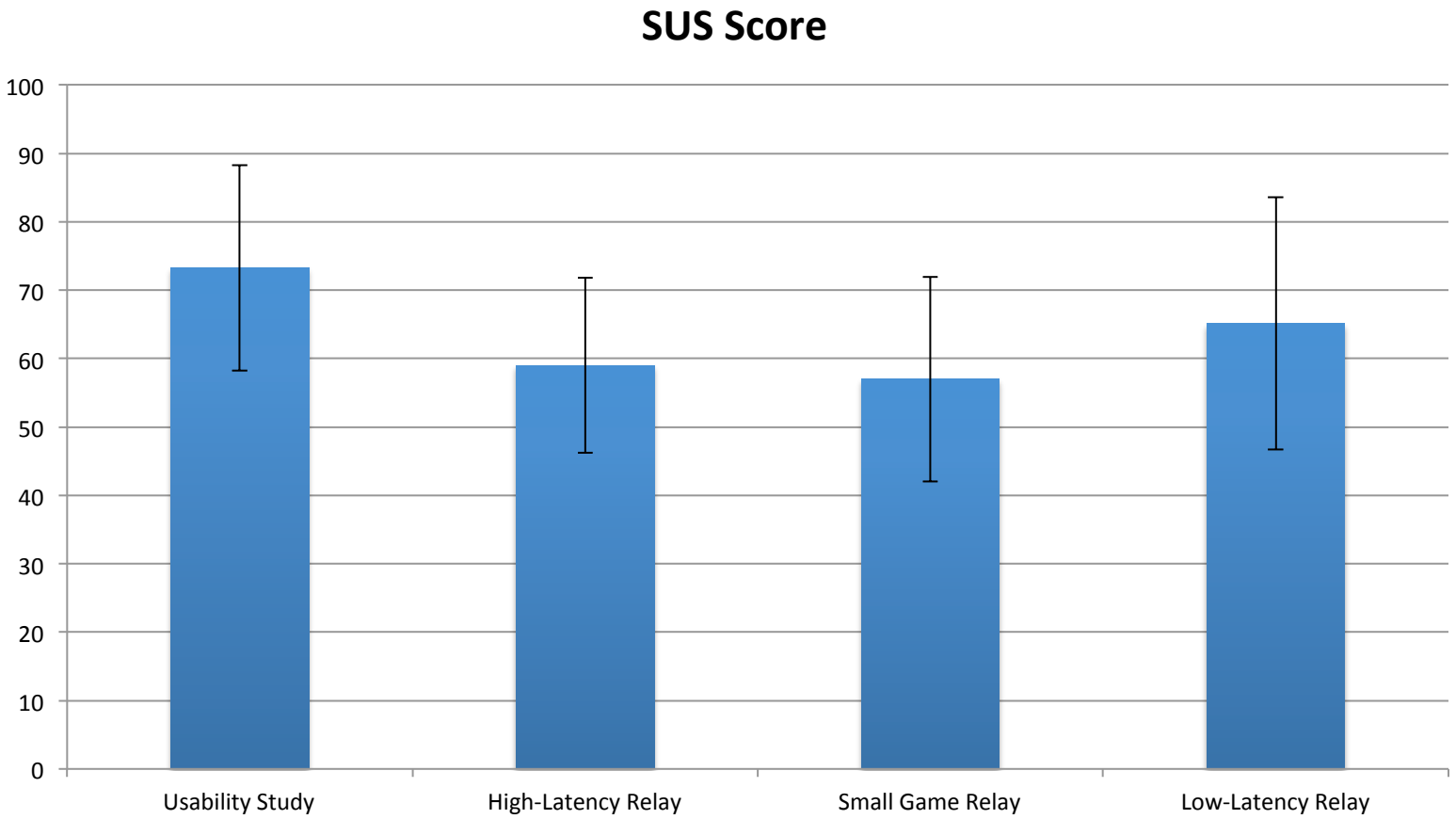
successful play time (Usability vs. Relay)



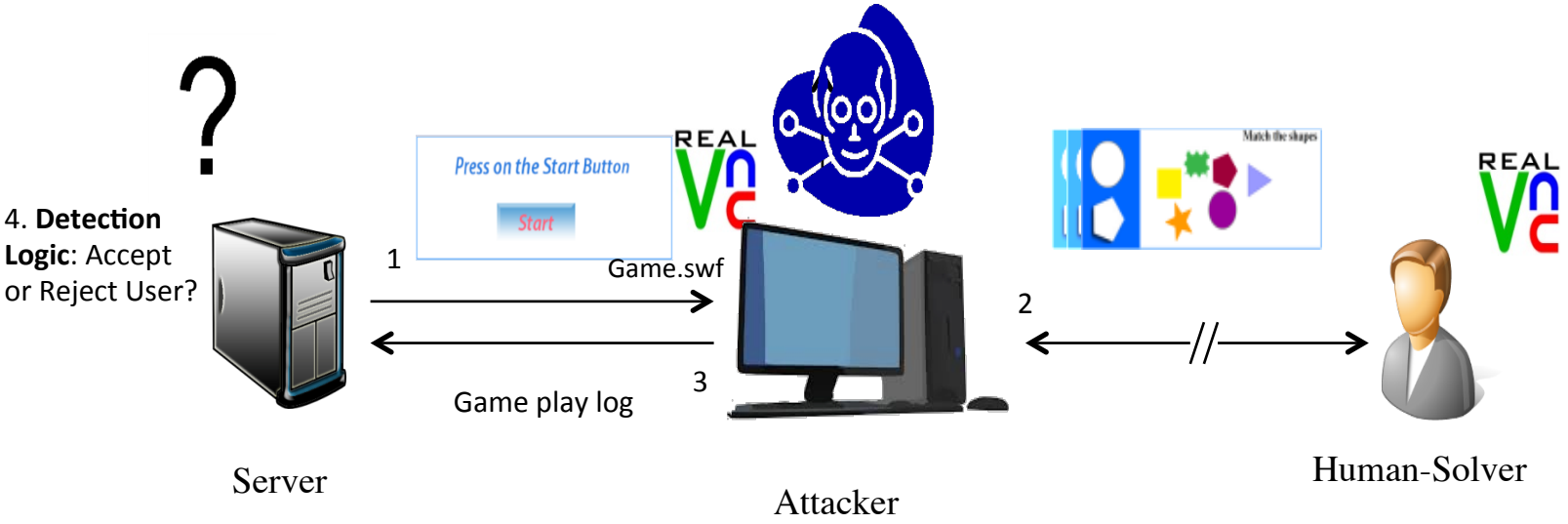
Results
Error Rate (Usability vs. Relay)



Results
SUS (Usability vs. Relay)



Stream Relay Attack Detection



Stream Relay Attack Detection

- We designed a Stream Relay attack detection mechanism based on data collected from the usability and relay attack study
- Our detection mechanism utilizes real-time game statistics, such as:
  - play duration
  - mouse clicks
  - incorrect drags
- Game metrics fed to machine learning algorithms, to differentiate legitimate user gameplay from human-solver gameplay

Stream Relay Attack Detection

Results of using the common optimal feature subset for each game in classification of *legitimate user* and *High-Latency* relay attacker

Game Name	Method	Average Accuracy	Average Precision	Average Recall
Animal	SVM	0.95	0.94	**0.98**
Parking	SVM	0.85	0.83	**0.95**
Shape	SVM	0.80	0.76	**0.94**
Ships	SVM	0.92	0.91	**0.94**

Stream Relay Attack Detection

Results of using the optimal feature subset for each game in classification of *legitimate user* and *(High- Latency, Low-Latency and Small Game)* relay attacker

Game Name	Method	Average Accuracy	Average Precision	Average Recall
Animal	SVM	0.85	0.75	**0.97**
Parking	SVM	0.74	0.65	**0.76**
Shape	KNN	0.78	0.66	**0.75**
Ships	SVM	0.83	0.73	**0.87**

Discussion and Conclusion

- DCG CAPTCHAs instances tested in this work are quite usable
- The proposed relay detection is very efficient.
  - When using SVM, it requires 0.224 msec training with 66 training records, and about 0.087 ms for testing a single record
- Our study suggests that increasing the interaction between users and CAPTCHAs improves the ability to detect relay attack
- DCG CAPTCHAs appear to be first CAPTCHAs that can offer resistance to relay attacks

Thank You!

	Usability	Stream Relay Attack		
Participant Location		Outside US		US
Game Size	360x130	360x130	180x65	360x130
Participant Size (N=120)	40	40	20	20
Gender (%)				
Male	67.5	67.5	80	80
Female	32.5	32.5	20	20
Age (%)				
<18	2.5	2.5	0	0
18 - 24	40	30	45	35
25 - 35	42.5	52.5	35	50
35 - 50	10	12.5	20	10
>50	5	2.5	0	5
Education (%)				
High school	10	0	0	55
Bachelor	60	57.5	75	40
Masters	27.5	42.5	25	5
Ph.D.	2.5	0	0	0
Field of Study/Profession (%)				
Computer Science	32.5	52.5	55	15
Engineering	20	20	30	5
Medicine	2.5	5	5	5
Law	2.5	2.5	0	0
Social sciences	5	0	0	5
Journalism	0	0	5	5
Finance	12.5	7.5	0	5
Business	10	0	0	20
Other	15	12.5	5	40
Country (%)				
Afghanistan	2.5	0	0	0
Australia	0	0	5	0
Egypt	2.5	0	2.5	0
India	62.5	92.5	85	0
Ireland	0	2.5	0	0
Italy	0	0	5	0
Macedonia	0	2.5	0	0
Romania	0	2.5	0	0
United Arab Emirates	2.5	0	2.5	0
United States	30	0	0	100
Vietnam	0	0	5	0

Stream Relay Attack Detection

Features used to train the classifiers:

1. *Play Duration*
2. *Successful drag rate*
3. *Number of attempts*
4. *Average dragging time*.
5. *The maximum duration among all invalid mouse drags in a gameplay instance*.
6. *Number of timestamps in the invalid mouse drag with the longest duration*.
7. *The product of Features 5 and 6*.