Project Proposal

Thomas Hybel, 201303525
Meinhard Dam, 201303531
Steffen Strunge Mathiesen, 201407114

October 2017

Introduction

For our project, we propose a distributed version of the card game Uno.

Use case

Alice, Bob and Eve are having a party, but they are bored. They would like to play a game of Uno, but Alice and Bob don't trust Eve – she always cheats when they play Uno.

Luckily, they all have access to computing devices connected to the same network. So they launch the application Distributed Uno and join a game. Their devices compute a distributed deck of cards which is shuffled. They are each assigned a hand from the deck, letting them play the classic Uno game using their devices.

The assignment of cards happens in a secure fashion, preventing Eve from cheating. Since the application is distributed among many peers, there is no central authority for Eve to attack either, so Alice and Bob feel at ease and have a good time.

Description of how and why IoT/P2P will be used

Our project mainly focuses on P2P to prevent cheating and avoid having a central trusted authority. Specifically, P2P will be relevant for the following features:

- Secure shuffling of the deck: no player should be able to choose the order of cards in the deck.
- Secure assignment of cards to players.
- Commitment of all players to every move, ensuring agreement between players and that moves cannot be undone at a later time.

- Distributed high-score lists could be maintained.
- A lobby system which easily lets players arrange games.

There will likely be many specific ways to cheat, and we plan to consider a subset of these and prevent them using P2P techniques.

It is also possible to extend the project to have IoT aspects by, e.g., adding special cards which interact with an IoT thing, such as a smartphone.

A sketch of the envisioned architecture

We have not yet decided on the specifics of our architecture, but it will incorporate a number of devices communicating with each other. Our architecture will feature the following concepts:

- A normal card, with a number and a color
- A special card, requiring a special action
- A hand of cards
- A deck of cards to pick from
- A stack to deposit cards onto
- Actions, such as picking up a card or passing on the turn
- Rounds
- A game which consists of rounds

There are various problems which we have not yet decided how to solve. Among these are the following considerations:

- How should communication between players work? Multicast? A ring? Etc.
- How should a shuffled deck be generated securely?
- How can we ensure that players can't pretend to have other cards than they do?
- Should the deck be replicated on every peer, or on some of them, or be stored distributed?

These open problems will be solved during our project work.

Weekly milestones

- After week 43, we expect to have read relevant papers and figured out how to solve many of the security problems in our architecture.
- After week 44, we expect to have implemented secure deck shuffling and hand assignment.
- After week 45, we expect to have a working, mostly secure subset of Uno with no special cards.
- After week 46, we expect to have added at least some special cards to our system.
- After week 47, we expect to have added some additional feature(s) to our system, such as a card based on an IoT-device, a lobby system, or such.