

Cheating, Game Security, and the Future of Global On-line Gaming Business

Presented at the March 2003, Game Developer's Conference

Speaker, Steven B. Davis, CEO, IT GlobalSecure, Inc.

For more information, visit www.itglobalsecure.com or www.secureplay.com

Introduction

Computer game companies have not typically needed to address cheating seriously. "Cheat codes", hacks, and other attacks were mainly of concern when they affected the revenue of the game company by allowing unauthorized copying of games by players, distributors, and video arcade operators. However, network games change the security requirements for computer games fundamentally. The core business models are intertwined with the play of games, not simply their production and distribution. Network or on-line games include the Internet, local and wide area games, and both low- and high-bandwidth games (provisioned by cable, phone, wireless, and satellite providers). This presentation will discuss the significance of cheating in a business and legal context.

To understand cheating, it is first necessary to review the revenue models for on-line gaming. This analysis is crucial to understand the importance of controlling the cheating problem and to accurately assess the threat of cheating to on-line gaming businesses. This paper provides a detailed overview of the cheating threat, examines its consequences for on-line businesses, and outlines technical solutions and implications.

Emerging network gaming businesses are a new kind of enterprise that fuses e-commerce with gaming operations. Network gaming operations include all of the typical security requirements that are necessary for an e-commerce business: privacy, confidentiality, financial security, and availability. Furthermore, network gaming businesses must deal with an additional set of game security concepts to protect against cheating and other forms of fraud and abuse at the game-level.

The On-line Gaming Market

Revenue estimates vary widely for the potential network gaming market. Industry revenue figures as high as \$26 Billion for interactive gaming by 2005¹ foretell an industry that will be one of the major forces in entertainment over the next decade and beyond. To reach even a significant fraction of these revenue numbers, on-line gaming must change its core business models – with serious implications for cheating and game security strategies.

Today, there are four basic revenue models used for on-line gaming businesses:

- **Courtesy Gaming** – free/for-fun games that are part of an overall on-line portal or gaming service. These games are not expected to generate much revenue (perhaps some modest advertising) and do not place a major burden on the game operators resources. These include basic party games, card games, and puzzles. These games are usually single player and are dynamically downloaded to the player's computer. The game operator provides, at best, a service to download the games, perhaps a shared "scoreboard" for posting results, and other community features. Simple multi-player games – certain traditional games such as bridge, checkers, chess, backgammon, etc. can also be supported without taxing the Game Operators resources (many of the games in Microsoft's Game Zone fall into this category).
- **Incentive Gaming** – free/for-prizes games where players earn prizes or chances for prizes through click-throughs and on-line purchases or other co-marketing tools. A number of the new game portals and several "dot-com" businesses have been built around this approach using virtual marketing and other such techniques as have several of the free, on-line lottery systems such as Iwon.com.
- **Marketing Gaming** – typically free/for-fun network gaming services to supplement and encourage the sale of traditional PC or console gaming products. These network services are basically used as a sales channel and are often complemented by level editors, shareware game servers, and other tools to further spur product sales.
- **Subscription Gaming** – fee-based/for-fun network gaming services such as Asheron's Call, Ultima On-line, or Everquest that charge a (usually) monthly subscription fee (in some cases in addition to product sales). These game services seem to be successful in niche markets, but to date have not broken out as mass-market phenomena. Recently, these services have created an interesting side business where players have bought and sold characters and other virtual assets acquired in the game for real money through e-Bay. This may create an additional revenue channel for these services in the future.

There is a fifth category of on-line gaming that should be included: Internet Gambling. Though this industry has notable legal issues in the US, the fact that over half of Internet users are now outside of the US and the popularity of gambling both in the US and abroad makes this business category one that should be watched. Its revenue model, pay-to-play/for-cash or prizes, is well-established and successful for traditional game operators (casinos) and has mass consumer appeal—according the American Gaming Association², nearly 80% of Americans either gamble or favor gambling as a valid form of recreation.

As noted above, there are several types of player incentives:

- Fun –players play a game simply for the satisfaction of playing.
- Prestige –players play and compete for status either via “scoreboard” systems or via tournaments
- Virtual Assets –players buy, find, or earn persistent, virtual assets. These can include the equivalent of collectible cards, players for virtual sports teams, more elaborate assets such as skills, weapons, tools, armor, and castles, etc. in massively multi-player role playing games.
- Prizes or Incentives –players play for prizes or other rewards including cross-marketing or other promotions.
- Cash – everyone’s favorite prize.

Prizes, Incentives, and Cash draw the most consumers into games, but cause on-line gaming operators to face legal challenges associated with gambling. Even if players are not paying to play, there is potential risk of having free gaming for prizes construed as gambling³ as well as the potential for fraud and consumer backlash. Most on-line gaming companies today take precautions to ensure that they do not cross the line into gambling, though they are well aware of the potential revenue opportunities. This can be easily seen with the popularity of games that can not be charged for, yet are conducive to contests or other more direct gambling-type revenue models⁴.

The On-line Gaming Business

These revenue models are changing the business environment for on-line gaming companies. The role of the publisher is less significant and is replaced by the Game Operator as the distributor and promoter of games. Financial institutions and the role of Regulators and the public as a whole become more directly entangled with game business operations. Finally, the Game Developer becomes even more of a “free agent” who must work hard to protect the reputation and revenue stream associated with his products:

- Game Operators – host the games that players play by providing the servers and network connections; promote the use of their service and the games that they host; and provide the e-commerce infrastructure and incentives to earn revenue from

game play. The distinction between developers and operators is widening as popular games are provided on servers or services owned by companies other than the publisher. As network gaming business models mature, the role of operators will expand as will potential issues with developers who wish to protect their revenue streams and the reputation of their on-line games.

- Game Developers – create the game content and systems that host games. Revenues are earned from the sale of copies of created games and from revenue sharing with game operators.
- Players – the individuals playing the games using the services provided by Game Operators.

Each of these parties may potentially benefit from cheating or defrauding the games: Game Operators may alter the game to reduce payouts to Players or change the odds in the game; Game Developers may embed codes and schemes in the software to allow themselves, or shells acting on their behalf, to automatically and undetectably win; and finally, Players may attempt to cheat or declare that they have been unjustly defrauded and claim compensation from the Game Operators.

The following two organizations have a supporting and oversight role for network games:

- Financial Institutions – provide the ultimate “back-end” operations where payments from players are credited. These institutions are often the first recourse for Players who believe that they have been defrauded or otherwise scammed.
- Government/Regulators/Public Interest Groups – as on-line gaming becomes a larger industry, issues of consumer protection, privacy, and fair play will be increasingly important.

Cheating and On-line Games

It was important to introduce the revenue models for On-line Gaming Businesses and the incentives for Players in order to recognize the critical role that cheating and game security will have on the future of On-line Gaming. There is little significant impact from cheating and game security without understanding the basic change to revenue models based on game operations from game publishing. The remaining discussion of cheating in this paper will focus on cheating and game security from the perspective of a Game Developer or Game Operator.

Game Developers earn revenue from the sale and licensing of their game products. Network gaming will make practical the licensing of game products to Game Operators on a per game basis or will encourage some form of revenue sharing to minimize risk. As the creator and owner of the product and brand, the Game Developer's security concerns include:

- Effectiveness of game security to protect revenues (earned through the game product by the Game Operator) against cheating by players,
- Effective revenue sharing mechanisms to ensure that the developer gets his "fair share" of game operations revenue, and
- Protection against cheating or fraud by game operators that may reduce the success of players.

Game Operators earn their revenue from players through the operation of games. The revenue may be earned from advertising and co-marketing incentive programs, subscriptions, and direct pay-for-play schemes. The revenue may be enhanced by incentive programs to encourage players to participate (for fun, pride or status, virtual assets, prizes, and cash). For the operator of a gaming site and its brand, the major cheating and game security issues include:

- Effectiveness of game security mechanisms to protect revenues earned through the game products, and protect the operational infrastructure against cheating by players,
- Protective mechanisms against fraud or manipulation by game developers, and
- Protection against consumer complaints and other liability issues.

Cheating becomes critical based on the following factors:

- The direct revenue impact of cheating on a Game Developer or Game Operator.
- The impact of cheating on the reputation, and therefore market share, of a Game Developer or Game Operator.
- The social and community impact on the industry in the case of major cheating incidents or scandals.

These factors drive Game Developers and Game Operators towards the creation and use of security mechanisms that address game security issues.

Cheating

Cheating at games has developed into something of a “high art” in the area of casino gaming. The heights (or depths) of human ingenuity have been focused on getting “an edge” at casino games – mankind’s first hackers⁵. Even the relatively benign world of free, for fun on-line gaming has been haunted by cheaters (see the excellent article “How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It” by Matt Pritchard⁶). The table below summarizes cheating techniques both in traditional an on-line gaming environments and offers a preliminary discussion of applicable countermeasures.

Table 1: Summary of Cheating Methods and Countermeasures

| Cheating Type | Cheating Methods | | Countermeasures |
|---|---|--|---|
| | Traditional | Computer /Internet | |
| <p>Manipulation: Altering the game events to the advantage of the cheater</p> | <p>Stacking, Second and bottom deals, Cold decks, Juiced tables for craps and roulette, Controlled shots in craps, loaded/altered dice.</p> | <p>Rigging the game events (card values, dice roll) to any desired value.</p> | <p>Secure Game Contract</p> |
| <p>Skimming: Under reporting gaming earnings to avoid taxes</p> | <p>Various</p> | <p>Various</p> | <p>Secure Game Contract</p> |
| <p>Rules/Game State Manipulation: Altering other players' perception of the game rules and game state to alter the game outcome</p> | <p>Bluff, bullying, and intimidation to "change" the rules.</p> | <p>Spoofing/Authoritative Clients - altering the end computer or network information/behavior in a way that changes the game rules or outcome.</p> | <p>Secure Game Contract</p> |
| <p>Collusion – Player/Dealer: Cooperation to give an unfair advantage against the Game Operator or against other players.</p> | <p>Alter game play, payout, or spying.</p> | <p>Significantly reduced in most electronic games by automating the dealer/games server. Software Substitution (see below) could be equivalent..</p> | <p>Secure Game Contract and Computer Security Techniques to Automate Server</p> |
| <p>Crooked Game Operator: A game server set up to defraud players.</p> | <p>Back alley or illegal casino.</p> | <p>Much worse – create a "fake" game server on the Internet or other network with the intent of defrauding consumers.</p> | <p>Secure Game Contract, Trusted Gaming Infrastructure, Regulation</p> |
| <p>Alteration/Treatments/ Spying: Accessing supposedly secret information that should not be available to the cheater</p> | <p>Marking cards, Spying (mirrors, accomplices).</p> | <p>Monitoring the network or computer to see other players' secrets.</p> | <p>Encryption and Transaction Security</p> |
| <p>Bet/Payment Manipulation: Altering the amount of a bet to improve winnings or reduce losses.</p> | <p>Changing the amount of a bet, Late bets, Chip Cups – false money stacks.</p> | <p>Inherently more difficult because the bets/payments are recorded electronically.</p> | <p>Transaction Security in Game Contract and E-commerce Security</p> |

| Cheating Type | Cheating Methods | | Countermeasures |
|--|--|---|---|
| | Traditional | Computer /Internet | |
| Pot/Pay Out Manipulation: Theft from the pot | Stealing from the pot. | Spoofing - altering the end computer or network data/behavior in a way that changes the game payout or perceived bet. | Transaction Security in Game Contract |
| Interruption– Departure: Interrupting the game to avoid an adverse outcome by leaving the game. | Not practical – getting up and leaving a game with your chips and not coming back. | Leaving the game due to player “network interruption” or player “computer problem” to avoid loss. | Transaction Security; Contract/Monitoring needed for multi-player Games |
| Tells/Signaling: Observing behavior that indicates information that is supposedly secret | Player behavior observation. | Tells - Mainly a problem if video or chat is supported. Signaling – via separate communication channel (e.g. telephone lines,.). | Tells – via system implementation (various) Signaling - Hard if not impossible to counter (see Player/Player Collusion) – best solutions are player rotation to minimize impact |
| Interruption– Server Shutdown: Interrupting the game to avoid an adverse outcome by causing the game operator to shutdown | Shutting off the lights or starting a fire at the casino to avoid losses. | Disabling the game operator computer or disabling the network connection to the game operator – Denial of Service Attacks. | High Availability systems and network connections. As seen by recent news stories, this is a hard problem for all networked computers. |
| Collusion– Player/Player: Cooperation to give an unfair advantage against the Game Operator or against other players. | Cooperation between players – usually to share information. | Easier to cheat– the computer and network provide communications means that are not easily detectable. (See also Tells and signaling). | Monitoring. Mainly a concern in player vs. player games such as poker and can be minimized by player rotation. Many computer games allow and encourage collusion between players and so this is not a problem |
| Theft/Theft of Service: Stealing of game operator assets by game operator personnel or others. | Raking – taking a portion of the pot or underpaying winnings and pocketing the rest. Robbing the cage | Hacking into the “cage” on an on-line system. Altering the game server software prior to installation or during operation – Trojan Horse, Virus, and other malicious software. | Computer Security Techniques/Monitoring |

| Cheating Type | Cheating Methods | | Countermeasures |
|--|---|---|--|
| | Traditional | Computer /Internet | |
| Hardware Tampering/Software Substitution: Altering game operator equipment to affect game outcomes or payouts. | Slots problem – drilling and other machine manipulation techniques. | Replacement/modification of player or game server software. This is also a concern for game operators and game developers relative to each other. | Secure Game Contract, Trusted Gaming Infrastructure, Regulation, Monitoring, and Computer Security Techniques |
| Counting and Optimal Game Play: Keeping track of previous game events (usually in card games) to determine the likelihood of future events and gain an advantage. | Various mental and technical counting and tracking systems. | Trivial to implement since a computer is available; | Mitigated by game operator game event processing (limited solution). Game operators and developers should assume some level of use of optimal game play tools in their game and system design. |
| Hybrids: Combinations of other techniques | Various | Various | Various |

The Secure Game Contract

The relationships between players in a game and those between the players and a service provider hosting a game have always been built on an informal, and sometimes more formal, set of rules. These rules provide an environment where a game may be played in a manner that provides confidence to players.

The migration to on-line gaming requires an evolution of this relationship between a game provider and player(s). The existing mechanisms and security models for computer and network security are not sufficient to ensure the security of the game itself. The game events (rolling dice, dealing cards, resolving combat), game rules, and game state **must all be protected**.

The secure game contract for on-line games becomes a true digital contract between the game player(s) and the game operator. The contract includes special features for the creation of an “honest” game. Additionally, it provides mechanisms to ensure that the game is played fairly, to guarantee the use of the techniques that themselves verify that honest-game mechanisms were used, and to certify the game results (see Figure 1, below). The process is described in more detail in Quixotic Solutions Inc. patent⁷.

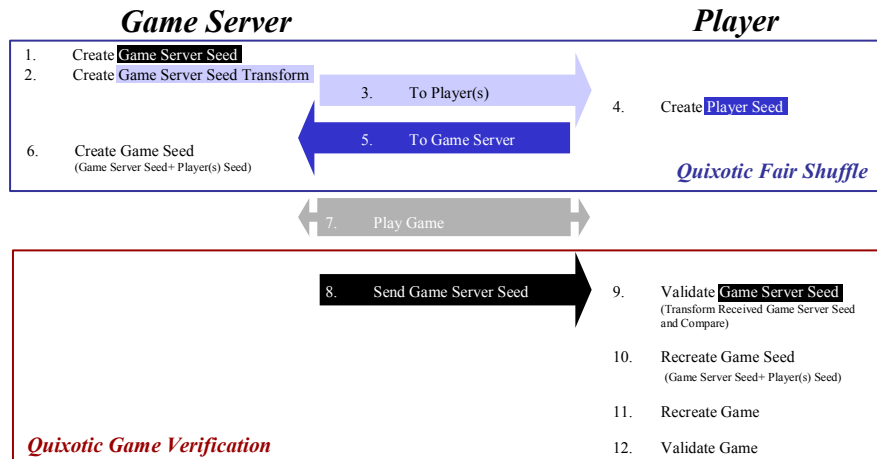


Figure 1: Quixotic Secure Game Contract Process Flow

This secure game contract requires software on the player client system as well as the game server, and it can be used with any game. The secure game contract must ensure full synchronization of game state information between all parties of a game (though it does not require that all participants have access to identical game state information) and reliable, non-repudiable communication of actions and state changes. Finally, the secure game contract must allow the independent reconstruction or reenactment of the game by the player or third party reviewer (such as a financial institution) for the purpose of certifying that the game was played properly, in accordance with the game rules, and with no manipulation of any random game events.

The game contract forms the core tool for protecting consumers from crooked game servers located anywhere in the world, and provides the means for game operators to protect their revenue and reputation from spurious player complaints.

Trusted Gaming Infrastructure

The Trusted Gaming Infrastructure includes both the network gaming operator's security infrastructure, interfaces between different parties (such as those between developers and operators and between financial institutions and operators) as well as the common elements shared by the network gaming community (for regulation, product or operator certification, etc.). Key features of the trusted gaming infrastructure include:

- Digitally signed and certified versions of games from the game developer or independent certification authorities.
- Registries of certified game developers and game operators. This will include both certified providers as well as lists of companies, products, and services that have gotten into trouble. These registries could be operated by or on behalf of governments or by industry associations for self-regulation.
- E-commerce interfaces between game operators and financial institutions.
- Mechanisms for consumer complaints to financial institutions, certification organizations, and possibly government regulators or oversight bodies.
- Mechanisms for registering the individual use of games by players and providing the information to game developers for revenue sharing and licensing.
- Mechanisms that allow insurance and other supporting organizations to collect necessary information.

Depending on how the on-line gaming industry develops, the specific mechanisms, protocols, and tools required and the organizations involved may vary. The on-line gaming industry has the opportunity to define the global agenda for how the industry is regulated. By acting early, industry can pre-empt intervention by governments and provide a standard global framework for the industry that will benefit all companies involved.

E-Commerce and Transaction Security

The established mechanisms for securing e-commerce transactions, such as digital signatures and certificates, as well as methods for reliable implementation of distributed transactions are as critical for network gaming businesses as they are for all other on-line e-commerce enterprises. These techniques are rapidly standardizing, but their implementation in specific game operations is always a concern. The recent incidents at several major e-commerce sites where sensitive personal information was compromised, including credit card numbers and social security numbers, should be a warning. Additionally, global gaming operations need to meet European and other emerging standards for the privacy protection. The success and growing revenue of on-line gaming will be directly correlated with the rise in criminal cyber-assaults – the most successful sites will become targets for criminals and hackers.

Encryption

Encryption is the most familiar security tool and is clearly useful for on-line gaming. Encryption complicates many hacker attacks intended to disrupt or defraud games. The main roles of encryption include the protection of the privacy of players and support for the security of e-commerce transactions. As with tools for e-commerce and transaction security, the proper implementation of encryption technology is critical to its effectiveness.

Regulation, Insurance, and Oversight

The computer gaming industry has been blessed with a minimum of government and public oversight –oversight has primarily come from organizations seeking to protect children against exposure to graphic or violent game content. As network gaming businesses begin to transition from a product sales focus to a rewards and services focus, more direct and active oversight should be expected.

The example of the casino industry is an excellent case study for the concerns and issues that may face network gaming companies. In the casino industry, both game developers and operators are regulated by state-level agencies. These agencies oversee and approve all principals in the game developer and game operator corporations; they review and certify all games and game implementations; and they license, oversee, and spot check game operations⁸. The casino industry accepts this burden because of the tremendous revenues associated with gaming – over \$22.2 billion in 1999 from US casinos alone⁹.

This regulatory process reviews the implementation of each game in great detail. The controlling agency keeps a reference copy of the PROM, which is actually installed in the gaming devices, and fully reviews the software encoded on the PROM. Similarly, game operations are carefully reviewed and continuously monitored to ensure the integrity of their processes.

On-line gaming will face major challenges if it seeks to meet this regulatory standard. Games are currently released and revised with patches and have very aggressive product cycles. If certification becomes necessary, additional time must be allotted and the stability of the game products must improve measurably.

There are several additional factors that already affect traditional casino games and should be considered for on-line games:

- Rate of Play - the control of how many games are played per hour. Slot machines, video poker systems, and other automated devices are configured to control the pace at which a player can play. This limits both losses and compulsive game play.
- House Hold – (or win) occurs when the net earnings of each game table is monitored (for on-line games, this could be for the server, specific random number generator, or instantiation of the game). This is mainly used as a management metric to identify machines, tables, or dealers that are not performing appropriately.
- House Advantage – measures the percentage-per-game or payout that favors the game operator. This can potentially be difficult for many network games as they have complicated play and control options that make the precise determination of the house advantage difficult. It is a parameter that needs to be tracked both for management purposes. It is also an important parameter for players so they know the likely consequences of participating in the game. Games that do not have a mathematically derivable house advantage should probably report the “observed house advantage” based on numerous player games.

Even without regulation, as the stakes increase for on-line gaming, liability and insurance issues will rise accordingly. Free games with player incentives have so far avoided loud player complaints, but this could easily change. Internet casinos already face consumer complaints, but there is little effective recourse due to the jurisdictional problems involved.

On-line gaming companies will need to show “due diligence” for the security and reliability of their games. The mechanisms described above, including the secure game contract and trusted gaming infrastructure, will be critical to protecting a gaming company. They will also be key elements to protect the revenue stream from players and minimize the potential for regulation. International insurance combined with aggressive self-regulation by the industry may be the sole means of preventing the piecemeal, jurisdiction-by-jurisdiction regulatory infrastructure that is associated with casino gaming today.

Architecture Implications

The new requirements for game security come as the engineering practices and methodologies for game development are maturing. The use of standard game engines with level editors to create a range of games from a single software infrastructure has both economic and security benefits. Historically, game development has tended to be based on monolithic development efforts in which the game programming team writes everything except

the compiler (or maybe the assembler) to ensure the maximum performance under limited hardware platforms.

Today, game engines (Quake, Half-Life, etc.) and infrastructures (DirectX) have worked to simplify and standardize game development so that game programmers can concentrate on the truly unique aspects of their games. To help ensure game security and minimize the certification effort and time for new games, this process will need to continue further. Also, games will need to be designed to isolate presentation and display information that is not relevant to game play from the core aspects of the game that do affect the game outcome (see Figure 2).

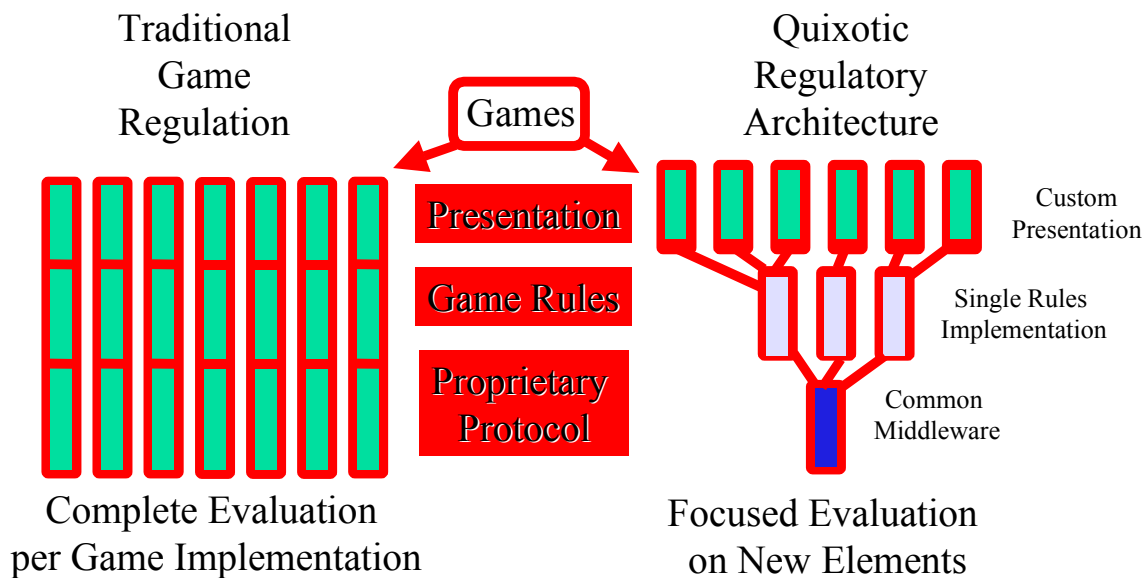


Figure 2: Game Architectures and Security Evaluation

One issue that may challenge developers will be the need to release access to significant design information about the game rules. In order to ensure successful certification by outside parties and to provide consumers with confidence that they are not being defrauded by the developer or operator, the rules that drive the game and significant information about the heuristics or AI used by machine-driven opponents will need to be released.

Conclusions

The network gaming business is poised for tremendous growth. The growth of the Internet globally (over 50% of Internet users are outside the US) presents a unique opportunity for the

gaming industry. Additionally, other network technologies and information services are expanding rapidly – wireless, broadband via local cable or telecommunications company, and satellite. Though industry growth from game sales will continue, the explosive opportunities are from game operations over new and existing network backbones.

Game security and the threat of cheating a critical issue for business leaders in this new world. Incentive programs and games are some of the few survivors of the dot-com meltdown. Melding entertainment and rewards together is key to future growth.

The threat of cheating continues to grow, as do the stakes for players and the game companies. Techniques such as the secure game contract, which assures the integrity and “fair play” of the game, are key to protecting against these problems, but they must be supplemented with the whole range of traditional computer and network security solutions. Also, game developers will need to integrate security into their development process from Day One. The consequences of poor coding and design will not be fixable simply by releasing a patch. This change will further accelerate the drive towards standard game infrastructures and further expand the use of engine-based development. These standard solutions will reduce development and operational costs, improve security, and allow developers to focus on the high-value, game specific portions of their product.

The network gaming industry should take the threat of regulation seriously. Unless companies involved take aggressive, proactive action, local regulation for each country, state, and locality worldwide will hobble the growth potential of the industry.

Solving the cheating problem will be key to the success of the network gaming business over the next decade. If network gaming is going to move beyond a marketing channel for the sale of software, the revenues from game operations will need to be protected to minimize or avoid government regulation and minimize the companies’ exposure to liability.

Endnotes

¹ Indirectly cited from a Forrester Research claims a market of \$6.5 Billion today – presumably driven by mostly software and hardware sales.

² State of the States: The AGA Survey of Casino Entertainment
(http://www.americangaming.org/survey2000/sur_index.html)

³ “Regulation needed for Internet gambling to succeed”, Lisa Snedeker, Associated Press, 13 January 2001, (<http://www.lasvegassun.com/sunbin/stories/archives/2001/jan/13/511294700.html?nevada+attorney+general+internet+casino>)

⁴ The popularity of games such as Spades & other “open source” games rivals the premium or games with a software product tie-in at Microsoft’s Game Zone (<http://zone.msn.com/blog.asp>). During a recent visit to the site (1/9/01 at 9:30PM) seven of the top ten games were “free” type puzzle, card or board games:

| | | | |
|-----------------|--------|--|----------------|
| Adventure Games | 17,012 | <u>Asheron's Call</u> | <u>Premium</u> |
| Puzzle | 9,849 | <u>Bejeweled</u> | Free |
| Card Games | 8,339 | <u>Spades</u> | Free |
| Puzzle | 3,651 | <u>Alchemy</u> | Free |
| Strategy | 3,523 | <u>Age of Empires II: The Conquerors</u> | Buy |
| Board Games | 3,398 | <u>Backgammon</u> | Free |
| Card Games | 3,350 | <u>Bridge</u> | Free |
| Board Games | 3,057 | <u>Checkers</u> | Free |
| Card Games | 3,038 | <u>Cribbage</u> | Free |
| Strategy | 2,828 | <u>Rogue Spear</u> | <u>Buy</u> |

⁵ [Gambling Scams : How They Work, How to Detect Them, How to Protect Yourself](#), by [Darwin Ortiz](#), published April 1990, this book is one of the most entertaining and/or scary books on gaming that everyone should read. It covers the entire range of cheating for games of chance (http://www.amazon.com/exec/obidos/ASIN/0818405295/o/qid=981471857/sr=8-1/ref=aps_sr_b_1_1/107-3384820-0605362).

⁶ “How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It” by Matt Pritchard, Gamasutra (http://www.gamasutra.com/features/20000724/pritchard_01.htm), 24 July 2000, reprinted from the June 2000 issue of Game Developer magazine.

⁷ [U.S. Patent 6,030,288](#), European Patent [EP1016049A1](#), International reference [WO9912135C1](#), further information available at the Quixotic Solutions Inc. web site (<http://www.quixotic-solutions.com/index.htm>).

⁸ See the Nevada Gaming Commission and State Control Board (<http://gaming.state.nv.us/>) and the New Jersey Division of Gaming Enforcement (<http://www.state.nj.us/lps/ge/>).

⁹ State of the States: The AGA Survey of Casino Entertainment (http://www.americangaming.org/survey2000/sur_index.html)