# Balancing Security Requirements and Emotional Requirements in Video Games

David Callele, Eric Neufeld, Kevin Schneider
*Department of Computer Science*
*University of Saskatchewan*
*Saskatoon, Saskatchewan, Canada S7N 5C9*
{*callele,neufeld,kas*}*@cs.usask.ca*

## Abstract

*A fundamental conflict exists between designers, players, and cheaters:* Who has control over how the game is played? *Resolving this conflict, by balancing the associated emotional and security requirements is challenging.*

*Emotional requirements can assist the development of security requirements and to prioritize their development. Failure to meet the player's emotional requirements can lead to market forces that override security requirements. We suggest that in-game justice systems would allow the players to act as a self-correcting mechanism for emotional requirement failures that lead to cheating or other threats to the integrity of the game experience. Further investigation into this form of just-in-time requirements negotiation is ongoing.*

*Keywords: Non-functional requirements, emotion, emotional requirements, security, security requirements, video game.*

## 1. Introduction

The dominant security goal for most video games is ensuring the integrity of the playing experience. This goal is shared by all constructive stakeholders; Consalvo [1] and others have shown that players need to trust the integrity of the game – the same rules must apply to all participants and no player should have an unfair advantage over another.

A developer might define the corresponding security requirement as "All players shall play the game only as the designer intended the game to be played." However, if players don't enjoy the approved method of gameplay they will turn to cheating in an attempt to get at least some value from their investment. And as Consalvo [*ibid.*] notes "...cheating isn't just about subverting the (game) system; it's also about augmenting the system. It's a way for individuals to keep playing through boredom, difficulty, limited scenarios, rough patches or just bad games."

These comments illuminate the fundamental conflict between the player and the designer: *Who has control over how the game is played?* Is the player only allowed to play the game as designed? Or does the player control how the game is played? Perhaps the answer lies somewhere in-between.

In this work, we explore the intersection of security requirements and emotional requirements, investigating the use of emotional requirements to assist in the development of security requirements and identifying justifications for overriding security requirements with emotional requirements.

## 2. Related Work

While there is no universal definition for cheating [3, 1], Yan provides a cheating classification [6] that builds on prior work in security issues, extending Pritchard's work [4] while relating it to more traditional mechanisms for understanding and defining security requirements and security design. The most detailed analyses of cheating in video games is that by Consalvo [1], broadening our understanding of player motivations for cheating. The motivating factors for grief play (play that deliberately disrupts other players) have been most extensively studied by Foo [2], and to a lesser extent, Consalvo [1] while justice systems [5] remain relatively ignored.

## 3. Evaluating Threats

Players are not usually a traditional security threat such as a disgruntled employee in search of revenge. They are more like a frustrated employee who attempts to use unauthorized (if not illegal) means to bypass what they perceive to be obstacles to the proper discharge of their duties.

Emotional requirements can assist in evaluating the risk levels of these security threats. Identifying the sources of greatest frustration to the player, the *emotional irritants* (a negative emotional requirement, or a failure to meet

1090-705x/08 $25.00 © 2008 IEEE
DOI 10.1109/RE.2008.45

an emotional requirement) will identify those issues most likely to sufficiently motivate the player to attack the game. The risk factor for an emotional irritant can be expressed as:

$$\text{Risk Factor}(\text{Emotional Irritant}) = \frac{\text{Level of Irritation}}{\text{Cost of Attack}}$$

Those security requirements associated with high risk emotional irritants should receive high priority in the development plan.

## 4. Resolving Requirement Conflicts

If the 'approved' method of gameplay is not actually fun for the players, the game may be a sales disaster. At this point, the developer and publisher will be strongly motivated to salvage some form of revenue stream – even if it means arbitrarily relaxing the security restrictions via a source code patch, or the publication of means for accessing alternative operating modes (*e.g.* developer shortcuts, *a.k.a* cheat codes). The initial security requirements are overridden in an attempt to salvage a flawed game – demonstrating that there do exist situations where emotional requirements can override security requirements.

There does not appear to be an optimal resolution to the conflict between security requirements and emotional requirements – the security goal of ensuring the integrity of gameplay is unlikely to be achieved. Instead, a negotiation process is needed that eliminates the requirement to identify and resolve all problems *a priori* yet allows them to be resolved as they occur and in a manner that addresses the emotional requirements of the stakeholders.

This resolution can be provided *just-in-time* by introducing an in-game justice system to apply corrective action to those who corrupt the integrity of the game experience. Sanderson [5] provides an informative view of such justice systems. For an in-game justice system to be effective, it must address issues of judicial authority, the penalties associated with various 'crimes', enforcement mechanisms, and whether enforcement has real-world consequences.

An in-game justice system can be used as a fall-back, catching those cases that were not considered in the requirements. Determining the requirements for a justice system, then developing and implementing it is expensive but we expect that some of the cost may be offset by reducing the number or scope of the initial security requirements.

Experience has shown that if griefing is not addressed, the griefers will come. Placing justice in the hands of the players means that they can act as dynamic systems that are able to adapt to, and counter, griefing tactics. We expect that the griefers will tire of victims that fight back and will move on to easier prey (in other systems).

## 5. Summary and Future Work

We have shown that emotional requirements can assist the development of security requirements by identifying the motivation behind security threats. The emotional irritants that motivate the attacks can be addressed proactively, potentially reducing the magnitude of the risk. Emotional requirements can also be used to help prioritize security requirements; strong emotional irritants that require low effort to overcome are the most likely attack vectors. The high-risk security requirements identified in this manner should be prioritized during development.

Failure to meet the player's emotional requirements can lead to market forces that override security requirements. If the emotional requirement failures are as a result of cheating or other threats to the integrity of the game experience, we suggest that in-game justice systems would allow the players to act as a self-correcting mechanism in the face of these security failures. The justice system places further requirement negotiation in the hands of the players, providing them with a framework wherein their own community values can develop.

Further investigation into the use of in-game justice systems as a form of just-in-time requirements negotiation is warranted and ongoing. The role of the community as a self-policing entity is worthy of further investigation, particularly with respect to the effects on the stringency necessary for the security requirements for that community: if the players will self-correct, it may not be necessary to invest as heavily in security infrastructure.

## References


[1] Mia Consalvo. *Cheating: Gaining Advantage in Videogames*. The MIT Press, 2007.

[2] Chek Yang Foo and Elina Koivisto. Grief Player Motivations. In *Proceedings of the Other Players conference*, page Online, Copenhagen, Denmark, 2004. IT University of Copenhagen.

[3] Julian Kuecklich. Other playings: cheating in computer games. In *Proceedings of the Other Players conference*, page Online, Copenhagen, Denmark, 2004. IT University of Copenhagen.

[4] Matt Pritchard. How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It. *Gamasutra*, 2000.

[5] Derek Sanderson. Online Justice Systems. *http://www.gamasutra.com/features/20000321/sanderson_01.htm*, 2001.

[6] Jeff Yan and Brian Randell. A systematic classification of cheating in online games. In *NetGames '05: Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games*, pages 1–9, New York, NY, USA, 2005. ACM.