


| Cheating Type | Traditional face-to-face Gaming | Network Gaming | Network Gaming Countermeasures |
|---|--|--|--|
| Alteration/ Treatments/ Spying: Accessing supposedly secret information that should not be available to the cheater | Marking cards, Spying (mirrors, accomplices) | Monitoring the network or computer to see other players' secrets Extracting or modifying local game state information | Encryption and Transaction Security |
| Rules/Game State Manipulation: Altering other players' perception of the game rules and game state to alter the game outcome | Bluff, bullying, and intimidation to "change" the rules | Spoofing/Authoritative Clients - altering the end computer or network information/behavior in a way that changes the game rules or outcome | SecurePlay™ Platform  |
| Collusion – Player/Operator: Cooperation to give an unfair advantage against the Game Operator or against other players | Alter game play, payout, or spying | Significantly reduced in most electronic games by automating the dealer/ games server (See Software Substitution) could be equivalent | SecurePlay Platform and Computer Security Techniques to Automate Server |
| 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 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 |
| Optimal Game Play and Counting Cards: 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 |
| Race Condition: Abusing time lags to manipulate game results or get superior knowledge | Difficult to implement | Usually Seen in Betting Systems | SecurePlay Platform, Careful Control of State, Time, and Synchronization |
| 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 (telephone lines, for ex.) | Tells — via system implementation (various) Signaling — Hard if not impossible to counter (See Player/Player Collusion) — best solutions are player rotation to minimize impact |
| Pot/Pay Out/Score 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, score or perceived bet | Transaction Security in Game Contract |

| Cheating Type | Traditional face-to-face Gaming | Network Gaming | Network Gaming Countermeasures |
|---|--|---|---|
| Payment Manipulation: Altering the amount of a payment to improve winnings or reduce losses | Changing the amount of a bet or payments, Late bets, Chip Cups — false money stacks | Inherently more difficult because the bets/payments are recorded electronically (See Race Condition) | Transaction Security in Game Contract & E-commerce Security |
| 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 |
| 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 Game Operator | Hacking into the E-Commerce System on an on-line game Altering the game server software prior to installation or during operation — Trojan Horse, Virus, and other malicious software. Can also be implemented by Authoritative Client | Computer Security Techniques/ Monitoring  |
| 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 | SecurePlay Platform, SecurePlay Infrastructure, Regulation, Monitoring, and Computer Security Techniques |
| 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 |
| Crooked Game Operator: A game server set up to defraud players | Back alley or illegal game operation | Much worse — create a "fake" game server on the Internet or other network with the intent of defrauding consumers | SecurePlay Platform, SecurePlay Infrastructure, Regulation |
| Skimming: Under reporting gaming earnings to avoid taxes | Various | Various | SecurePlay Platform by tying game outcomes to financial results |
| Hybrids: Combinations of other techniques | Various | Various | Various |