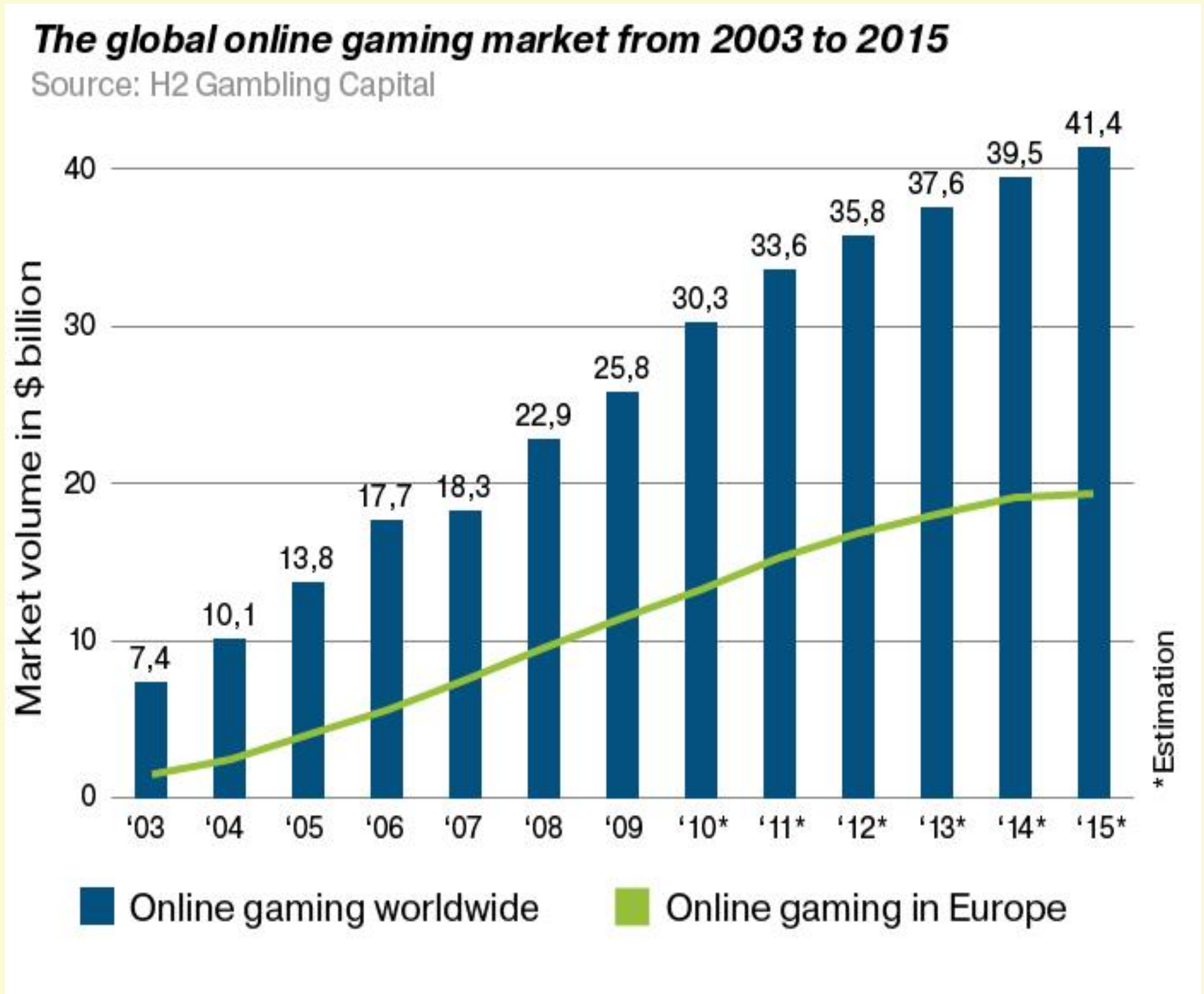
Security Evaluation Of Online Multiplayer Poker Game

Aabha Biyani and Manish Choudhary, {abiyani7, mchoudhary8}@mail.gatech.edu, M.S. in Information Security, Georgia Institute of Technology
Mentor: Professor Patrick Traynor, traynor@cc.gatech.edu, Georgia Institute of Technology

PROBLEM

- **Global online gaming market share is around 40 Billion USD**
- Online poker game rooms involve an alluring amount of money seeking attention of adversaries
  - In 2008, **100,397 number of gaming Trojans** were designed to steal passwords to several online games at once
- Worse, colluding cheaters can use these poker sites as major **money-laundering channels**



- **Humongous financial risk and threat to privacy** demand the security evaluation of online games to create awareness about the technical and design flaws in the system

FINDINGS

PASSWORD POLICY/ AUTHENTICATION

- Only **optional password** policy
- **Clear-text display** of passwords on the screen
- Unencrypted transmission of passwords
- **No policy** to strengthen the passwords or to prevent password cracking

CONFIDENTIALITY AND INTEGRITY

- **Unencrypted transmission** of passwords, chat messages and table information
- No integrity check may lead to **impersonation by sniffing client's UUID**
- Man in the middle attack: **Interception/modification of opponent's cards**

CHAT SERVER

- Upper bound of 200 characters in a single message
- **Chat flood protection** to prevent resource exhaustion
- Unencrypted transmission of chat messages **vulnerable to interception and modification**

AVAILABILITY

- Default restrictions on number of connections
  - Maximum connections per IP: 3
  - Maximum active games per client: 2
- **Denial of Service:** Maximum capacity could be consumed easily

CHEATING STRATEGIES

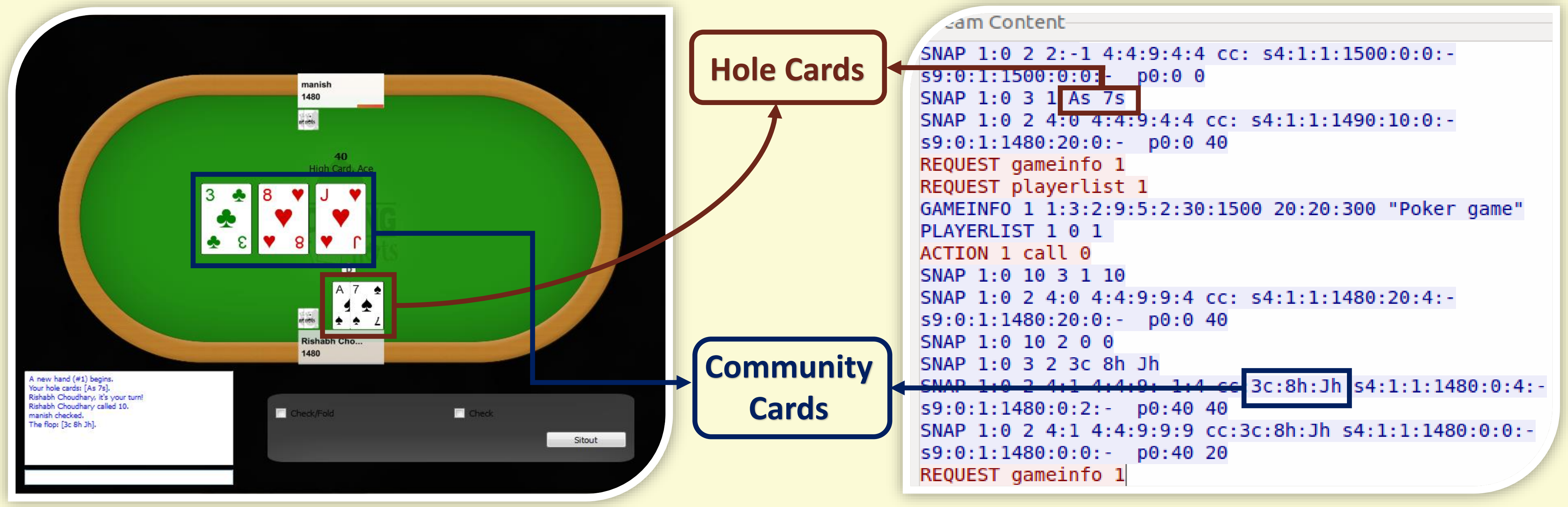
- Shuffling
  - Randomly seeded random_shuffle() API
- **Exposal of Hole Cards**
  - Table information transmitted in clear-text
- **Collusion**
- **House Cheating**

COLLUSION

- **No collusion detection algorithm**
- **External communication channels can be used to collude** using following strategies:
  - Raise to kick players out
  - Raise to impose bad odds
  - Raising each other for more profit
  - Avoid playing themselves
- Random allocation of positions to players tries to restrain collusion

GAME DESIGN

- Use of C++ STL's random_shuffle API to provide randomness
- Input Validation
- Checks for buffer bounds
- Network disruption on a client's end leads to that **client getting folded pushing the pot to the opponent**



```
SNAP 1:0 2 2:-1 4:4:9:4:4 cc: s4:1:1:1500:0:0:-
s9:0:1:1500:0:0:-  p0:0 0
SNAP 1:0 3 1 As 7s
SNAP 1:0 2 4:0 4:4:9:4:4 cc: s4:1:1:1490:10:0:-
s9:0:1:1480:20:0:-  p0:0 40
REQUEST gameinfo 1
REQUEST playerlist 1
GAMEINFO 1 1:3:2:9:5:2:30:1500 20:20:300 "Poker game"
PLAYERLIST 1 0 1
ACTION 1 call 0
SNAP 1:0 10 3 1 10
SNAP 1:0 2 4:0 4:4:9:9:4 cc: s4:1:1:1480:20:4:-
s9:0:1:1480:20:0:-  p0:0 40
SNAP 1:0 10 2 0 0
SNAP 1:0 3 2 3c 8h Jh
SNAP 1:0 2 4:1 4:4:9: 1:4 cc 3c:8h:Jh s4:1:1:1480:0:4:-
s9:0:1:1480:0:2:-  p0:40 40
SNAP 1:0 2 4:1 4:4:9:9:9 cc:3c:8h:Jh s4:1:1:1480:0:0:-
s9:0:1:1480:0:0:-  p0:40 20
REQUEST gameinfo 1
```

Packet capture exposing the game cards of an opponent

METHODOLOGY

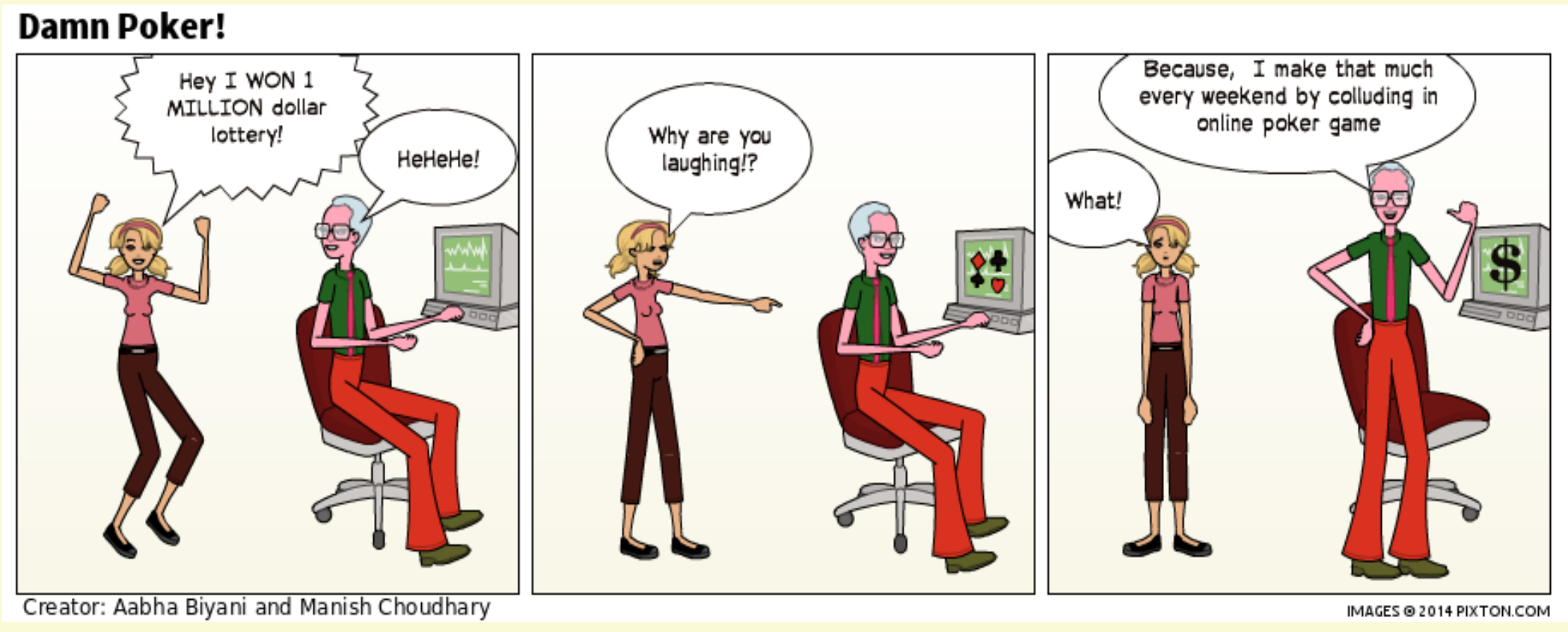
- Evaluation of "**Holding Nuts** – an open source poker application" to understand the potential flaws in an online poker room
- Static and Dynamic analysis
- **Evaluated Areas:**
  - Confidentiality & Integrity
  - Availability
  - Password Policy
  - Authentication
  - Chat Server
  - Network Communication
  - Collusion
  - Cheating Strategies
  - Game Design

RECOMMENDATIONS

- Use of **TLS/SSL**
  - Secure network communication
  - Mutual authentication
- **Scalable** and **Fault tolerant server**
- **Collusion detection and Auditing systems**
- Use of **Strong Authentication** mechanisms
  - One time passwords
  - Two factor authentication
  - Strong and mandatory password policy

TAKE AWAY

- **Security of online games is paramount** from financial and privacy aspects
- **Attention of security research community is required** for secure and trusted gaming environment
- Should use (only) **standard cryptographic protocols**
- Should build **dependable servers** and **Strong authentication systems**
- Should implement **Cheating Prevention/Detection** systems


Damn Poker!
Hey I WON 1 MILLION dollar lottery!
HeHeHe!
Why are you laughing!?
What!
Because, I make that much every weekend by colluding in online poker game
Creator: Aabha Biyani and Manish Choudhary
IMAGES © 2014 PIXTON.COM

ACKNOWLEDGEMENTS: We are grateful to **Professor Patrick Traynor** for valuable guidance, **Brad Reaves** for reviewing and sharing insights on poster design and **Library Staff of Multimedia Lab** for helping us to print the poster