Requirements in Conflict: Player *vs.* Designer *vs.* Cheater

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

There are significant interactions between video game stakeholder emotional requirements and security requirements. Counter-intuitively, some traditional security requirements are not necessarily met by the game implementation – some forms of security breaches are condoned by the stakeholders (if not actually demanded by them) and the requirements engineering process must support these contradictions.

We present an overview of security requirements for video games and show how stakeholder diversity introduces significant complexities to the requirements negotiation process. Our analysis of certain security threats, and their emotional motivations, shows that these motivations form an important element of the emotional requirements and that significant context is necessary for properly capturing the emotional requirements related to security. Finally, we show how emotional requirements can be used to guide security goal development for this domain and propose the use of in-game justice systems to allow players to address security violations in realtime.

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

1. Introduction

Stakeholders often have differing opinions on the relative importance of a requirement. For productivity applications, the set of stakeholders is typically dominated by the users of the application and their immediate management. The stakeholder domain for video games must be more diverse. The entertainment aspect of the product means that emotions are involved and that there may be interactions that are not necessarily logical.

The stakeholders range from financiers to players and they share the common desire for a great game. However, great games are not easy to create. In prior work we showed that capturing the game designer's vision was difficult [4] and we introduced emotional requirements, emotion timelines, and emotion terrains [5, 6] to help capture that vision. Using a detailed case study performed with an industrial partner, Alves *et al* [3] elaborate on the challenges faced in requirements engineering for mobile video games, extending our work on requirements engineering for video games[4].

Emotional requirements, as originally envisioned, were a constructively motivated, creative affordance, used to help deliver the intended emotional experience to a willing audience. All stakeholders were assumed to be similarly constructively motivated, desiring the best entertainment experience that they could achieve.

But not all players are the 'good guys'. Not everyone plays fair. In fact, a significant number cheat and, even worse, some of them actively attempt to disrupt or destroy the game experience for other players. We can model these stakeholders as security threats of a very particular type: they are willing, but apparently hostile and destructive, users.

These destructive stakeholders are motivated in some way to act as they do. It is these motivations that we capture as (perhaps unfulfilled) emotional requirements. Rather than adopting a simple "all destructive stakeholders are the enemy" attitude, in this paper we explore the intersection of security requirements and emotional requirements, asking:

- Can we use emotional requirements to assist in the development of security requirements?
- Can emotional requirements be used proactively, to identify the motivations behind the security threat?
- Can emotional requirements be used to ameliorate security risks by providing insight into threat motivation?

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

- Are there situations where emotional requirements can override security requirements? And if so, with what justification?

To begin, we identify the constructive and destructive stakeholders and briefly explore their motivations. We review the related work and then present an overview of a generic security model for a typical multiplayer video game. A threat analysis is performed and possible attack vectors are explored to demonstrate how the related security requirements can be enhanced by emotional requirements. Conflicting emotional requirements are investigated to determine how they impact security requirements, and how the various demands can be balanced. We conclude with a demonstration of guiding security goal development for this domain with emotional requirements by deploying an in-game justice system then provide directions for future work.

2. Stakeholders

Consalvo [10] introduced the concept of *gaming capital* as a motivator for, and means of valuing, interactions between stakeholders in the gaming domain. Gaming capital is based upon economic principles, with *capital* an abstract representation of value or worth that has the (potential) ability to be exchanged between stakeholders. We motivate the stakeholder identification process with a simple producer / consumer model.

2.1. Producers

A functional analysis of the production process identifies the following primary contributors. The *Designer* works for a *Developer* that has a publication agreement with a *Publisher*. The Publisher arranges distribution with a *Distributor* that delivers the game to a *Vendor* who sells it to the final consumer. The secondary contributors include the *Financier*, who provides the necessary financial capital to all parties, the *Marketer*, who stimulates demand for the product, often working closely with the *Media*, who report upon the product. There are also *After-market suppliers*, providers of information, software, and hardware that interacts with the product and *Regulators*, that ensure compliance with regulations imposed by *Society*, an abstraction that exhibits (often contradictory and unpredictable) emotional responses to the product.

The supply side of the model is relatively straightforward and follows well-established free-market principles. The supply chain starts with a designer that we shall denote as principally artistically motivated. The developer, representing the studio that transforms the game from concept to product is denoted as motivated both artistically and economically, with the economic motivation dominant (those studios that are principally artistically motivated rarely survive for long). It is worth noting that, in the domain of multiplayer gaming, the Developer also has a long-term economic commitment to operating a game related service of some form.

The remainder of the primary supply side contributors are fundamentally economically motivated. So are the secondary supply side contributors, with the exception of *society* which we denote as emotionally motivated, but in a manner that we can not predict.

The economically motivated stakeholders are modeled here as perfect capitalists. Their sole emotional requirement is for success, as measured by their ability to make a profit. While this abstraction may ignore the contributions of their other emotional factors, it is sufficient for this work.

2.2. Consumers

The consumer stakeholders do not always follow the traditional user behavior patterns. Their behavior is complicated by the fact that they expect that their (non-functional) emotional requirements for entertainment will be satisfied.

However, when the playing experience goes poorly then player emotions, attitudes, motivations, and actions change dramatically. The player finds that their emotional requirement for *fun* is not being met. For example, they may perceive that their efforts to play are being thwarted, they may feel betrayed by the game, or they may even feel threatened by other players. The player now views some element(s) of the game playing experience in an adversarial manner.

Independent of the reason for the shift, while the player maintains this attitude we consider them a destructive stakeholder. However, the player still wants to play – it is just that they can not find satisfaction so they turn to alternatives that many would consider cheating.

Since the player still wants to fulfill their emotional requirement for fun, they should not be considered a traditional security threat. They are not, for example, 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.

Within our economic model, these players are consumers that are willing to invest in purchasing the product. However, if the product fails to deliver its promised utility, they are willing to 'do what it takes' to get what they perceive to be value for their money (even if that means bending or breaking the 'law' as a last resort).

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

2.3. An Example

The relative nature of the definition of a destructive stakeholder (judged by intent rather than perception) means that we are exposed to observational error. However, in this work, we are looking for ways to be proactive, not reactive, so the temporal accuracy of an observation is not as important, just whether or not the player entered an adversarial attitude.

For example, assume that the player is unable to progress beyond a certain point in a game because they can not solve a particular puzzle[4]. They are unable to find any clues in the game as to how to proceed and their frustration level is very high. From their perspective, the game is a failure. In order to salvage their investment, they turn to the Internet for help. After a few minutes of searching, they find a guide (commonly termed a *walkthrough*) that explains how to get past this puzzle. Using this advice, they are finally able to continue with the game.

Did the player cheat?

For now, at least, the answer is irrelevant. What is relevant is the difference between intent and perception. The player perceives that the game is flawed: the puzzle was too difficult, and the designer neglected to provide a support mechanism of some form. Their emotional requirements for "fun", and for "receiving value for my money" dictate that they go out-of-game to meet their requirements.

Contrast this with the perception of the game designer: the player cheated, they went outside of the game for help and the player has broken the implied contract to "play the game as intended". The player has violated the designer's emotional requirement for maintaining the integrity of their artistic vision.

The emotional requirements for the designer and the player are in conflict; the designer now considers the player to be a cheater and the player feels that the designer has betrayed them. The *reason* for the conflict is always important, knowing *when* the conflict occurred is important only if the designer wants to reduce or eliminate a specific conflict.

2.4. The Exception to the Rule

It should be noted that there exists a class of players that do not fit well into this economic model. These are the *griefers* (players who participate in the game for the purpose of interacting with other players in a negative manner, see Section 3.6 for further details). They have no apparent rational economic basis for their actions; their behavior appears to be a manifestation of an emotional requirement for power (over others). As such, they appear willing to perform a direct exchange of game capital for emotional capital (gratification) – a currency exchange not willingly shared by the other stakeholders.

3. Related Work

We now review the security requirements literature, literature on player types, motivations, and their attributes as destructive stakeholders. We close with related work on negotiating conflicting requirements.

3.1. Security Requirements

Due consideration of security goals within the requirements engineering process is expensive and an informed cost-benefit decision is strongly recommended. Crafting security requirements is challenging [19, 13, 24] and many factors [26, 30] should be considered. Prioritizing security requirements [24] for video games is made even more difficult by problems with determining the economic value of play.

Security requirements also conflict with the emotional requirements of an immersive play experience. For example, authentication can be an intrusive operation. However, if a constructive player perceives that the game is prone to attack by destructive players, they may feel that there is sufficient justification for the authentication measures.

Moffet *et al* [26] state that it is not necessary to know the goals of the individual attackers when performing risk analysis, just what kind of attack they will mount. We substantively differ in this work: we look directly at motivation (the *why* behind the threats, and security in general) and try to determine if there are emotional requirements that can be met that mitigate the risk factors. Unlike the general practice of attempting to resolve all conflicting requirements, emotional requirements may not be resolvable – all that may be achieved is a set of requirements that lead to a state of constant, small-scale skirmishes between constructive and destructive stakeholders.

3.2. Misuse, Abuse, and Anti-Requirements

We have identified destructive stakeholders by their behavior patterns. These behavior patterns have strong parallels in the requirements engineering literature. Misuse and abuse cases [23, 36, 2, 18] are use cases that explicitly identify threatening scenarios (such as cheating) so that they may be proactively considered during systems design. The role of griefers and grief play is most similar to anti-requirements [11], a "requirement of a malicious user that subverts an existing requirement."

Emotional requirement failures are closely related to Pott's obstacles [31, 37]. The player's goal (to have fun) is blocked by failures in the game design [1].

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

3.3. Threats and Attacks

Attacks can be modeled [27] in many ways - most commonly in scenario form [28]. Difficulties [27] include organizing, managing, and prioritizing.

Resources detailing known attacks on games are readily available [7, 17]. These attacks have been roughly categorized [22] as cheating against the provider, other players, or the virtual society. There are active efforts [32, 16] to reduce the effectiveness of such attacks. However, Golle [16] notes that "...no defense appears possible against an adversary who has more intrinsic utility for using a bot than for winning the game." In other words, if the player is simply being destructive, with no rationale consistent with the game, then there is no protection against their actions.

3.4. Player Types

Numerous researchers have studied players in attempts to provide taxonomies of player types and player motivations. In particular, Yee [42, 41] has extensively studied players in massively-multiplayer online games. While most of the player types and their motivations are constructive, his analysis has confirmed the presence (and disruptive capabilities) of grief players but does not investigate cheating behaviors in detail.

3.5. Cheating

While there is no universal definition for cheating [21, 20], Yan provides a cheating classification [40] that builds on prior work in security issues [39, 38]. Yan extends Pritchard's work [32], 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 [8, 9, 10] broadening our understanding of player motivations for cheating. These motivations have strong parallels with emotional requirements and form the basis for parts of this work

Most research into cheating does not address justice systems [35] although some do report on common practice at the time [38, 10].

Issues of morality and ethics have been addressed [34, 29, 10] and it is instructive to understand what mechanisms can be used to evaluate *good vs. bad* or *right vs. wrong*. Only then can questions like this be answered: If there are no consequences to breaking the rules, can an act be called cheating? Can a player cheat in a single-player game?

3.6. Grief Play and Griefers

Grief play (play that is intentionally disruptive of the game and other player's game experiences) and griefers (those who perpetuate grief play) have come to significantly greater attention with the advent of multiplayer online games. While there have always been those who play in this manner, they could only affect those in physical proximity; their actions were self-limiting. With the Internet, griefers can disrupt players anywhere in the world.

The motivating factors for grief play have been most extensively studied by Foo, and to a lesser extent, Consalvo [10]. Foo [14] reviews the prior work, compares it with other research into bullying and teasing and identifies four motivating influences: game (and game management) influenced, player influenced, (other) griefer influenced and self (griefer) influenced.

In later work, Foo [15] presents a more detailed analysis of the concept of grief play, looking at intention, perception, and side-effects. Three rule classes are identified: those in the code, those in the service contract (including game rules), and those implied by the game community via social etiquette. The importance of perception, particularly of motivation, is brought forward and is related to our work on stakeholder differences. As above, there remains an open question of rule enforcement and justice systems: Who has authority and what are the penalties?

3.7. Emotions in Requirements

Now that we have broadened the applicability of emotional requirements, we note that Ramos *et al* [33] performed earlier investigations into the interactions between change (organizational transformation, most particularly in Information Technology systems), requirements engineering, and the emotions of those affected by the change(s). In particular, they address the issue of including the users emotional responses into deployment planning, attempting to mitigate any issues before they become blockers – a proactive approach similar to our current work.

3.8. Negotiating Requirements

Easterbrook *et al* [12] describe a development environment quite similar to game development. The different viewpoints utilized in this work correspond to the perspectives of the constructive stakeholders in this work and consistency checking within a viewpoint is analogous to resolving emotional requirement conflicts. Of particular interest is the observation that requirements inconsistencies are not failures, they only need to be resolved if the owner of one of the inconsistencies requires resolution.

Menzies *et al* [25] describe a negotiation process

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

whereby the mutually agreeable set of common viewpoints are identified such that a group can constructively work together. They note the importance of *buy-in*, an emotional commitment to the success of the endeavor. By adjusting perspectives, they show that the common set of requirements can be larger than anticipated.

The multi-disciplinary nature of the present work has been reflected in the breadth of the related work. It represents a synthesis of security analysis, security requirements, emotional requirements, requirements negotiation, and motivational psychology.

4. Security and Video Games

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 and others (see Section 3.5) have shown that players need to trust the integrity of the game – the same rules must apply to all participants and their playing experience should never include attacks by other players unless they have agreed to that playing mode[1]. We restrict our current analysis to this single goal.

In practice, "ensuring the integrity of the playing experience" is an excessively vague goal. The Developer may define the corresponding security requirement as:

> The player shall play the game as the Designer intended the game to be played.

Once the requirements engineering team is done with it, the same requirement might look like:

> All inputs to the system must be validated according to the Input Validation Rules as defined in Appendix A: Acceptable Game Play.

where Appendix A is a formidable document that, given the complexities of the typical video game, would be unlikely to provide complete coverage of all potential interactions.

The cost/benefit analysis for this scenario is complex. What is the value associated with ensuring that the game is played only in the intended manner? Such a constraint might benefit the rest of the production channel by reducing support costs after the game is sold. However, if the approved method of gameplay is not actually fun for the players then 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).

[1] In gaming parlance, the two most common playing styles are *PvG*: Player *vs.* Game and *PvP*: Player *vs.* Player. PvP can also allow *Pk*: Player killing by other players.

The player, of course, doesn't care about any of this, they only care about having fun. If relaxing the security restrictions to allow alternative gameplay means that players can enjoy the game, it may become a success simply by word of mouth about the "player-first" attitude of the Developer and Publisher.

5. The Player's Perspective

A sample of typical player emotional requirements for this context, condensed from experience and the cited literature, is presented in Table 1. The underlying emotions are heavily abstracted and are best interpreted as a motivating factor, as a *need* that the player attempts to satisfy by playing the game.

When these (and other) emotional requirements are not met, then otherwise constructive players may become destructive stakeholders. They are more likely to turn to some form of cheating and their observable actions may become beligerent toward other players. As Consalvo 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". Some players make comments that indicate they cheated only because they were stuck, that they wanted to play the game in a different way (for the alternative experience), or because they were facing time constraints (they couldn't spend hours performing repetitive tasks just to meet the Designer's vision).

We note that the player comments indicate conflict between the Player and the Designer. The players do not share the designer's vision and demand the freedom to play the game in a manner of their choice. Thus we arrive at the fundamental requirements conflict for all video games:

> *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? Or is the answer somewhere in-between?

Ensuring that the game can be played, only as designed, requires significant investment in security infrastructure (and the associated demands on algorithmic correctness). As noted earlier, market forces can override the Designer's intent. Because a game is experiential, absolute control over the player's experience is only a goal, it can not be guaranteed and there may be real world moral or legal issues associated with fine control over the player experience – blatantly manipulating the player may not be socially acceptable.

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

Table 1. Emotional Requirements

Emotional Requirement	Description	Player Comments
Escape, Experience	Distraction from (pressures and influences of) physical reality	I like to explore, especially in God mode. I want to be anonymous. I want to do things I can't do in real life.
Reward	Need for immediate feedback (of success or failure)	I *love* finding hidden rooms! The feeling when I finally mastered that move...
Posture, Image	How the player believes they are perceived by others	I love being the hero; It's cool to be bad!
Acceptance	Finding and becoming part of a community	These are my real friends...
Power, Control	Exercise power, control and influence	I love being able to dispense justice!
Accomplishment	Long-term accumulation of experience and reward	Figuring out how to advance my character, all the way to the highest levels – that's what I play for...

5.1. Alternative Play as Threat

For discussion, we classify any deviation from the intended play experience as a threat. Not all threats must be addressed; their severity can vary greatly.

From the gameplay perspective, these threats manifest as follows:

- Conferring an unfair advantage; (deliberately) breaking a rule *and* deriving a benefit[2]. Examples include using cheat codes to bypass parts of the gameplay and programmatic assistance such as macros or *bots* (from ro*bot*, an automated assistant).
- Using information from outside the game. Examples include employing hints, guides, and walkthroughs. The game is played as intended, but the player doesn't do the 'work'.
- Exploiting the implementation, gaming the game. Includes breaking the rules of the game (because the rule was not enforced), taking advantage of bugs, emergent gameplay (particularly taking advantage in a covert *vs.* an overt manner)
- Technological Cheating. The hardware or communication channels are modified in some manner.
- Hacks. The binary expression of the rules, communications, the game engine itself, are modified to change the play experience.

Consalvo [9] notes that "...much of the time, cheating actually implies a player is actively engaged in a game and wants to do well, even when the game fails *them*." Given that the the player's feelings convert them to a security threat, emotional requirements are a useful means for capturing player motivation, even when it is destructively focused. We conclude that emotional requirements can be used to ameliorate security risks by providing insight into threat motivation.

[2]Implies a zero-sum game, that one player cheating causes another player harm. This is not always true: what about single-player games? Is it even possible to cheat against a "game as opponent"?

6. The Developer's Perspective

There are many ways that the integrity of the play experience can be compromised. We classify these threats as follows.

1. Physical. Attacks upon, or requiring access to, the physical devices used in gameplay. This can include player computers, controllers, communications links, servers, *etc.*
2. Logical. Attacks upon the rules of the game, principally exploits on unexpected interactions.
3. Temporal. Attacks that manipulate time, calibration, or sequencing – both within the virtual reality as well as in physical reality.
4. State (information). Attacks upon the information used to control the game. Typically performed in realtime but may also be attacks upon data repositories between games.
5. Social (player). Out-of-game attacks upon the players themselves. Also known as social-engineering attacks.

All of these threats distort the virtual reality in some way.

To better understand these threats, they shall be addressed in the context of the generic, multiplayer video game architecture shown in Figure 1 (loosely based upon

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

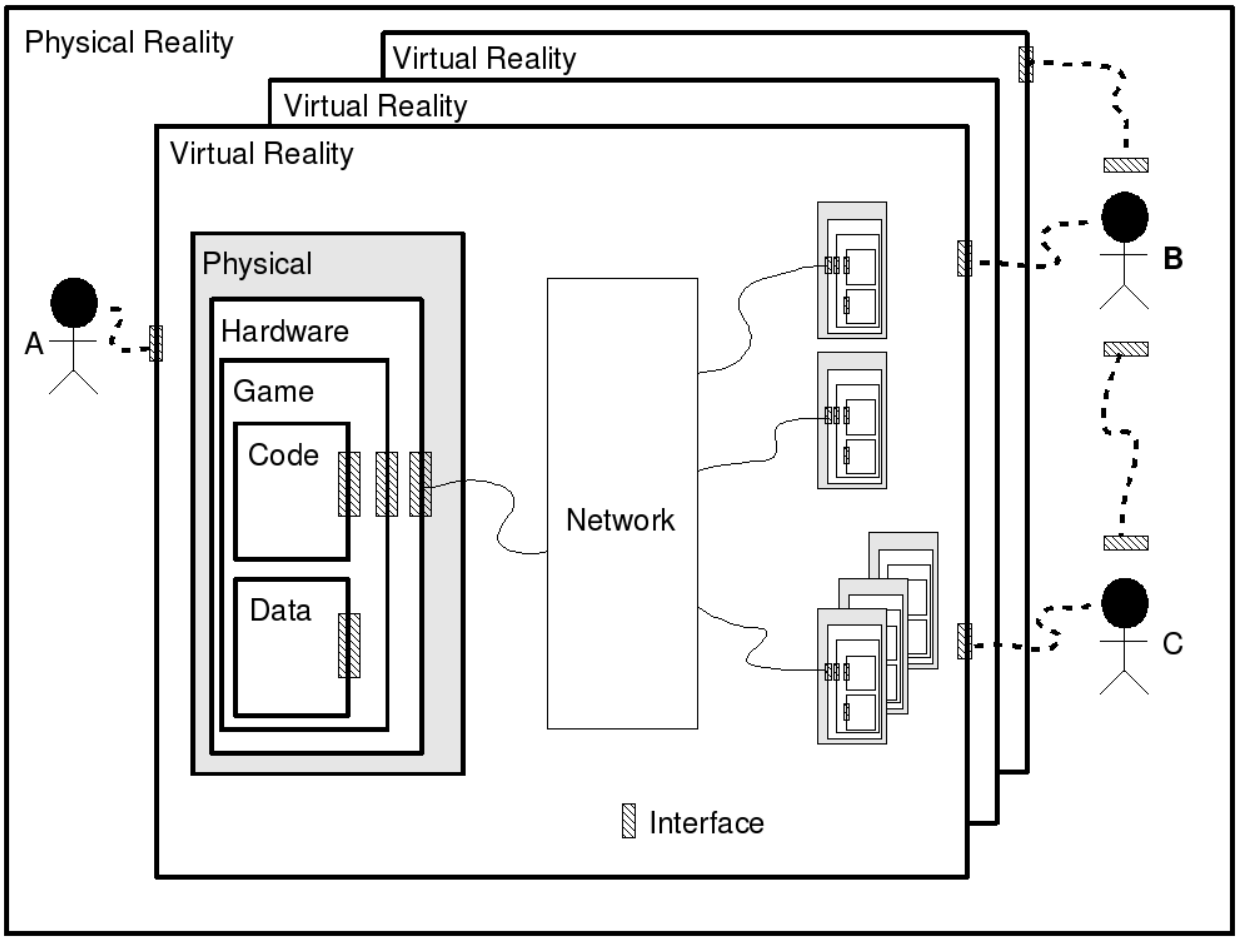

Figure 1. Generic Video Game Architecture

the OSI network model). One or more *Virtual Realities* are situated within a *Physical Reality*. Each computer is composed of a *Physical* aspect that includes the associated operating system, and these computers are connected via some form of communications *Network*. The *Game* is a software artifact composed of *Code* and *Data* elements.

The integrity of the game can be threatened in many ways (see Sections 3.5, 3.6). In practice, the actual techniques most often used compromise the integrity of one or more of the interfaces shown in Figure 1. Hoglund and McGraw [17] use a set of prepositions (*over, under, into, outside*) to denote how the attack is made. For example, the *Game* relies upon the *Hardware* to perform certain tasks such as rendering the virtual world. If the expected video drivers are replaced with new video drivers that render all walls translucent (thus enabling the player to see oncoming attackers through the walls) then this attack occurs *under* the game...the integrity of the *under*lying infrastructure was compromised.

The four attack modes exploit assumptions about the integrity of the system on the other side of the interface. An attack positioned *over* a layer manipulates the input channels, *under* a layer manipulates the output channels. An *outside* attack is directed at a specific layer but is launched from at least one layer away (*e.g.* an outside attack on a *Game* is launched from the *Network* or from another *Physical* location). The final attack position, *into*, refers to manipulating the internals of the *Game* as represented by the *Code* and *Data*.

We also extend this paradigm to include an *inside* attack. An inside attack "games the game" by attempting to exploit the rules of the game in some way. As such, an *inside* attack is a meta form of an attack that gets *into* the game internals but does not rely upon direct manipulation of code or data

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

representations in memory.

Given this context for attacks upon this architectural model, security requirements are most likely to focus on the integrity of the interfaces. A complete analysis would result in security requirements for each interface, addressing each attack mode.

Implementing such a thorough set of requirements may be prohibitively expensive. While emotional requirements do not appear to have a role in formulating security requirements (security requirements should manifest from security goals), they can be used to guide the prioritization process. Identifying the sources of greatest frustration to the player, the *emotional irritants* (a negative emotional requirement, or a failure to meet an emotional requirement will identify those issues most likely to sufficiently motivate the player to become a destructive stakeholder.

Removing or defeating these emotional irritants will require attacking the system in some way. If the player is willing to pay the cost of successfully attacking the system, they will do so. It follows that inexpensive attacks on significant irritants are the most likely to proceed so the risk factor for an emotional irritant is expressed as

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

We recognize that it is difficult to be precise in a matter such as this. However, we feel that even informed estimates based on prior experience are better than no guidance at all. Those security requirements associated with emotional irritants with high risk factors should receive high priority in the development plan.

7. A Process

The model presented herein has been relatively simple: Play is going well but something bad happens and the player becomes a threat to the integrity of the game. If the irritant is sufficiently large, and the player is willing to pay the cost of attacking the game, then they will do so.

The provider of the game can attempt to ensure that this scenario does not come to pass by following this process.

1. Identify the player's generic emotional requirements – for your studio and/or the genre of the game.

2. Quantify the relative importance of each emotional requirement, even if it is just an informed estimate.

3. Identify corresponding emotional irritants, failures to meet the emotional requirements.

4. Identify the emotional irritants associated with gameplay elements specific and/or unique to this game.

5. Quantify the magnitude of the irritants and determine the associated risk factors.

6. Identify security requirements corresponding to the emotional irritants.

7. Prioritize corresponding security requirements according to the risk factors.

8. Resolving Requirement Conflicts

We noted earlier that a Developer or Publisher may override security requirements in order to salvage a flawed game. Given that this action is in response to the player's reactions to the game, there exist situations where emotional requirements can override security requirements. From a pragmatic financial standpoint, positive emotional reactions sell the game while negative reactions will kill it.

The addition of mechanisms that satisfy the player's emotional requirement for instant gratification via reward systems, by definition, weaken the security requirements for the main game by introducing complexity.

As noted earlier, there does not appear to be an optimal resolution to these conflicts – 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 resolve all problems *a priori* yet allows the problems to be resolved as they occur and in a manner that addresses the emotional requirements of the stakeholders.

This just-in-time conflict resolution can be provided by introducing an in-game justice system. This justice system is then used to apply corrective action to those who corrupt the integrity of the game experience.

Sanderson [35] provides an informative view of such justice systems. These systems range from those where the Developer is also a Service Provider who acts as judge, jury, and executioner through to player policing systems wherein players are allowed to administer 'justice' upon each other.

Unfortunately, in-game justice systems suffer from the same issues as our real justice systems including false accusation, atonement, recidivism, and the need for appellate review. However, linking the justice system to the game capital system has been shown [35] to act as a deterrent to abuse, particularly if the cost is proportional to a player's wealth (to prevent the wealthy from preying upon the poor).

For an in-game justice system to be effective, it must address these issues:

- Who has judicial authority?
- What are the *penalties* associated with various *crimes*?
- What enforcement mechanisms are available?

2008 Third International Workshop on Multimedia and Enjoyable Requirements Engineering (MERE'08)
978-0-7695-3626-2/08 $25.00 © 2008 IEEE

- Does enforcement have real-world consequences?

A 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 security requirements.

Griefers and grief play remain an issue for it is difficult to judge the value of protecting other players. If there are few incidents of grief play then it may not be worth investing heavily. However, past experience [21] 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 griefing tactics. We expect that, eventually, the griefers will tire of victims that fight back and will move on to easier prey.

9. 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 have suggested 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 emotional requirement negotiation in the hands of the players, providing them with a framework wherein their own community values can develop.

In the future, we hope to extend the economic model begun here to provide more concrete mechanisms for valuing *fun* and *irritation*. Interactions with gambling research and decision-theoretic frameworks appear promising.

The risk factor analysis mechanism could then be extended by a detailed case study that compares the predicted attacks against actual attacks once the game is in production.

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 so heavily in security infrastructure.

References

[1] Ernest Adams. The No Twinkie Database. *http://www.designersnotebook.com/Design_Resources/No_Twinkie_Database/no_twinkie_database.htm*, Accessed January, 2008.

[2] Ian Alexander. Misuse cases: Use cases with hostile intent. *IEEE Software*, 20(1):58–66, 2003.

[3] Carina Alves, Geber Ramalho, and Alexandre Damasceno. Challenges in requirements engineering for mobile games development: The meantime case study. In *Proceedings of the 15th IEEE International Conference on Requirements Engineering (RE 2007)*, pages 275–280, Washington, DC, USA, 2007. IEEE Computer Society.

[4] David Callele, Eric Neufeld, and Kevin Schneider. Requirements engineering and the creative process in the video game industry. In *Proceedings of the 13th IEEE International Conference on Requirements Engineering (RE 2005)*, pages 240–250, Washington, DC, USA, 2005. IEEE Computer Society.

[5] David Callele, Eric Neufeld, and Kevin Schneider. Emotional requirements in video games. In *RE '06: Proceedings of the 14th IEEE International Requirements Engineering Conference (RE'06)*, pages 292–295, Washington, DC, USA, 2006. IEEE Computer Society.

[6] David Callele, Eric Neufeld, and Kevin Schneider. Emotional Requirements. *IEEE Software*, 25(1):43–45, 2008.

[7] Simon Carless. *Gaming Hacks*. O'Reilly Media, Inc., 2004.

[8] Mia Consalvo. Gaining Advantage: How videogame players define and negotiate cheating. In *Proceedings of the Second Annual conference of the Digital Games Research Association*, page Online. IT University of Copenhagen, 2005.

[9] Mia Consalvo. Cheating Is Good For You. *Forbes Magazine*, 12, 2006.

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

[11] Robert Crook, Darrel Ince, Luncheng Lin, and Bashar Nuseibeh. Security requirements engineering: When anti-requirements hit the fan. In *Proceedings of IEEE International Requirements Engineering Conference (RE 2002)*, Washington, DC, USA, 2002. IEEE Computer Society.

[12] Steve Easterbrook, Anthony Finkelstein, Jeff Kramer, and Bashar Nuseibeh. Coordinating distributed viewpoints: The anatomy of a consistency check. *Concurrent Engineering: Research and Applications*, 2(3):209–222, 1994.

[13] Donald Firesmith. Engineering security requirements. *Journal of Object Technology*, 2(1):53–68, 2003.

[14] 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.

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

978-0-7695-3626-2/08 $25.00 © 2008 IEEE

[16] Philippe Golle and Nicolas Ducheneaut. Keeping bots out of online games. In *ACE '05: Proceedings of the 2005 ACM SIGCHI International Conference on Advances in computer entertainment technology*, pages 262–265, New York, NY, USA, 2005. ACM.

[17] Greg Hoglund and Gary McGraw. *Exploiting Online Games: Cheating Massively Distributed Systems (Addison-Wesley Software Security Series)*. Addison-Wesley Professional, 2007.

[18] Paco Hope, Gary McGraw, and Annie I. Antón. Misuse and abuse cases: Getting past the positive. *IEEE Security and Privacy*, 2(3):90–92, 2004.

[19] Cynthia Irvine, Timothy Levin, Jeffery Wilsonz, David Shifflett, and Barbara Pereira. A Case Study in Security Requirements Engineering for a High Assurance System. In *Symposium on Requirements Engineering for Information Security, Held in conjunction with the 9th IEEE International Conference on Requirements Engineering (RE'01)*. Online, 2001.

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

[21] Andy Kuo. A (very) brief history of cheating. *http://shl.stanford.edu/Game_archive/StudentPapers /BySubject/AI/ C/Cheating/Kuo_Andy.pdf*, 2001.

[22] Y Lyhyaoui, A Lyhyaoui, and S Natkin. Online games: Categorization of attacks. In *Proceedings of EUROCON 2005*, pages 1340–1343, Washington, DC, USA, 2005. IEEE Computer Society.

[23] John McDermott and Chris Fox. Using abuse case models for security requirements analysis. In *ACSAC '99: Proceedings of the 15th Annual Computer Security Applications Conference*, page 55, Washington, DC, USA, 1999. IEEE Computer Society.

[24] Nancy Mead and Ted Stehney. Security quality requirements engineering (square) methodology. In *SESS '05: Proceedings of the 2005 workshop on Software engineering for secure systems − building trustworthy applications*, pages 1–7, New York, NY, USA, 2005. ACM Press.

[25] Tim Menzies, Steve M. Easterbrook, Bashar Nuseibeh, and Sam Waugh. An empirical investigation of multiple viewpoint reasoning in requirements engineering. In *RE '99: Proceedings of the 4th IEEE International Symposium on Requirements Engineering*, page 100, Washington, DC, USA, 1999. IEEE Computer Society.

[26] Jonathan Moffett, Charles Haley, and Bashar Nuseibeh. Core security requirements artefacts. Spiral Development Workshop Technical Report 2004/23, The Open University, Department of Computing, June 2004. Edited by Wilfred J. Hansen.

[27] A. Moore, R. Ellison, and R. Linger. Attack modeling for information security and survivability. Technical Report CMU/SEI-2001-TN-001, CMU/SEI, 2001.

[28] Andrew Moore. Security Requirements Engineering through Iterative Intrusion-Aware Design. In *Symposium on Requirements Engineering for Information Security, Held in conjunction with the 9th IEEE International Conference on Requirements Engineering (RE'01)*. Online, 2001.

[29] David Myers. What's good about bad play? In *IE2005: Proceedings of the second Australasian conference on Interactive entertainment*, pages 133–140, Sydney, Australia, Australia, 2005. Creativity & Cognition Studios Press.

[30] U.S. Department of Homeland Security. Build security in: Setting a higher standard for software assurance, Accessed January, 2008.

[31] Colin Potts. Using schematic scenarios to understand user needs. In *DIS '95: Proceedings of the 1st conference on Designing interactive systems*, pages 247–256, New York, NY, USA, 1995. ACM.

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

[33] Isabel Ramos, Daniel M. Berry, and João Alvaro Carvalho. Requirements engineering for organizational transformation. *Information & Software Technology*, 47(7):479–495, 2005.

[34] Ben Reynolds. Playing a "good" game: A philosophical approach to understanding the morality of games. *http://www.igda.org/articles/rreynolds_ethics.php*, 2002.

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

[36] Guttorm Sindre and Andreas L. Opdahl. Eliciting security requirements by misuse cases. In *TOOLS (37)*, pages 120–131, 2000.

[37] Axel van Lamsweerde and Emmanuel Letier. Handling obstacles in goal-oriented requirements engineering. *Software Engineering*, 26(10):978–1005, 2000.

[38] Jeff Yan. Security design in online games. In *ACSAC '03: Proceedings of the 19th Annual Computer Security Applications Conference*, page 286, Washington, DC, USA, 2003. IEEE Computer Society.

[39] Jeff Yan and Hyun-Jin Choi. Security issues in online games. *The Electronic Library*, 20(2), 2002.

[40] 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.

[41] Nick Yee. Unmasking the Avatar: The Demographics of MMO Player Motivations, In-Game Preferences, and Attrition. *Gamasutra*, 2004.

[42] Nick Yee. Motivations of Play in MMORPGs: Results from a Factor Analytic Approach. *http://www.nickyee.com/daedalus/motivations.pdf*, Accessed January, 2008.

978-0-7695-3626-2/08 $25.00 © 2008 IEEE