Workshop on: Exploring the Challenges of Ethics, Privacy and Trust in Serious Gaming

Rod McCall[1], Lynne Baillie[2], Franziska Boehm[1], and Mike Just[2]

[1]EMACS Research Unit & Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg-Kirchberg, L-1359
[2]Interactive and Trustworthy Technologies Research Group, Glasgow Caledonian University, Glasgow, G4 0BA

```
roderick.mccall@uni.lu, l.baillie@gcu.ac.uk,
franziska.boehm@uni.lu, mike.just@gcu.ac.uk
```

Abstract. The workshop will explore the core challenges associated with the increasing use of serious gaming in particular those systems that seek to persuade users to alter their behavior. The workshop will focus on three main areas: data privacy, trustworthiness and usability. The workshop particularly welcomes submissions from people who seek to bridge the divide between these topics.

1 Introduction

Serious gaming technologies are being used to address a number of societal challenges such as traffic congestion, e-health, cross cultural awareness and education. Furthermore, as these technologies become increasing mobile, social and ubiquitous in nature a number of core challenges arise.

Firstly, as has been documented within the media, mobile phone manufacturers and operating system developers often insert clauses that allow their platforms to store the location and other private information. As users frequently fail to read the full terms and conditions they are often unsure of precisely what is being stored about them and how it will be used. The problem of data retention also extends to massive multiplayer online games and worlds such as SecondLife. This leads to a perceptual gap in terms of what users believe they have signed up to and what they have actually agreed to.

As a result there is a need to explore the data privacy and protection issues that surround serious and persuasive gaming. For example, at present data is often stored by the provider or manufacturing company e.g., SecondLife, Google or Apple who have access to all the user actions and information. The data privacy issue is even more problematic in areas such as ehealth.

Currently many games platforms and technologies are being used for e-health and rehabilitation in particular e.g. the Wii, Kinect etc. This has shifted the gaming platforms from being technologies for play into being medical devices for rehabilitation and monitoring. What are the implications of this from a privacy and trust perspec-

tive? Further how can we ensure that we design ehealth serious games to ensure that they are fit for purpose?

User acceptance of games as a viable tool is necessary for users to fully engage in a consistent and accurate manner. A lack of acceptance or trust in how the games behave (the "rules") and how it treats them and information could reduce or nullify potential game benefits. In particular, proper design and interaction with the user are critical to ensure appropriate and acceptable game actions and responses, especially for applications such as e-health where some users might already be in sensitive or vulnerable situations. Trust may also be derived from the game results and how they are presented and conveyed, as can be seen in a workplace environment where colleagues may be able to see the results of others, especially if game results were to portray a user in a particularly negative way.

In multi-player games, trust in player authenticity is important to ensure that impersonators cannot access personal information, or attempt to receive game benefits belonging to other users. Trust also hinges upon games being played "within the rules", including the behavior of the game players and the game manager. Proper design and interaction with users is thus important in terms of a trustworthy design and in conveying this to participating users.