**Online Gaming Technology**

**Last Lab**

**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.**

When two devices behind separate NAT routers want to talk to directly to each other, this hole punching technique is used to over come this problem as it can be difficult.

1. Both devices connect to a server on the internet (helps to find each other)

2. They share their private Ip with the server and also port numbers .

3. The server tells Device A the public Ip and port of Device B and vice versa.

4. Now Device A and Device B start sending packets.

5. When the NAT routers of Device A and Device B receive these messages, they briefly open temporary holes in their setup. This allows the incoming messages to go through and reach the devices behind the NATs.

6. When temporary holes are open they can talk to each other and server is not needed anymore.

Device B (Private IP: Port)

Device A (Private IP: Port)

Server (Public IP: Port)

Server (Public IP: Port)

Nat Device B (Public IP: Port)

Nat Device A (Public IP: Port)

**[hole Punching packets] [hole Punching packets]**

**Direct communication established**

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

The two coming methods/ techniques are: Spatial Partitioning: This technique splits the game world into sections. Each player is put in a specific section based on where they are in the game. They only receive updates about their own section, so they don't get unnecessary information. This saves bandwidth by sending only the important updates.

View Frustum Culling: In 3D games, this technique figures out what the player can see on their screen. Objects that are outside of their view are not sent to them, which reduces the amount of data that needs to be sent. This saves bandwidth by leaving out things that the player can't see.

**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?**

The dynamic collection of items or entities that a player might be able to see depending on their position and line of sight is known as the potentially visible set (PVS). As the player moves, a real-time update is made. By prioritizing rendering and simulating only what the player can see, this aids the game engine in easing network load and enhancing speed.

On the other hand, regardless of whether players are present or not, static zones are predetermined locations in the game world that are always loaded and simulated. They have particular gaming components.

The primary distinction between static zones and PVS is that the latter are dynamic and change according on the player's perspective. Both methods have advantages.

**The benefits are:** Network Performance: Because PVS decreases the quantity of data that must be transmitted over the network, there is less lag and improved performance. It only delivers updates for things that are visible to the player.

PVS concentrates on rendering and simulating only what is required, which conserves processing resources. Gameplay becomes more fluid as a result, while loading times and frame rates increase.

**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.**

Client-side attack example: Phishing attack

Deceptive emails or messages are sent to users, tricking them into clicking malicious links or opening attachments.

Prevention: Be cautious of unknown sources, verify senders' identities, check URLs before clicking, keep software updated, and educate users.

Server-side attack example: SQL injection attack

Exploits vulnerabilities in a web application to insert malicious SQL commands into database queries.

Prevention: Implement input validation, parameterized queries, principle of least privilege, use a Web Application Firewall (WAF), apply security updates, and conduct security testing/code reviews.

**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.**

**Aimbot:** Aimbot is a cheat that automatically targets opponents, giving players precise and quick aiming. It's detected by Valve Anti-Cheat (VAC), an anti-cheat system in CS:GO. VAC regularly updates its detection algorithms and relies on player reports to catch cheaters.

**Wallhacks:** Wallhacks allow players to see through walls, revealing enemy positions. CS:GO prevents wallhacks with client-side occlusion culling and server-side position monitoring. Players can report suspected cheaters for investigation.