1. In the context of IP restricted NAT devices, what does the hole-punching technique do? Describe this technique, using a diagram to aid your explanation if appropriate.

Answer :

It is a technique used to established communication between 2 devices that are located in separate NAT devices with IP restrictions.

How it works:

1. Both device send a message to a third party server that they both can reach
2. The server then record the IP address and port number of both device and send the information to the other devices.
3. Each device then send packets to the other device’s IP address and port number

This will create a direct communication path between 2 devices that are located behind separate NAT devices.

2. In multiplayer online games, interest management cuts down the bandwidth usage by filtering irrelevant updates. Describe two common techniques of interest management.

Answer :

The 2 techniques is:

1. Entity Component System where each game object is divided into components. Updates regarding that specific component are only send to player who need it. If player need to know another player location, it will only send that information and not any other information like health or attack stats.
2. Spatial Partitioning is when the game world is divided into multiple regions or parts and updates are only send to player in that region or parts.

3. Interest management is important for good network performance in massively multiplayer games. What is a potentially visible set, and how does this approach differ from static zones? How do these interest management approaches benefit the game?

Answer :

Potentially Visible Set (PVS) is an interest management technique used in massively multiplayer games to reduce the number of objects that need to be rendered or updated by only rendering or updating objects that are potentially visible to the player's current position or view. Compared to static zones ,PVS provides a dynamic and responsive gameplay experience, while reducing network bandwidth usage and improving game server scalability.

4. Describe one example for client-side attack and server-side attack, respectively. Please include details of how this attack works and a mechanism to prevent it.

Answer :

Client-side attack:

Cross-site scripting which exploits the vulnerabilities in a website's code to inject malicious scripts into web pages viewed by other users. The attacker can use these scripts to steal sensitive information which then can be used to install virus or malware on their system.

Websites can use input validation and sanitization and users can also protect themselves by using browsers that have in-built XSS protection features such as script filtering.

Server-side attack:

SQL injection exploits the vulnerabilities in a web application's database by inserting malicious SQL code into user input fields, such as login forms or search boxes which allow the attacker to have full access of the web application and system.

web application firewalls can help to detect and block SQL injection attempts by analysing traffic patterns and signatures associated with known SQL injection attacks.

5. Cheating in online games is the action of pretending to comply with the rules of the game, while secretly subverting them to gain an unfair advantage over an opponent. Describe two ways of cheating. Please include details of how each cheating works and a mechanism to prevent it.

Answer :

Both of these cheats are used in First person shooter.

Aimbot

* Aimbot is a program that automatically aims and shoots at opponents without the player's input. It uses the game memory to get opponents positions and then adjust player aim to target them accurately.
* Instead of relying on the player's computer to detect when shots hit opponents in a game, the game's server can do this instead. This makes it harder for cheating programs like aimbots to manipulate the game and gives a fair chance to all players

Wallhack

* Wallhack allow player to see through walls or other obstacles that should be blocking their view. It uses cheat software that modifies the game's graphics engine to render objects that should be hidden.
* Developers prevent this by encrypting game data to make it more difficult for cheat programs to modify the game's graphics engine